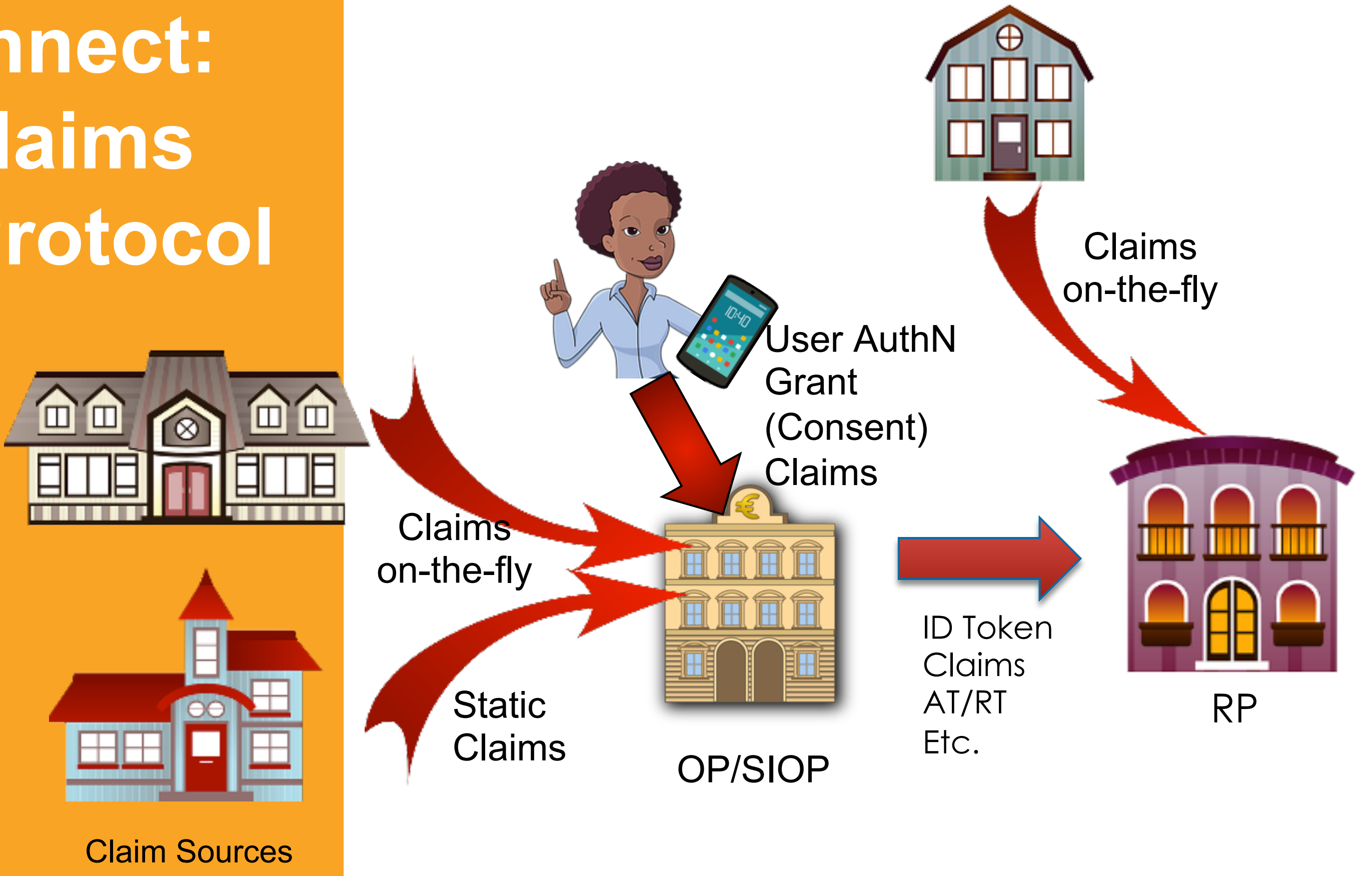
OpenID Connect & FAPI Overview

2020-10-28
OIDF Workshop - FAPI

OpenID Connect: Selective Claims Provision Protocol

Which also forms Basis for ABAC.



Claims on-the-fly

User AuthN Grant (Consent) Claims

Claims on-the-fly

Static Claims

OP/SIOP

ID Token
Claims
AT/RT
Etc.

