Standardized, Fine-Grained Authorization Using OAuth2 Grant Management and OAuth2 Rich Authorization Requests

Dima Postnikov
OpenID Foundation, Vice Chair

Gail Hodges
OpenID Foundation, Executive Director

19 March, 2025

Contributors

Authors: Dima Postnikov and Gail Hodges

Nat Sakimura
Serj Hallam
Mike Leszcz
Mark Haine
Joseph Heenan
Ralph Bragg

This article is also published at https://medium.com/@dimapostnikov/standardized-fine-grained-authorization-using-oauth2-grant-management-and-oauth2-rich-c42f7286c410

Table of Contents

1. Open Banking and Open Data journey

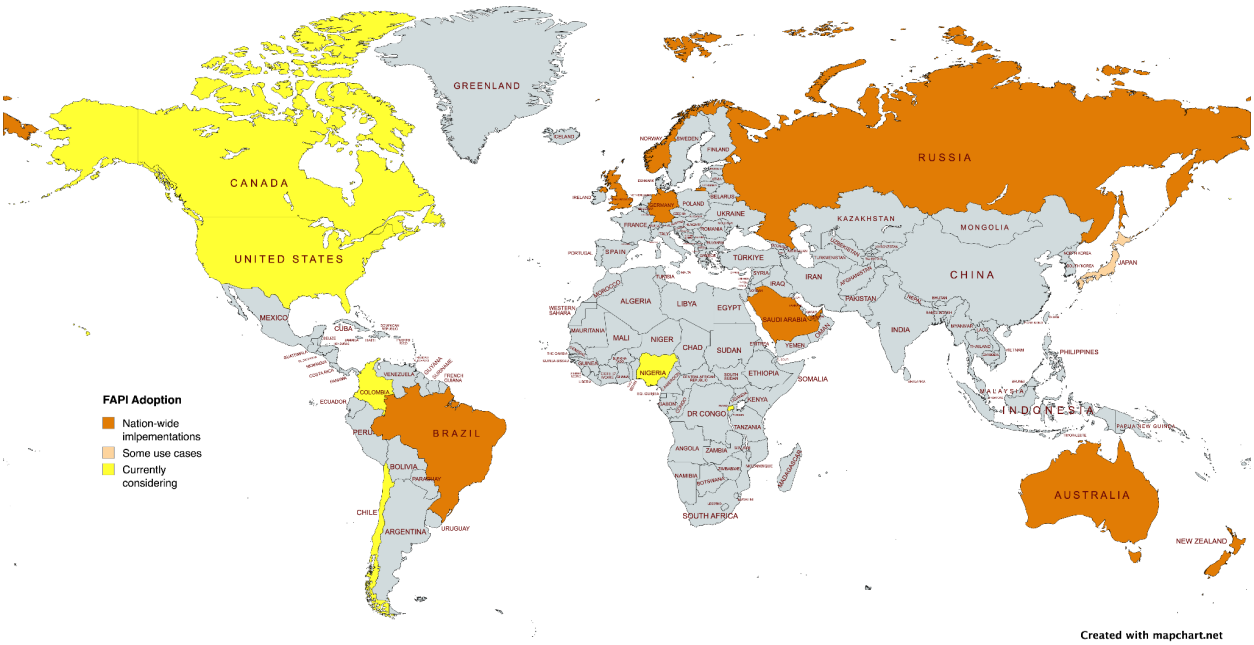
Open Banking is not new.

Since 2018, the OpenID Foundation FAPI WG and the global community have been developing standards to support Open Banking and Open Data.

Many ecosystems have gone live:

- Open Banking in the UK
- Consumer Data Right in Australia
- yes.com in Germany
- Open Banking in Brazil
- ConnectID in Australia
- Open Insurance in Brazil
- HelseID in Norway
- Open Banking in Saudi Arabia
- Open Finance in the UAE

Several ecosystems have selected FAPI and are in the process of deploying it. Other ecosystems are conducting due diligence on FAPI, such as the US and Canada (Financial Data Exchange), Colombia, New Zealand, Rwanda, and Nigeria. And the number of countries will grow: according to the Judge School of Business, over 90 countries actively pursue open banking and data.



The global standards community has collaborated and learned from all these implementations. Based on the experience of previous deployments, every new ecosystem has improved.

