Data Standards Body
API Standards Technical Working Group

Noting Paper – White Label Conventions

Publish Date: 3rd March 2021

Context

The CDR standards have been designed for data sharing under a direct brand scenario (where the data holder is also the brand owner for the services offered), but it has also been designed to accommodate white label scenarios.

A white label scenario occurs where one entity (a white labeller), provides products and services which are then branded and retailed to consumers by another entity (a brand owner). These scenarios occur in many industry sectors and the standards provide a sector agnostic approach to managing these scenarios as much as possible.

For the banking sector, there are many different white label scenarios in place and it is not always obvious to data holders how they should implement the standards for their specific context. This noting paper is intended to provide guidance for these data holders and will be converted to a CDR Support Portal convention article in due course.

Additional notes regarding white labelling:
- This document has been developed in alignment with the guidance provided by the CDR rules team on white labelling. This guidance can be found at the links below:
    - [Approach to disclosure of product data: white label products](#)
    - [Approach to disclosure of consumer data: white label products](#)
- This guidance is designed to give implementation certainty for the majority of white label scenarios. The DSB will be hosting a workshop in early April to work with data holders that have arrangements that they do not believe fit within the scenarios presented in this noting paper.
- This paper will not cover options and processes for configuring products in the CDR Register, only the configuration of aspects of the CDR regime governed by the standards such as payloads, metrics and base URIs.

Guidance for the different white label scenarios

The section outlines a series of generic white label scenarios and provides specific conventions for each of them.

Scenario 1: Secondary Master Brand

Description
A single designated data holder has a second master brand that is perceived by consumers as being a separate entity. Examples of this in the banking sector would include a major bank with a second bank operating under their ADI license.

Commentary
Although not specifically a white labelling arrangement, banks which have subsidiary brands in the market may in some situations operate in a similar fashion to white label arrangements for part of their service and product offering. In this context specific guidance may remove ambiguity for implementation teams developing CDR compliant solutions.

Guidance
As each brand is separately known to consumers in the market, these secondary brands should be configuired in the register such that data recipients are able to present the brand as a distinct data holder when they are asked to share their data.

As far as the ADR and the consumer is concerned the second brand would appear and act as an independent data holder for the purposes of data sharing under the CDR

This mean that
- The secondary brand would have independent base URIs that are not shared with another brand for all of the configurable base URIs
- Product reference data should be exposed under an indendent base URI and should not be combined with any other brand using the product reference data brand feature as this is intended only for sub-brands or a master brand.
- Metrics should be recorded and reported separately for this brand using the metrics end point.
- Outages and status should be reported separately for this brand using the common end points for this purpose.
- IDs under the ID permanence rules, subject identifiers and client IDs provided via dynamic client registration should not be shared between this brand and another brand.

Scenario 2: Distribution only brand

Description
A designated data holder sells a product that is separately branded or co-branded with another organisation but the data holder services the products and the consumer sees it as another product

in their portfolio with the data holder. They do not see this as a product as being provided by a separate organisation.

Commentary

This is the simplest white label scenario. Some examples of how this scenario exists in the banking sector are:
- where a bank offers a co-branded mortgage or credit card but the resulting relationship is directly with the bank. The consumer understands that this branding is for sales purposes only but all authentication and servicing is performed by the bank
- where banks will sometimes create industry specific product lines, such as agribusiness or small business, and these product lines are facilitated via a distribution partnership
- where a bank has previously purchased, or invested in, a brokerage firm and brands certain products using that firm's brand

Guidance

In this scenario the product should be treated as a part of the portfolio of the data holder and should be accessible in that context.

This mean that
- There would be no separate register entry or independent base URIs expected.
- Product reference data should be exposed alongside the other products of the data holder. The product reference data brand feature may be used to differentiate these products at the discretion of the data holder.

Scenario 3: Full service white label brand

Description

A designated data holder provides the capability for a range of products that are sold and serviced under a separate brand owned by a non-designated organisation.

Commentary

For the banking sector this scenario was directly addressed in the guidance from the ACCC. One of the key issues with this scenario is how compliance obligations should be interpreted, which is addressed in the ACCC guidance. An example of this scenario would be where a supermarket offers a financial product under their own brand but the provision of service and the maintenance of the product are all provided by an underlying ADI. From a standards perspective, however, this scenario is essentially identical to Scenario 1. Consumers and ADRs would interact with the brand as if it was an independent data holder.

