Australian Government

Consumer Data Right

Participant on-boarding guide

Version 1.4

April 2023

Table of Contents

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have a specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy with the ACCC prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Such queries should be addressed to ACCC-CDR@accc.gov.au.

Guidance Revision History

Version 1.4 of this Guide, published in April 2023, includes the following changes that have been made since the Guide was last published in June 2021:

- References section: updated link to the Certificate Management information
- References section: updated link to Certificate agreements and policy documents
- Section 6.3: removed acronym in Table 2
- Section 7.3: reference to screenshot in Appendix E removed and replaced with link to Participant Portal Guide
- Section 7.4: updated values in Table 5
- Section 7.8: updated values in Table 6
- Appendix E: screenshots of the CTS certificate section of the Participant Portal removed
- Throughout Guide: updated email address to contact the On-boarding team

References

Table 1: References

#	Title	Location
R1.	On-boarding frequently asked questions (FAQs)	https://cdr-support.zendesk.com/hc/en-us/sections/900000436843-On-boarding
R2.	CDR Support Portal	https://cdr-support.zendesk.com/hc/en-us
R3.	CDR implementation call	https://github.com/ConsumerDataStandardsAustralia/standards/wiki/Meetings#consumer-data-right-implementation-call
R4.	Submission questions for CDR implementation call	https://cdr-support.zendesk.com/hc/en-us/requests/new
R5.	CDR website	https://www.cdr.gov.au/
R6.	Certificate agreements and policy documents	https://www.cdr.gov.au/resources/agreements/digital-certificate-agreements
R7.	Certificate Validation	https://cdr-support.zendesk.com/hc/en-us/articles/900005826963-Certificate-Validation
R8.	CDR Trade Mark Licence Agreement	https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-trade-mark-licence-agreement
R9.	Consumer Experience (CX) Standards and Guidelines	https://consumerdatastandardsaustralia.github.io/standards/#consumer-experience
R10.	Certificate Signing Request (CSR)	https://www.digicert.com/kb/csr-creation.htm
R11.	Conformance Test Suite (CTS) guidance material	https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-conformance-test-suite
R12.	Consumer Data Right (CDR) Participant Portal User Guide	https://www.cdr.gov.au/resources/user-guides/cdr-participant-portal-user-guide
R13.	Consumer Data Standards	https://consumerdatastandardsaustralia.github.io/standards/#introduction
R14.	CDR Register Design	https://cdr-register.github.io/register
R15.	CDR - Become an accredited data recipient	https://www.cdr.gov.au/for-providers/become-accredited-data-recipient
R16.	Competition and Consumer (Consumer Data Right) Rules 2020	https://www.legislation.gov.au/Series/F2020L00094
R17.	CDR Participant Portal	https://portal.cdr.gov.au
R18.	Register Design - Certificate Management	https://consumerdatastandardsaustralia.github.io/standards/#certificate-management

1. What is on-boarding?

1.1 Overview

On-boarding is the process of a participant new to the Consumer Data Right (CDR) ecosystem (the ecosystem) preparing to commence active participation. The goal of the on-boarding process is to confidently introduce data holders (DHs) and Accredited Persons who may receive data (data recipients or DRs), into the ecosystem. In this guide we refer to **participants** to cover both DHs and DRs.

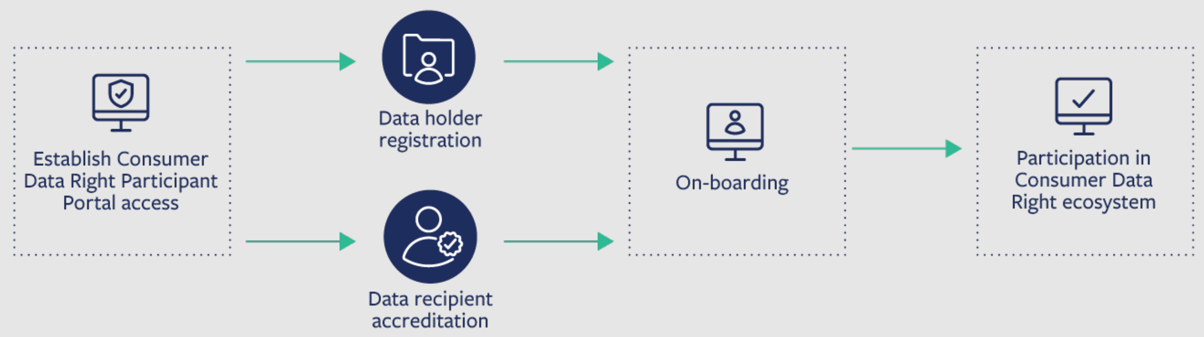
A more detailed overview of the on-boarding process can be found in the *On-boarding process* section of this document. Moreover, this guide will provide information for participants on technical, legal and testing requirements, and outlines the steps to be completed before the participant can be activated on the CDR Register (the Register).

The on-boarding process outlined in this document does not apply to existing DHs who wish to on-board an additional brand. DHs in this situation should email the ACCC for guidance at CDROnboarding@accc.gov.au.

1.2 Context

The on-boarding process occurs after registration (for DHs) and accreditation (for ADRs) activities have successfully completed. DHs and DRs must be on-boarded before they are able to participate in the production ecosystem, as depicted in Figure 1.

Figure 1: On-boarding context


Establish Consumer Data Right Participant Portal access
Data holder registration
Data recipient accreditation
On-boarding
Participation in Consumer Data Right ecosystem

1.3 Role of the CDR Registrar

The on-boarding process is managed by the ACCC acting as the CDR Registrar (the Registrar). The ACCC's role is to maintain the security, integrity and stability of the Register. It can issue requests to DRs and DHs to provide information or to do particular things so that it can fulfil its functions. It must publish certain information about DRs and DHs and it may include in the Register other information that it considers is required in order for DRs and DHs to process requests in accordance with the CDR Rules (the Rules) and Consumer Data Standards (the Standards).

1.4 Registering as a data holder

As per section 56AJ of the *Competition and Consumer Act 2010* and the Rules, if you are obligated to become a DH and are in a position to commence on-boarding, you should initiate the DH registration process via the CDR Participant Portal [R17] (the Participant Portal). Please refer to the CDR Participant Portal user guide [R12] for guidance on this step. Note that you will have to request access to the Participant Portal before you can register as a DH.

1.5 Seeking accreditation as a data recipient

Consult the website for more information about becoming an accredited data recipient (also referred to DR) [R15].

2 Getting help

The key resources available to support participants through the on-boarding process (also in *On-boarding process* section of this document) and their commencement in the ecosystem are outlined below. The links to the resources can be found in Table 1.

On-boarding FAQs

FAQs [R1] have been prepared to address questions about the on-boarding process for the ecosystem.

CDR Support Portal

The CDR Support Portal (the Support Portal) [R2] is maintained by both the Australian Competition and Consumer Commission (ACCC) and the Data Standards Body (DSB). It provides information to participants on the Rules, the Standards, the Register, the accreditation and registration process, on-boarding and activation in the ecosystem, and ongoing reporting and compliance obligations. The On-boarding FAQs are contained on the Support Portal.

You can also use the Support Portal to raise general questions about on-boarding.

CDR website

The public facing CDR website (the website) [R5] provides prospective participants with general information on the process of getting on-boarded to the ecosystem.

CDR implementation call

The CDR implementation call [R3], co-facilitated by the ACCC and the DSB, takes place on a weekly basis. The purpose of this call is to provide a forum that is accessible to everyone and offers a way to raise questions for clarification that are related to DH and DR obligations, while getting access to important updates on the CDR, such as the Rules and Standards changes, early. These meetings offer an opportunity to better understand how to interpret and implement the Rules, CX Standards and Guidelines, and the Standards.

Questions related to the on-boarding process can be raised during the weekly call, though questions submitted via GitHub [R4] or by email at support@cdr-support.zendesk.com before the call will be discussed first.

Seeking assistance from the CDR On-boarding Team

As you work through the steps of the on-boarding process, you may need to reach out to the CDR On-boarding Team with questions and clarifications. The CDR On-boarding Team is on hand to help and answer your queries. They also look for opportunities to disseminate information more broadly in order to help all participants.

The CDR On-boarding Team can be contacted by email at CDROnboarding@accc.gov.au.

3 Getting started checklist

Before you can start on-boarding to the ecosystem, there are a number of pre-requisite activities that need to be completed. It is highly recommended that you read this section to ensure you are in a position to commence on-boarding.

Pre-requisites	Completed
The legal entity has been granted access to the CDR Participant Portal (the Participant Portal) [R17] and all appropriate users from my organisation have been delegated access, including the Primary IT Contact / Authorised IT Contacts who have the ability to provide technical information regarding your technology solution. If your Participant Portal access is not yet complete, consult the *CDR Participant Portal User Guide* [R12] for more information on how to do this.	□
In order to on-board to the CDR as a DR, the legal entity has already applied for, and been granted accreditation. If you have not yet applied for accreditation, find out how to become an accredited data recipient [R15]. -or- In order to on-board to the CDR as a DH, the legal entity has been registered (see ***Registering as a data holder***). If you have not yet applied for registration, register via the Participant Portal [R17] -or- In order to on-board an additional brand to an existing DH legal entity, please email the ACCC at CDROnboarding@accc.gov.au.	□
A duly authorised representative (Legal Authority Contact) that has the authority to sign, and accept the required agreements, on behalf of the legal entity has been identified. The details of the Legal Authority Contact have been entered into the Participant Portal [R17]. See the *CDR* ***Participant Portal User Guide*** [R12] for more information.	□
If you intend to operate under a Collection Arrangement, consult **Appendix C: Collection arrangements** for considerations relating to on-boarding.	□
Consult Appendix D: White label products for consideration if one of the white labelling scenarios applied to you.	□

4 Participant responsibilities

In order to successfully join the ecosystem, the participant is responsible for a variety of activities regarding the development, release and support of their solution, including (but not limited to):

- putting in place infrastructure operations and IT services/support procedures
- setting up the participant's production environment and the environment the participant wants to test in
- training of the participant's technical users (e.g. to perform back-up, code migration, or technical verifications)
- maintaining the participant's solution related documentation as up-to-date
- configuration within the participant's control (e.g. installation of test and production certificates)
- management and coordination of release management functions
- performance, scalability and security testing of the participant's solution
- participant communications to the market and their CDR consumers (consumers)
- undertaking internal quality assurance of the participant's software solution (see **Appendix B: Testing guidance** for further information)
- ensuring the participant's on-going compliance with the CDR regulatory framework (regulatory framework) and participant obligations (contained in the CDR legislation, Rules and Standards)

! Note

The ACCC will not ask for evidence relating to these responsibilities as part of the on-boarding process.

In accordance with best practice, participants should ensure that they keep appropriate records relating to these responsibilities.

5 Use of the CDR logo

In order to use the CDR logo (the logo) in your solution, participants will need to sign the CDR Trade Mark Licence Agreement [R8] (Trade Mark Licence Agreement), which sets out the terms and conditions of the logo's use. The Trade Mark Licence Agreement is non-negotiable. The latest version of the Trade Mark Licence Agreement is available on the website [R8]. It is also mandatory under the CDR rules for DR's to be licensed in order to use the CDR logo.

The logo is intended to be a symbol of trust in the ecosystem. Under the Trade Mark Licence Agreement, the logo can be used by a licenced DR when asking a consumer to give consent to collect and use CDR Data, and by a DH when asking a consumer to give authorisation to disclose CDR Data. These are listed in the *Field of Use* in the Trade Mark Licence Agreement. Other than licenced DR's and DH's the use of the ACCC CDR logo to is not permitted.

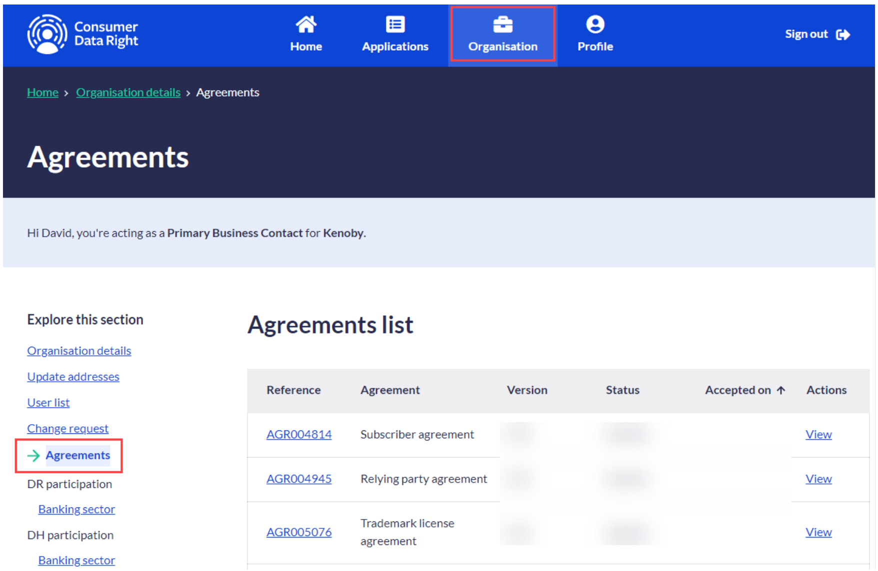
The term of the licence will commence when the ACCC registers a particular CDR participant as a user of the CDR logo, and the term of the licence will continue until that CDR participant is no longer registered with the ACCC as a user of the logo (for example, if the obligations in relation to use of the CDR logo are breached). The Register and Accreditation Application Platform may, in the future, accommodate registration of CDR logo use. In the meantime, the ACCC will maintain a record of persons who have indicated to the ACCC in writing that they will use the CDR logo and agree to take a licence to use the CDR logo.

In the future, the ACCC expects that the Rules and CX Standards and Guidelines [R9] will provide additional requirements and recommendations respectively regarding mandatory use of the logo by a DR and optional use by a DH.

If the Trade Mark Licence Agreement is accepted, the logo is provided in various styles (see Table 7) and file formats (see Table 8) to the participant for inclusion within their solution (see *Appendix G: CDR logo formats and styles*).

Confirming your intention to use the CDR Logo

- Login to the CDR Participant Portal [R17] and navigate to your Organisation record.
- Select the Agreements option to view the list of agreements:



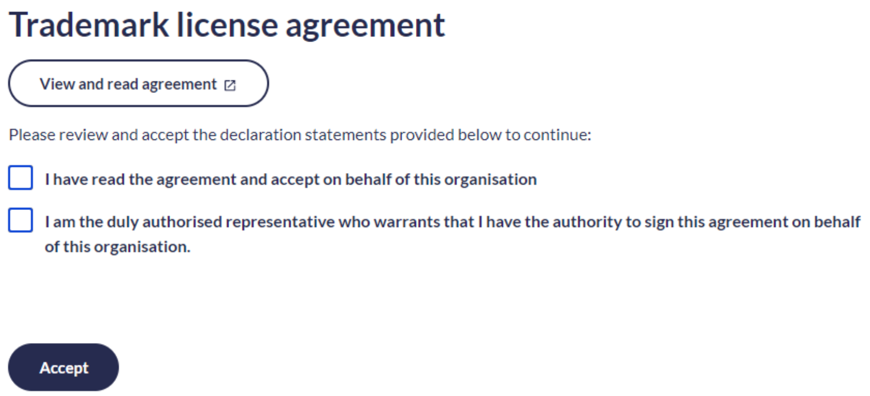
Agreements

Hi David, you're acting as a **Primary Business Contact** for **Kenoby**.

