WSO2 Open Banking
WSO2 Australia Pty Ltd., Level 13, 135 King Street, NSW 2000.
Tel: +61 2 8973 7550 | Email: bizdev@wso2.com

20 July 2020

CDR Rules Team
Australian Consumer and Competition Commission
Submitted via email to ACCC-CDR@accc.gov.au

WSO2 Submission on the CDR Rules Consultation (22 June 2020)

WSO2 welcomes the opportunity to submit our views on the draft rules to facilitate the participation of 'intermediaries' in the Consumer Data Right (CDR) regime.

We make these submissions, based on our experience of providing open banking technology to Data Holders in Australia and also in Europe, the UK, Singapore and several other countries, and based on our active participation in the Consumer Data Standards Data Holder Working Group facilitated by Data61.

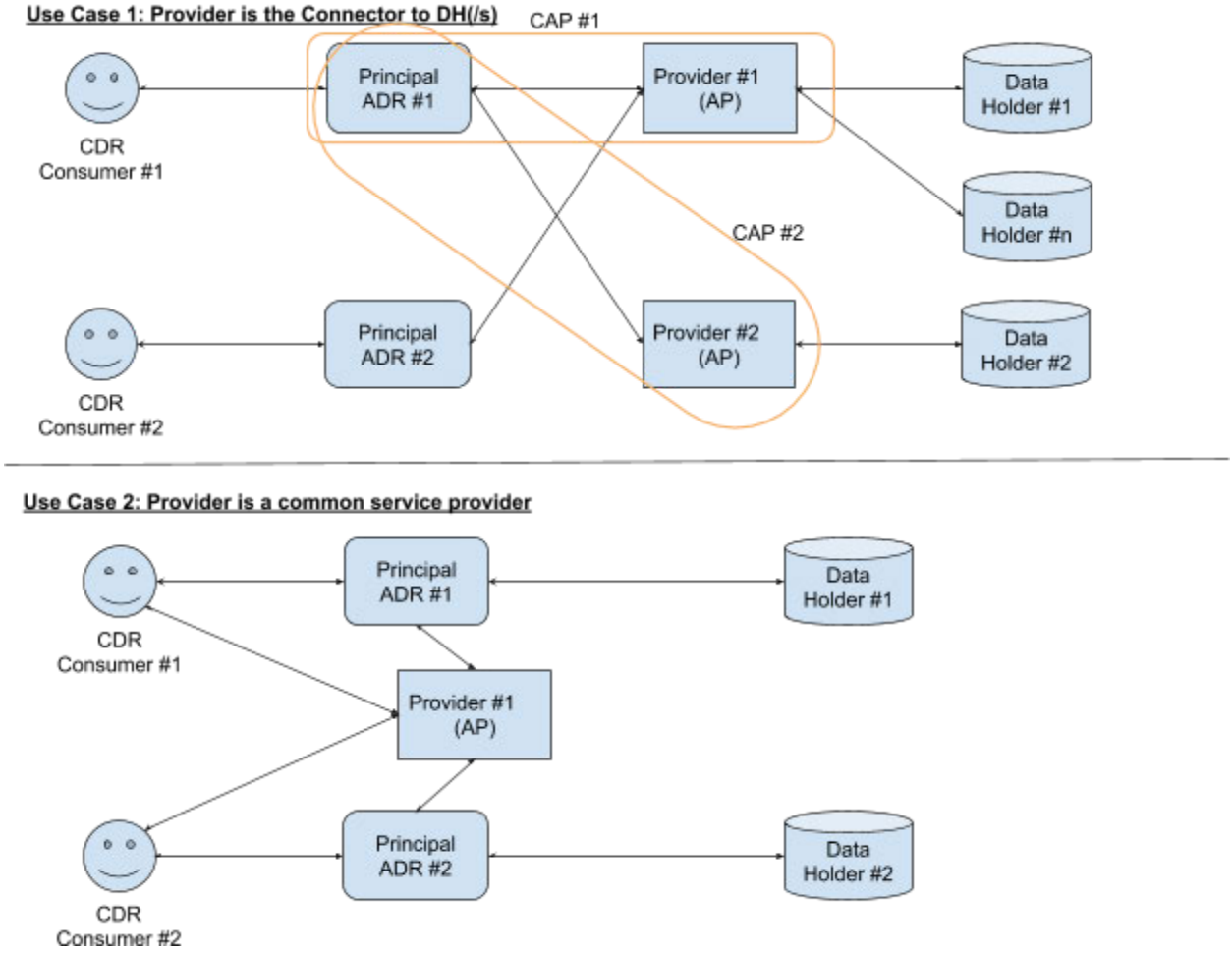
Our submissions focus on certain technical aspects arising from the draft rules and are set out below.

