OAuth for Financial APIs

The OAuth approach of Berlin Group's PSD2 API

Torsten Lodderstedt, YES.com AG/OpenId Foundation
OAuth Security Workshop, Trento, 14.03.2018

EU Payment Services Directive 2 (PSD2)

- Goals
  - Foster innovation in online and mobile payments
  - Increase security of payment transactions and access to account information (strong customer authentication, regulation, screen scraping(?))
- *Banks must allow access to*
  - account information (balance, transactions, account holder) and
  - payment initiation (e.g. SEPA credit transfer)
- *to any party accredited with a local competent authority, e.g. Bafin or FCA*
- All Banks in the EU must comply until May 27 2019 by providing appropriate APIs
- Ongoing debate on use of screen scraping (as fallback) and **redirects**

PSD2 API Specifications

- PSD 2 does not dictate a certain API, instead European Banking Authority (EBA) on behalf of European Commision published “Requirements for Technical Specifications” (RTS)
- Details and maps legal requirements to technical requirements, e.g. regarding Strong Customer Authentication* (SCA)
- Several groups are working on specifications, e.g.
  - Open Banking UK (https://www.openbanking.org.uk/
  - STET (https://www.stet.eu/en/psd2/)
  - Berlin Group (https://www.berlin-group.org/psd2-access-to-bank-accounts)
  - Further national activities (PL, SK, …)

* term introduced by PSD2, 2FA with dynamic binding of the 2nd factor to the particular transaction and independent elements

Berlin Group

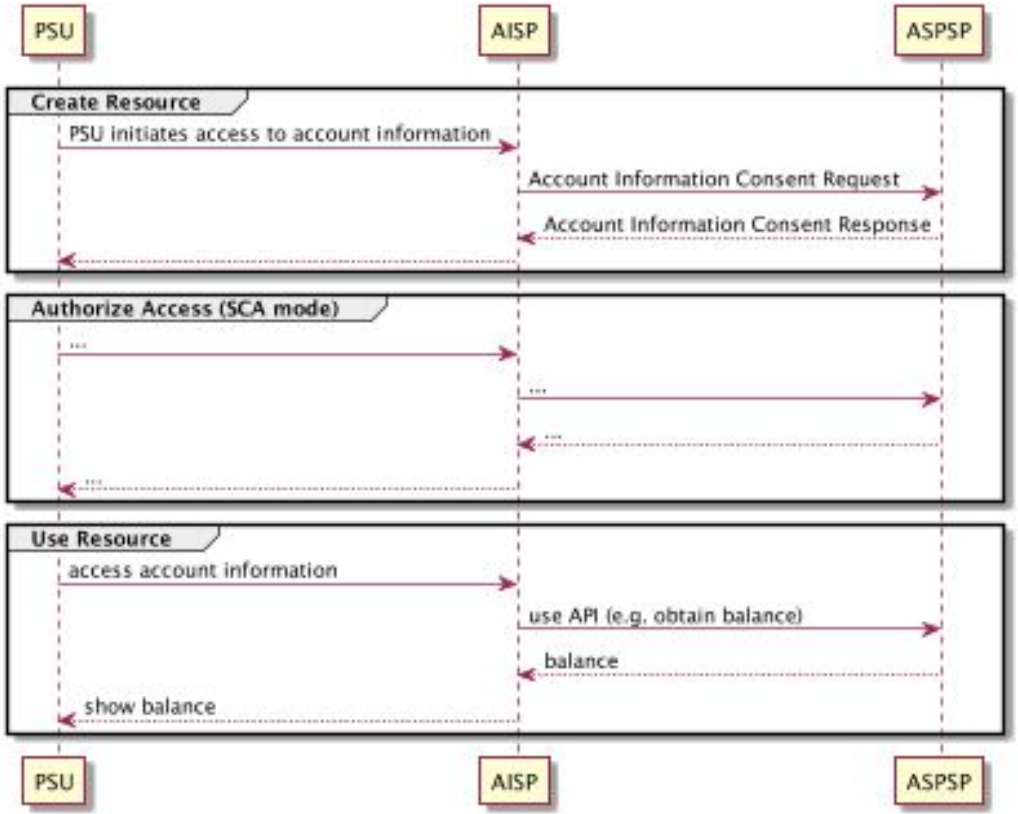
- Participants: Banks & Banking Associations, Payment Processors from across the EU
- *NextGenPSD2* working group tasked with development of PSD2 API
- First version published in Oct 2018
  - HTTP based API with features for AIS and PIS (and PII)
  - Payload JSON and XML
  - Application level signing
  - Different SCA Approaches: Redirect, Decoupled, Embedded
  - **OAuth supported for so-called pre-authorization only**
- My role: OpenID Foundation (FAPI WG) liaison, first contact in early October
- Latest version, published in Feb 2018, adds new **OAuth SCA Approach**