Here are just some of the examples:

1. Open Banking UK pioneered using FAPI 1 by adopting early specification drafts.
2. CDR in Australia has narrowed implementation options to facilitate the participants' work and expanded the mandate to other industries. Open Banking UK and CDR helped improve FAPI1 before the specification became final.
3. Open Finance Brazil productionised automatic conformance testing based on the OIDF conformance suite.
4. Yes.com, ConnectID, and HelseID have pioneered using the FAPI 2 security profile, a newer and simpler version of the FAPI security profile redesigned based on a defined attacker model and formally tested for vulnerabilities.

Every new ecosystem also took less time to implement because of industry community experience and growing vendor support.

When so many ecosystems implement FAPI side by side, they yield additional security benefits. For example, when an academic security risk was identified under formal security analysis, ecosystems known to use the impacted specs were amongst the first to be briefed so they could evaluate the impact on their ecosystem and take any mitigating actions. In short, “more eyes” on standards, security, and operational challenges benefits all ecosystems.

2. Open Banking high-level architecture

Our experiences show that a security profile like FAPI alone cannot deliver a fully functioning and secure data-sharing ecosystem.

A typical data-sharing ecosystem requires assembling many technical building blocks by ecosystem governing bodies and their implementers.

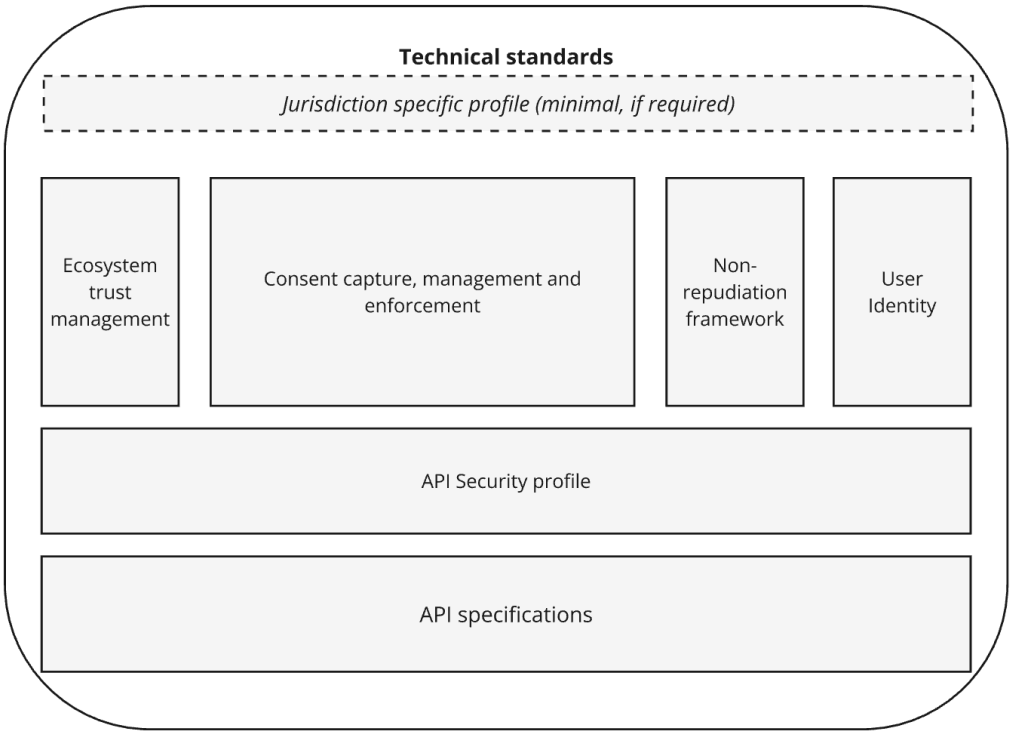


Diagram 1

OpenID Foundation and FAPI WG have delivered some of the key building blocks to date:

- **FAPI 2 Security profile** for OAuth 2 protected APIs;
- **FAPI 2 Message Signing** for non-repudiation;
- **OpenID Connect** for user authentication and **OpenID for Identity Assurance** for extended identity attributes ;
- **FAPI CIBA** for decoupled authentication.