Overview of use cases

Based on the details published for Combined Accredited Person (CAP) arrangements we have identified 2 main use cases.

- Use Case 1: where the Provider acts as a hub to maintain communication with the Data Holder.

- Use Case 2: where the Provider provides certain ancillary services such as dashboard services or data analysis services.



Implications for DCR

Based on the above use cases there could be different approaches to facilitate the Dynamic Client Registration (DCR) flow.

- Use case 1 depicts a solution which is quite similar to the approach taken by open banking in Europe to implement the “on-behalf” functionality.
- In use case 1, if the Principal always relies on the Provider to maintain the interaction with the Data Holder, our recommendation would be to allow only the Provider to on board with the Data Holder (via the DCR flow.)
- This would allow Providers to send relevant requests on behalf of the Principal as and when required.

- In this scenario data requests would be required to contain additional claims and security policies in authorization requests in order to:
    - Perform the relevant validations against the Provider (to validate whether the Provider is authorized to make requests for the Principal and the Principal is actively involved in the initiated data request.)
    - Display the Principal's details in the consent authorization flows and the Data Holder's dashboard (post-authorization) for the relevant CDR Consumer.
- Validation of the Principal in the scope of accreditation validity and software assertions validity should be handled by the Provider, as it would be the main party that interacts with the Principal. Hence if data requests initiated from a Principal who violates one of the above should be rejected by the Provider.
- Additionally, the CDR Register could be used as the medium to identify the association between Provider and the Principal.
- Accordingly, responses for relevant data requests would flow through the Provider and it would also include any notifications to be indicated to the CDR Consumer (e.g., notifications on consent revocation from the Data Holder dashboard, incorrect data sharing notification containing a request to correct the data.)
- If both parties (Principal and Provider) are to be registered with the Data Holder, it would complicate the CDR technology implementation of the Data Holder and would introduce inefficiencies for user workflows.

Additional observations

We would also like to raise the following queries, answers to which may be important in establishing an effective framework for the participation of intermediaries in the CDR:

- What would the mechanism be if a Data Recipient connecting directly with a Data Holder outside of a CAP arrangement opted to move to a CAP arrangement, and vice versa? How would this transition impact CDR Consumer interactions in terms of perceptions of trust, privacy and reliability?
- If a Principal has decided to switch to a different Provider, how should the consents be managed and how would the CX be managed for consent transfers?
- Would a mechanism be added for Data Holders to know the Principal data recipient in an authorization request?

    - This will help in displaying this information in the Data Holder's CDR Consumer dashboard. This should be applicable only if the Provider is retrieving CDR data on behalf of the Principal.
    - Also, if the Principal is retrieving the data (where a CAP arrangement is set up for a CDR Consumer dashboard service), does the Data Holder mention the Provider in the Data Holder dashboard?
- When performing metadata validations for Data Recipients, is it sufficient to validate only the Provider, or should both Principal and Provider be validated?
- What would be the impact if the accreditation of a Provider is terminated? Should all consents initiated from the Provider (of multiple Principals) be revoked or disabled?

We hope our submissions above would be useful in shaping the rules to best facilitate the participation of intermediaries in the CDR, and we look forward to participating in the proposed workshop in this regard in the near future.

Thank You,

Sincerely,

Selvaratnam Uthaiyashankar
Senior Vice President - Engineering
Acting Head of the Open Banking Business Unit