

OFFICIAL



Participant on-boarding guide

Version 2
February 2025

Version Control		
December 2020	Version 1.0	First version of Guide.
March 2021	Version 1.2	Updated references to White label products
June 2021	Version 1.3	Update references to Participant Contacts
April 2023	Version 1.4	Updated link to the Certificate Management information, certificate agreements and policy documents. Screenshots of the CTS certificate section of the Participant Portal removed.
February 2025	Version 2	Updates to the on-boarding process and relevant screenshots throughout the guide. Updated references to White label products Updates to improve readability of guide.

Table of Contents

Table of Contents	1
1. What is on-boarding?	4
1.1. Overview	4
1.2. Context.....	4
1.3. Role of the Accreditation Registrar	4
1.4. Registering as a data holder	4
1.5. Become an accredited data recipient	5
2. Getting started checklist.....	6
3. Participant responsibilities	7
4. On-boarding process - High level overview.....	8
4.1. Overview of the on-boarding process.....	8
4.2. Indicative timeframe.....	9
5. On-boarding process - Step-by-step instructions	11
5.1. Step 1: Receive on-boarding information	11
5.2. Step 2: Acceptance of Public Key Infrastructure certificate agreements	11
Subscriber Agreement	11
Relying Party Agreement	12
Policy and Procedural Documents	12
Accepting the agreements.....	12
5.3. Step 3: Enter participation details.....	14
5.4. Step 4: Provide technical details of your test environment.....	19
Providing the details	19
5.5. Step 5: Generate certificate signing request for test PKI certificate.....	21
Generating a Certificate Signing Request (CSR)	21
5.6. Step 6: Confirm environment is configured and available for testing	22
5.7. Step 7: Complete CTS conformance testing	22
Executing CTS	22
CDR Service Management Portal (Jira).....	22
5.8. Step 8: Provide technical details of production environment.....	23
5.9. Step 9: Generate certificate signing request for a production certificate	24

Generating a Certificate Signing Request (CSR)	24
5.10. Step 10: Confirm production environment and readiness.....	24
Providing confirmation of readiness.....	24
5.11. Step 11: Activation on the Register and associated database.....	25
6. Participation	26
Appendix A: Testing guidance	27
Overview	27
Testing principles	27
Participant testing scope.....	27
Testing tools	28
Completion of testing	28
Appendix B: Getting help	29
CDR Support Portal.....	29
CDR website.....	29
CDR implementation call.....	29
Seeking assistance from the CDR Participant Engagement team.....	29
Appendix C: White label products	30
Appendix D: Use of the CDR logo.....	31
Confirming your intention to use the CDR Logo	31
Appendix E: Participant Contacts	35

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@acc.gov.au.

1. What is on-boarding?

1.1. Overview

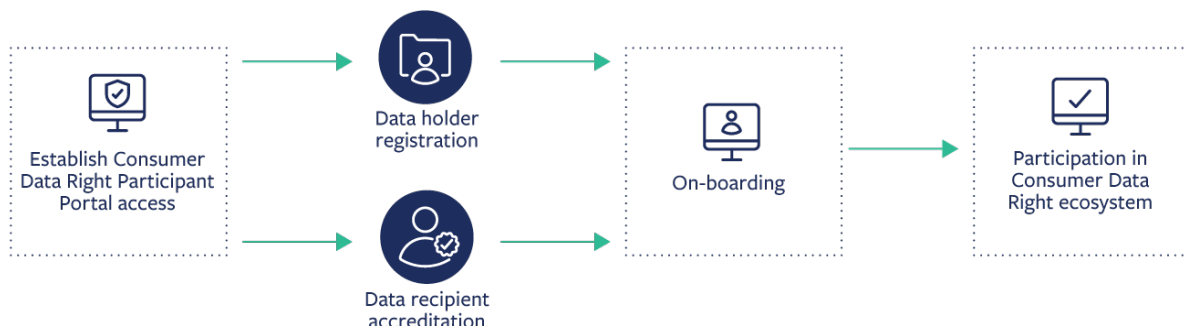
On-boarding is the process Consumer Data Right (CDR) participants undergo to commence active participation in the CDR ecosystem. The goal of the on-boarding process is to confidently introduce data holders, accredited data recipients and their additional brands and software products into the CDR ecosystem to ensure the security, integrity and stability of the Register of Accredited Persons (Register) and the associated database. In this guide we use the term participants to cover both data holders and accredited data recipients.