RP

Claim Sources

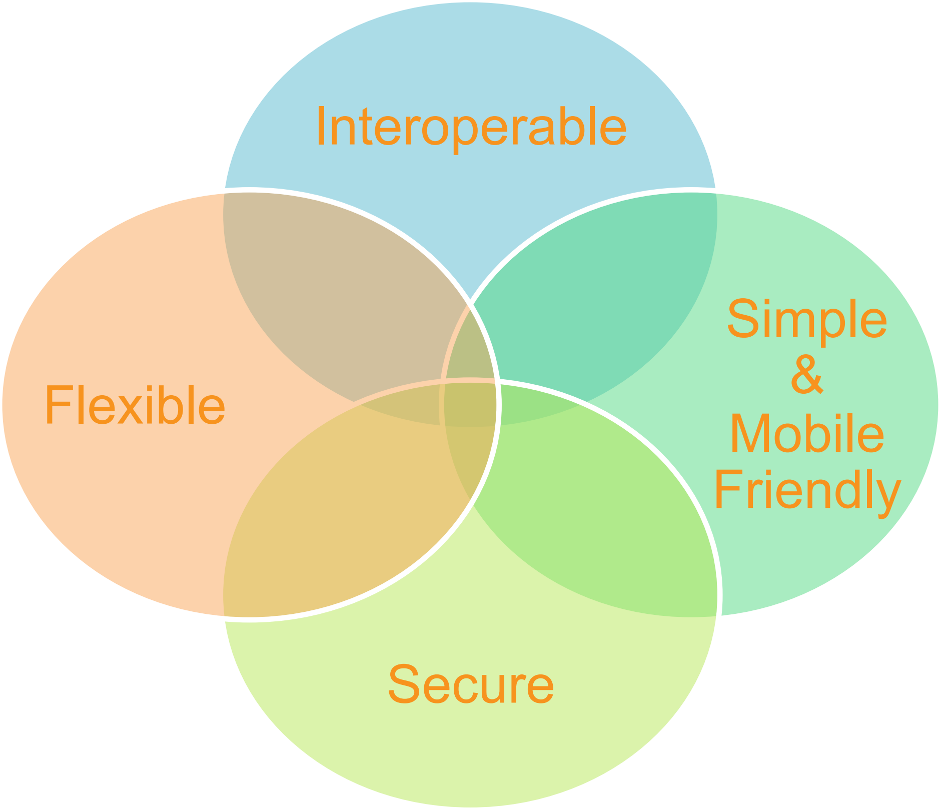
An Identity Layer provides:

Who	• is the user that got authenticated
Where	• was he authenticated
When	• was he authenticated
How	• was he authenticated
What	• attributes he can give you
Why	• he is providing them

Identity = Set of Claims related to an entity

```
{
 "iss": "https://server.example.com",
 "sub": "248289761001",
 "aud": "example.net",
 "acr": "https://tf.example.com/gold",
 "iat": 1311280970,
 "exp": 1311281970,
 "nonce": "n-0S6_WzA2Mj"
}
```

OpenID Connect



Interoperable

Flexible

Simple
&
Mobile
Friendly

Secure

Interoperable

Standard scopes	• openid, profile, email, address, phone
Method to ask for more granular claims	• Request object and claims
ID Token	• Info about the authenticated user
UserInfo endpoint	• Get attributes about the user • Translate the tokens