SCA Approaches

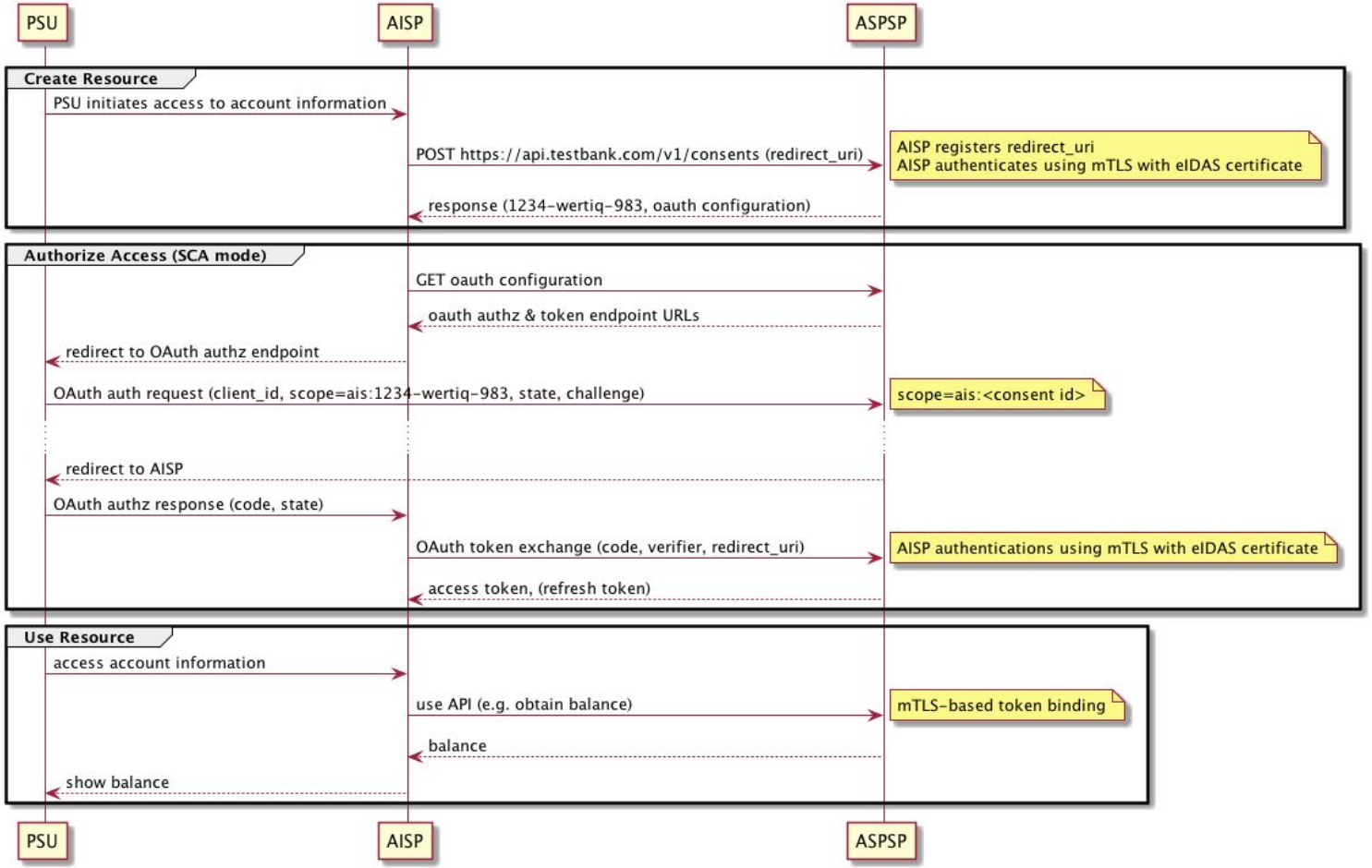
1. Redirect: proprietary redirect-based protocol
2. Decoupled:
    - user is asked to authorize TX on another device in an bank app
    - no credentials through TPP
3. Embedded:
    - all messages for authentication and authorization flow through TPP
    - ASPSP tells TPP what is needed
    - TPP renders UI, let the user enter the credentials and passes it to the bank
    - User Consent coupled would with SCA
4. OAuth: uses OAuth to authorize payment/access to account information