A more detailed overview of the on-boarding process can be found in section 4 & 5. This guide provides information for participants on technical, legal and testing requirements, and outlines the steps to be completed before the participant can be activated on the Register of Accredited Persons (the Register) and the associated database.

1.2. Context

The on-boarding process occurs after registration (for data holders) and accreditation (for accredited data recipients). Data holders and accredited data recipients must be on-boarded before they are able to participate in the CDR ecosystem, as depicted in Figure 1.

Figure 1: On-boarding context



1.3. Role of the Accreditation Registrar

The Australian Competition and Consumer Commission (ACCC), acting as the Accreditation Registrar (the Registrar), manages the on-boarding process. One of the ACCC's functions, as the Registrar, is to maintain the security, integrity and stability of the Register and associated database. It can issue requests to accredited data recipients and data holders to provide information or to do specified things to fulfil its functions. It must publish certain information about accredited data recipients and data holders, and it may include in the associated database other information that it considers is required for accredited data recipients and data holders to process requests in accordance with the [Competition and Consumer \(Consumer Data Right\) Rules 2020](#) (CDR Rules) and Consumer Data Standards (the Standards).

1.4. Registering as a data holder

You should initiate the data holder registration process via the [CDR Participant Portal](#) (the Participant Portal) if you are obligated to become a data holder as defined in section 56AJ of the *Competition and Consumer Act 2010* (CCA). Please refer to the [CDR Participant](#)

[Portal user guide](#) for guidance on this step. Note that you will have to request access to the Participant Portal before you can register as a data holder.

1.5. Become an accredited data recipient

Please refer to the “[Become an accredited data recipient](#)” page on the CDR website and the [Accreditation Guidelines](#) for information about seeking accreditation to be a data recipient.

2. Getting started checklist

There are several pre-requisites to be completed before you can start on-boarding to the ecosystem. It is highly recommended that you read this section to ensure you are prepared to commence on-boarding.

Table 2: Getting started checklist

Pre-requisites	Completed
<p>Access to the Participant Portal</p> <p>The legal entity must be granted access to the CDR Participant Portal (the Participant Portal) and all appropriate users from your organisation must be delegated access, including the Primary IT Contact / Authorised IT Contacts who have the ability to provide technical information regarding your technology solution.</p> <p>If your Participant Portal access is not yet complete, consult the CDR Participant Portal User Guide for more information on how to do this.</p>	<input type="checkbox"/>
<p>Accreditation or registration</p> <p>The legal entity needs to be accredited to be on-boarded to the CDR as a data recipient</p> <p>If you have not yet applied for accreditation, you can find out how to become an accredited data recipient and refer to the Accreditation guidelines.</p> <p>-or-</p> <p>The legal entity needs to be registered as a data holder to be on-boarded to the CDR as a data holder.</p> <p>If you have not yet applied for registration, register via the Participant Portal.</p>	<input type="checkbox"/>
<p>Identifying a Legal Authority Contact</p> <p>A duly authorised representative (Legal Authority Contact), who has the authority to sign and accept the required agreements on behalf of the legal entity, needs to be identified.</p> <p>The details of the Legal Authority Contact should be entered into the Participant Portal. See the CDR Participant Portal User Guide for more information.</p>	<input type="checkbox"/>
<p>White Label Products</p> <p>Consult Appendix C: White label products for consideration if one of the white labelling scenarios applied to you.</p>	<input type="checkbox"/>

3. Participant responsibilities

The participant is responsible for a variety of activities regarding the development, release and support of their solution in order to be successfully on-boarded to the CDR ecosystem, including (but not limited to):