Simple & Mobile Friendly

JSON Based

REST Friendly

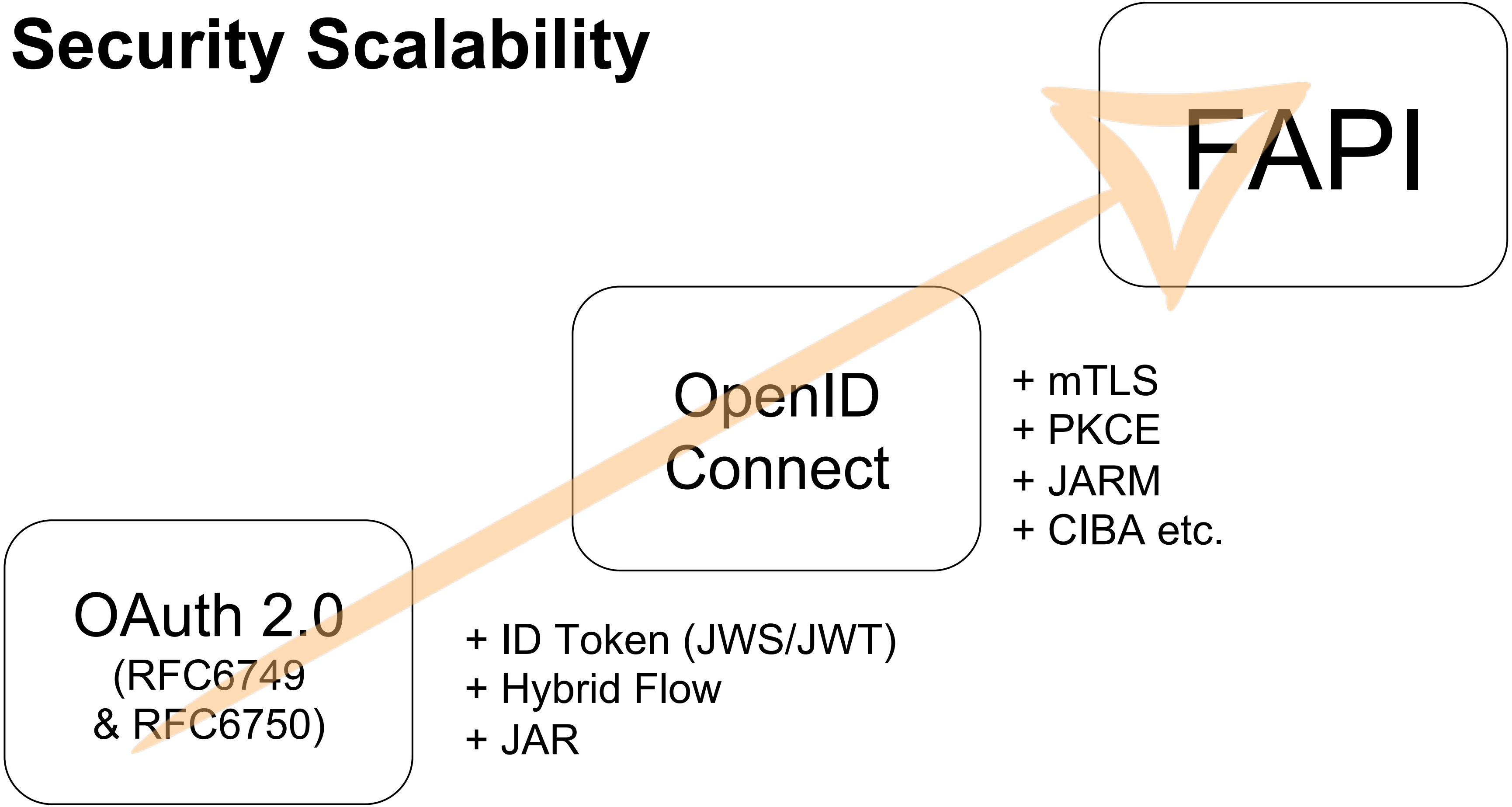
In simplest cases, just copy and paste

Mobile & App Friendly

e.g., ID Token is signed JSON

```
{
    "iss": "https://client.example.com",
    "user_id": "24400320",
    "aud": "s6BhdRkqt3",
    "nonce": "n-0S6_WzA2Mj",
    "exp": 1311281970,
    "iat": 1311280970,
    "auth_time": 1311280969,
    "acr": "2",
    "at_hash": "MTIzNDU2Nzg5MDEyMzQ1Ng"
}
```

Security Scalability



OAuth 2.0
(RFC6749
& RFC6750)

+ ID Token (JWS/JWT)
+ Hybrid Flow
+ JAR

OpenID
Connect

+ mTLS
+ PKCE
+ JARM
+ CIBA etc.

FAPI

FAPI - Financial-grade API Security Profile

Designed for higher security

For transactions with higher values at stake or to exchange sensitive data.

Formally Verified

Security Properties Formally verified against Web Attacker Model.

Flexible

Granular Request	• Through Request Object (JSON) • Data Minimization
Aggregated Claims	• Does not disclose data recipients to data sources
Distributed Claims	• Decentralized Data Storage

FAPI - Ver1 & Ver2

FAPI ver.1 is to become final specification this year.

