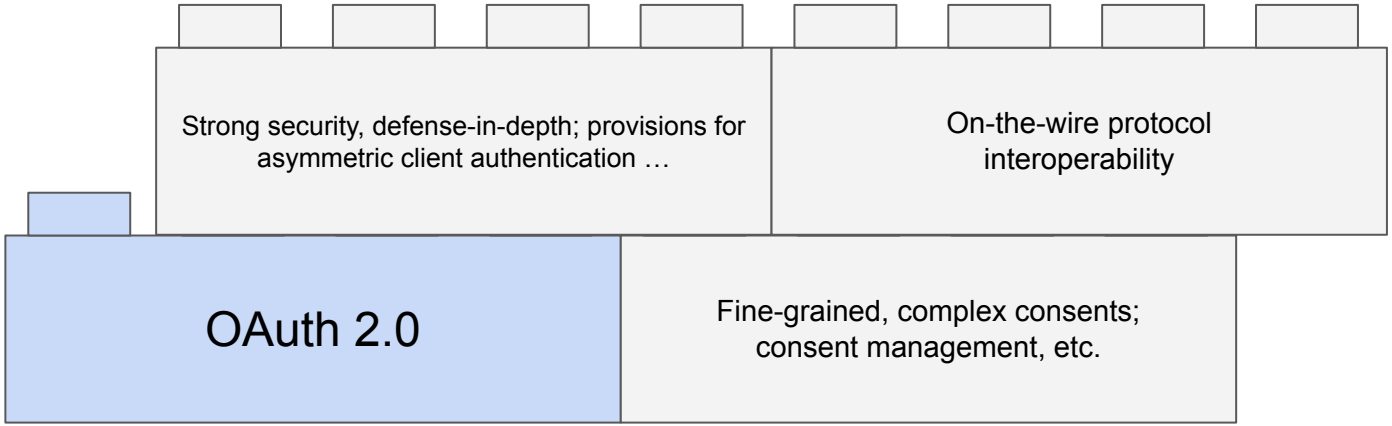
FAPI 2.0

Torsten Lodderstedt, yes.com

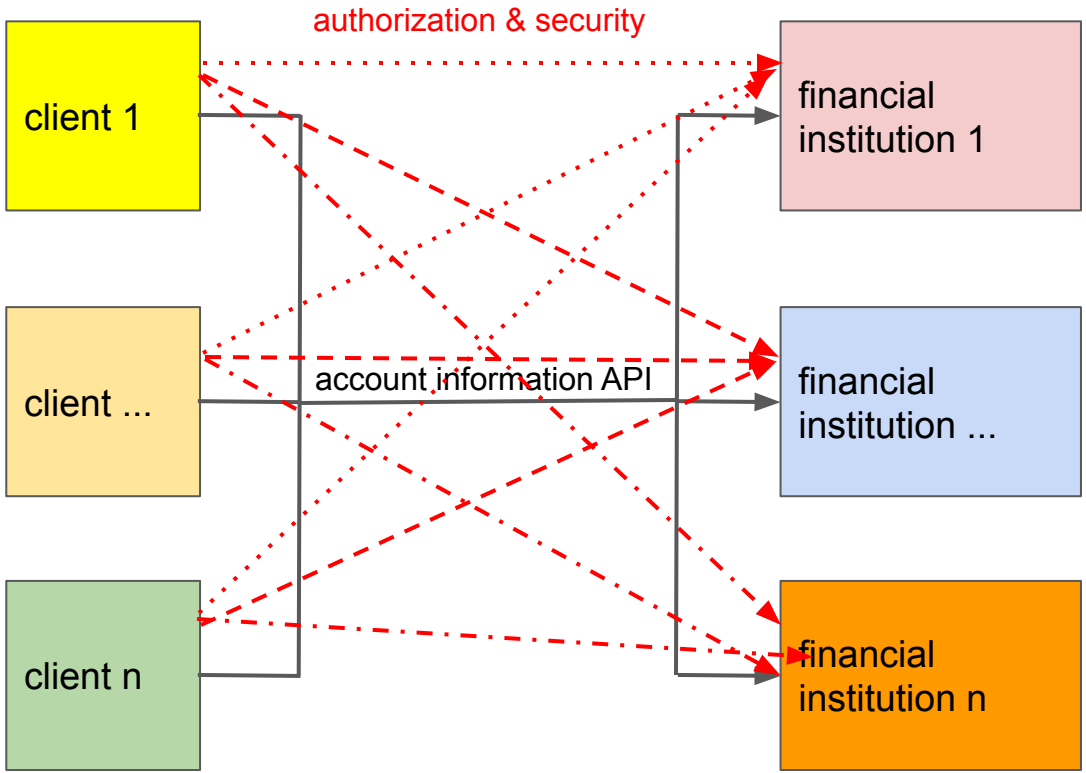
Authorization in Open Banking Standards

- Usually based on OAuth 2.0, the industry standard for API authorization
- … but that is not sufficient!