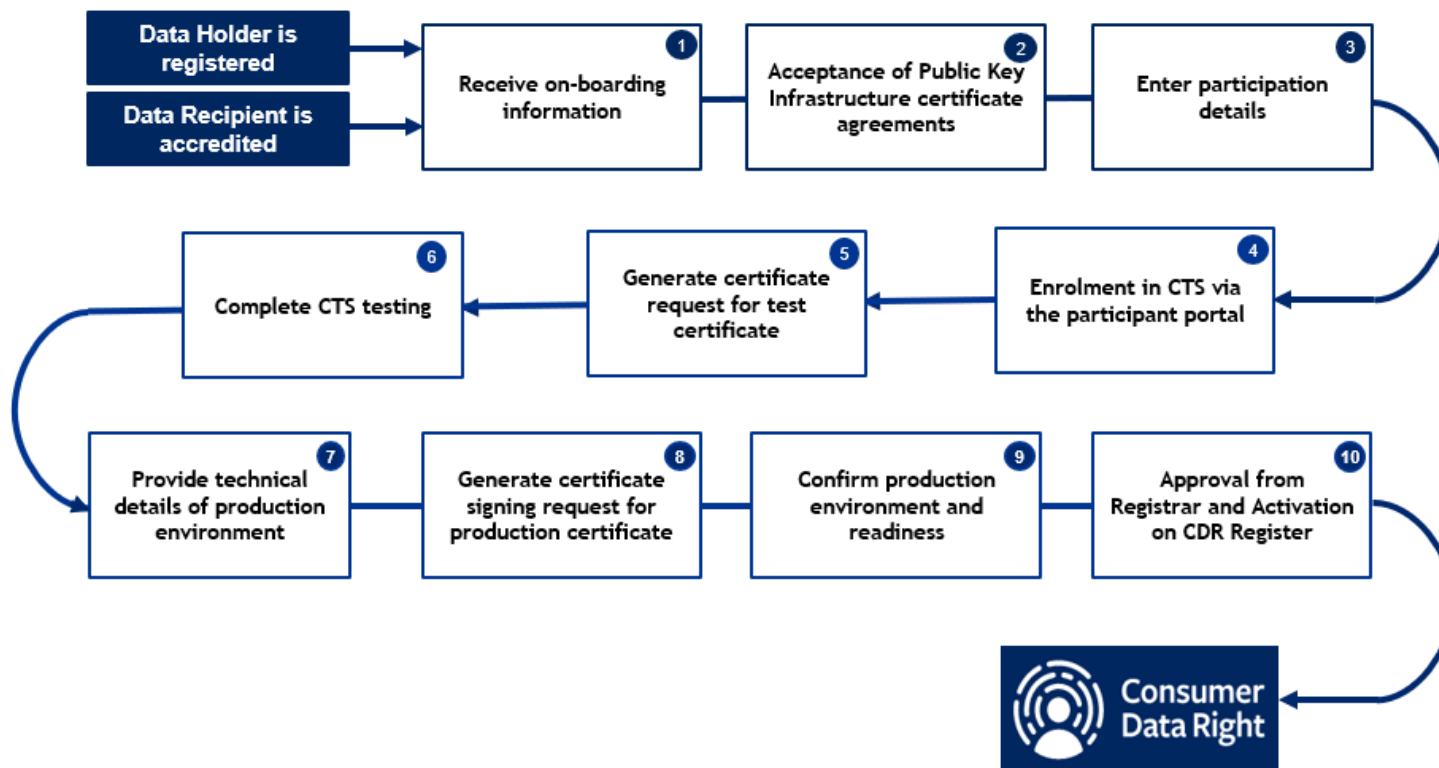
- putting in place infrastructure operations and IT services/support procedures
- setting up the participant's production environment and the environment the participant wants to test in
- training of the participant's technical users (e.g., to perform back-up, code migration, or technical verifications)
- 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 A: 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 CCA, the CDR Rules and the Standards).

4. On-boarding process - High level overview

4.1. 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 the on-boarding process



4.2. Indicative timeframe

The length of time it takes to complete the on-boarding steps will vary based on participant circumstances and completion of the on-boarding steps. Table 3 outlines indicative timings for each step in the process.