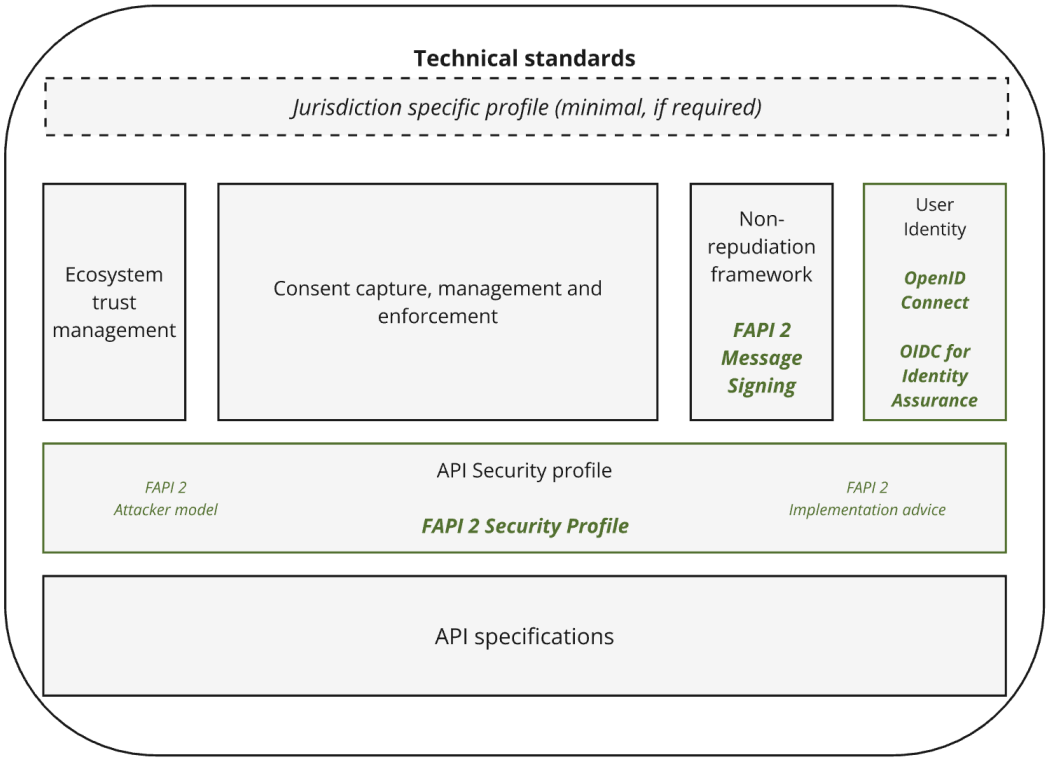


Diagram 2

Some areas are more challenging to standardize and have been left with each ecosystem to develop, for example:

- A functional API specification and
- A jurisdiction-specific profile.

Some other areas are still yet to be standardized:

- Ecosystem trust management
- Fine-grained authorization

Unfortunately, each ecosystem currently develops its approach to solving this, very often based on a specific vendor chosen.

3. FAPI WG mission

The primary objective of the OpenID Foundation FAPI Working Group is to enable secure, interoperable, and privacy-preserving data-sharing ecosystems.

To help these ecosystems scale quickly with minimal cost and to provide necessary vendor support, we need to:

- Provide as many as possible standardized building blocks to FAPI-based ecosystems;
- Ensure all building blocks and their relevant combinations have their security properties formally analyzed.
- Ensure all building blocks have full OIDF conformance testing coverage and can be tested together.
- Make sure all components work together without requiring additional effort from implementers or ecosystem governing bodies;
- Provide reusable profiles of the specifications.

The FAPI WG is working on an FAPI 2 framework outlining the standards recommended for adopting new ecosystems.

4. Introducing Standardized fine-grained authorization

4.1 Rich Authorisation Request - adding fine-grained details to the request

The use of OAuth 2.0 Rich Authorization Requests (RAR) [https://www.rfc-editor.org/info/rfc9396] is recommended by FAPI WG when the scope parameter is not expressive enough to convey the authorization that a client may want to obtain:

- Implementers can use RAR to standardize the envelope and data payload to convey complex, fine-grained authorization requests (for example, for privacy-preserving data sharing or payments).
- RAR allows the expression of local requirements and data models specific to locally defined functional APIs or other functionality. OIDF intends to work on multiple templates with different ecosystems to create a shared library, like the JSON schema for OpenID Connect for Identity Assurance. These schemas ideally can be plugged into the OIDF conformance test suite via configuration and not additional build.
- RAR can be used across existing authorization flows and express the grant's fine-grained permissions desired by the client. The authorization server would be responsible for initial RAR processing.