OAuth SCA Approach - Starting Point

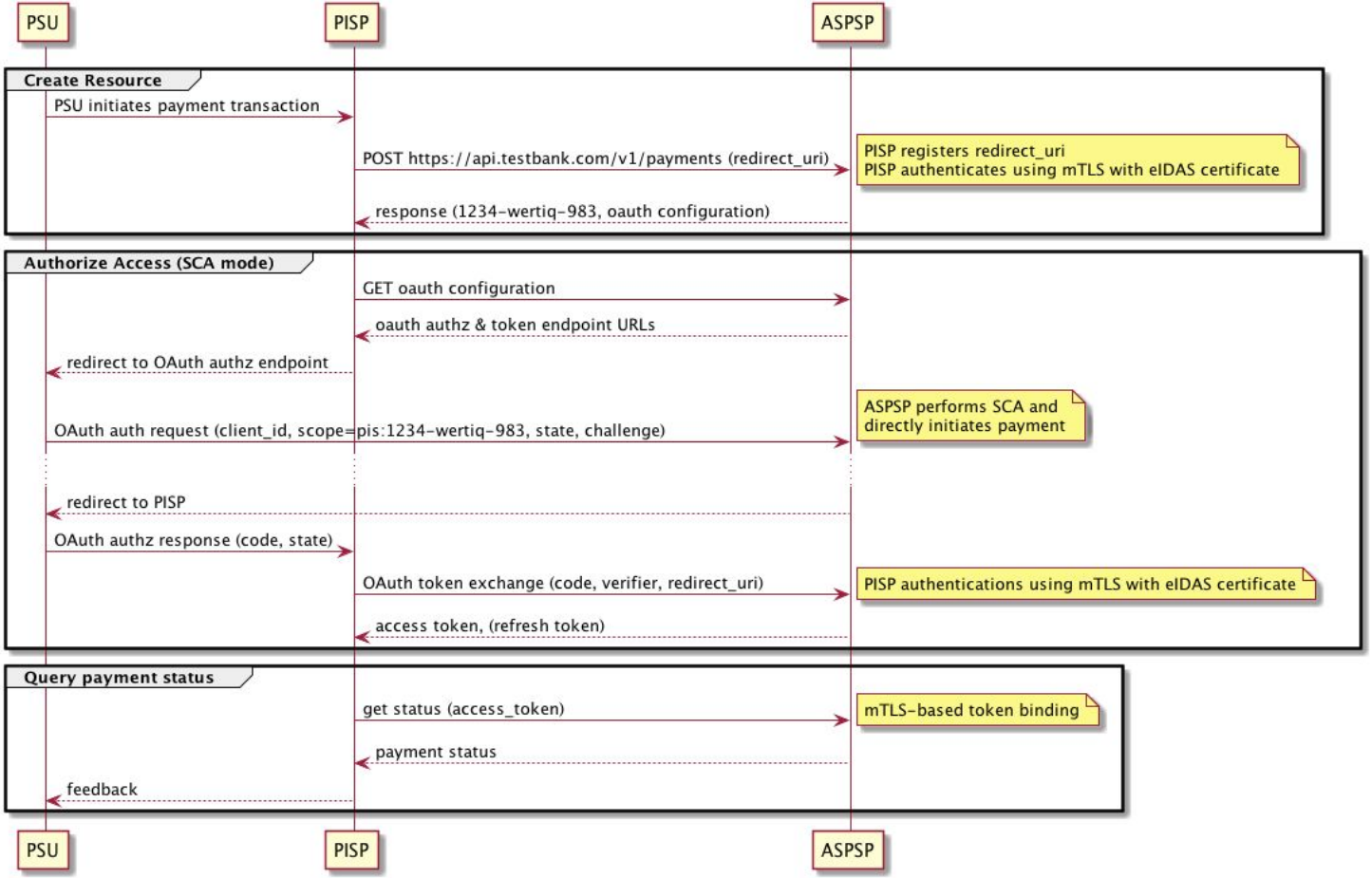
- Proposal with least disruption to existing BG approach
- Avoid client registration to improve compliance with latest EBA RTS
- Terms
  - PSU: user
  - AISP: account information service provider
  - ASPSP: account serving payment service provider (e.g. bank)



OAuth SCA Approach (Account Information)



OAuth SCA Approach (Payment Initation)



Client Management (Challenges & Solutions)

- EBA RTS §32 prohibits the ASPSP to require “...additional authorisations and **registrations** in addition to those provided for in Articles 11, 14 and 15 of Directive 2015/2366.”
  - OAuth Approach directly uses eIDAS certificates issued to PSD2 TPPs to authenticate the respective OAuth clients (based on mTLS for OAuth)
- eIDAS Certificates do not contain *client_ id* nor *redirect_uri*
  - Use aisp/pisp id in the cert + country id as *client_id*
  - register *redirect_uri* with every transaction (mTLS protected)

Further Details

- OAuth Server Metadata
- PKCE for injection prevention

Status

- Current draft has serious issue - all OAuth parameters were “camel cased”
  - Example: **client_id** -> **clientId**
  - **Causing the spec to be incompatible to RFC6749**
  - Will be correct in next revision
- Redirect-based flows are still subject to debates
  - EC and ECB do not want to allow banks to use redirects without previous approval by the respective TPP
  - EBA has not taken a position yet

Please review the BG specification, in particular the OAuth SCA Approach!

https://www.berlin-group.org/nextgenpsd2-downloads