Table 3: Indicative timeframe

#	Step	Participant	ACCC
1	Receive on-boarding information	N/A	1-3 business days Once a participant is accredited or registered on the CDR portal, the ACCC will send on-boarding information to the relevant participant contacts.
2	Acceptance of Public Key Infrastructure certificate agreements	1-5 business days Dependent on the participant's legal review and acceptance processes	N/A
3	Enter participation details	1-5 business days Dependent on whether the participant has participation information at the ready	N/A
4	Enrolment in CTS via the participant portal	1-14 business days Dependent on the readiness of the participant's testing environment and the availability of the technical information	N/A
5	Generate certificate signing request for test certificate	1 business day Dependent on the participant's certificate management processes	1 business day Upon successful certificate signing request submission, test certificate will be provided on the same day
6	Complete CTS testing	1-30 business days Dependent of the maturity, readiness and conformance of the participant's solution, as well as the ability to troubleshoot and resolve issues if and when they occur	1-30 business days The ACCC will support the participant through CTS execution

OFFICIAL

#	Step	Participant	ACCC
7	Provide technical details of production environment	1-5 business days Dependent on the readiness of the participant's technical information	N/A
8	Generate certificate signing request for production certificate	1-5 business days Dependent on the participant's certificate management processes	3-5 business days Once the correct information is received, the ACCC will review and provision the production certificate.
9	Confirm production environment and readiness	1-14 business days Dependent on the participant's change/release management practices as the solution needs to be configured with the Register of Accredited Persons and the associated database details and production certificate installed	N/A
10	Approval from the Registrar and Activation on Register of Accredited Persons or associated database	N/A	5-14 business days Dependent on details provided by the participant as appropriate and sufficient for Registrar approval and to pass required technical assessments.
Indicative Total Timeframe		3 weeks - 5 months	

5. 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.

! 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 in the ecosystem. These steps may occur in the order specified in this guide, however certain steps may be done at other times (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.

5.1. Step 1: Receive on-boarding information

After you are granted accreditation (data recipient) or registration (data holder), your primary business contact will receive an email from the Participant Engagement team detailing information about the on-boarding process.

If you do not receive this email, please contact CDROnboarding@accc.gov.au

5.2. 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 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 security, integrity and stability of the Register and associated database, as well as 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

OFFICIAL

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 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](#), which defines the overarching framework for management and administration of the ACCC PKI.
- The [Certification Practice Statement](#), 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.

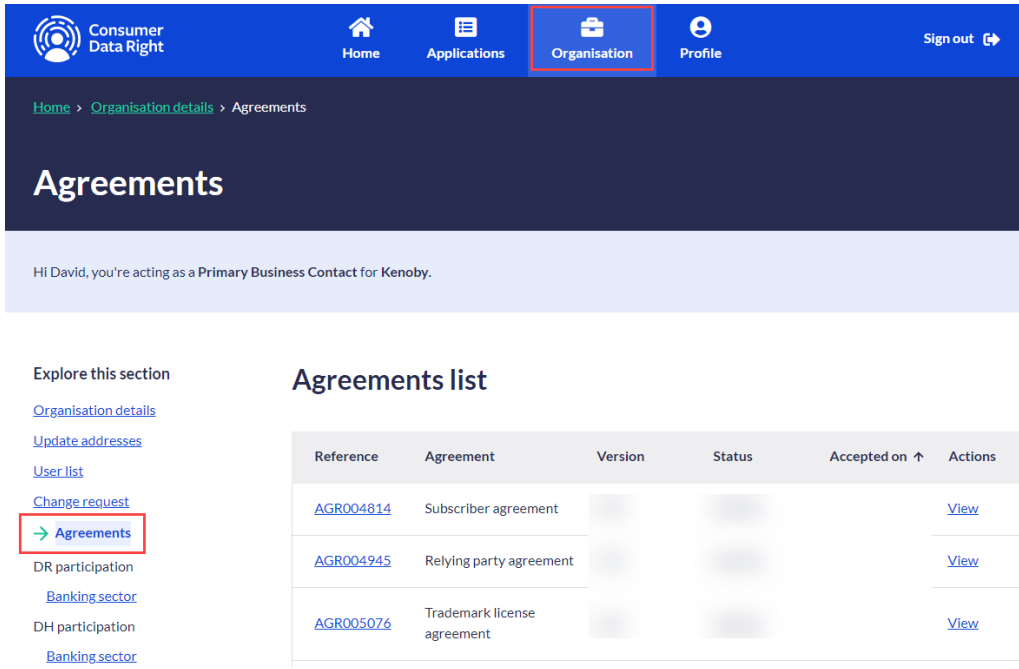
! Note

You must have the legal authority contact role in the CDR Participant Portal to accept these agreements.