Agreements list

Reference	Agreement	Version	Status	Accepted on ↑	Actions
AGR004814	Subscriber agreement	[redacted]	[redacted]		View
AGR004945	Relying party agreement	[redacted]	[redacted]		View
AGR005076	Trademark license agreement	[redacted]	[redacted]		View

- Select the *Trademark licence agreement* in order to view the contents.
- On the agreement page, click on the *View and read agreement* button to review the agreement.



Trademark license agreement

View and read agreement

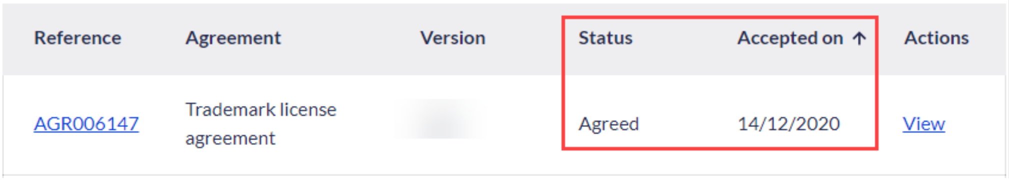
Please review and accept the declaration statements provided below to continue:

□ I have read the agreement and accept on behalf of this organisation

□ I am the duly authorised representative who warrants that I have the authority to sign this agreement on behalf of this organisation.

Accept

- If you wish to accept the agreement and have the authority to accept the agreement on behalf of your organisation, tick both of the checkboxes and press the Accept button.
- When you return to the Agreements list the agreement should now be shown as Agreed:



Reference	Agreement	Version	Status	Accepted on ↑	Actions
AGR006147	Trademark license agreement	[redacted]	Agreed	14/12/2020	View

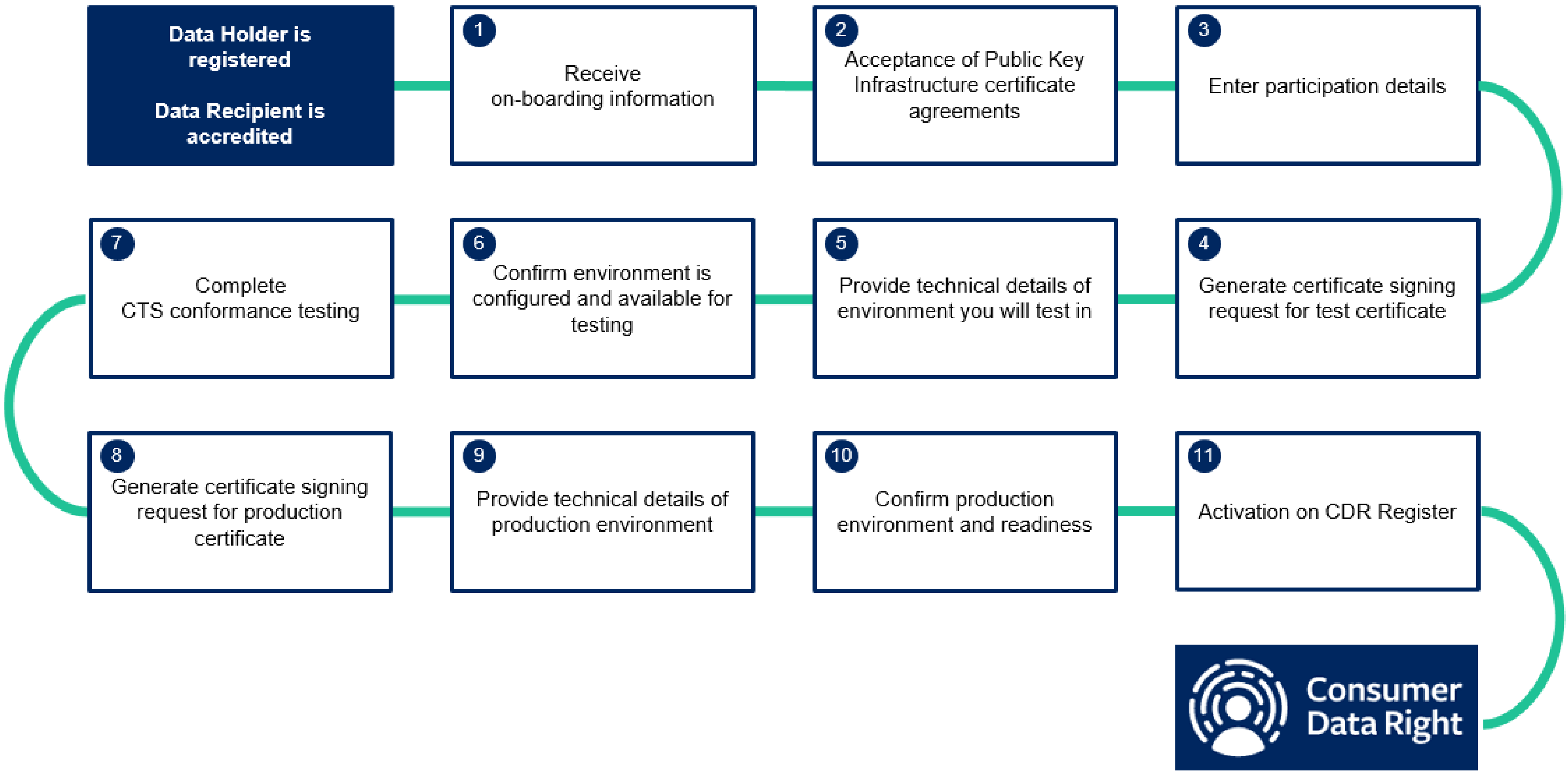
- See the CDR Participant Portal User Guide [R12] for more information on viewing and accepting the Agreements within the Participant Portal.
- In response, you will receive the CDR logo in various formats.

6 On-boarding process – High level overview

6.1 Overview of the on-boarding process

Each participant needs to complete the steps outlined in Figure 2 to be on-boarded to the ecosystem. A detailed description and associated activities for each step can be found in the *On-boarding process – Step-by-step instructions* section of this document.

Figure 2: Overview of on-boarding process


Data Holder is registered
Data Recipient is accredited
1 Receive on-boarding information
2 Acceptance of Public Key Infrastructure certificate agreements
3 Enter participation details
4 Generate certificate signing request for test certificate
5 Provide technical details of environment you will test in
6 Confirm environment is configured and available for testing
7 Complete CTS conformance testing
8 Generate certificate signing request for production certificate
9 Provide technical details of production environment
10 Confirm production environment and readiness
11 Activation on CDR Register
Consumer Data Right

6.2 CDR Registrar request

The ACCC, as part of the on-boarding process, will issue a request to all participants to complete the steps as set out in this Guideline so as to enable the ACCC, as the Registrar, to activate a Participant on the Register.

6.3 Expected timings

The length of time it takes to complete the on-boarding steps will vary based on each participant and how responsive they can be to successfully perform their necessary actions. Table 2 outlines indicative timings for each step in the process.

Table 2: Expected Timings

#	Step	Participant	ACCC
1	**Receive on-boarding information**	N/A	1-3 days As soon as a participant is accredited or registered the ACCC will send on-boarding information to the Primary Business Contact
2	**Acceptance of PKI certificate agreements**	1-5 days Dependent on the participant's legal review and acceptance processes	N/A
3	**Enter participation details**	1-3 days Dependent on whether the participant has participation/brand/software product information at the ready	N/A
4	**Generate certificate signing request for test certificate**	1-3 days Dependent on the participant's certificate management processes	N/A
5	**Provide technical details of environment you will test in**	1-5 days Dependent on the readiness of the participant's testing environment and the availability of the technical information	1-3 days Once the information is received, the ACCC will provision the test certificate and prepare the CTS test plan
6	**Confirm environment is configured and available for testing**	1-14 days Dependent on the participant's change/release management practices as the solution needs to be configured with the CTS environment details and test certificate installed	N/A
7	**Complete CTS conformance testing**	1-30 days Dependent of the maturity, readiness and conformance of the participant's solution, as well as the ability to	1-30 days The ACCC will support the participant through CTS execution

#	Step	Participant	ACCC
		troubleshoot and resolve issues if and when they occur	
8	**Generate certificate signing request for production certificate**	1-3 days Dependent on the participant's certificate management processes	N/A
9	**Provide technical details of production environment**	1-5 days Dependent on the readiness of the participant's testing environment and the availability of the technical information	1-3 days Once the information is received, the ACCC will provision the Production Certificate
10	**Confirm production environment and readiness**	1-14 days Dependent on the participant's change/release management practices as the solution needs to be configured with the CDR Register details and production certificate installed	N/A
11	**Activation on CDR Register**	N/A	1-3 days
	Indicative Total Timeframe	**2 weeks - 3 months**	

7 On-boarding process – Step-by-step instructions

This section provides detailed information and guidance for each step outlined in the overview of the on-boarding process diagram [Figure 2].

! Note

For the purposes of identification in this guide, the on-boarding process is represented as a sequential set of steps that a participant navigates through prior to activation on the ecosystem. These steps may occur in the order specified in this guide, however certain steps may also occur at any time (i.e. in a different order to what is specified in this guide), or in parallel with other steps.

For example, if your production environment has been provisioned you may provide your production details or request a production certificate in the Participant Portal before completing the Conformance Test Suite (CTS).

Ultimately, all steps specified in this guide need to be completed, and all on-boarding requirements met by the participant, before they can be activated in the ecosystem.

7.1 Step 1: Receive on-boarding information

- When you complete accreditation (DR) or registration (DH), your *Primary Business Contact* will receive on-boarding information by email.
    - If you have not received this information, please contact CDROnboarding@accc.gov.au by email to request a copy.
    - Some of this information is sensitive in nature and cannot be made publicly available on the CDR website, and includes information aimed to assist in the preparation of your technical infrastructure environments (e.g. it includes the technical details of the CTS and the Register).
    - As part of the on-boarding information received via email, you will also receive a CTS enrolment pack, which includes various artefacts relating to CTS.

! Note

The CTS enrolment form completed within the Participant Portal contains the *Consumer Data Right Conformance Test Suite Acknowledgement (CTS Acknowledgement)*.

It is important to review the *CTS Acknowledgement* as it contains information about participant responsibilities and must be accepted before allowing access to CTS.

7.2 Step 2: Acceptance of Public Key Infrastructure certificate agreements

Public Key Infrastructure (PKI) certificates are a key component used in the ecosystem to provide secure and private communications between participants. The ACCC, as the Registrar, is responsible for issuing PKI certificates to participants.

The procedural and operational requirements relating to the use of (and reliance on) the digital PKI certificates issued to (or used by) participants are governed by two, non-negotiable agreements; the Subscriber Agreement and the Relying Party Agreement (the Agreements).

Subscriber Agreement

The Subscriber Agreement [R6] establishes the basis on which digital PKI certificates are issued to participants. Subscriber Agreements also establish the role subscribers are required to play in safeguarding and managing PKI certificates issued to them to maintain the overall integrity, security and stability of the Register and ecosystem more broadly.

ACCC certification services, and the use of PKI certificates, are governed by the ACCC Certificate Policy, which is incorporated in its entirety in the Subscriber Agreement. Full details of the role and obligations of all entities associated with operation of the ACCC PKI are included in the Certificate Policy.

The Subscriber Agreement contains the contractual rights and obligations that govern use of a digital PKI certificate. This agreement contains some very important provisions governing the subscriber's responsibility and legal liability for using a PKI certificate. Participants should read this Subscriber Agreement, and the documents referenced in it, carefully.

Relying Party Agreement

The Relying Party Agreement [R6] establishes the basis on which participants rely on information protected by ACCC digital PKI certificates.

The ACCC Certificate Policy (the Certificate Policy) is also incorporated in its entirety in the Relying Party Agreement. The Certificate Policy includes a full description of the terms and conditions associated with reliance on ACCC digital PKI certificates.

The Relying Party Agreement contains the contractual rights and obligations that govern reliance on a digital PKI certificate. This agreement contains some very important provisions governing the relying party's responsibility and legal liability in relying on a certificate. Participants should read this Relying Party Agreement, and the documents referenced in it, carefully.

Policy and Procedural Documents

Two policy and procedural documents underpin the use of PKI certificates in the ecosystem:

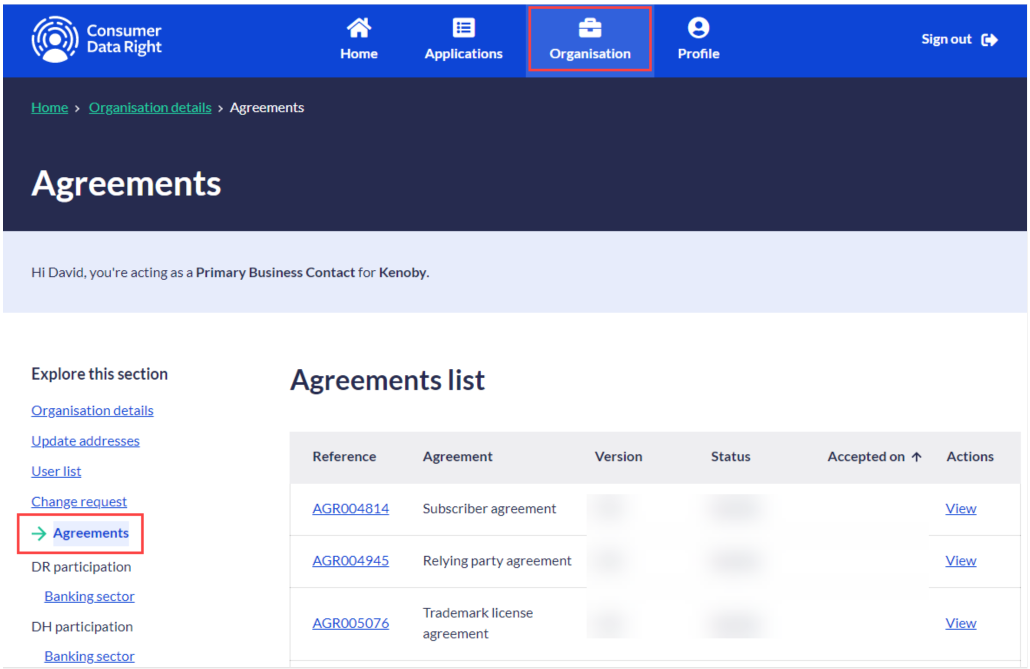
- The **Certificate Policy document** [R6], which defines the overarching framework for management and administration of the ACCC PKI
- The **Certification Practice Statement** [R6], which is a detailed procedural document describing how the ACCC intends to implement its Certificate Policy.

These documents are part of the agreements, so that the obligations in them are part of the contractual responsibility held by relying parties and subscribers. The latest versions of the Agreements, Certificate Policy and Certification Practice Statement are available on the website.

> **! Note**
>
> You must have the *Legal Authority Contact* role in order to accept agreements in the CDR Participant Portal.

