


Consumer Data Right (Australia)

Consent Management

2020-02-27

FAPI WG



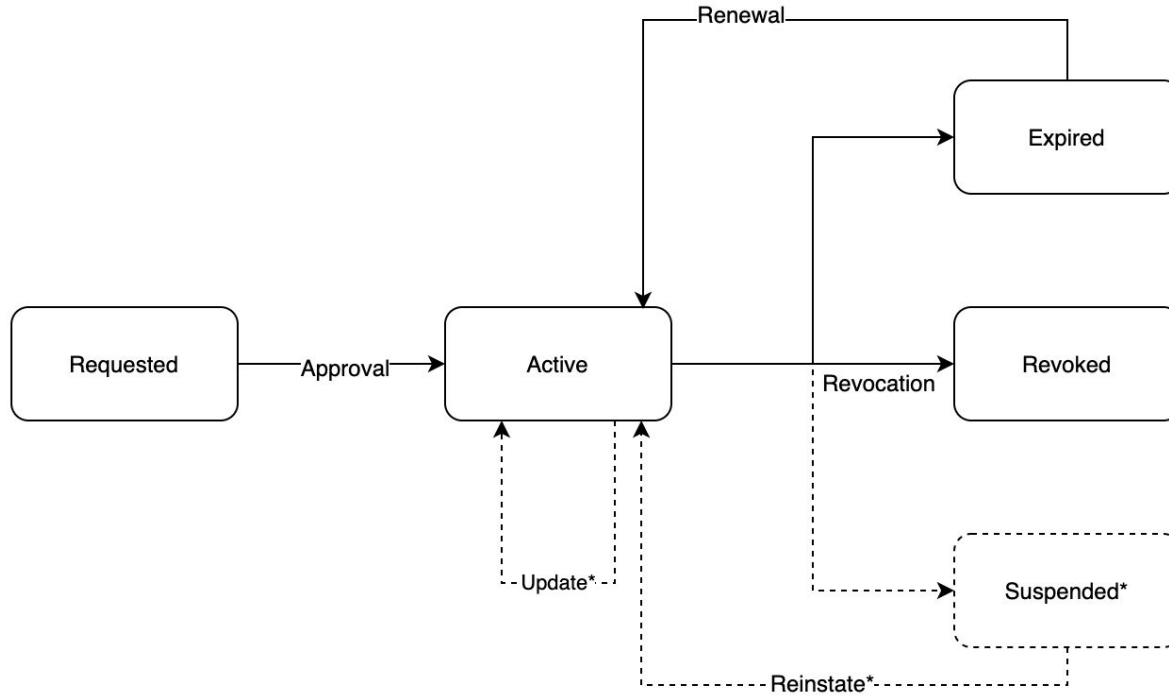


Consent principles (CDR)

- **Lawful**
"Before making a consumer data request on behalf of a CDR consumer, the consumer must first have consented to the accredited person collecting and using specified CDR data to provide the requested goods or services"¹
- **Fair**
"An accredited person must not seek to collect CDR data under the consumer data rules from a CDR participant for the CDR data unless [...] a CDR consumer for the CDR data has requested this by giving a valid request under the consumer data rules"¹
- **Transparent**
"An accredited person must provide an online service that [...] contains the details of each consent to collect and use CDR data given by the CDR"¹
- **Clearly communicated**
"An accredited person's processes for asking a CDR consumer to give consent [...] be as easy to understand as practicable, including by use of concise language"¹
- **Specific and relevant to purpose**
"Collection and use of CDR data under this Part is limited by the data minimisation principle, under which the accredited person [...] must not collect more data than is reasonably needed in order to provide the requested goods or services"¹

1. <https://www.legislation.gov.au/Details/F2020L00094>

Consent lifecycle



* if trust ecosystem requires these states and transitions

CDR Consent Current State



What it has?

- Sharing Duration abstracted but bound to token
- Single consent per user / client ID at a time
- Mixing Security and Business concerns.
Coupling of refresh token lifecycle to sharing arrangement lifecycle.
- Authorisation request transmitted via front channel
- Coarse grained scopes for “data clusters”

A nighttime photograph of a city skyline with several illuminated skyscrapers and a body of water in the foreground. The text 'CDR Consent Current State' is overlaid on the top left of the image.

CDR Consent Current State

What's missing?

- No support for concurrent consents with the same client (to support different purposes, expiry dates and partial data deletion).
- No support for fine-grained control (for example limited depth of transactions)
- No support for complex multi-party consents (for example, joint and business accounts)
- No support for delegated accounts
- No support for re-authorisation
- No visibility of consent status for data recipient (no consent API)
- No external consent identifier (no consent ID)
- No support for intermediaries
- Resource identifiers are not disclosed to Recipient during token issuance (e.g. customer or account identifiers)

Current State Consumer Impact



Poor Control

- Limited control over how much data is shared (coarse-grained permissions)
- Limited ability to change what data is shared (no Consent Identifier and Consent API)

Confusion

- Disconnect between additional context if required and what a Holder is being asked to disclose

Trust(!)