Accepting the agreements

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

Figure 3: Agreements list



- 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.

Figure 4: Relying Party agreement

Relying party 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 checkboxes and press the Accept button.

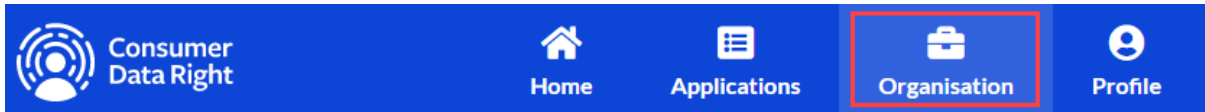
- When you return to the Agreements list the agreement should now be shown as Agreed.

! Note

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

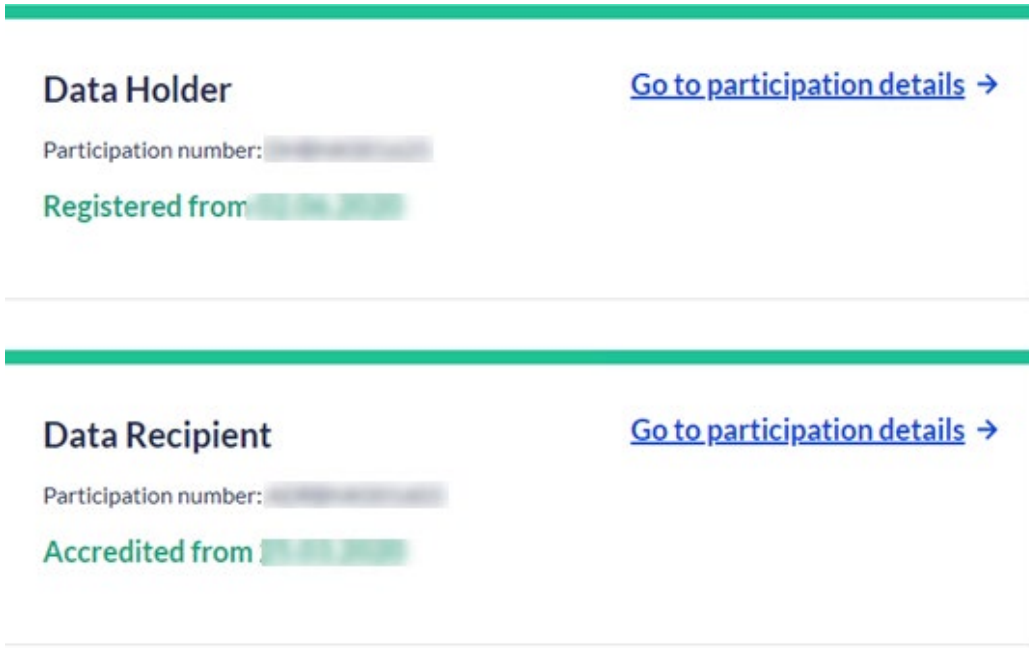
5.3. Step 3: Enter participation details

- Login to the [CDR Participant Portal](#) and navigate to your Organisation record.



- You should be able to see your participation status (data holder and/or data recipient), as shown in Figure 5.

Figure 5 Data recipient and data holder status in CDR Participant Portal



For data holders:

- Based on your data holder participation status, enter details as listed in Table 4 below.
- Screenshots are provided below to assist with entry of this information. Consult the [CDR Participant Portal User Guide](#) for additional guidance, if needed.

Table 4: Data holder participation details

Section	Field name
Legal entity details - see Figure 6	Legal entity website URL
	Legal entity logo URI
	Legal entity CDR policy URL
Brand details - see Figure 7	Brand name
	Brand description
	Brand type
Brand details - see Figure 8	Participation type
	Logo URL
	Website URL
	CDR policy URL

Figure 6: Data holder participation details

Legal entity website URL *

Legal entity logo URI *

Legal entity CDR policy URL

[Update legal entity details](#)

Figure 7: Brand details

Brand name *
Provide the name by which you are known to your consumers (brand name), for example 'Smarty Money'.

Brand description *
Provide an elevator statement for your brand, for example 'Smarty Money offers products to help customers organise their money, tracking expenses, subscriptions and payments'.