Accepting the agreements

- Login to the CDR Participant Portal [R17] and navigate to your Organisation record.
- Select the Agreements option to view the list of agreements:



Home › Organisation details › Agreements

Agreements

Hi David, you're acting as a **Primary Business Contact** for **Kenoby**.

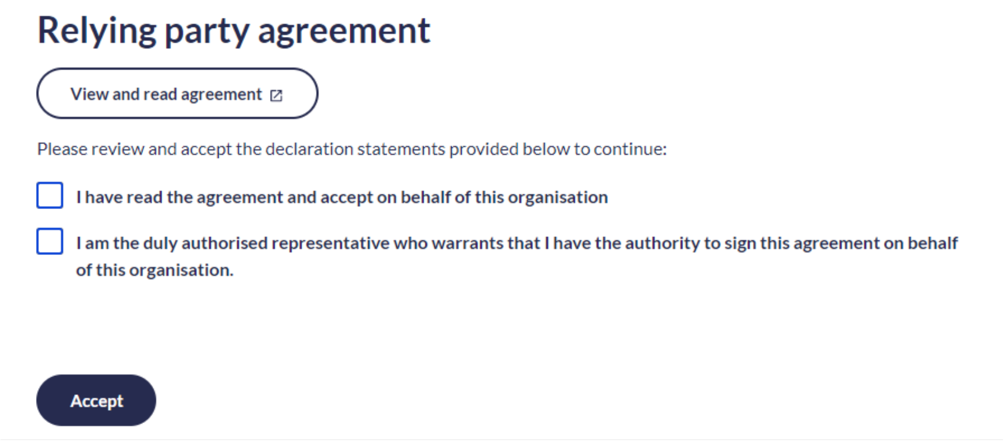
Explore this section

- Organisation details
- Update addresses
- User list
- Change request
- → Agreements
- DR participation
  - Banking sector
- DH participation
  - Banking sector

Agreements list

Reference	Agreement	Version	Status	Accepted on ↑	Actions
AGR004814	Subscriber agreement	[redacted]	[redacted]		View
AGR004945	Relying party agreement	[redacted]	[redacted]		View
AGR005076	Trademark license agreement	[redacted]	[redacted]		View

- Select an agreement (Subscriber agreement or Relying party agreement) in order to view the contents.
- On the agreement page, click on the View and read agreement button to review the agreement.



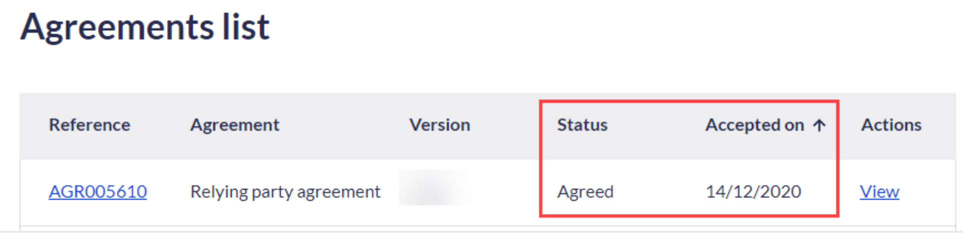
Relying party agreement

Please review and accept the declaration statements provided below to continue:

☐ I have read the agreement and accept on behalf of this organisation

☐ I am the duly authorised representative who warrants that I have the authority to sign this agreement on behalf of this organisation.

- If you wish to accept the agreement and have the authority to accept the agreement on behalf of your organisation, tick both of the checkboxes and press the Accept button.
- When you return to the Agreements list the agreement should now be shown as Agreed:



Agreements list

Reference	Agreement	Version	Status	Accepted on ↑	Actions
AGR005610	Relying party agreement	[redacted]	Agreed	14/12/2020	View

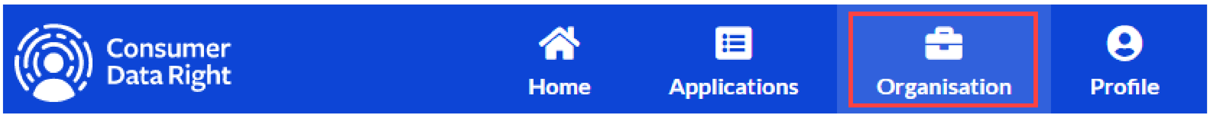
- See the CDR Participant Portal User Guide [R12] for more information on viewing and accepting the Agreements within the Participant Portal.

! Warning

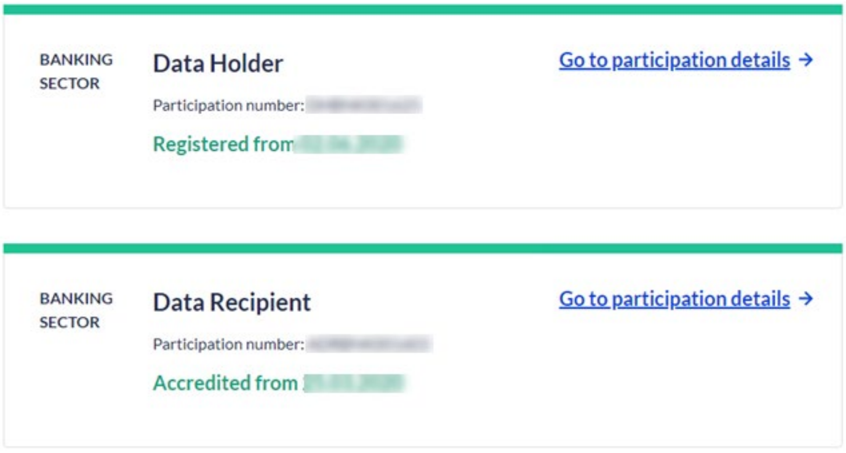
Without accepting the Subscriber Agreement and Relying Party Agreement, PKI certificates cannot be provisioned by the ACCC and you cannot proceed through the on-boarding steps.

7.3 Step 3: Enter participation details

- Login to the CDR Participant Portal [R17] and navigate to your Organisation record.



- You should be able to see your participation status (DH and/or DR), as shown in Figure 3.



BANKING SECTOR

Data Holder

Participation number: [redacted]

Registered from [redacted]

Go to participation details →

BANKING SECTOR

Data Recipient

Participation number: [redacted]

Accredited from [redacted]

Go to participation details →

Figure 3: DR and DH status in CDR Participant Portal

> **! Note**
>
> At this stage, not all of the details may be known or confirmed by the participant. If this is the case, complete the mandatory information and re-visit the details prior to production activation (7.9).

For data holders:

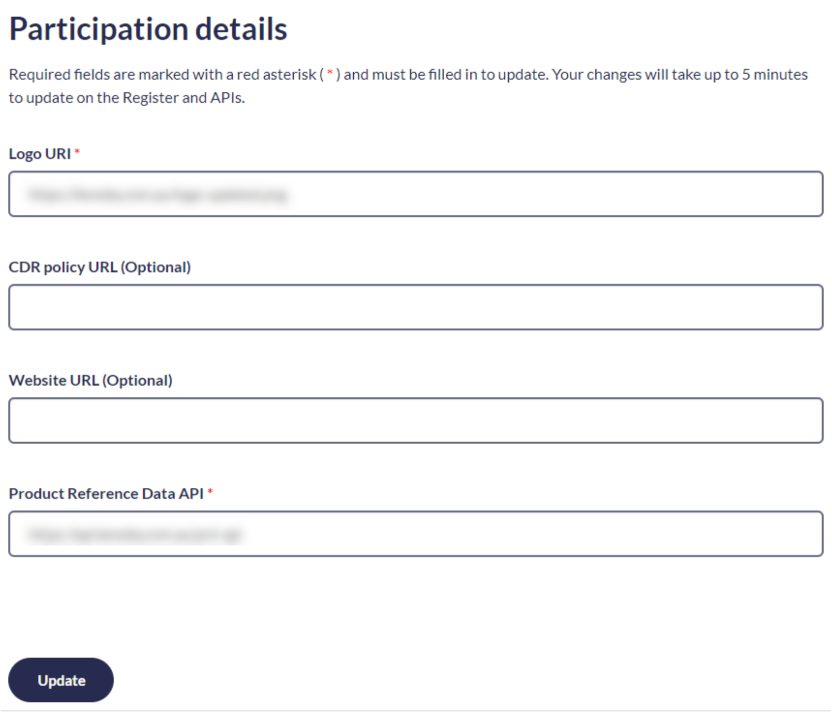
- Based on your DH participation status, enter details as listed in Table 3 below.
- Screenshots are provided below to assist with entry of this information. Consult the ***CDR Participant Portal User Guide*** [R12] for additional guidance, if needed.

Table 3: Data holder participation details

Section	Field name
Participation details - see *Figure 4*	Logo URI
	CDR Policy URL
	Website URL
	Product Reference Data API
Brand details - see *Figure 5*	Brand name
	Brand description
	Logo URI

	CDR Policy URL Website URL

Figure 4: Data holder participation details



Participation details

Required fields are marked with a red asterisk (*) and must be filled in to update. Your changes will take up to 5 minutes to update on the Register and APIs.

Logo URI *

[redacted]

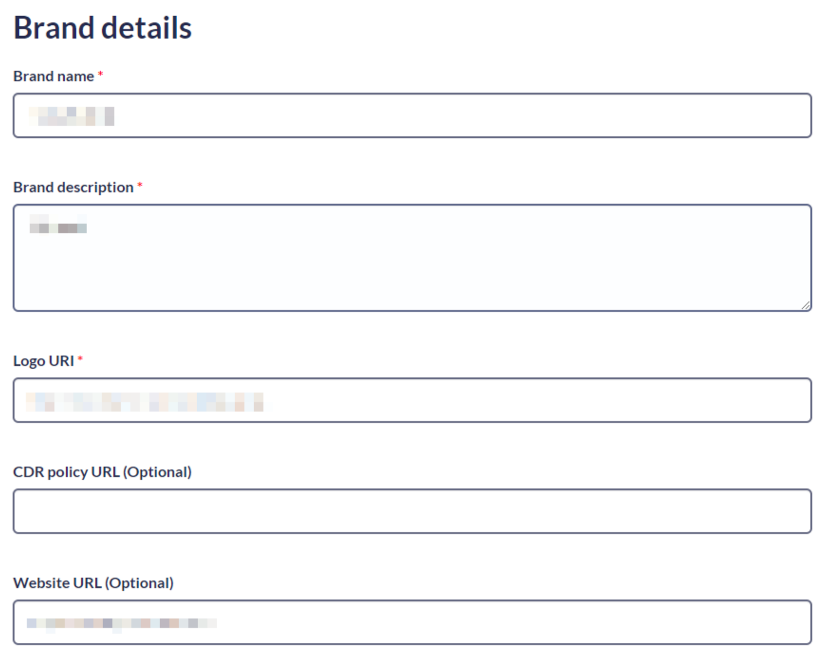
CDR policy URL (Optional)

Website URL (Optional)

Product Reference Data API *

[redacted]

Figure 5: Data holder brand details



Brand details

Brand name *

[redacted]

Brand description *

[redacted]

Logo URI *

[redacted]

CDR policy URL (Optional)

Website URL (Optional)

[redacted]

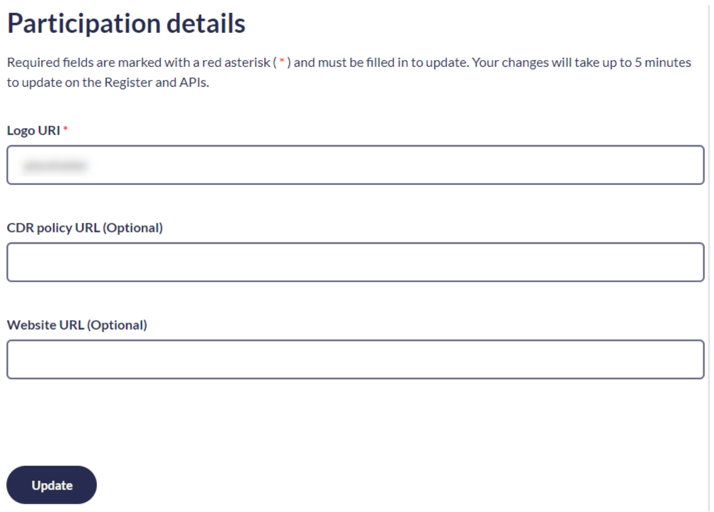
For data recipients:

- Based on your DR participation status, enter details as listed in Table 4 below.
- These details should have been pre-filled based on the data received during the accreditation application process. Ensure that the details are correct and any missing information is entered (if known).
- Screenshots are provided below to assist with entry of this information. Consult the ***CDR Participant Portal User Guide*** [R12] for additional guidance, if needed.

Table 4: Data recipient participation details

Section	Field name
Participation details - see *Figure 6*	Logo URI
	CDR Policy URL
	Website URL
Brand details - see *Figure 7*	Brand name
	Brand description
	Logo URI
	CDR Policy URL
	Website URL
Software product details - see *Figure 8*	Description
	Name

Figure 6: Data recipient participation details



Participation details

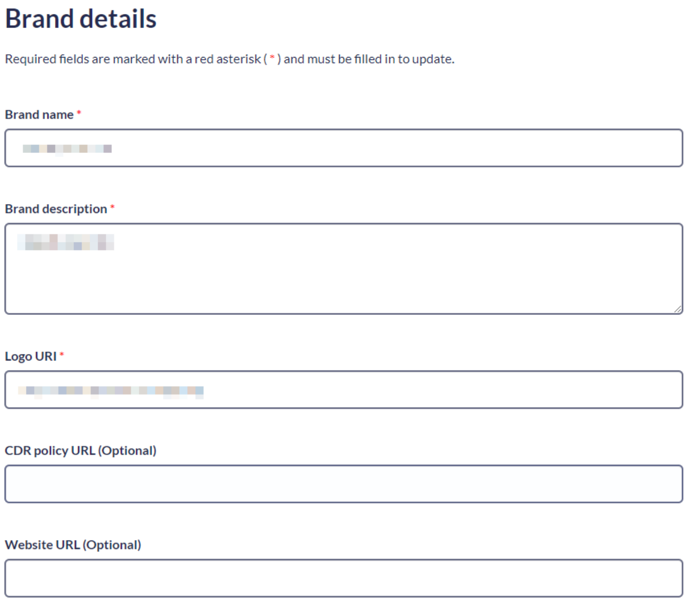
Required fields are marked with a red asterisk (*) and must be filled in to update. Your changes will take up to 5 minutes to update on the Register and APIs.

Logo URI *

CDR policy URL (Optional)

Website URL (Optional)

Figure 7: Data recipient brand details



Brand details

Required fields are marked with a red asterisk (*) and must be filled in to update.