- Requirement to trust new entrants with more data raising Privacy and Security concerns
- Less likely to adopt new services as a result

Current State Holder Impact



Engagement

- Limited use case support resulting in lower uptake within the CDR ecosystem

Customer Safety

- Increased privacy and security concerns for customers
- Increased responsibility to ensure customers are informed about the risks

Current State Recipient Impact

A nighttime photograph of a city skyline reflected in water. The skyline includes several illuminated skyscrapers and a prominent bridge with blue lighting. The water in the foreground shows clear reflections of the city lights and the bridge.

Engagement

- Limited use case support resulting in lower uptake within the CDR ecosystem

Security(!) and Cost(!)

- Increased operational costs due to CDR specific security requirements
- Increased costs of implementing controls to handle different and potentially unnecessary data
- Increased technical complexity to redact data that is not required



Current State Government Impact

Risk (!)

- Holder concerns over inability for Consumers to maintain more explicit control over sharing of data may result in “brand risk” to Recipients and the wider ecosystem
- A Data Recipient breach event is more likely to have a higher impact as customers have shared access to more data than strictly required to service specified need

Adoption

- Limited use case support resulting in a less vibrant ecosystem

Solution approach and opportunities

A photograph of Uluru, a large sandstone rock formation in Australia, during sunset. The rock is illuminated with a warm orange and red glow, and the sky is a mix of dark blue and orange. The foreground shows some sparse, dry vegetation.

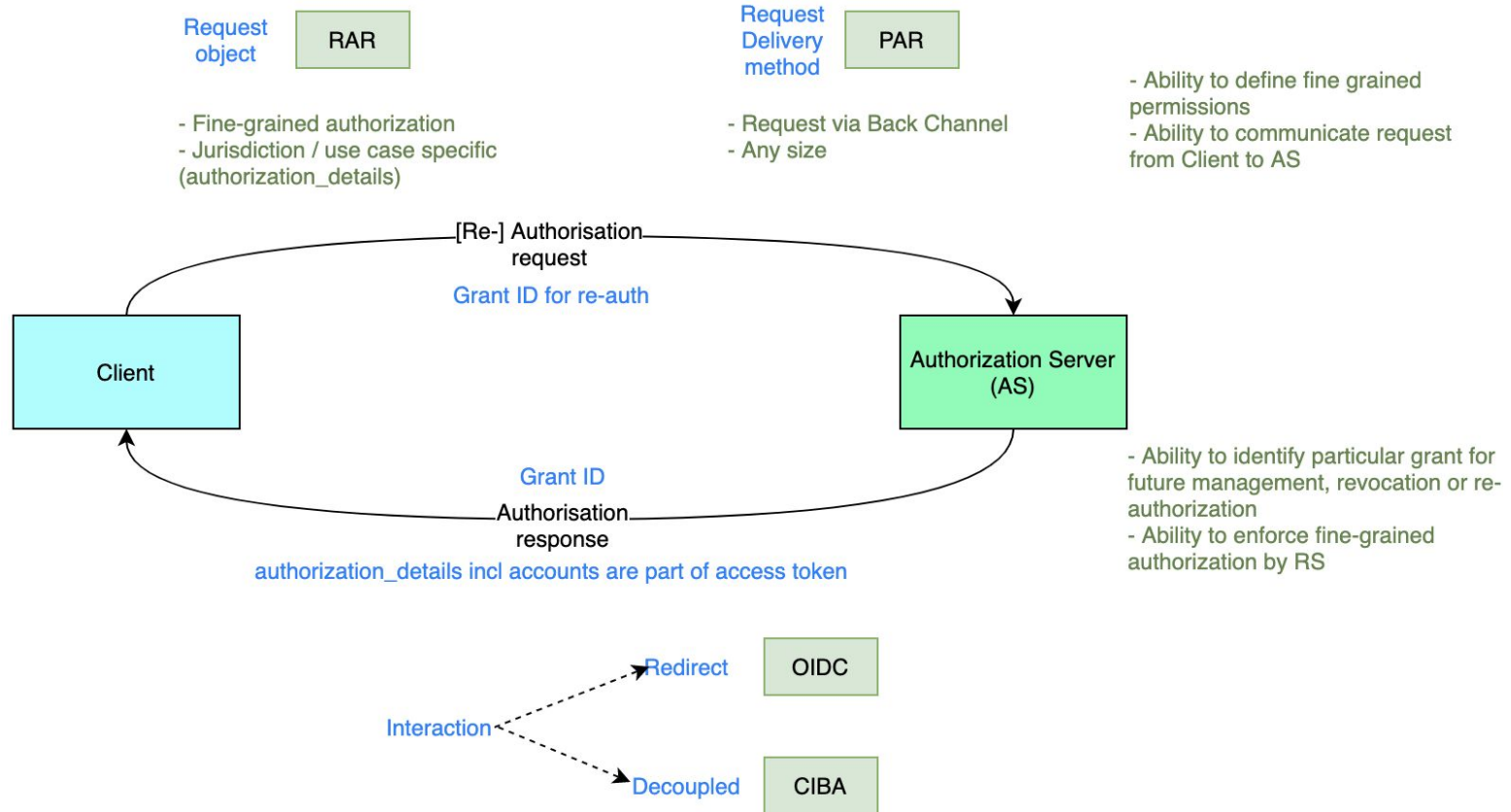
- Leverage Financial-grade API Working Group and OpenID Foundation's proven expertise in identity, security and consent
 - *Note: Other alternatives would likely result in a solution which is architecturally exclusive to the Australian market leading to limited technology choices for implementers*
- Collaborate in a workshop fashion to be a significant contributor to the next version of FAPI ("FAPI Evolution"). FAPI is a foundational industry standard for the current version of CDR Security profile.
- Expand the world leading CDR policy framework into technical domains with internationally adopted specification and standards
- Interoperability across jurisdictions with quality assurance and vendor support backed by OpenID Foundation's pioneering self certification process and software certification suite.

