Australian Banking Association

DP-245 – Enhancing Data Recipient Accreditation Negotiation

The Australian Banking Association (ABA) welcomes the opportunity to provide comment to the Data Standards Body (DSB) decision paper proposal number 245. We provide answers to the raised questions below:

Responses

1. **What additional information will the CDR Register require to convey the trust of different types of Data Recipients in the ecosystem?**

As the ecosystem evolves, a finer grained accreditation model would allow for greater access to the CDR by lowering the technical barriers to entry, thereby providing ADRs with the opportunity to seek accreditation for only those actions (be they read or write) that they intend to perform. It would also allow for enhanced security requirements for actions that carry greater risks. This will be an important requirement for the introduction of 'action initiation' functionality in the CDR.

However, based on the information we have, the ABA believes that the current model and use of OAuth authorisation scopes to represent accreditation status is sufficient to accommodate additional functionality and additional industries.

If DSB thinks that the current model is not sufficient, we suggest that the future consultation process on the introduction of action initiation is the preferable forum to address these questions. We also note that any such changes are likely to require significant implementation effort, and as such it is crucial that sufficient lead times are provided for both the consultation and the implementation process.

2. **How can bilateral trust and accreditation be issued by Data Holders to individual Data Recipients?**

Bilateral trust has the potential to be able to allow greater levels of innovation through the introduction of use cases beyond the current CDR scope, whilst leveraging the existing CDR ecosystem.

However, in order to successfully put in place a solution that would allow such arrangements to be confidently and securely managed, there would be a large effort required to define the most appropriate way to manage such relationships within the CDR guidelines. Consequently, the ABA submits that the review and implementation of an approach to establishing bilateral trust should not be prioritised at this time.

In our view, establishing bilateral trust would likely require a significant amount of effort on the Register side. Given the large volume of activity underway in the ecosystem, it would be considered preferable at this point in time to prioritise existing work in the Register space. For example, the introduction of an unauthenticated get Data Recipients API, as raised in Add an unauthenticated GetDataHolderBrands endpoint exposed as a public API · Issue #444 · ConsumerDataStandardsAustralia/standards-maintenance (github.com) which has the potential to lower the barrier of entry to non-accredited participants, allowing them to more easily access the data they require without having to source it through means other than the CDR ecosystem.

In addition, Decision Proposal 229 - CDR Participant Representation · Issue #229 · ConsumerDataStandardsAustralia/standards (github.com) (currently a placeholder) and Decision Proposal 225 - Data Recipient Security Standards · Issue #225 · ConsumerDataStandardsAustralia/standards (github.com) (currently pending decision) both seek to address known issues already impacting the ecosystem with relation to the different arrangements that can exist between ADRs and third parties, such as sponsorship, trusted advisors and insights, and how these are represented to the end consumer, and managed from a security perspective.

We would like to note that when the issue of introducing bilateral trust arrangements is addressed at a future date, any solution proposed and its associated implementation effort should be optional for parties wishing to enter into these arrangements, and not impose undue burden on parties not wishing to enter into such arrangements.

3. What additional capability should be investigated to address current OAuth authorisation scope negotiation limitations?

In order to implement any payment initiation, consent must be uplifted to fine-grained consent by using FAPI 2 framework specifications like RAR and Grant management specifications. For more details please see ABA paper published last year.[1] This is consistent with CDR's proposed adoption of the FAPI 2 framework and makes our ecosystem more interoperable, secure and privacy-preserving.

In order to design CDR specific consent / grant payload, we suggest to use the future consultation process related to the introduction of action initiation.

4. What additional Accredited Data Recipient and associated Software Product lifecycle information should be available from the CDR Register

The ABA has previously raised the issue of Data Holders not having visibility of ADRs entering the ecosystem until they are activated, and the challenges this brings with regard to whitelisting for security purposes in CDR Data Holders outbound connection whitelisting · Issue #418 · ConsumerDataStandardsAustralia/standards-maintenance (github.com). Accordingly, the ABA would strongly support this limitation being addressed, and would refer to the solution options outlined in the paper attached to Issue 418. The preferred solution option is option 2, 'Make the domain/URIs available in the register API', which aligns with the pre-activation step being proposed in DP-245. In order to ensure that whitelisting can be successfully performed prior to Dynamic Client Registration, the full FQDN of the URI would be required, and it would be of optimal benefit for ADRs to enter the pre-active state as early as possible.

[1] See ABA paper published here: Decision Proposal 182 - InfoSec Uplift for Write · Issue #182 · ConsumerDataStandardsAustralia/standards (github.com)