Here is an example of the fined grained authorization request:

```
"authorization_details":[
    {
       "type":"account_information",
       "actions":[
          "list_accounts",
          "read_balances",
          "read_transactions"
       ],
       "locations":[
          "https://example.com/accounts"
       ]
    }
 ],
```

The outer part of the data envelope **(above, in bold)** and outer data structure are standardized. This part is in the scope of OIDF certification and is covered by formal security testing.

The inner part of the data envelope (above in blue) is localized to ecosystem-specific and local requirements. OIDF sees value and can facilitate ecosystems by maintaining common templates for some local requirements

Some ecosystems, such as Open Finance UAE, have already implemented RAR in their ecosystem.

The previous non-standardized and non-interoperable alternative used a custom payload with a custom API and scope values. Every ecosystem had to re-invent one or copy and paste it from another.

4.2. Grant Management - Adding fine-grained authorization to the transaction flow

FAPI WG and OpenID Foundation recommend OAuth 2 Grant Management (GM) [https://openid.net/specs/oauth-v2-grant-management-ID1.html] for ecosystems that require interoperable grant (authorization) management.

OAuth 2 Grant Management is a simple OAuth extension implemented by Authorization Servers to provide third parties with a standardized ability to:

- Identify a specific authorization (grant) using grant_id. It is beneficial where multiple-party authorization or concurrent consents[1] are required;
- View the details of the specific authorization. For example, in a case where multi-party approval is required, a client can query the authorization server to find out if the grant has been fully authorized or not yet;
- Change/update/replace/withdraw a specific authorization opens up a range of business and technical use cases that can now be supported interoperably, such as simpler UX for consent re-authorization and amendment or technical migration to consents.

Before Grant Management, all authorization servers already managed grants internally, but there was no standardized interface for third parties to understand (let alone request changes), so the internal behavior diverged.

Current ecosystems have had to forgo fine-grained authorization or use non-standardized Consent or Intent APIs. OpenID Foundation's formal analysis and conformance testing don't cover custom solutions. Non-standard APIs can also be deployed outside your security infrastructure, thus creating additional security risks.

Grant management was initially designed to address the complex requirements of emerging ecosystems like CDR in Australia. In 2023, the OpenID Foundation and its community reviewed and approved the second implementer's draft.

This specification closes the gap in a standardized way that aligns with the other specifications in the FAPI 2.0 framework, as seen in Diagram 2.

4.3 Grant Management / RAR comparison to custom Consent or Intent APIs

The table below compares Grant Management plus Rich Authorization Requests (RAR) with the current proprietary and ecosystem-specific Consent or Intent APIs.

	Grant Management + RAR	**Consent / Intent API**
Standardized	Yes	No
Authorisation Server vendor support	Yes, it can already be supported by some vendors. Anticipated: support and adoption are key objectives of standardization.	Not in an interoperable way. Current implementations are custom, highly fragmented, and prone to vendor lock-in.
Part of the security infrastructure	Yes	No* As a non-standard extension,

[1] Concurrent consents allow establishment or multiple consents between a client and AS for the same user. It's a regulatory requirement in some ecosystems like CDR.

(Authorization Server)		depending on the implementation.
Part of the OIDF conformance test suite	Yes, planned It's a key outcome of standardization.	No* It could be customized.
Formal security analysis coverage.	Yes, planned. It's a key outcome of standardization.	No
Availability	Now Some effort is required initially. Most Authorization Server vendors can implement it without changing the core product. Still, the long-term intent is to implement GM as part of many vendors' core products, reducing effort and cost for future implementers.	Now A relatively smaller effort is required upfront due to its custom nature and typical implementation outside security infrastructure. A much greater effort is required to migrate to a standardized solution later.
Existing Implementers	In progress, none live yet. - anticipating initial ecosystem adoption.	Many non-standard and snowflake (different variants) implementations are unique to each ecosystem or deployment.
Interoperability	Key design goal.	Not planned.

FAPI WG requires more implementers to progress Grant Management and RAR to the final specification stage, which includes OIDF conformance testing updates and formal security analysis.

ConnectID in Australia and SelectID in the UK have already stated their intent to enable Grant Management and to collaborate with the next wave of Open Banking implementers.

5 An opportunity

Previously deployed ecosystems did not have an opportunity to use a standard-based approach in fine-grained authorization.