Brand name *

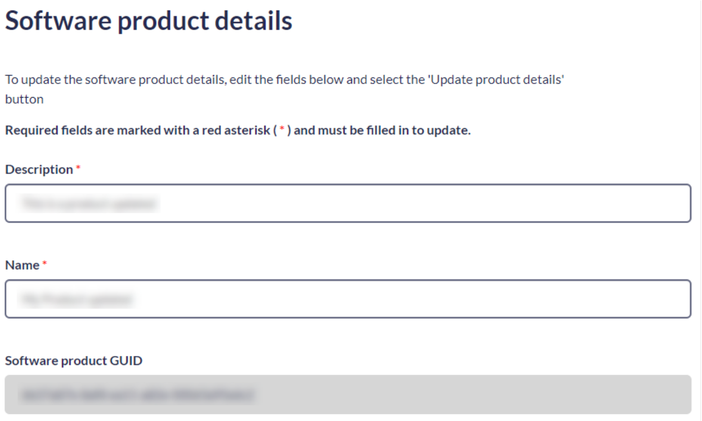
Brand description *

Logo URI *

CDR policy URL (Optional)

Website URL (Optional)

Figure 8: Data recipient software product details



Software product details

To update the software product details, edit the fields below and select the 'Update product details' button

Required fields are marked with a red asterisk (*) and must be filled in to update.

Description *

Name *

Software product GUID

> **! Note**
>
> Once the participation details have been entered, the **Brand GUID** (DH and DR) and **Software Product GUID** (DR) are generated and available for viewing within the CDR Participant Portal. These identifier values are utilised in later steps of the on-boarding process.
>
> Please refer to the ***CDR Participant Portal User Guide*** [R12] for mapping information.

7.4 Step 4: Generate certificate signing request for test PKI certificate

In order to be provided with a PKI certificate for the environment you will test in, you are asked to generate a certificate signing request (CSR). The CSR is then used by the ACCC in the PKI certificate creation process, and allows the participant to keep their private key confidential.

Generating a CSR

- The participant should follow their internal processes and procedures for generating a CSR and the management of certificates.
- Consult the Certificate Management guidance [R18] to understand the type of certificates (server and/or client) required for each participant type.
- When generating a CSR, ensure the details in Table 5 are used.

Table 5: CSR values

	Participant Details	
CSR	Server Certificate	Client Certificate
Common Name (mandatory)	Primary DNS Name e.g. api1.test.entity.com	Software Product Name
SAN (optional)	Secondary DNS Name(s) e.g. Api2.test.entity.com	N/A
Organization (mandatory)	Brand Name	Brand Name
Organizational Unit (mandatory)	Consumer Data Right	Consumer Data Right
Country (mandatory)	Country of participant e.g. AU	Country of participant e.g. AU
State (optional)	State of the Participant e.g. New South Wales	State of the Participant e.g. New South Wales
Locality (optional)	Locality of the Participant e.g. Sydney	Locality of the Participant e.g. Sydney
Email Address (optional)	Participant's email address to be displayed in the issued certificate	Participant's email address to be displayed in the issued certificate
Signature Algorithm (mandatory)	SHA256	SHA256
Key Algorithm (mandatory)	RSA	RSA
Key Size (mandatory)	2048	2048

- For more information on generating a CSR, consult [R10]. The generated CSR should be provided to the ACCC in 7.5.
- The generated CSR is then added by the Participant in the Participant Portal, which is explained in 7.5

7.5 Step 5: Provide technical details of environment you will test in

To be able to conduct conformance testing via the CTS, the technical details of the participant’s target testing environment must be provided to the ACCC. Interactions with CTS are expected to occur with the participant’s solution in an environment which represents a similar configuration and infrastructure setup to their future production environment for the ecosystem.

Providing the details

- Complete the CTS enrolment form which will be available in the Participant Portal to the Primary business contact, primary IT contact and authorised IT contact to complete upon acceptance of the public key infrastructure (PKI) certificates (see 7.2).
    - The CTS enrolment form includes brand authentication details, endpoint URIs, CSR for a test certificate, and details of your environment.
    - In this form you will also need to nominate a CTS contact user, who must have a valid Participant Portal user account role as “Authorised CTS Tester”.
- The participant will then be enrolled into CTS based on the technical details that are provided during this step. After successful submission of the form, the CTS enrolment form will be displayed and sent to the Primary Business Contact by email (and will include the CTS conformance ID). The CTS conformance ID is required to access the CTS. Further details on CTS are outlined in step 7.7. Please refer to the CDR Participant Portal User Guide [R12] for more information on how to complete the CTS enrolment form.
- The test PKI certificate can be requested in this same section of the Participant Portal. Section 10 of the CDR Participant Portal User Guide [R12] explains the steps in more detail. The PKI test certificate will be generated by the ACCC and emailed to the contact specified in the certificate request.

! Note

If your details change after you submit your CTS enrolment form, these details can be amended in the Participant Portal directly by the Primary Business Contact, primary IT contact and authorised IT contact before submission is completed.

In the event that an adjustment to the CTS enrolment form data is required after submission, contact the On-boarding Team via CDROnboarding@accc.gov.au.

Also, you will need to have a role of *Primary IT Contact* or *Authorised IT Contact* in order to request a PKI certificate

7.6 Step 6: Confirm environment is configured and available for testing

Based on the information that was provided in the on-boarding email from the ACCC in 7.1, the participant's target environment needs to be configured to allow communication with CTS.

In 7.1, the ACCC provided you with details such as IP addresses and URLs to access the CTS. Infrastructure changes, such as firewall rules or IP whitelisting, may need to be performed based on this information.

You should have also received a test PKI certificate from the ACCC based on the CSR (7.4). This test PKI certificate also needs to be installed into your infrastructure environment to enable secure communication with CTS.

Providing confirmation of readiness

- Once your environment has been configured and is ready for testing, send an email to CDROnboarding@accc.gov.au titled **Commence CTS testing - [LEGAL ENTITY NAME]** to confirm your readiness for CTS conformance testing.
- You will receive a CTS URL and a Conformance ID via return email. These identifiers are unique for each participant and, once received, you can continue to 7.7 and commence CTS conformance testing.

7.7 Step 7: Complete CTS conformance testing

The CTS is maintained by the ACCC and provides a suite of automated test cases that are to be executed against DR and DH solutions.

As per standard software development life cycle practices, it is assumed participant solutions have been developed and quality assured **before** requesting access to CTS. See **Appendix B: Testing guidance** for further information.

The primary purpose of the CTS is to test the interactions of the solution against the Register interactions, utilising simulated implementations of DRs and DHs, as well as a mock Register.

Executing CTS

- Consult the ***CTS guidance material*** [R11] for more information about conformance testing with CTS.
- You will be able to see your progress and results either:
  - through the CTS web portal (for DHs); or
  - by contacting your ACCC support officer (for DRs) on CDROnboarding@accc.gov.au and requesting a CTS report.
- Jira will be used for defect management during conformance testing. Once you complete CTS enrolment you will be provisioned with one Jira account. In Jira each participant will only be able to view defects related to their own organisation.

! Note

Once you have completed all testing activities, you are now ready to proceed to the CDR production environment (the production environment).

7.8 Step 8: Generate certificate signing request for production certificate

Similar to 7.4 of the on-boarding process, you will now need to generate a CSR for your production environment.

Generating a CSR

- The participant should follow their internal processes and procedures for generating a CSR and the management of certificates.
- Consult the Certificate Management guidance [R18] to understand the type of certificates (server and/or client) required for each participant type.
- When generating a CSR, ensure the details in Table 6 are used.

Table 6: CSR values

	Participant Details	
CSR	**Server Certificate**	**Client Certificate**
Common Name (mandatory)	Primary DNS Name e.g. api1.test.entity.com	Software Product Name
SAN (optional)	Secondary DNS Name(s) e.g. Api2.test.entity.com	N/A
Organization (mandatory)	Brand Name	Brand Name
Organizational Unit (mandatory)	Consumer Data Right	Consumer Data Right
Country (mandatory)	Country of participant e.g. AU	Country of participant e.g. AU
State (optional)	State of the Participant e.g. New South Wales	State of the Participant e.g. New South Wales
Locality (optional)	Locality of the Participant e.g. Sydney	Locality of the Participant e.g. Sydney
Email Address (optional)	Participant’s email address to be displayed in the issued certificate	Participant’s email address to be displayed in the issued certificate
Signature Algorithm (mandatory)	SHA256	SHA256
Key Algorithm (mandatory)	RSA	RSA
Key Size (mandatory)	2048	2048

- For more information on generating a CSR, consult the guidance on *Certificate Signing Requests* [R10].
- The generated CSR is then added in the Participant Portal, which is explained in 7.9.

7.9 Step 9: Provide technical details of production environment

Technical details required for your production environment, similar to those provided for your testing environment in 7.5, are added via Participant Portal.

Some of these details have been previously entered in 7.3. Ensure that any previously entered values are still accurate and any missing information is entered prior to production activation.

! Note

You will need to have a role of *Primary IT Contact* or *Authorised IT Contact* in order to request a PKI certificate, maintain authentication details, maintain software products and maintain endpoints.

Consult the ***CDR Participant Portal User Guide*** [R12] for guidance on this step, as well as **Appendix E: Participant Portal screenshots** for sample screenshots of this process. The figures listed below relate to Appendix E.

Providing the details

- For data recipients:
    - DRs must provide the ACCC with:
        - Participation details (Figure 9)
        - Brand details (Figure 10)
        - Certificate request (Figure 11 and Figure 12)
        - Authentication details (Figure 13)
        - Software product details (Figure 14)
        - Software product authentication details (Figure 15)
        - Software product endpoints (Figure 16)
- For data holders:
    - DHs must provide the ACCC with:
        - Registration details (Figure 17 and Figure 18)
        - Registration details for non-ADIs (Figure 19)
        - Participation details (Figure 20)
        - Brand details (Figure 21)
        - Certificate request (Figure 22 and Figure 23)
        - Authentication details (Figure 24)
        - Endpoints (Figure 25).

! Note

When these details are added in the CDR Participant Portal, the various identifiers are generated and should be included in the participant's software solution.

The CDR Register design [R14] includes a section on Identifiers for the ecosystem entities. The discovery location of these identifiers in the CDR Participant Portal are listed in Appendix F.

7.10 Step 10: Confirm production environment and readiness

Once you have received your production PKI certificate, it needs to be configured within your production environment prior to go live.

This step allows you to confirm when your infrastructure is in place and configured, and your solution is ready to make and receive requests within the ecosystem.

Providing confirmation of readiness

- To confirm your production readiness, the Primary Business Contact of your legal entity needs to send an email to CDROnboarding@accc.gov.au.

! Note

This step is especially important for DHs, as it is the step that the DH requests to be made active on the register. Many DHs may choose to hold off taking this step until the date of their compliance obligations.

As soon as a DH is made active on the Register, they are discoverable and must be ready to start servicing requests from DRs. Therefore, their production environment must be available, with the production PKI certificate installed, before being made active. This ensures that the participant is in control of the release of their production solution into the ecosystem.

There is more flexibility for **DRs** as it is their responsibility to perform Dynamic Client Registration (DCR) requests when they are ready to commence participation.

7.11 Step 11: Activation on CDR Register

The ACCC receives the participant’s production readiness confirmation, which the participant sent in 7.10.

Confirmation that all the necessary on-boarding steps have been completed and the required information has been provided will enable the ACCC to activate the participant on the Register.

The ACCC will then activate the participant on the Register and will inform you via email when this step is completed.

8 Participation

Once you have completed the on-boarding process and the ACCC has made you **active** on the Register, you are able to operate within the ecosystem as a DH or a DR.

As your solution continues to evolve and change over its life cycle, there may be a need to revisit certain aspects of the on-boarding process, such as CTS, to ensure new features meet conformance requirements, and the ACCC may issue requests for further information or further testing. Further guidance on participant testing is to be provided on the website.

Participants will be notified by the ACCC of additional requirements, and any changes to the on-boarding process for new DRs or new DHs will be reflected in an updated version of this guide.

Appendix A: Terminology

Shortened form	Extended form
ACCC	Australian Competition and Consumer Commission.
Accreditation	The process a DR undertakes to become accredited, whereby the DR Accreditor makes a decision to grant accreditation to a person (Legal Entity) where it is satisfied that the entity meets the criteria for accreditation specified in the CDR Rules.
ADI	Authorised deposit-taking institution.
CDR	Consumer Data Right.
CDR Registrar	The person or entity appointed as the **Accreditation Registrar** under the CDR legislation, currently the ACCC.
CDR Register	Register of Accredited Persons and the associated database (as defined in the CDR Legislation and the CDR Rules).
CDR Rules	*Competition and Consumer (Consumer Data Right) Rules 2020* as amended from time to time.
CDS	Consumer Data Standards made by the Data Standards Chair.
CSR	Certificate signing request.
CTS	Conformance Test Suite.
CX	Consumer experience.
Data holder	A Legal Entity (participant) that is a **data holder** subject to CDR data sharing obligations (data sharing obligations) under the CDR Rules.
Data recipient	A Legal Entity (participant) who has been granted accreditation by the DR Accreditor and is able to receive CDR data.
DR Accreditor	The person or entity appointed as the **DR Accreditor** under the CDR Legislation, currently the ACCC.
DH	Data holder.
DR	Data recipient.
DSB	Data Standards Body.
FAPI	Financial-grade API is an industry-led specification of JSON data schemas, security and privacy protocols to support use cases for commercial and investment banking accounts as well as insurance and credit card accounts
Legal Entity	A legal person (an individual, company, other incorporated body or government entity).
Participant	For the purposes of this guide, a participant is a Legal Entity that has been accredited (as a DR) or registered (as a DH) and is preparing to undertake or currently undertaking on-boarding processes in order to participate in the ecosystem.
PKI	Public key infrastructure.
Registration	Is the process a Legal Entity undertakes to register as a data holder and commence on-boarding

Appendix B: Testing guidance

Overview

A critical element of the ecosystem is the successful operation of participants' technology solutions. This section provides a brief overview of the ACCC's testing requirements for new ecosystem participants to prepare for the production release of their solution.

CTS conformance testing is the final checkpoint prior to a participant being activated in the ecosystem and focuses on critical risk points for the ecosystem. It does not include all possible scenarios relevant to CDR.

Consult the ***CTS guidance material*** [R11] for further information about CTS, including how to prepare for and execute the CTS tests.

This appendix contains general information designed to assist participants with their testing activities for participation in the CDR ecosystem. However, Participants are responsible for ensuring their solutions meet all requirements for participation in the ecosystem, including undertaking testing activities to ensure quality and conformance to the Standards and CDR obligations

! Note:

The scope of CTS will evolve over time to include additional test cases and adapt to scope changes. See the Conformance Test Suite: version history and scenarios for scope changes

Testing principles

The ACCC's testing requirements are underpinned by the following principles:

- Each new participant can enter the ecosystem without disruption to existing participants and thus ensure scalability and continued operation of the ecosystem.
- Participants are to ensure the functionality of their solution is extensively tested internally.
- Participants are expected to complete all their internal testing activities prior to starting CTS conformance testing (as per 7.7).
    - During the on-boarding process, the ACCC will not ask for evidence of testing. However, evidence may be requested by the ACCC at a later date to inform other activities, including incident management and compliance and enforcement.
- Participants are expected to conduct relevant non-functional testing, such as security testing, performance testing, availability testing, usability testing, etc. to ensure that their solution meets the non-functional requirements before 7.8 of the on-boarding process. Detailed information on the non-functional requirements for participants' solutions can be found in the Standards.