Brand type *

[← Back](#) [Save](#)

Figure 8: Brand participation details

Brand participation details

Participation type *

Logo URI *

Website URL *

CDR policy URL *

← Back Add participation

For accredited data recipients:

Based on your data recipient participation status, enter details as listed in [5](#) 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](#) for additional guidance, if needed.

Table 5: Data recipient participation details

Section	Field name
Brand participation details - see <i>Figure 9</i>	Participation type
	Logo URI
	Website URL
	CDR policy URL
Brand details - see <i>Figure 10</i>	Brand name
	Brand description
	Brand type
Software product details - see <i>Figure 11</i>	Name
	Description

Figure 9: Data recipient participation details

Participation type *

Logo URI *

Website URL *

CDR policy URL *

[← Back](#) [Add participation](#)

Figure 10: Data recipient brand details

Add new brand

Brand name *

Provide the name by which you are known to your consumers (brand name), for example 'Smarty Money'.

Brand description *

Provide an elevator statement for your brand, for example 'Smarty Money offers products to help customers organise their money, tracking expenses, subscriptions and payments'.

Brand type *

[← Back](#) [Save](#)

Figure 11: Data recipient software product details

Software product details

Name *

If the software product is used in a CDR representative arrangement, please include the full name of the CDR representative. A brand name can also be included in this software product name, for example 'Financial Services Company Pty Ltd (Smarty Money)'.

Description *

Describe the features or benefits of the software product with reference to how the CDR data will be used, for example 'Smarty Money's expense manager uses CDR data to allow you to see all your balances in one application!'

Add software product

! Note

NAMING CONVENTION - for data recipient software products with existing CDR representative arrangements.

All data recipient software products registered in the CDR participant portal must include the full name of the CDR representative to establish a clear link for the users of the Register and associated database, including consumers, between the representative arrangement and the relevant software product. This is an important component of the Register's and associated database's integrity.

There is some flexibility when the naming the software to include additional information. For example, the product could be listed as CDR Representative Name (Brand Name), or Brand Name (CDR Representative Name). This way both the CDR Representative name and their consumer facing branding can be identified in the software product name.

5.4. Step 4: Provide technical details of your test environment

To be able to conduct conformance testing via the Conformance Test Suite (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

- The CTS enrolment form will be available in the Participant Portal to the primary business contact, primary IT contact and authorised IT contact role. This can be completed after the acceptance of the PKI certificates.
 - For a data holder, the CTS enrolment form location is as follows: “Participation” > “Data Holder” > “Brand” > “View Brand” > “View Brand Participation” > “CTS Details” > then “CTS Enrolment”.
 - For a data recipient, the CTS enrolment form location is as follows: “Participation” > “Data Recipient” > “Brand” > “View Brand” > “View Brand Participation” > “Software Product” > “CTS Details” > then “CTS Enrolment”.
- In this form, you will also need to nominate an authorised CTS tester who must have a valid Participant Portal user account.
- The CTS enrolment form can be amended in the Participant Portal directly by the primary business contact, primary IT contact and authorised IT contact before submission is completed.
- If an adjustment to the CTS enrolment form data is required after submission, contact the Technical Operations team via CDRTechnicalOperations@accc.gov.au.
- After completion of the CTS enrolment form, you will be able to generate the CTS PKI certificates, add CTS authentication details and CTS endpoint URIs for testing (see *figure 12*).

Figure 12: CTS Technical Details

CTS Enrolment Start CTS enrolment

Participation Type ↑	Status	Date submitted	Submitted by	Actions
There are no records to display				

CTS Certificates Request a CTS certificate

Certificate ref ↑	Common name	Status	Expiry date	Actions
There are no certificates to display				

CTS Authentication details

Name ↑	Status	Purpose	Actions
There are no authentication details to display			

CTS Endpoints

Name ↑	Status	Actions
There are no endpoints to display		

- After successful submission of the CTS enrolment form, your CTS conformance ID will be displayed on screen and sent to the primary business contact by email. You will need to configure this in your software solution to access the CTS APIs. Further technical information can be found in the guidance documents located at [Conformance Test Suite: version history and scenarios](#).

! Note

If your technical details change at any point 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.

5.5. Step 5: Generate certificate signing request for test PKI certificate

The primary business contact, primary IT contact and authorised IT contact of a data holder and data recipient can maintain their CTS certificates on the Participant Portal.