Australia has the opportunity to become a world leading technology reference case for worldwide open data initiatives

Main Specifications Used

Specification	Description	Outcome
PAR (Active WG item)	OAuth 2.0 Pushed Authorization Requests https://tools.ietf.org/html/draft-ietf-oauth-par-01 *Replacing and consolidating multiple & fragmented Lodging Intent pattern	Secure delivery of authorisation requests from data recipients to a data holder (any size, via back channel)
RAR (Active WG item)	OAuth 2.0 Rich Authorization Requests https://tools.ietf.org/html/draft-ietf-oauth-rar	Support for fine grain consent Support for complex authorisation requests allowing for jurisdiction and use case specific payloads
Grant Management APIs (New WG Item)	Emerging OAuth extension actively being worked on by FAPI WG members and designed around understood requirements of the Australian CDR	Support for consent state synchronisation between data recipients and data holders (required for complex joint and business consents) Consent revocation Support for concurrent consents , better support for dashboards
CIBA (Second Implementers Draft)	Financial-grade API: Client Initiated Backchannel Authentication Profile https://openid.net/specs/openid-financial-api-ciba-ID1.html	Support for “ <i>decoupled</i> ” authorisation and re-authorisation use cases (when user is not present, initiated by data recipient)

Consent authorisation + re-auth - Proposed



CDR Consent

Proposed State

Grant Management

High Level



Grant Management: the set of permissions confirmed by the Consumer of services or data for a certain Recipient

Objectives:

- Make grant (status) accessible and manageable by Recipients
- Support concurrent, independent grants (aka “consents”)

Proposal:

- Define OAuth extension to make **grants** (including all authorisation details) identifiable and manageable
- Allow Recipients to use independent grants for same Consumer

Consent Management - Proposed



CDR Consent

Proposed State



What it has based on Current State:

- Support for concurrent consents with the same client (to enable different purposes, expiry dates and partial data deletion).
- Support for fine-grained control
- Support for complex multi-party consents (joint and business accounts)
- Support for shared and delegated accounts
- Support for re-authorisation
- Visibility of consent status for data recipient
- External Consent identifier (“Grant ID”)
- Facility for future intermediary support
- Elevated security options (write APIs)
- Resource Identifiers disclosed as part of Consent
- Separation of Security and Business concerns.

Additional Value created:

- (Optional) Support for declared purpose of consent within rich authorisation
- Sharing Duration bound to Consent/Grant identifier
- Authorisation request transmitted via backchannel
- Internationally aligned rather than jurisdictionally proprietary
- Framework allows
 - Use case specific and jurisdiction specific payloads
 - AS to front grant management requests and pass business consent to an appropriate system for mastering.

Side by Side

Goal	Existing CDR (Single)	Proposed CDR (Existing Refresh Token)	Lodged Intent (UK OBIE)	FAPI WG Proposal
Concurrent Consent Support	✗	✓	✓	✓
Fine-Grained Consent	✗	✗	✓	✓
Multi-party Consent (Joint & Business Accounts)	✗	✗	✓	✓
Shared & Delegated Accounts	✗	✗	✓	✓
Re-authorisation Support	✗	✓	✓	✓
Consent status visibility for Data Recipients (RP/TPP)	✗	✗	✓	✓
Consent Identifier Support	✗	✗	✓	✓
Capability to support enveloped intermediaries	✗	✗	✗	✓
Elevated security options (write APIs)	✗	✗	✓	✓
Resource Identifiers disclosed as part of Consent	✗	✗	✓	✓
Separation of Security and Business concerns	✗	✗	✓	✓
Global Standard	✗	✗	✗	✓

Next Steps



- *Workshop with Industry Participants and FAPI WG to verify requirements and validate assumptions*
- *Collaborate with Government and Industry Participants to define CDR specific Rich Authorisation Request Payload*
- *Utilise International Subject Matter expertise to hone formal specification*
- *Leverage OIDF vendor members to deliver diverse software ecosystem*



Create the future together.

<https://openid.net/>