Participant testing scope

Participants need to ensure that their solution aligns to the requirements required for participation in the ecosystem. It is recommended that the testing scope for each participant is defined in a way that can be traced back to the Rules, the Standards, the Register Documentation and CX Guidelines and Standards.

The testable items artefacts available from CDR Phase 1 test scenarios July 2020 and CDR Phase 2 Test Strategy November 2020 provide examples of testable items that trace back to the technical requirements in scope for the July 2020 and November 2020 obligation dates. These items can be used as an example for participants to construct the relevant internal testing scenarios that will allow robust and thorough testing of the solution.

Testing tools

It is likely participants will utilise tools to support their testing activities for the purposes of the ecosystem, such as internally built testing tools, market-based tools, or testing tools offered through industry standards bodies, e.g. FAPI.

The ACCC does not intend to recommend or certify specific testing tools.

Completion of testing

Should the ACCC need clarification of any aspect of a participant’s completion of testing, it may seek further information from the participant including by issuing a request under the CDR Rules.

Appendix C: Collection arrangements

The ACCC permits the use of accredited intermediaries to collect data through an expansion of the rules relating to outsourced service providers (also referred to as 'collection arrangements').

In this context, the term Provider refers to an accredited data recipient who is also undertaking the role of an outsourced service provider (OSP) to collect CDR data on behalf of another accredited data recipient, the Principal in this context. Both the Provider and Principal must be accredited at the unrestricted level.

The following should be considered if you intend to operate under a collection arrangement:

- Providers must be accredited and commenced (or completed) on-boarding to the ecosystem before a Principal can nominate their Provider during the on-boarding process.
- While the Provider's software product will not appear on the Public CDR Register, the legal entity and brand will. However, both the Provider and the Principal must undertake CTS conformance testing (7.7).
- As both the Provider and the Principal must undertake CTS conformance testing, both parties will require a test certificate (7.4). In addition, the Principal will always require a production certificate under the Collection Arrangement (7.8). This should not be required for the Provider as the Principal would usually own the domain name for the certificate requests.
- As the Provider collects the CDR data on behalf of the Principal, the software product collecting CDR data from DHs appears on the Register as the Principal's software product. Hence, the DH recognises the Principal and not the Provider.
- The relationship between a Principal and a Provider will not be visible on the Register, however, this relationship must appear in the consumer's consent agreement, with the Principal supplying their Provider's accreditation number during on-boarding, when there is a collection arrangement in place.

Appendix D: White label products

White label products are typically supplied by one legal entity (a white labeller), and branded and retailed to consumers by another entity (a brand owner). White labelling is a feature of a number of products in banking, including credit cards and home loans.

In banking, white labellers are often authorised deposit-taking institutions (ADIs). Some brand owners are also ADIs. These parties are likely to be data holders for CDR data they hold in respect of the white label product, and potentially subject to obligations under the CDR Rules.

There are two options for brand owners to be recorded on the CDR Register.

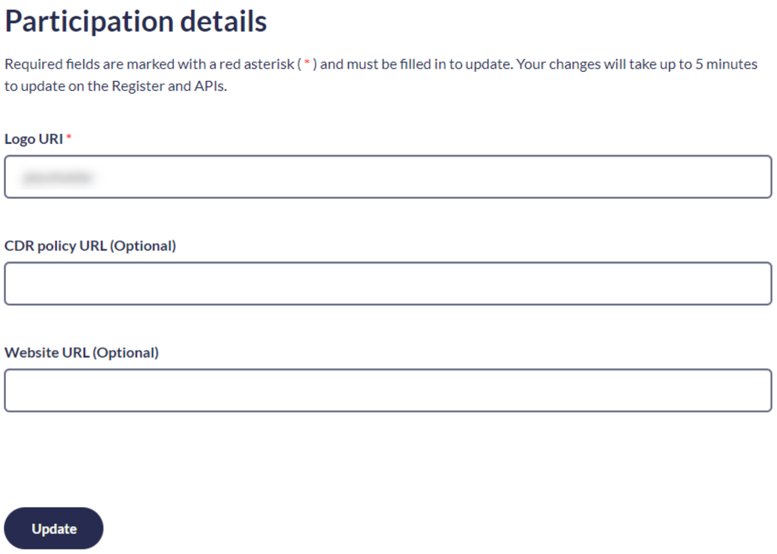
Option	Description
1	The brand owner is an ADI: • The brand owner will be responsible for adding and managing their data holder brand/s on the Register. They will work with the while labeller to determine the configuration of the brand identity. • Both parties must work together and with the on-boarding team to ensure the brand identity is optimised for consumer experience.
2	The brand owner is not an ADI: • The white labeller will be responsible for adding and managing brands on the Register. • Both parties must work together and with the on-boarding team to ensure the brand identity is optimised for consumer experience

The ACCC understands there is a wide variety of white label arrangements in the banking sector and beyond and the above options do not cover all potential scenarios. We are not seeking to mandate any particular commercial model, and are seeking to enable flexibility for parties in how they comply with the rules. We are therefore open to discussing any aspect of this guidance, or our technical guidance in future, with stakeholders for whom this may pose compliance issues, especially those with complex white labelling arrangements.

For further information on white labelling see *Noting Paper - White Label Conventions* and the knowledge article on White Labelled brands in the CDR. For technical guidance on how to list your brand on the CDR Register with a white label product, contact CDROnboarding@accc.gov.au

Appendix E: Participant Portal screenshots

Figure 9: Data recipient participation details



Participation details

Required fields are marked with a red asterisk (*) and must be filled in to update. Your changes will take up to 5 minutes to update on the Register and APIs.

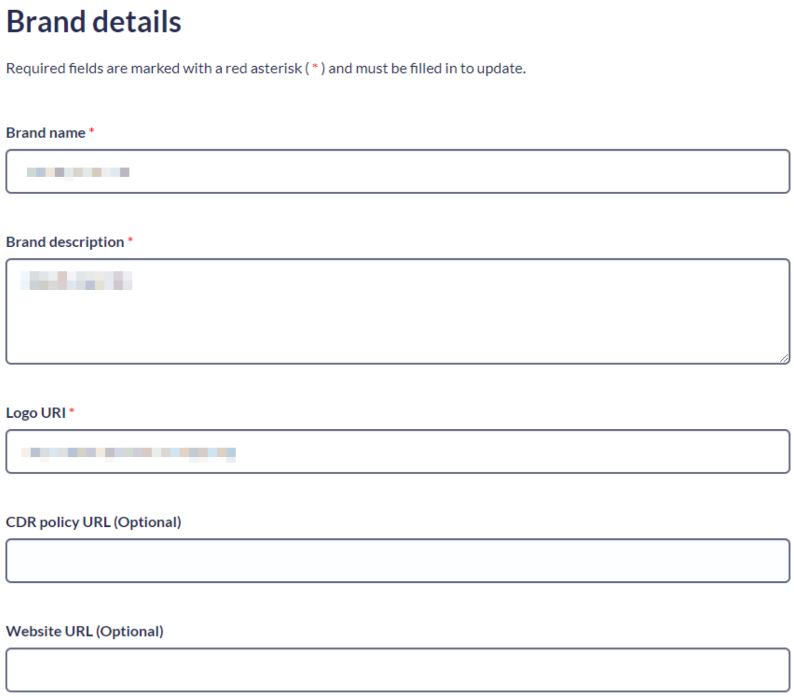
Logo URI *

[redacted]

CDR policy URL (Optional)

Website URL (Optional)

Figure 10: Data recipient brand details



Brand details

Required fields are marked with a red asterisk (*) and must be filled in to update.

Brand name *

[redacted]

Brand description *

[redacted]

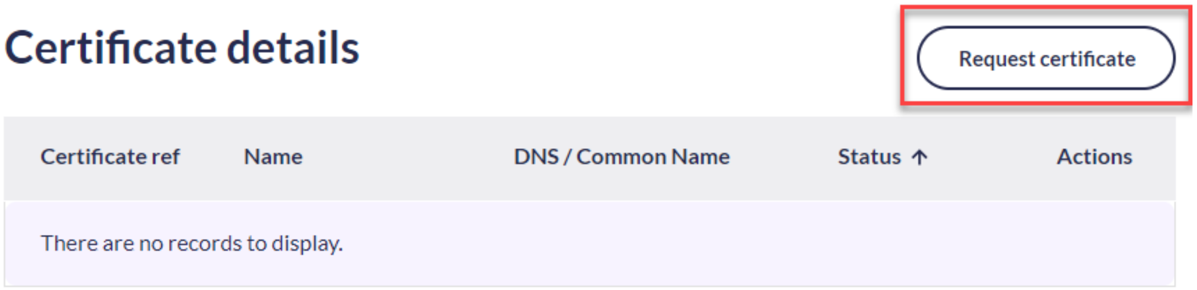
Logo URI *

[redacted]

CDR policy URL (Optional)

Website URL (Optional)

Figure 11: Data recipient production certificate details



Certificate details

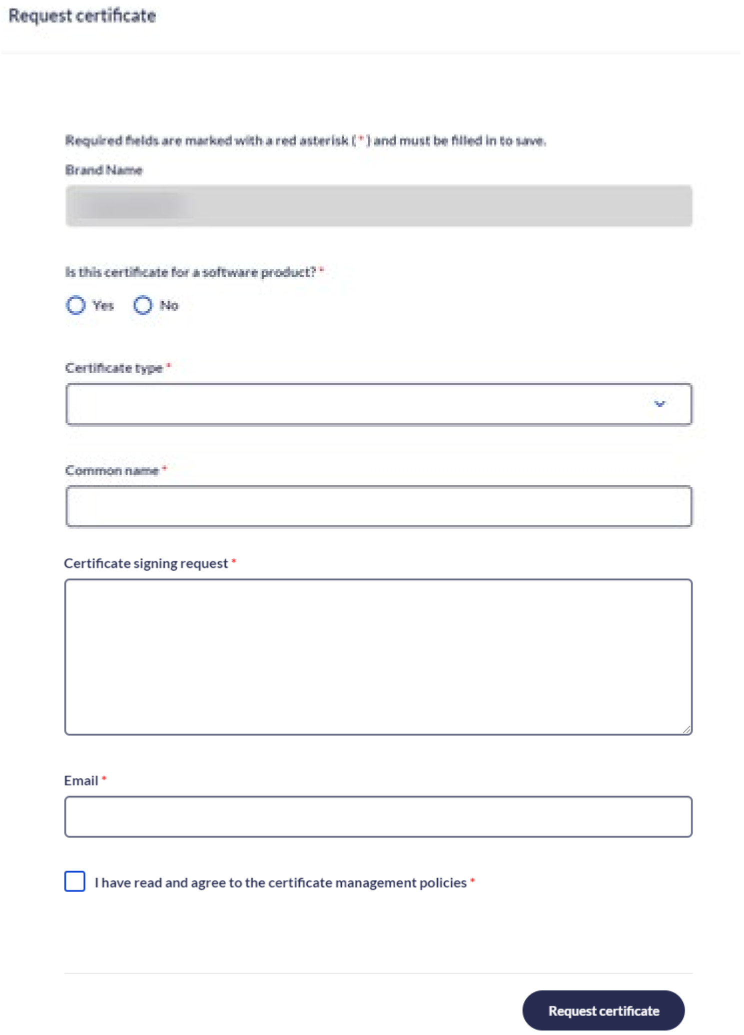
Request certificate

Certificate ref	Name	DNS / Common Name	Status ↑	Actions
There are no records to display.				

Figure 12: Data recipient request production certificate

! Note

Your CSR, generated in , needs to be included in this section. The production certificate cannot be generated without the CSR.



Request certificate

Required fields are marked with a red asterisk (*) and must be filled in to save.

Brand Name

[redacted]

Is this certificate for a software product? *

○ Yes ○ No

Certificate type *

Common name *

Certificate signing request *

Email *

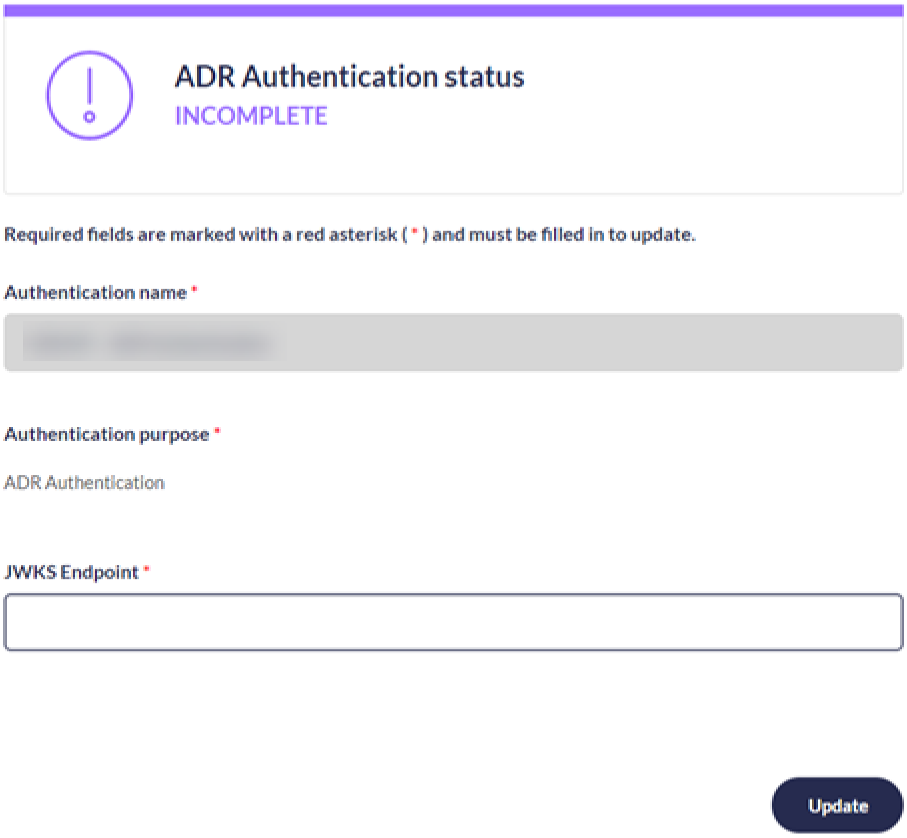
□ I have read and agree to the certificate management policies *

Request certificate

! Note

ACCC will now generate your production certificate and email to the contact specified in the production certificate request.

Figure 13: Data recipient authentication details



ADR Authentication status

INCOMPLETE

Required fields are marked with a red asterisk (*) and must be filled in to update.

