Data Standards Body

Technical Working Group

Decision Proposal 245

Enhancing Data Recipient Accreditation Negotiation

Contact: Ivan Hosgood, Mark Verstege

Publish Date: 31st March 2022

Context

Discussion with industry throughout Maintenance Iteration #10 has highlighted the current Client Registration and Software Statement Assertion (SSA) models doesn't provide sufficient flexibility with the management of OAuth authorisation scopes as the CDR expands to multiple industry sectors. Limitations in this flexibility extends beyond OAuth authorisation scopes and should also consider how Data Recipient accreditation information is negotiated between Data Recipients, Data Holders, and the CDR Register.

Currently, Data Recipients are issued an accreditation status by the Registrar during their onboarding into the CDR. The lifecycle of the accreditation status is represented by a high-level accreditation for the Data Recipient entity as well as individual accreditation statuses for each of the Data Recipient's Software Products. This model is documented in the Participant Statuses section and supports movement between an active and inactive state as well as a removed state. Whilst this caters for many situations, it has limitations with emerging requirements including any pre-activation status to enable Data Holders to discover and prepare for new Data Recipients (e.g., whitelist Data Recipient Software Product domains); similarly, it does not cater for temporary offline status or suspended status (e.g., in the advent of a critical incident or trading halt).

When a Data Recipient is activated, it is accredited to a whole-of-economy level. This means that once a Data Recipient is accredited, they may collect data for all sectors designated within the CDR. This is facilitated through the assignment of OAuth authorisation scopes. At a coarse-grained level this represents high level data clusters for data sharing where OAuth authorisation scopes (technical) act as a proxy for accreditation (business). Whilst this worked for obligated data sharing, it has limitations when expanding to fine-grained accreditation, per-sector accreditation, write access action accreditation and extensible APIs where bilateral trust between a single Data Holder and Data Recipient is commercially agreed.

The future state of how Data Recipient accreditation is negotiated in the Consumer Data Right ecosystem needs to be assessed against current limitations and future requirements. This proposal raises the following questions to help consider the requirements and mechanisms for Data Recipient accreditation negotiation.

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

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

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

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

Decision To Be Made

Identify the requirements and mechanisms that should be considered to define the future state of Data Recipient accreditation negotiation between Data Recipient Software Products, Data Holder Brands, and the CDR Register.

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

In addition to Banking and Energy, the CDR is expanding to include the Telecommunications and Open Finance (non-bank lenders, superannuation, and general insurance) sectors. Additionally, the CDR is evolving from a data sharing ecosystem to action initiation where operations can be performed against a Data Holder, including making payments, rolling over term deposits, originating new accounts, managing customer contact details, and switching accounts.

As at 28/03/2022 all Accredited Data Recipients who align to the Consumer Data Standards information security profile are accredited at the unrestricted level. Software Statement Assertions (SSA) are currently used to convey this level of accreditation by defining a set of OAuth authorisation scopes assigned to their Software Products. However, currently all OAuth authorisation scopes are assigned to all Software Products.

The SSA design allows for subsets of OAuth authorisation scopes to be used to represent categories of accreditation. There are limitations as OAuth authorisation scopes are appropriate to describe high levels of authorisation but are unwieldly as the information required to convey authorisation increases in complexity.

Therefore, a model of accreditation that only maps to OAuth authorisation scopes may prove insufficient in the long term if certain actions require additional accreditation requirements (e.g., making domestic or international payments).

It may also benefit Data Recipients to request limited accreditation to lower technical complexity, insurance costs and liability risk.

Use cases may not require all data or actions within a sector. For example, a personal information management (PIM) application may only seek accreditation to read and manage contact details, not banking transactions or energy usage. Therefore, restricted accreditation can be aligned to purpose, further limiting data sharing risk, whilst testing can be strongly aligned to accreditation status. Changes of accreditation can in future be tied to successful conformance testing.

For this variety of reasons, the CDR Register may want to have control categorising Data Recipients.