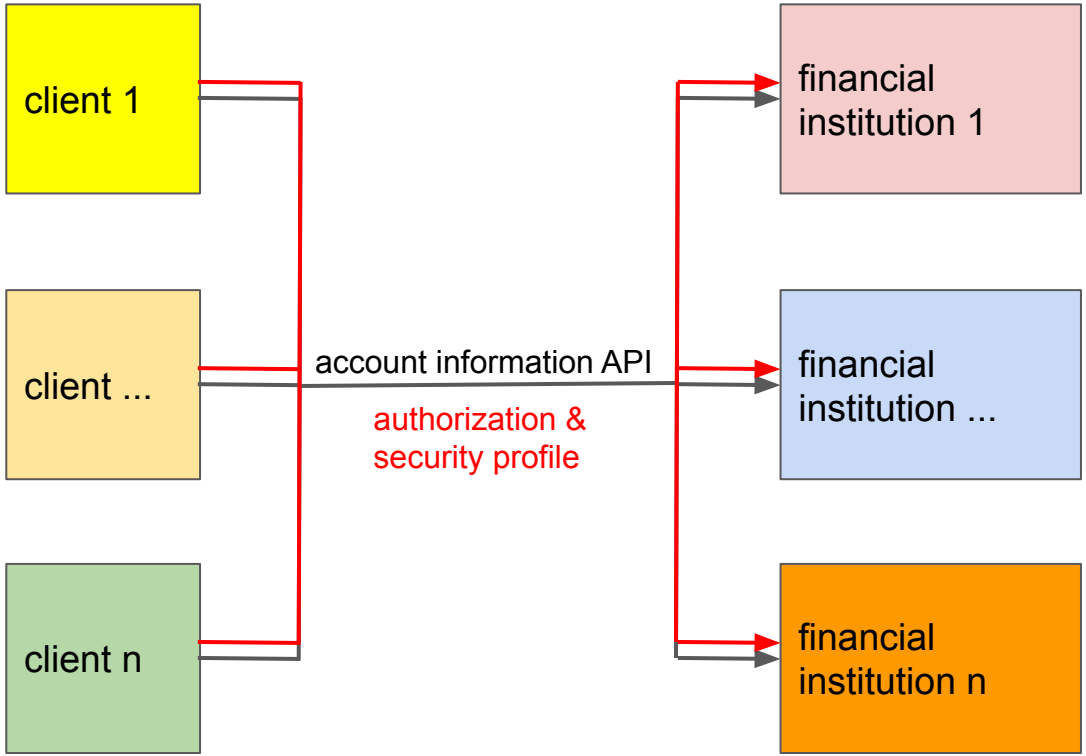
OpenID

Open Banking and Interoperability



OpenID

Interoperable Security Profile

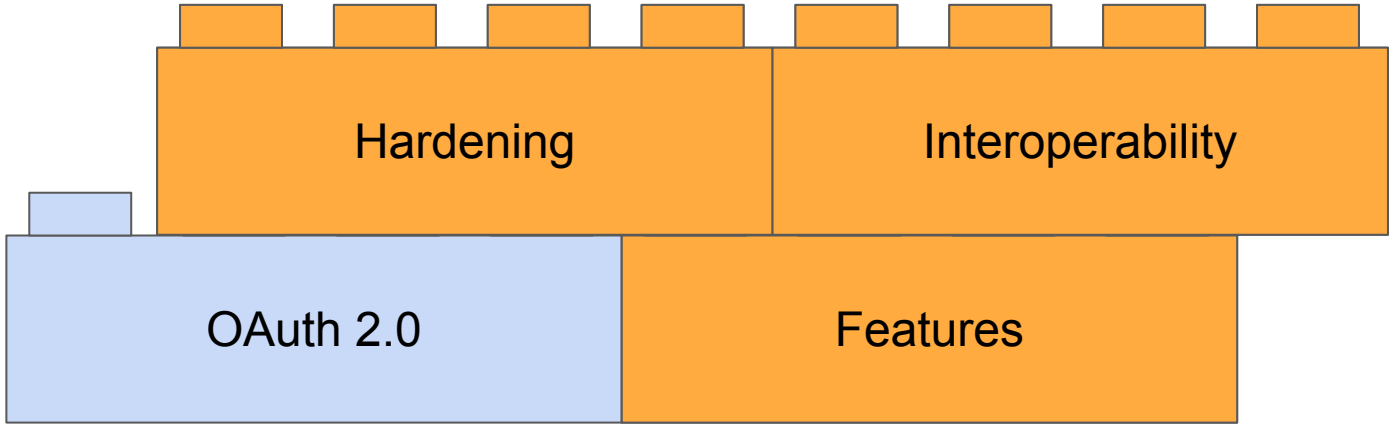


OpenID

FAPI is a reusable Security Profile

- for any kind of security sensitive API
- Security, interoperability, and feature profile for OAuth 2.0