Generating a Certificate Signing Request (CSR)

- The participant should follow their internal processes and procedures for generating a CSR and the management of certificates.

While generating the certificate signing request please refer to the [Certificate Management - Consumer Data Standards](#)

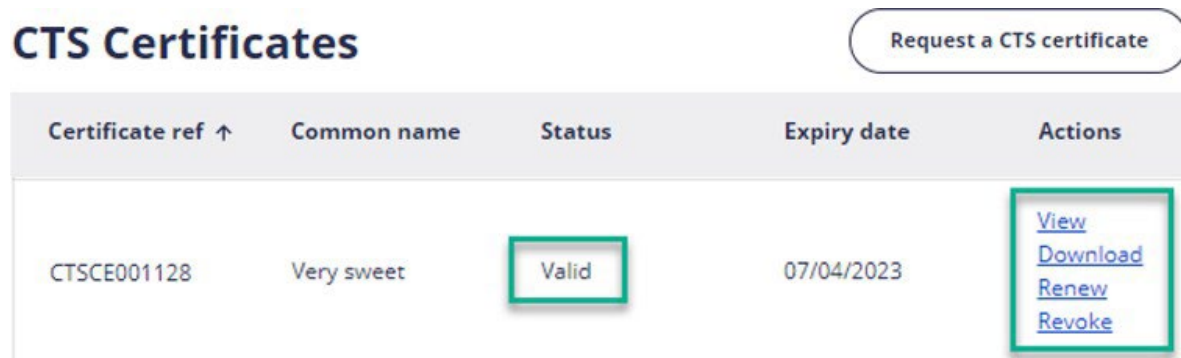
Accredited data recipients and data holders will receive notifications on the outcome of the CTS certificate request. An email advising the outcome (either an approval or rejection) will be sent to the participant email associated with the request and next steps for action.

Upon successful request submission, an approval success page will be displayed with a CTS certificate Download hyperlink and a button to return to an updated CTS Details page.

The email address specified while requesting the CTS PKI certificate will receive the certificate. Alternatively you may download the certificate later via the “CTS Certificates” section in the CDR Participant Portal. The root and intermediate certificate chain for the generated CTS Certificate can be found in the [CTS connection data sheets](#).

The CTS Details page is updated to show the certificate status as valid and provide actions to view, download, revoke and renew the CTS certificate. The option to renew a certificate will only be available 30 days before a valid certificate’s expiry date.

Figure 13: Request a CTS certificate



The screenshot shows the 'CTS Certificates' section of a web interface. At the top right, there is a button labeled 'Request a CTS certificate'. Below it is a table with the following columns: 'Certificate ref ↑', 'Common name', 'Status', 'Expiry date', and 'Actions'. A single row is visible with the following data: 'CTSCE001128', 'Very sweet', 'Valid', '07/04/2023', and a list of actions: 'View', 'Download', 'Renew', and 'Revoke'. The 'Valid' status and the 'View' action are highlighted with a green box.

Certificate ref ↑	Common name	Status	Expiry date	Actions
CTSCE001128	Very sweet	Valid	07/04/2023	View Download Renew Revoke

Data holders and accredited data recipients can view current and historical CTS certificates from the Participant Portal by selecting View from the Actions column.

Viewing the CTS Certificate will provide details of the CTS Certificate and provide certificate installation instructions.

5.6. Step 6: Confirm environment is configured and available for testing

Your test environment needs to be configured to allow communication with CTS. Please refer to the [CTS connection data sheet](#) for more information. Infrastructure changes, such as firewall rules or IP whitelisting, may need to be performed based on this information.

Your CTS certificate now needs to be installed into your infrastructure environment to enable secure communication with CTS.

Once your environment has been configured and is ready for testing, send an email to CDROnboarding@acc.gov.au titled **Commence CTS testing - [legal entity name]** to confirm your readiness for CTS conformance testing. We will then assign you a test plan for completion.

Consult the [CTS guidance material](#) for more information about conformance testing with CTS.

5.7. 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 data recipient and data holder 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 [Participant conformance approach](#) for further information.

The primary purpose of the CTS is to test the interactions of the solution against the Register and the associated database interactions, utilising simulated implementations of accredited data recipients and data holders, as well as a mock Register and the associated database.