Guidance

The technical guidance for this scenario is essentially the same as for secondary brands (ie. Scenario 1). As each brand is separately known to consumers in the market, these secondary brands should be configured in the register such that data recipients are able to present the brand as a distinct data holder when they are asked to share their data.

This mean that
- The white label brand would have independent base URIs that are not shared with another brand for all of the configurable base URIs
- Product reference data should be exposed under an indendent base URI and should not be combined with any other brand using the product reference data brand feature as this is intended only for sub-brands or a master brand.
- Metrics should be recorded and reported separately for this brand using the metrics end point.
- Outages and status should be reported separately for this brand using the common end points for this purpose.
- IDs under the ID permanence rules, subject identifiers and client IDs provided via dynamic client registration should not be shared between this brand and another brand.

Scenario 4: Portfolio extension

Description
A designated data holder offers a series of products but extends their portfolio with a product white labelled by a different designated data holder. The white label product is seen to be part of the customer's portfolio with the brand owner and a single authentication is used to service both the directly offered products and the white labelled products.

Commentary
This a common scenario in the banking industry. A common example is where an ADI offers a series of lending and transaction products but will white label a credit card product in partnership with another ADI. This scenario is also common in other industries and will become more prevalent as more sectors are designated. For example, it is conceivable that a data holder in energy may offer white label products in telecommunication. This scenario may end up being applicable if both sectors were to be designated.

Guidance
The ACCC has provided guidance on how obligations should be managed for this scenario and this will not be addressed further in this document.

From a standards perspective, as a single consumer identity is used for both the direct and white label products, it would be expected that the white label arrangement would not be exposed either to the consumer or the ADR from a technical perspective.

This mean that
- There would be no separate register entry or independent base URIs.
- Product reference data should be exposed alongside the other products of the data holder. The product reference data brand feature may be used to differentiate these products at the discretion of the data holder.
- The white labelled product would be treated the same as other products offered by the brand owner during authorisation, joint account management and in the sharing of data.
- It would be expected that the brand owner data holder would act as the authorisation server and would augment endpoint responses involving the white labelled product with

data obtained from the white labeller data holder. The mechanisms for doing this augmentation of payloads is left to the discretion of the two parties.
- Metrics, status and outages would be reported at the brand owner brand level.

Scenario 5: Portfolio extension with separate authentication

Description

This scenario is a minor variation on Scenario 4. Both the brand owner and the white labeller are designated data holders and the brand owner also offers other products directly. The variation is that, instead of both direct and white label products being serviced under a single user identity a separate servicing facility, that the consumer is aware of, exists and they use different credentials to access this facility.

Commentary

This is a more nuanced and complex scenario and can vary depending on the way two separate avenues for servicing are presented. The brand owner may provide the consumer with two completely separate digital experiences with different entry points or they may keep the user experience similar but offer different login screens when the customer comes to a unified landing page to access their accounts.

Guidance

As there is more variation in this scenario there are two separate options for this scenario to be handled in the standards:

Option 1

The guidance for Scenario 4 is adopted but, within the constraints of the CDR federation statements in the standards, the customer is asked which identity they wish to share from prior to the authentication step of the consent authorisation flow. The path they select will determine which authentication is used and which accounts are available to be shared. Only one brand exists in the Register under this option.

Option 2

The two different facilities are considered master brands and have their own independent entries in the CDR Register. Whether the technical implementation for the white labelled brand is managed by the brand owner (aligned to Scenario 3) or by the white labeller (aligned to Scenario 1) is a decision to be determined by the two parties.

Conclusion

This paper considered some of the most common white labelling arrangements. Whilst other white label arrangements may exist, no additional data standards are required to support the common scenarios presented within this paper. It is hoped that this will provide greater clarity for implementation teams.

Integrations between data holders (brand owner and white labeller) are left to the competitive space as much as possible to support existing commercial contracts and existing investment in software integration can be leveraged or extended.

If further clarification is required queries can be raised via the CDR Support Portal or posed in the planned workshop to be organised in early April 2021.