Provided by FAPI

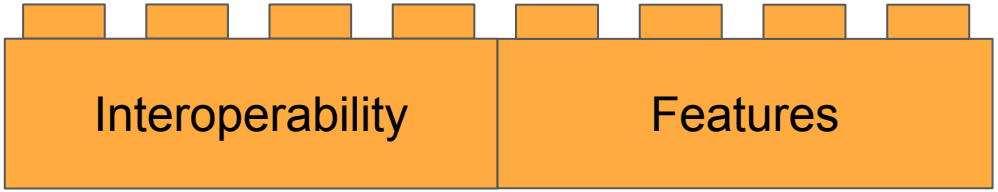


OpenID

FAPI

- FAPI 1.0 adopted in Open Banking
- FAPI 2.0: Evolution of FAPI 1.0 based on industry experience
  - Extended Scope
  - Improved interoperability
  - Improved security
  - Simplified development

FAPI 2.0



Pushed Authorization Requests (PAR) replace bespoke solutions like external resources with references in scope/claims, custom authorization request parameters, …

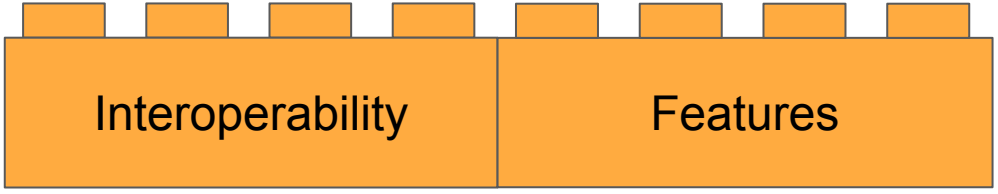
→ Simplified development through vendor support (expected)

→ Minimize data in front-channel to improve security

```
POST /as/par HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0Mzo3Rmp..

response_type=code
&client_id=s6BhdRkqt3&state=af0ifjsldkj
&redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
<voluminous payload goes here>

HTTP/1.1 201 Created
Cache-Control: no-cache, no-store
Content-Type: application/json

{
  "request_uri":"urn:example:bwc4JK-ESC0w8acc1...",
  "expires_in": 90
}
```


OpenID

FAPI 2.0

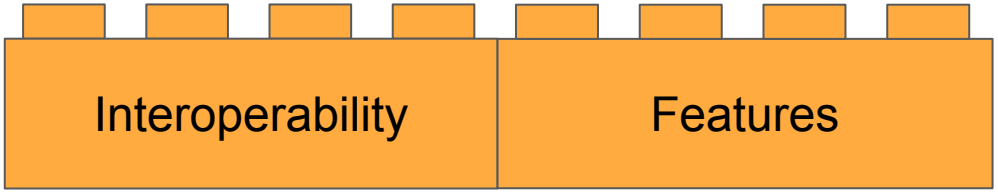


Rich Authorization Requests (RAR)

enable fine-grained and complex consents.

```
[
  {
    "type": "payment_initiation",
    "actions": [
      "initiate", "status", "cancel"
    ],
    "locations": [
      "https://example.com/payments"
    ],
    "instructedAmount": {
      "currency": "EUR",
      "amount": "123.50"
    },
    "creditorName": "Merchant123",
    "creditorAccount": {
      "iban": "DE02100100109307118603"
    },
    "remittanceInformationUnstructured": "Ref Number"
  }
]
```

FAPI 2.0

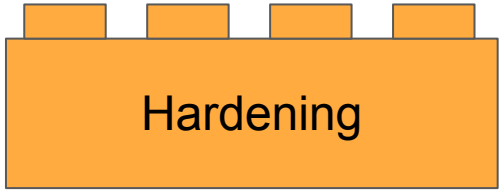


Grant Management API
enables support for

- consent state synchronization
- consent revocation
- concurrent consents
- dashboards

OpenID

FAPI 2.0



OAuth Security Best Current Practice RFC draft incorporated for latest OAuth security recommendations.

OAuth Mutual TLS for client authentication and sender-constrained access tokens.
(as in FAPI 1.0)

→ Protect against code replay, mix-up attacks, etc.

FAPI Security

The security of FAPI is very well understood:

- FAPI 1.0
  In-depth security analysis based on latest web security research methods

- FAPI 2.0
  - Clearly defined attacker model (threat model)
  - Reduced number of options
  - → Baseline Profile defends against all threats from attacker model
  - → Advanced Profile additionally provides non-repudiation

Outlook

Current Status of FAPI 2.0:

- Baseline Profile: Working Group Draft
- Attacker Model: Working Group Draft
- Grant Management: Working Group Draft
- Advanced Profile: In preparation

Adoption by external entities:

- Norwegian e-Health systems: integration ongoing
- Australian Consumer Data Right: movement towards adoption