Authentication name *

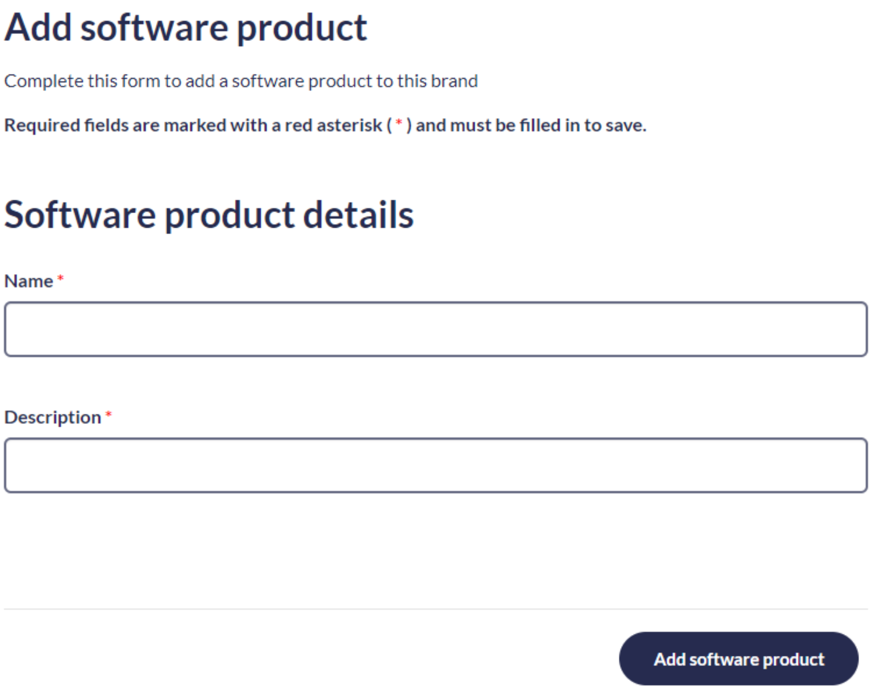
[redacted]

Authentication purpose *

ADR Authentication

JWKS Endpoint *

Figure 14: Data recipient software product details



Add software product

Complete this form to add a software product to this brand

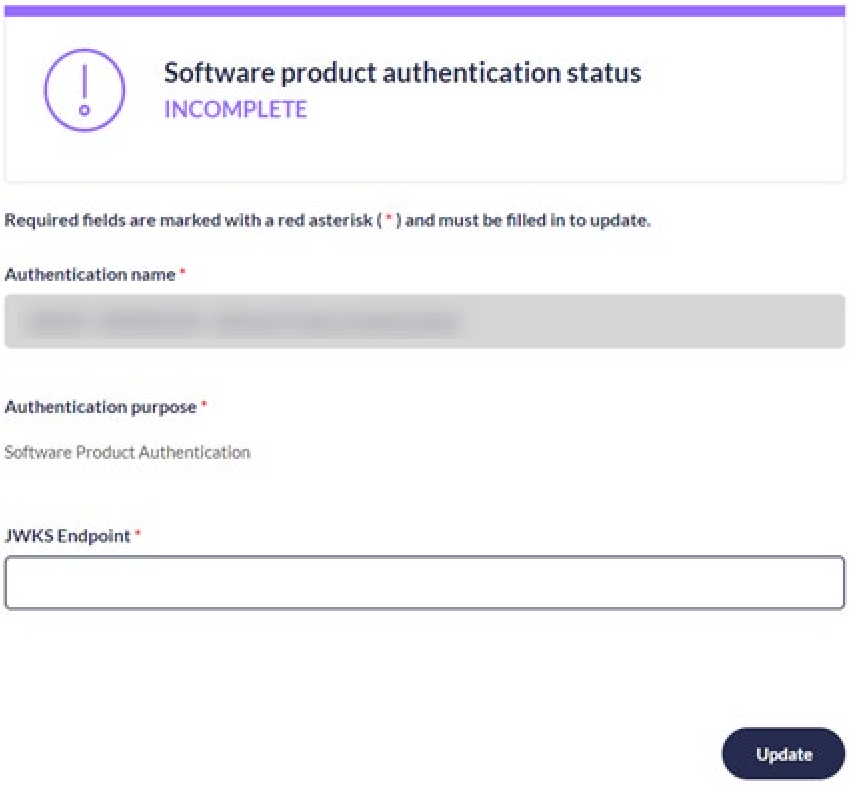
Required fields are marked with a red asterisk (*) and must be filled in to save.

Software product details

Name *

Description *

Figure 15: Data recipient software product authentication details



Software product authentication status

INCOMPLETE

Required fields are marked with a red asterisk (*) and must be filled in to update.

Authentication name *

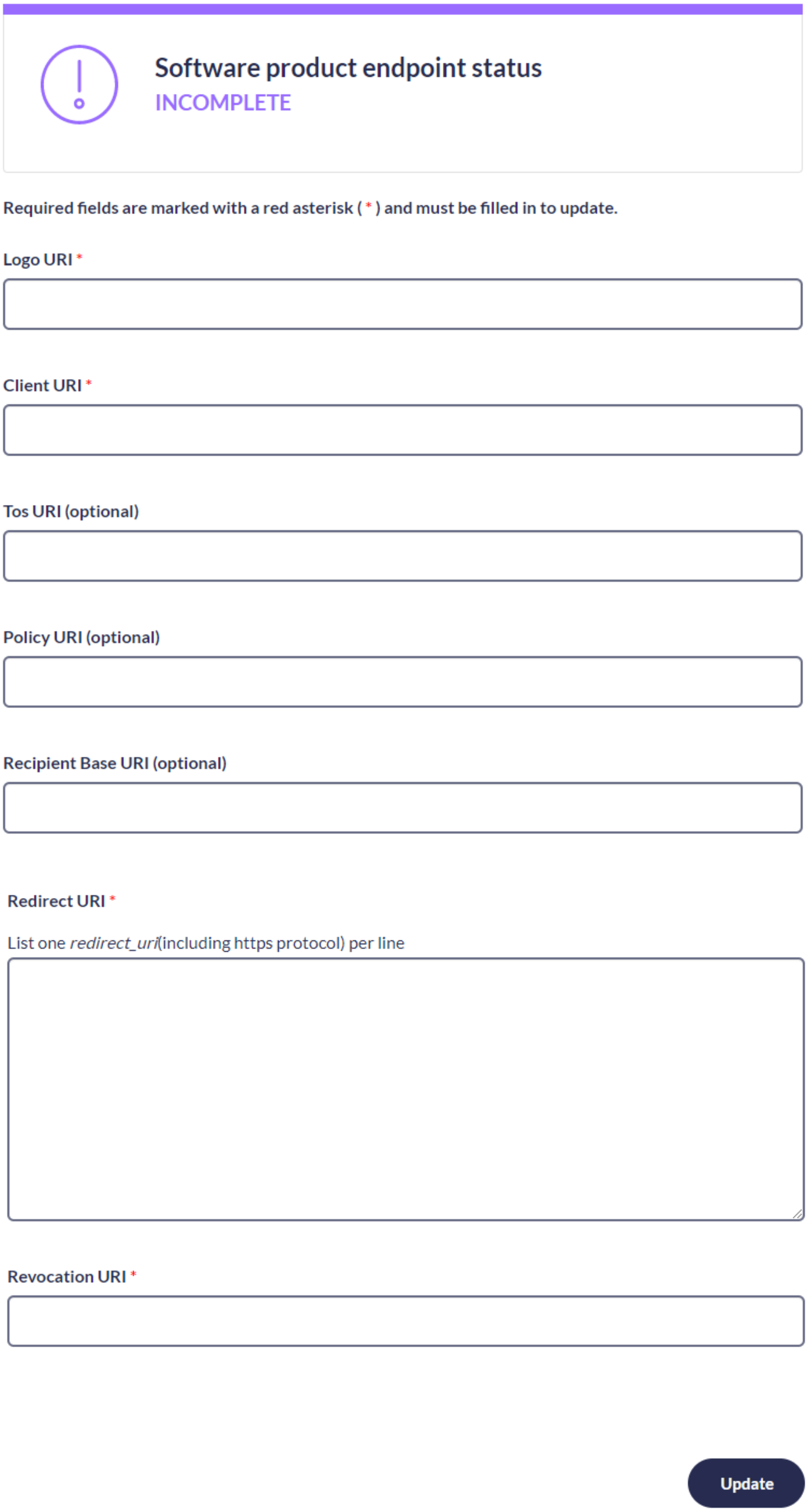
[redacted]

Authentication purpose *

Software Product Authentication

JWKS Endpoint *

Figure 16: Data recipient software product endpoint details



Software product endpoint status

INCOMPLETE

Required fields are marked with a red asterisk (*) and must be filled in to update.

Logo URI *

Client URI *

Tos URI (optional)

Policy URI (optional)

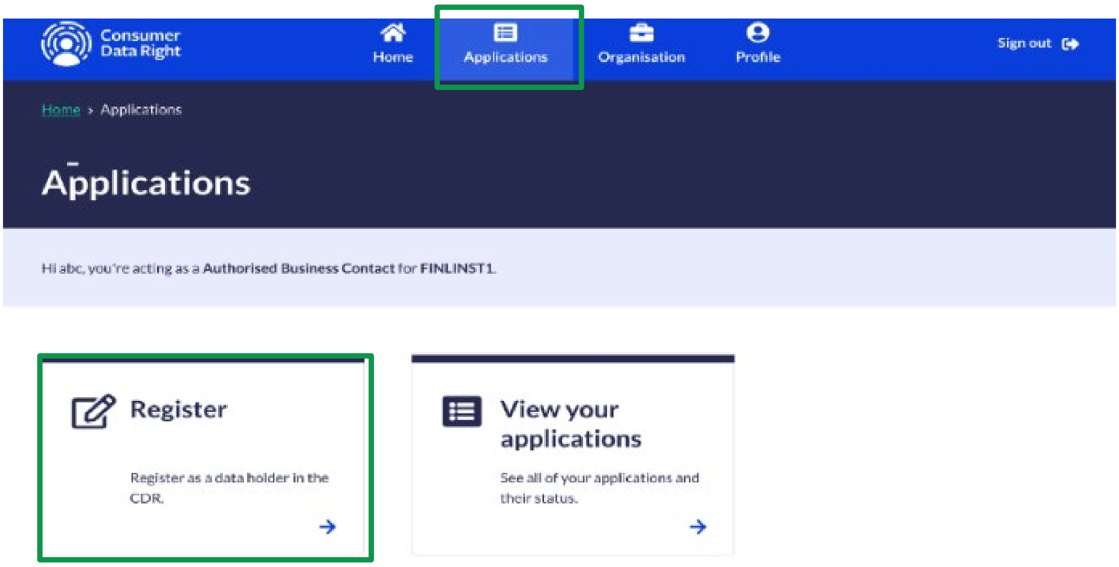
Recipient Base URI (optional)

Redirect URI *

List one *redirect_uri*(including https protocol) per line

Revocation URI *

Figure 17: Data holder registration (part 1)



Applications

Hi abc, you're acting as a **Authorised Business Contact** for **FINLINST1**.

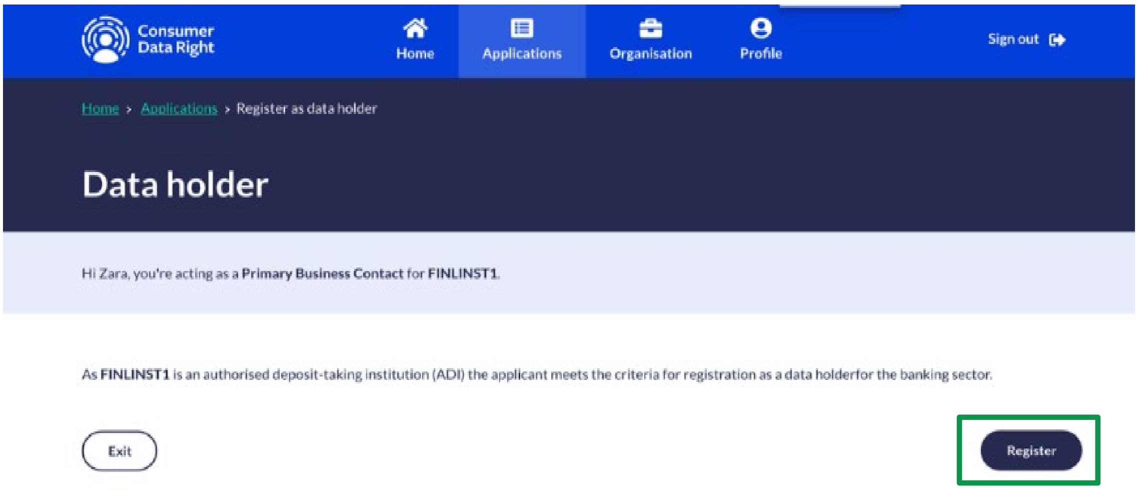
Register

Register as a data holder in the CDR.

View your applications

See all of your applications and their status.

Figure 18: Data holder registration (part 2)

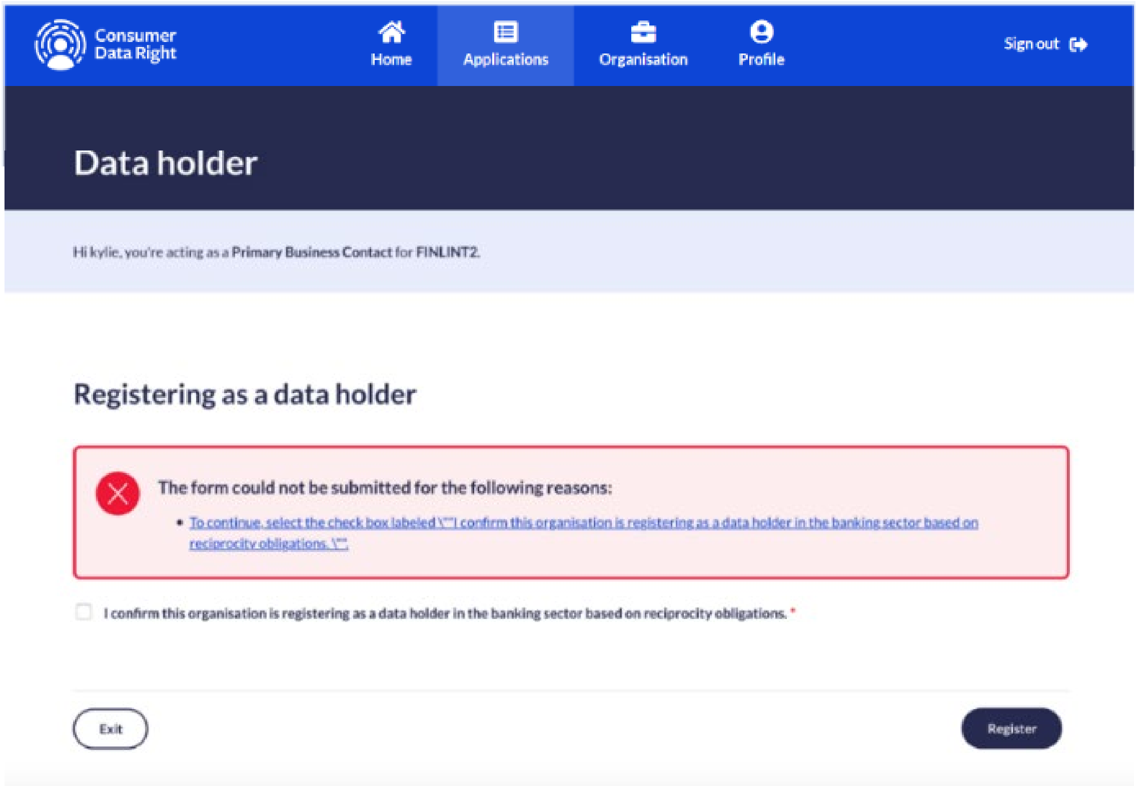


Data holder

Hi Zara, you're acting as a **Primary Business Contact** for **FINLINST1**.