Design Questions:

a) Are OAuth authorisation scopes a resilient way of representing accreditation status, or should a different approach be considered?
   For example, accreditation by business classifications could categorise accreditation by purpose or a fine-grained accreditation model (e.g., accredited for making domestic payments but not international payments; accredited for managing accounts within a Data Holder but not making external payments or switching accounts)
b) What metadata is necessary to establish trust between a Data Recipient Software Product and the Data Holder?
c) Is a finer grained accreditation model required? Examples include accreditation by consumer class (e.g., for retail energy customers but not corporate and institutional customers); product category (e.g., term deposit accounts but not credit cards); or action (e.g., accredited for data sharing but not account opening or account management).
d) Should accreditation models support limiting accreditation to single sectors or data clusters?
e) Should expanded accreditation be tied to successful execution of conformance testing?

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

The Consumer Data Standards caters for API extensibility. This enables Data Holders to leverage the CDR infrastructure to provide commercial extensions to the core set of CDR APIs and offer competitive API-enabled service offerings. For example, a Data Holder may offer large accounting ADRs bulk transaction APIs, first-to-market payments APIs or value-add APIs.

Currently accreditation status is assigned solely by the CDR Register as a static list of OAuth authorisation scopes, making bilateral commercial extensions difficult. Either the CDR Register must expand its capabilities to allow for non-CDR OAuth authorisation scopes to be issued or a way for Data Holders to issue their own bilateral accreditation metadata to Data Recipients.

Since the CDR Register issues OAuth authorisation scopes to Data Recipient in a Data Holder agnostic format, it would mean that if commercial OAuth authorisation scopes were included, then all Data Holders would see all bilaterally assigned commercial scopes. Also, there is the consideration how bilateral accreditation may be facilitated without causing clashes across Data Holders (e.g., non-colliding namespaces).

Design Questions:

a) What metadata is required for the successful negotiation of commercial Data Holder specific accreditation?
b) Should the CDR Register allow Data Holders to self-service assignment of extensible accreditation metadata to specific ADRs?
c) Should the CDR Register issued SSAs be extended to cater for commercial extensibility, maintaining the CDR Register as the trust line between the Data Recipient Software Products and Data Holder Brands)?
d) If not, what other mechanisms for bilateral accreditation other than SSAs and Dynamic Client Registration should be considered?

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

The current negotiation of OAuth authorisation scopes relies on the Client Registration mechanism to exchange OAuth authorisation scopes.

This has three parts:

1. A Data Holder Brand advertises which scopes are supported through the OpenID Provider Configuration End Point **scopes_supported** value.
2. The Data Recipient requests an SSA be issued by the CDR Register with all allowable OAuth authorisation scopes assigned
3. The Data Recipient presents the SSA to the Data Holder Brand via the Registration Endpoint and a client registration is created by the Data Holder Brand, including the authorisation scopes which intersect the **scopes_supported** and CDR Register assigned scopes.

There are some limitations with this approach:

1. The Registration Request using JWT payload does not allow for subsets of OAuth authorisation scopes to be specified
2. The CDR Register does not have a technical control to force registrations to reduce OAuth authorisation scopes. Registration updates are driven by Data Recipients which is beneficial as they can manage the rollout of changes to the registrations of their software products, however, it limits the ability for the CDR Register to constrain the OAuth authorisation scopes specified per Software Product.
3. Data Holder extensible OAuth authorisation scopes cannot currently be added to an SSA
4. The Data Recipient has no ability to assign a subset of OAuth authorisation scopes to a Software Product
5. The Data Recipient has no ability to register Software Products with different OAuth authorisation scopes to different Data Holder Brands
6. The Data Recipient has no ability to leverage extended OAuth authorisation scopes from specific Data Holders

Design Questions:

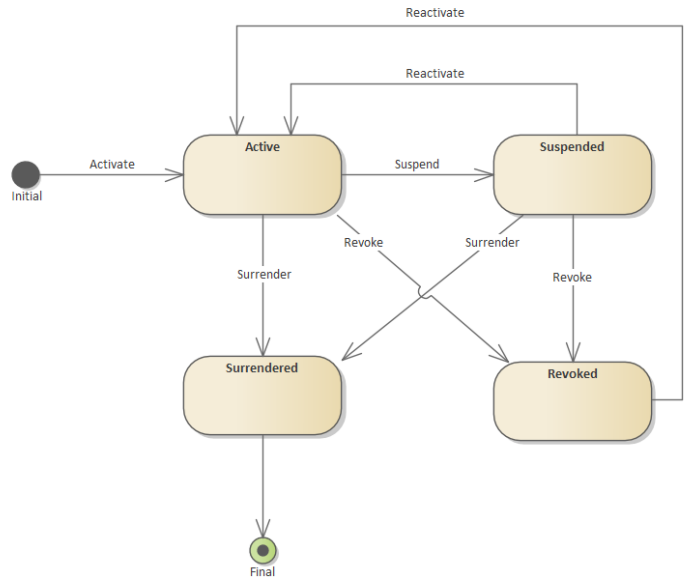
a) What other limitations or known constraints does the current model have?

b) Which of these limitations should the Standards seek to address?
c) How should the current mechanisms be enhanced to address these limitations, and/or;
d) Should other mechanisms be considered?

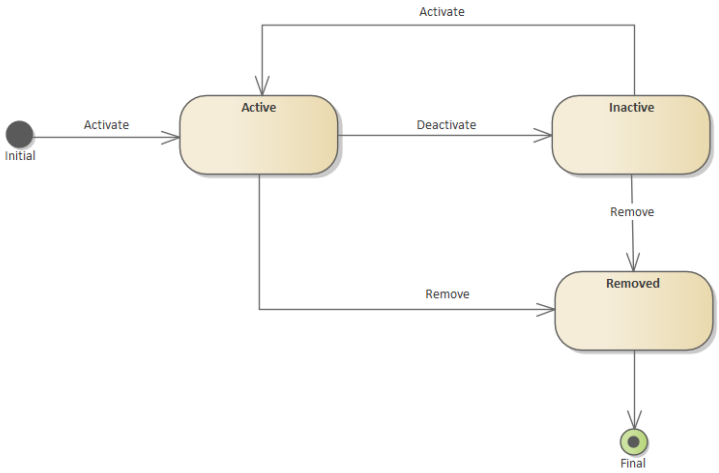
4. What additional Accredited Data Recipient and associated Software Product lifecycle information should be available from the CDR Register?

The current states of Accredited Data Recipients and Software Products are documented in the Participant Statuses section of the Consumer Data Standards. This documentation has been extracted as follows:

Data Recipient Status



Software Product Status



The current model only allows Data Holders to retrieve Accredited Data Recipient / Software Product information from the CDR Register APIs once these entities have entered the initial state of active.

This limitation prevents Data Holders from having visibility into Data Recipient and associated Software Product information outside of the activation process.

Potential limitations which can be considered are:

1. Data Holders are not able to anticipate Data Recipients entering the ecosystem until they are activated. Is there motivation for having a pre-activation step so this information becomes visible allowing for activities such as white-labelling of Software Product domains?

2. There is no mechanism for the CDR Register to temporarily deactivate a Software Product outside of the Data Recipient suspension use case. Consideration should be made to determine if there is a need to deactivate Software Products on a temporary basis, (e.g., to cater for scenarios such as a critical incident or trading halt) and what the associated obligations will be on Data Holders.

Design Questions:

a) Is this list of limitations complete?
b) Which of these limitations should the Standards seek to address?

Next steps

Based on the feedback provided on this Decision Proposal the Data Standards Body will either:

- formulate a position for further consultation(s);
  or
- accept the current limitations are an adequate state for the ecosystem to operate and make explicit binding statements in the Standards.