It is also hard to migrate existing ecosystems to a new approach because changing a fundamental authorization flow requires delivering additional business value.
Potential migration effort is an important reason why new ecosystems should carefully consider the options and tradeoffs to help future-proof their deployments.

Ecosystems new to open banking and open data can standardize another critical building block and help mature the grant management and RAR implementations, just as their ecosystem peers did with FAPI 1.0 and FAPI 2.0 before them.

We encourage new ecosystems to become early adopters of Grant Management and RAR specifications. The OpenID Foundation and the FAPI Work Group are interested in collaborating.

Summary

For most emerging open banking and open data ecosystems, the OIDF recommends using FAPI 2.0 Security Profile, Grant Management, and RAR and joining the next wave of early adopters to help mature the specifications and open source tests. These will serve as another critical building block in the FAPI 2.0 Framework.

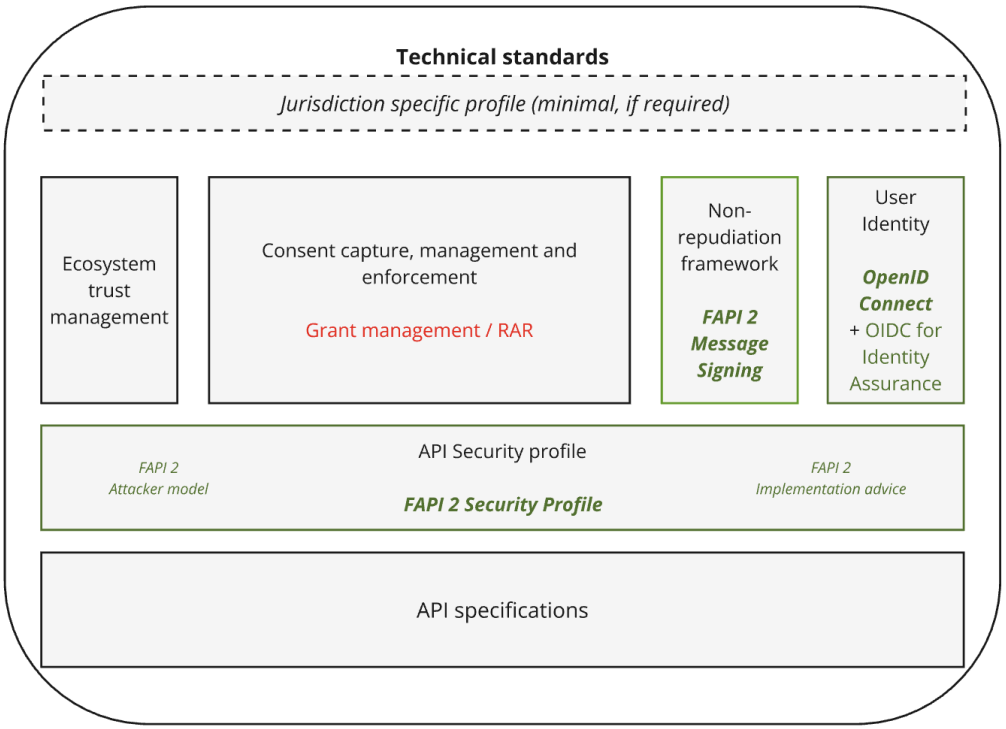


Diagram 3

Implementers interested in being early adopters of Grant Management and RAR should contact openid-specs-fapi-owner@lists.openid.net to discuss the next steps.

More broadly, the FAPI Working Group is open to the public, and anyone can contribute at no cost by signing a contribution agreement. To learn more about FAPI or the FAPI Working Group, visit https://openid.net/wg/fapi/, sign up for the mailing list, and attend WG meetings.

We also recommend that all current and new ecosystems join the newly established Ecosystem Community Group to help the OIDF community provide ongoing support for ecosystem leaders. To learn more about Ecosystem Community Group, visit https://openid.net/cg/ecosystem-support-community-group/, sign up for the mailing list, and attend CG meetings.

The OpenID Foundation

The OpenID Foundation is a non-profit, international standardization organization specializing in identity standards for the Internet. OpenID Foundation standards are deployed by millions of applications and enable billions of users to access services online. OpenID standards are applicable across a wide range of use cases, including identity services, financial services, mobile networks, healthcare, government, and other verticals. To learn more about how you can contribute to the OpenID Foundation Working Groups or Community Groups, visit openid.net.