OpenID Foundation response to the Consumer Data Right Issues Paper

Prepared by: OpenID Foundation (https://openid.net/)

Prepared for: Secretariat. Inquiry into Future Directions for the Consumer Data Right. The Treasury.

Date: 21-May-2020

Introduction

This is the OpenID Foundation's response to the Australian Government's Inquiry into Future Directions for the Consumer Data Right Issues Paper, dated March 2020 - see https://treasury.gov.au/sites/default/files/2020-03/200305_issues_paper.pdf

About the OpenID Foundation

The OpenID Foundation is a non-profit International standardization organization founded in 2007, specialized in the standardization of internet identity and API access management.

The OpenID Foundation welcomes Consumer Data Right's decision to adopt the OIDF FAPI profile as the base for security standards.

The FAPI profile

The Financial-grade API (FAPI) profile is a secure profile of OpenID Connect, OAuth 2 and other standards to make it suitable for financial and other transactions requiring higher security and non-repudiation.

Members of FAPI working group are the authors and contributors of FAPI profile, OpenID Connect, OAuth 2, JWS, JWT and other standards adopted by the many industries and countries worldwide.

Australia is not alone in standardising it's security around FAPI profile which is already adopted or being adopted in the UK, Europe, Brazil and New Zealand and other jurisdictions.

Global adoption of FAPI profile allows Australian consumers to have access to innovative fintechs developed overseas and, also, it allows Australian fintechs to expand overseas without re-developing / duplicating part of their offering.

These FAPI standards are evolving and we would like Australia to continue to benefit from this evolution by adopting them:

- FAPI 2.0
  Defines a profile incorporating the next generation of specifications targeted at Financial-grade API services. FAPI 2.0 incorporates a well defined attacker model and brings together a combination of specifications including:
    - OAuth 2.0 Proof Key for Code Exchange (PKCE)
    - OAuth 2.0 Mutual-TLS Client Authentication
    - OAuth 2.0 Pushed Authorisation Request (PAR)
    - OAuth 2.0 Rich Authorisation Request (RAR)
    - OAuth 2.0 Authorisation Server Metadata (the next evolution of OpenID Discovery)
    - OpenID Connect Core 1.0 incorporating errata set 1
    - Grant Management for OAuth 2.0
      Defines a standardised method of managing consent. This specification also incorporates a Management API allowing for read/create/update/delete operations of assigned resources.

      This specification was described for application to the Consumer Data Right within the OIDF's consent proposal (https://github.com/ConsumerDataStandardsAustralia/standards/issues/99#issuecomment-592320557) and introduces capability for future requirements related to complex consents and consent taxonomy suitable for write access APIs.

Future roles and outcomes of the Consumer Data Right

International context

We believe that compliance with international standards:

- Increases interoperability with other similar regimes internationally.
- Creates opportunities for Australian fintechs to participate in similar regimes globally
- Creates opportunities for Australian consumers to access the global fintech community and innovation. This also increases competition locally.

Read access

We believe that compliance with international standards:

- Ensures efficiency by utilising existing products, exiting testing frameworks, minimising costs for all participants.
- Improves privacy and security by leveraging global expertise.
- Future proofs Australian technical standards to leverage future enhancements.

Adopting FAPI Grant Management can assist 'consent' taxonomy and consent enhancements by utilising a standard approach (OAuth2 extension) that focuses on user authorisations and caters for a variety of use cases, industries and different trust ecosystem requirements.

Additional security and usability enhancements could be made to CDR by adopting app-2-app authorization flow.

Write access

We believe further security enhancements to improve the strength of customer authentication are required to be implemented before introducing write access to CDR.

Adopting FAPI Grant Management can assist with setting up a fine-grained authorization framework required for write access.

Adopting FAPI CIBA can support a range of payment-related use cases that can utilise standard based decoupled authentication flow. The development of the CIBA specification is a result of the EU's 2nd Payment Services Directive (PSD2), which mandates that banks allow their customers to access their data and make payments via authorized third parties.

Linkages and interoperability with existing frameworks and infrastructure

By adopting international standards like FAPI, Australia can lead the way towards global interoperability international data portability regimes that started with Open Banking UK, and expanding it to other countries like the United States, Canada, Brazil and many others.

Conformance and certification

The OpenID Foundation have developed a FAPI conformance suite, which is now being used by vendors and all the major banks in the UK to test and certify implementations. This low cost/ high integrity self certification model has been adopted by the UK OBIE and is seen by many as an important element of ongoing conformance to technical standards.

Banks in the UK who have used this suite have seen significant benefits as follows:

- Speeding up the development and testing process.
- Enhanced security to better protect access to customer data.
- Greatly reduced volume of complaints from third parties.

These benefits, especially the latter two, give the regulators comfort that the banks are implementing the standard correctly, and taking reasonable steps to protect the rights of both customers and third parties. Banks in the UK have also had far easier time getting their services live and working where they have used products that vendors have already certified are FAPI compliant.

The Financial Conduct Authority (FCA) have not mandated use of the conformance suite, nor certification, for all UK banks - however the Competition and Markets Authority (CMA) do require this for the largest 9 banks in the UK.

However, this conformance suite is currently not utilised by Consumer Data Right. It’s an open source framework that provides the ability to automate functional and security conformance to increase the quality and trust of the ecosystem. OpenID foundation believes it will be extremely beneficial for CDR to utilise conformance test suites.

We strongly believe that CDR should at the very least promote and encourage the use of this conformance suite by all data holders. Ideally, we would recommend that all data holders are mandated to certify on a regular basis (at least every 12 months, and whenever any changes are made to authorization servers), in order to demonstrate that the standard has been implemented correctly and that the rights of customers and third parties are being enabled.

Consumer protection

Adopting FAPI Grant Management specification can assist with setting up a fine-grained authorization framework required for:

- Data minimisation, to only allow sharing the data required for a specific use case.
- Greater customer control and privacy.

A helping hand

The OpenID Foundation would like to offer help in interpreting the standards, and adapting the standards to fit your jurisdiction’s requirements.

By collaborating in this way, we can help ensure that one of your key objectives - global interoperability with other jurisdictions - is met.

Contact details: Don Thibeau, OIDF Executive director, don@oidf.org