As **FINLINST1** is an authorised deposit-taking institution (ADI) the applicant meets the criteria for registration as a data holderfor the banking sector.

Figure 19: Data holder registration as a non-ADI



Data holder

Hi kylie, you're acting as a **Primary Business Contact** for **FINLINT2**.

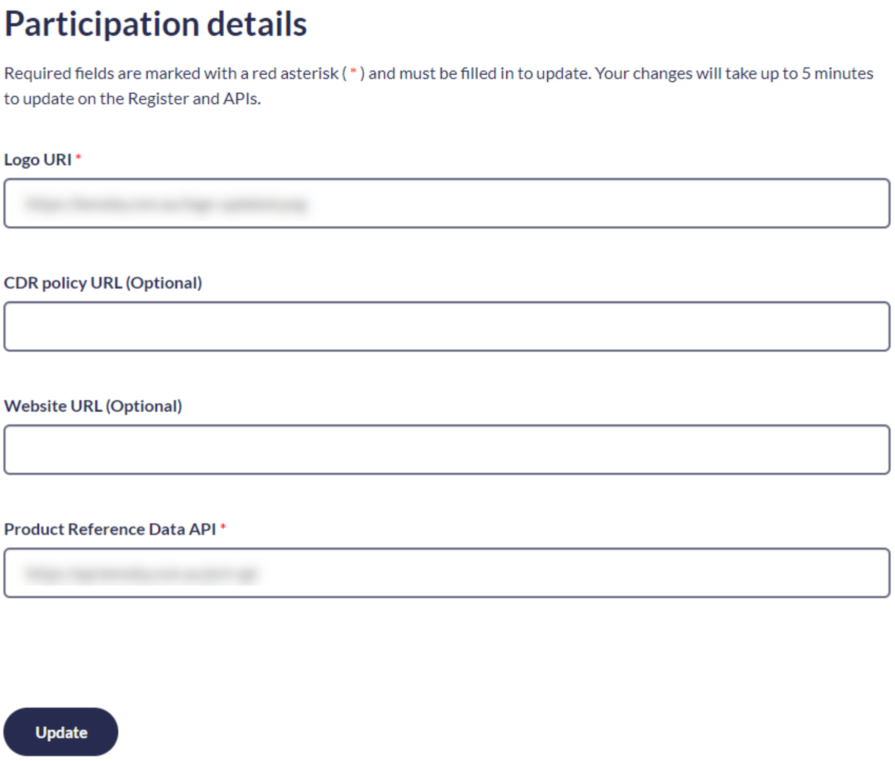
Registering as a data holder

The form could not be submitted for the following reasons:

- To continue, select the check box labeled \""I confirm this organisation is registering as a data holder in the banking sector based on reciprocity obligations. \"".

□ I confirm this organisation is registering as a data holder in the banking sector based on reciprocity obligations. *

Figure 18: Data holder participation details



Participation details

Required fields are marked with a red asterisk (*) and must be filled in to update. Your changes will take up to 5 minutes to update on the Register and APIs.

Logo URI *

[redacted]

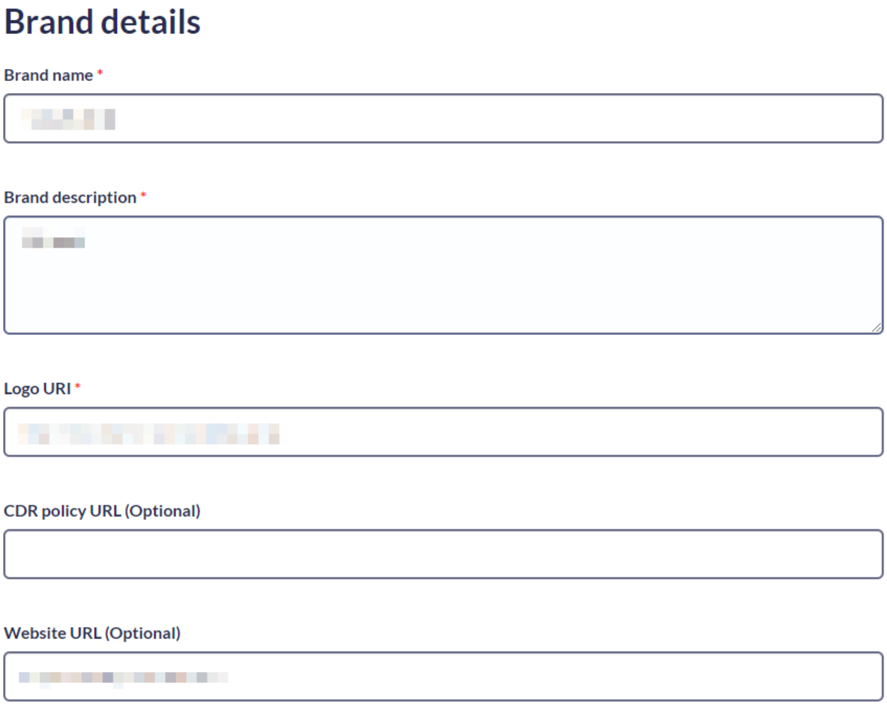
CDR policy URL (Optional)

Website URL (Optional)

Product Reference Data API *

[redacted]

Figure 19: Data holder brand details



Brand details

Brand name *

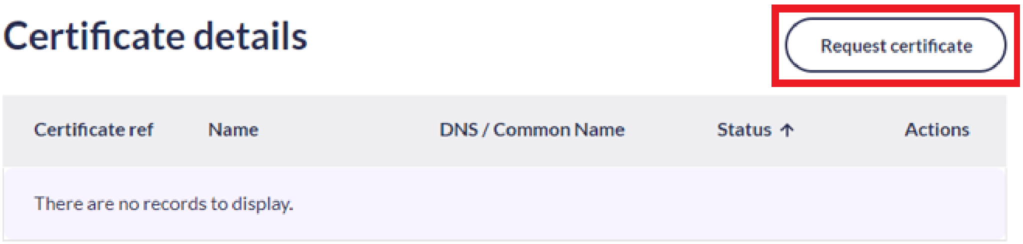
Brand description *

Logo URI *

CDR policy URL (Optional)

Website URL (Optional)

Figure 20: Data holder production certificate details



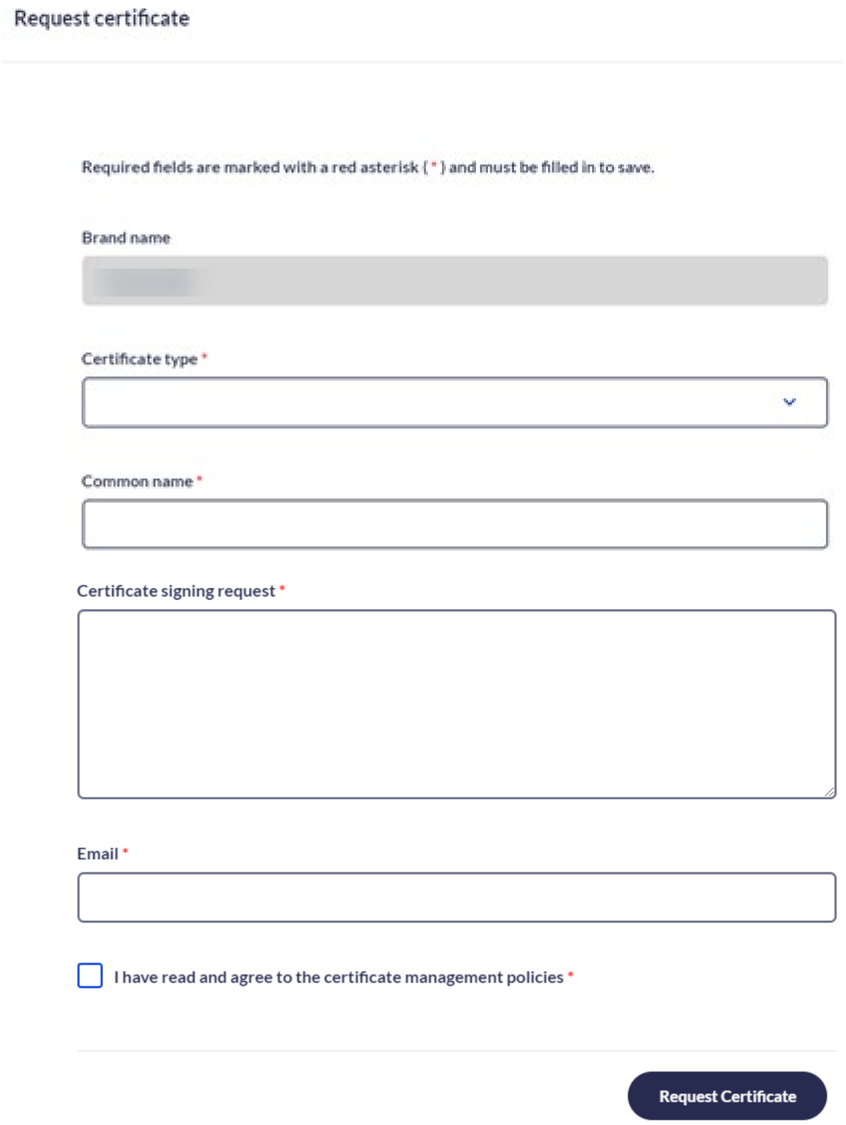
Certificate details

Certificate ref	Name	DNS / Common Name	Status ↑	Actions
There are no records to display.				

Figure 21: Data holder request production certificate

! Note

Your CSR, generated in , needs to be included in this section. The production certificate cannot be generated without the CSR.



Request certificate

Required fields are marked with a red asterisk (*) and must be filled in to save.

Brand name

Certificate type *

Common name *

Certificate signing request *

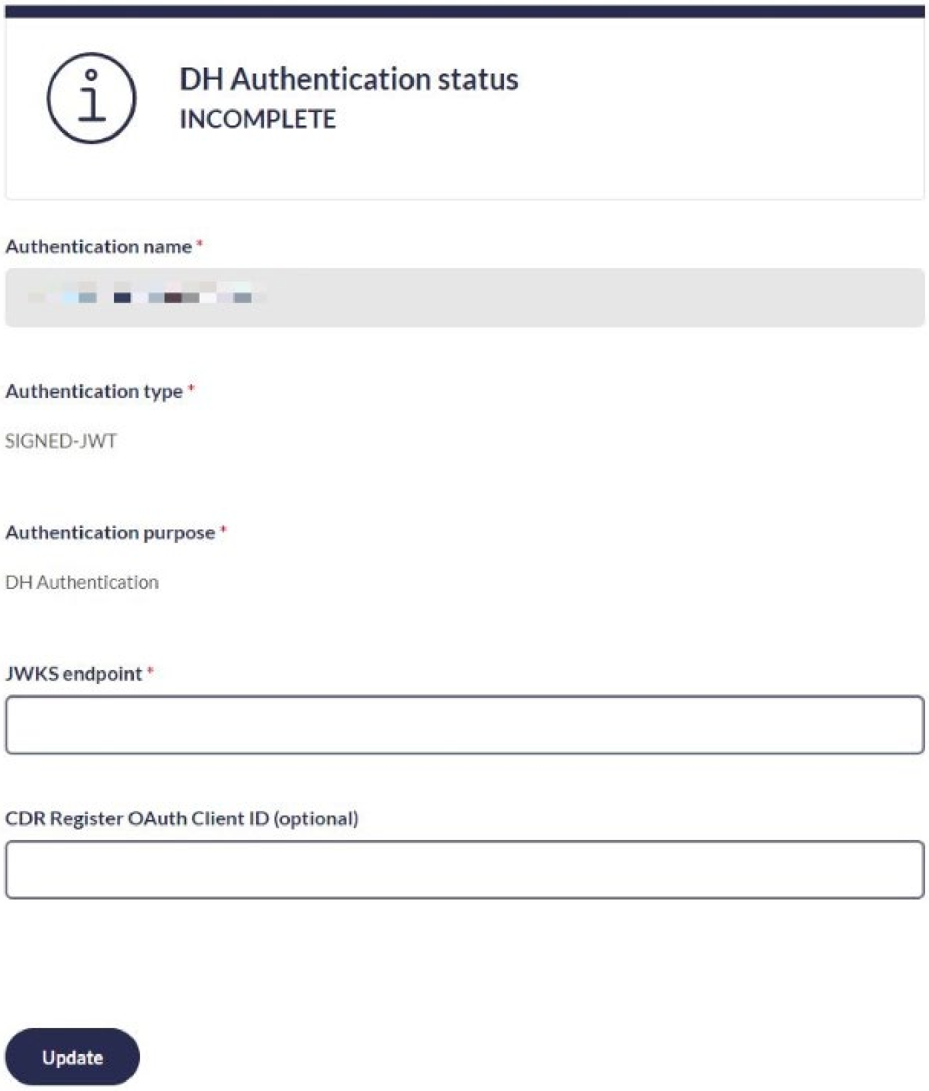
Email *

□ I have read and agree to the certificate management policies *

! Note

ACCC will now generate your production certificate and email to the contact specified in the production certificate request.