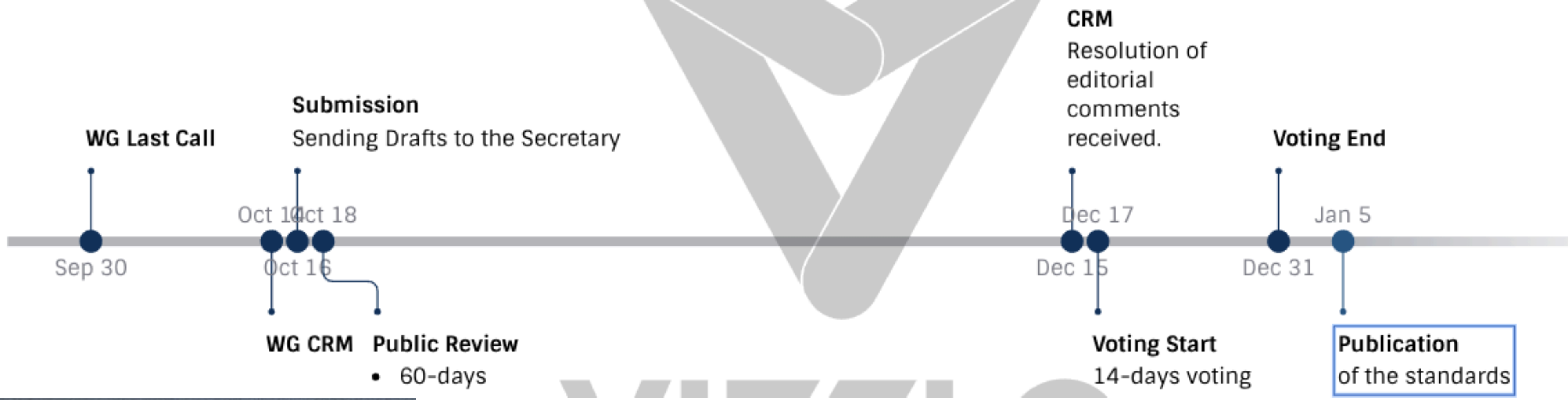
- Formally verified
- Open Banking UK
- Open Banking AU - https://consumerdatastandardsaustralia.github.io/infosec/#2-overview
- FDX North America coming onboard on FAPI ver.1

FAPI ver.2 is in the making.

- Streamlining
- Clearer security target
- Yet to be Formally Verified
- OBIE, AU CDR, FDX will contribute in ver.2

FAPI ver.1

- Part 1 - Baseline (was Read Only)
- Part 2 - Advanced (was Read & Write)
- Part 3 - CIBA Profile
- Part 4 - JARM



WG Last Call
Sep 30

WG CRM
Oct 14

Oct 16

Submission
Sending Drafts to the Secretary
Oct 18

Public Review
- 60-days

CRM
Resolution of editorial comments received.
Dec 15

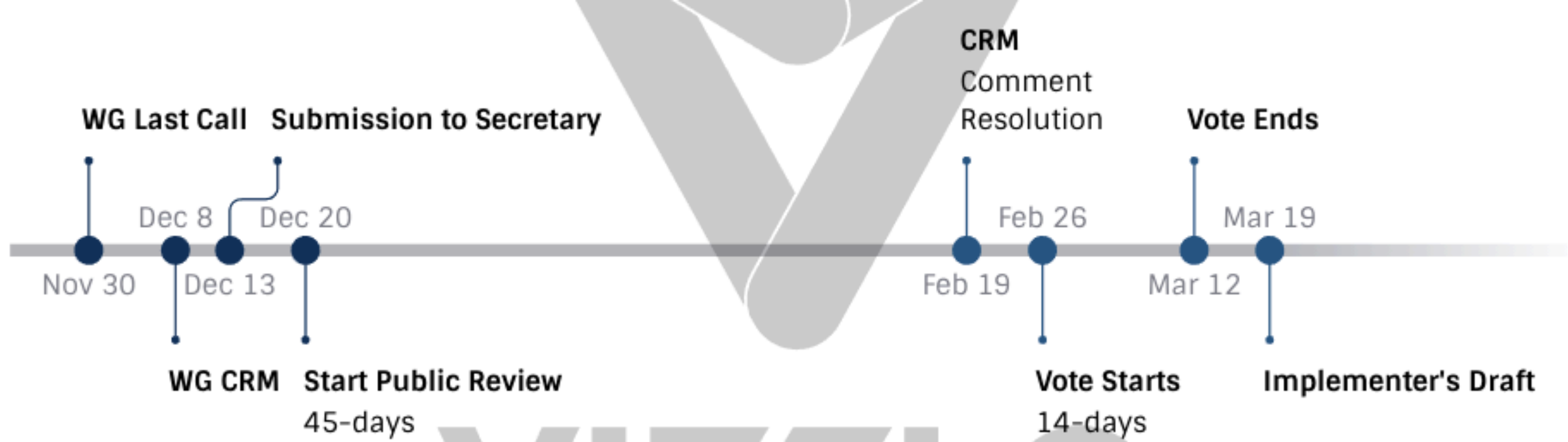
Dec 17
Voting Start
14-days voting

Voting End
Dec 31

Jan 5
Publication
of the standards

FAPI ver.2
(Proposal)

- Grant/Consent Management
- Event Notification.
- etc



Nov 30
WG Last Call

Dec 8
WG CRM

Dec 13
Submission to Secretary

Dec 20
Start Public Review
45-days

Feb 19
CRM
Comment
Resolution

Feb 26
Vote Starts
14-days

Mar 12
Vote Ends

Mar 19
Implementer's Draft

Conformance Test

OpenID®

Create the future together.