Figure 22: Data holder authentication details



DH Authentication status

INCOMPLETE

Authentication name *

[redacted]

Authentication type *

SIGNED-JWT

Authentication purpose *

DH Authentication

JWKS endpoint *

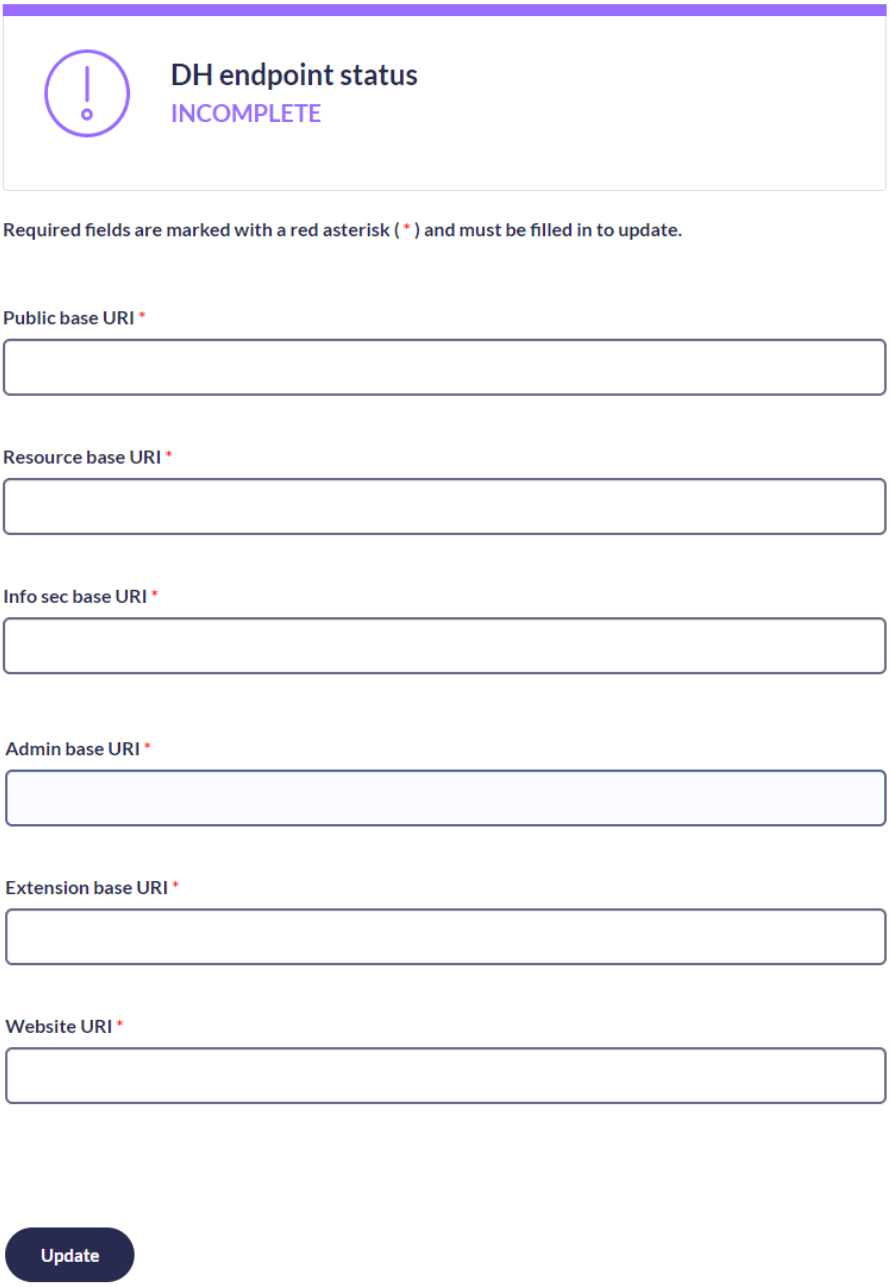
CDR Register OAuth Client ID (optional)

! Note

The CDR Register OAuth Client ID field should be used by Data Holders who have adopted the *private_key_jwt* client authentication mechanism at their admin endpoints.

This field is an alpha-numeric string (maximum 50 characters)

Figure 23: Data holder endpoint URIs



DH endpoint status

INCOMPLETE

Required fields are marked with a red asterisk (*) and must be filled in to update.

Public base URI *

Resource base URI *

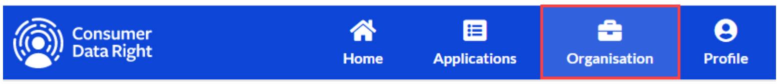
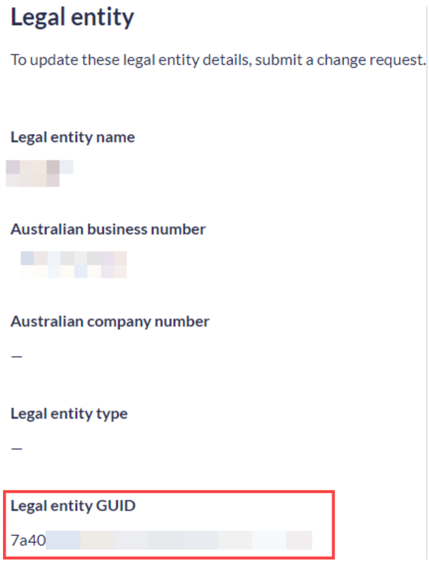
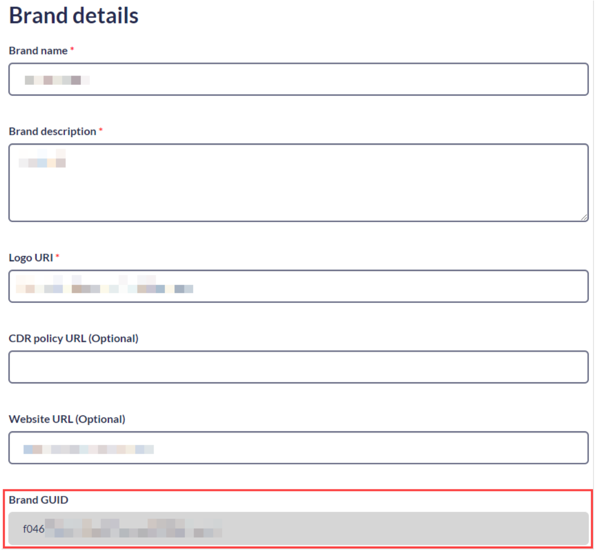
Info sec base URI *

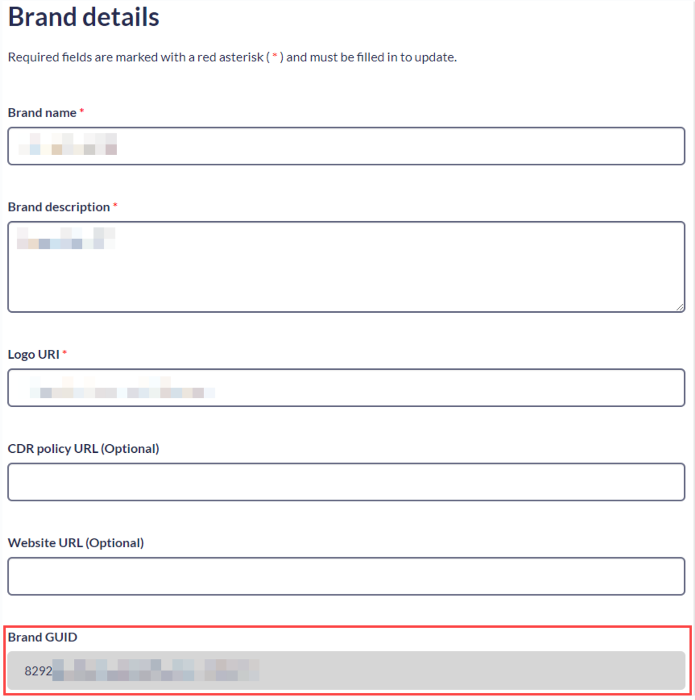
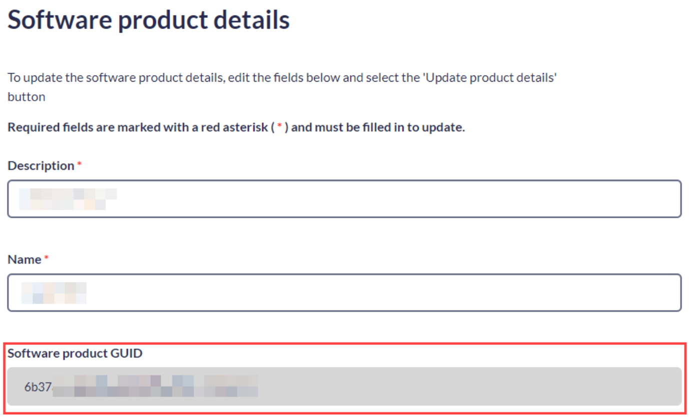
Admin base URI *

Extension base URI *

Website URI *

Appendix F: Identifiers

Identifier	CDR Participant Portal Discovery Location
legalEntityId	 Consumer Data Right Home Applications Organisation Profile  **Legal entity** To update these legal entity details, submit a change request. Legal entity name [redacted] Australian business number [redacted] Australian company number – Legal entity type – Legal entity GUID 7a40[redacted]
dataRecipientId	Equivalent to the legalEntityId described above
dataHolderBrandId	Organisation > DH Participation > Brand > Brand Details  **Brand details** Brand name * [redacted] Brand description * [redacted] Logo URI * [redacted] CDR policy URL (Optional) Website URL (Optional) [redacted] Brand GUID f046[redacted]
dataRecipientBrandId	Organisation > DR Participation > Brand > Brand Details

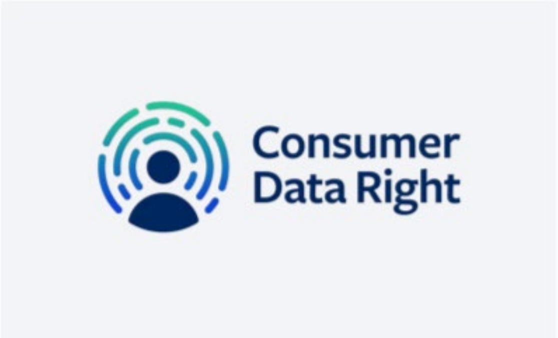
Identifier	CDR Participant Portal Discovery Location
	 Brand details Required fields are marked with a red asterisk (*) and must be filled in to update. Brand name * [redacted] Brand description * [redacted] Logo URI * [redacted] CDR policy URL (Optional) Website URL (Optional) Brand GUID 8292[redacted]
softwareProductId	Organisation > DR Participation > Brand > Software Product  Software product details To update the software product details, edit the fields below and select the 'Update product details' button **Required fields are marked with a red asterisk (*) and must be filled in to update.** Description * [redacted] Name * [redacted] Software product GUID 6b37[redacted]

Appendix G: CDR logo formats and styles

Table 7: CDR Logo Styles

The primary lockup consists of the logo mark and the wordmark. This lockup should be the favoured orientation whenever possible. Refer to the master assets for the source files.

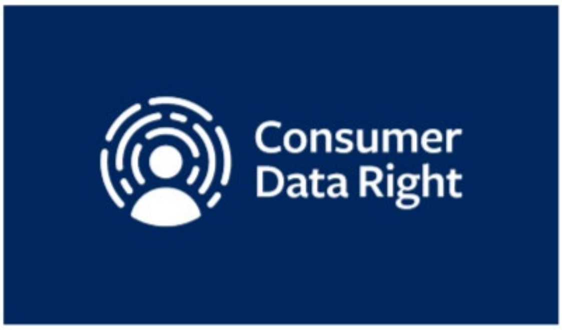
Coloured version (Primary logo)



Mono version:

White version

Only used when colours are not allowed or if used over a busy background



Mono version:

Black version

Only used when colours are not allowed or if used over a busy background

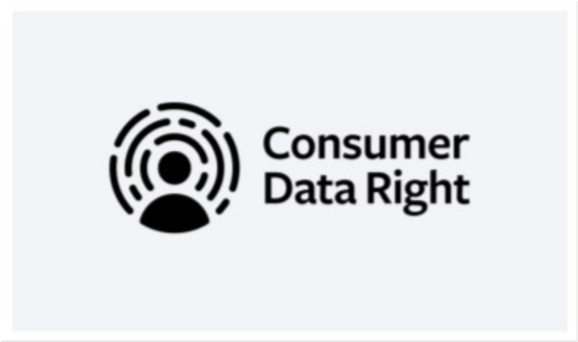


Table 8: CDR Logo Formats

File Format	Style	Colour Scheme	Width	Height
PNG	Monogram	Black	1413	1412
PNG	Monogram	Colour	1413	1412
PNG	Monogram	White	1412	1412
PNG	Primary	Black	3845	1396
PNG	Primary	Colour	3844	1396
PNG	Primary	White	3845	1396

File Format	Style	Colour Scheme	Width	Height
PNG	Short	Black	1413	2076
PNG	Short	Colour	1439	2137
PNG	Short	White	1412	2076
SVG	Monogram	Black	*Scalable*	
SVG	Monogram	Colour		
SVG	Monogram	White		
SVG	Primary	Black		
SVG	Primary	Colour		
SVG	Primary	White		
SVG	Short	Black		
SVG	Short	Colour		
SVG	Short	White		

Appendix H: Participant Contacts

The ACCC will have the need to communicate with your organisation from the point in time you commence on-boarding through to active participation for a number of reasons. Each **Communication purpose** tabled below explains who will be contacted and where contacts for your organisation can be maintained.

Communication Purpose	Contact	System Nominated/ Maintained in	Communication method	Comments
CDR ecosystem incidents	Agent licence	Service Management (Jira)	System notification (Jira) / Email / Phone	Where tickets have been raised by the participant alerting the ACCC to issues emerging in the ecosystem, from on-boarding commencement through to activation and ongoing participation.
CDR Logo - CDR Trademark Licence Agreement	Legal Authority Contact	CDR Participant Portal | User Guide	Email / Phone	The ACCC will make contact if the terms in the Licence Agreement change or if there are any other changes to the CDR Logo, from on-boarding commencement through to activation and ongoing participation. Refer Rule 5.12(1)(f)
Certificates (Agreements)	Legal Authority Contact	CDR Participant Portal | User Guide	Email / Phone	The ACCC will make contact if the terms in the Agreements change or if any other changes affect use of the certificates. This communication purpose excludes technical configuration of the certificates.
Certificates (Technical)	Primary IT Contact (PITC)	CDR Participant Portal | User Guide	Email / Phone	The ACCC will use this communication method to make contact with a Primary IT Contact for the purpose of support, or to request an action of the PITC as part of steps 7.5 and 7.9 of the on-boarding process and for PKI certificate renewals. The ACCC will not utilise this method to transfer sensitive certificate related information or data. Participant PITCs should utilise the CDR Participant Portal to action Certificate related requests.

Communication Purpose	Contact	System Nominated/ Maintained in	Communication method	Comments
Compliance and Enforcement	Primary Business Contact	CDR Participant Portal | User Guide	Letter / Email / Phone	Where there is a need for the ACCC CDR Compliance and Enforcement team to contact you about CDR compliance-related matters, from on-boarding commencement through to activation and ongoing participation.
Conformance Test Suite	Primary IT Contact	CDR Participant Portal | User Guide	Email / Phone	Communication likely from on-boarding commencement through to activation and ongoing participation.
Get Metrics	Primary IT Contact	CDR Participant Portal | User Guide	Email / Phone / Jira?	Where the ACCC experiences issues obtaining operational statistics from Data Holders when they are active in the CDR ecosystem, such as, unable to connect to the endpoints, identification of Data Quality issues etc.
On-boarding	Authorised Business Contacts / Authorised IT Contacts	CDR Participant Portal | User Guide	Email / Phone	Coordination of On-boarding and CTS activities through to activation on the CDR Register.
PRD Data Quality	Data Holder email address	CDR Participant Portal | User Guide	Email	This information is provided during on-boarding and appears in the 'email' field for the Data Holder once selected on the CDR Register find-a-provider page. Applies to all Data Holder Brands for a Data Holder.

Communication Purpose	Contact	System Nominated/ Maintained in	Communication method	Comments
Reporting	Primary Business Contact	CDR Participant Portal | User Guide	Letter / Email / Phone	Explore issues with reporting for purposes of rule 9.4, including data inaccuracy or anomalies emerging in analysis on data collected in the CDR ecosystem. Refer Rule 9.4
Temporary direction to refrain from Processing consumer data requests	Primary and Authorised Business Contacts; Primary and Authorised IT Contacts	CDR Participant Portal | User Guide	Trusted communications	This could stem from ecosystem wide issues such as a cyber-attack, major issues with participants platforms, unplanned and extended outages, data breaches etc. Refer Rule 5.34
Temporary restriction on use of Register (DH)	Primary and Authorised Business Contacts; Primary and Authorised IT Contacts	CDR Participant Portal | User Guide	Trusted communications	This could stem from ecosystem wide issues such as a cyber-attack, major issues with the platform, unplanned and extended outages etc. Refer Rule 5.33