Executing CTS

- You will be able to see your progress and results either:
 - through the CTS web portal; or
 - by contacting the Participant Engagement team on CDROnboarding@acc.gov.au and requesting a CTS report.

CDR Service Management Portal (Jira)

The CDR Service Management Portal (Jira) is available to raise tickets for issues encountered while conducting CTS testing and once active in the CDR ecosystem. After activation in the CDR ecosystem you will also be able to see tickets raised from other participants and the ACCC.

Please note you can only have 5 customer and 2 agent licences. Reach out to the Participant Engagement team to inform who you would like to add as agents and customers (with their names and emails) and the team will organise your access.

Figure 14: CDR Service Management Portal

Role Type	Description
Customer	Has restricted access that allows this role to raise new incidents and service requests, view and comment on incidents that are shared with them.
Agent	Can access queues, raise and process incidents and service requests (i.e. move incidents through workflows, reassign incidents to other teams and make customer-facing comments).

Please refer to [CDR Service Management portal user guide](#) for Participants, which contains useful information on how to raise tickets and extra tips.

Please refer to this [article](#) for information on how to get access to the CDR Service Management Portal.

5.8. Step 8: Provide technical details of production environment

Technical details required for your production environment, similar to those provided for your testing environment in 5.3, are added via the Participant Portal.

Some of these details have previously been entered as part of the processes described in 5.3. 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 business contact, primary IT contact or authorised IT contact to request a PKI certificate, maintain authentication details, maintain software products and maintain endpoints.

Consult the [CDR Participant Portal User Guide](#) for guidance on this step

- Accredited data recipients must provide the ACCC with:
 - Participation details
 - Brand details
 - Certificate request
 - Authentication details
 - Software product details
 - Software product authentication details
 - Software product endpoints
- Data holders must provide the ACCC with:
 - Registration details
 - Registration details for non-ADIs
 - Participation details

- Brand details
- Certificate request
- Authentication details
- Endpoints

5.9. Step 9: Generate certificate signing request for a production certificate

Generating a Certificate Signing Request (CSR)

- The participant should follow their internal processes and procedures for generating a CSR and the management of certificates.
- Consult the [Certificate Management](#) guidance to understand the type of certificates (server and/or client) required for each participant type.
- Generate the certificate signing request for your production certificate - please refer to the [Participant Portal User Guide](#) for more guidance on this step. Please note, it will take us 3 - 4 days to issue your production certificate.
- Please reach out to the CDR Technical Operations team via CDRTechnicalOperations@acc.gov.au if you require any assistance with your production certificate.

! Note

Please note, data holders need to provide their production end points before they request their production PKI certificate, or we will not be able to process this request

5.10. 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

Once you receive your production PKI certificate the Participant Engagement team will provide the production readiness confirmation email template. This needs to be completed and returned by the primary business contact, including a proposed activation date, to CDRONboarding@acc.gov.au.

Please allow at least 5 business days between when the production readiness confirmation is provided and your proposed activation date.

! Note

As soon as a data holder is made active on the Register and the associated database, they are discoverable and must be ready to start servicing requests from accredited data recipients. 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 accredited data recipients as it is their responsibility to perform Dynamic Client Registration (DCR) requests when they are ready to commence participation.

5.11. Step 11: Activation on the Register and associated database

Once we receive the participant's production readiness confirmation we will review the information and the Registrar will assess this information to determine if the participant can be activated on the Register of Accredited Persons and associated database. Should further information be needed the Participant Engagement or Technical Operations teams will request this from the primary business contact.

Confirmation that all the necessary on-boarding steps have been completed and the required information has been provided will enable the Registrar to activate the participant on the Register or associated database, as relevant.

We will inform you about the Registrar's decision and, if approved, will confirm the timing of your activation on the Consumer Data Right (CDR) ecosystem.

Please note, if issues are found with your production details after the Registrar has provided approval, we may need to delay your activation until these issues are resolved.

The ACCC will then activate the participant on the Register or associated database, as relevant, and will inform the participant via email when this step is completed.

6. Participation

Once you have completed the on-boarding process and the ACCC has made you active on the Register or associated database, you are able to operate within the ecosystem.

As your solution continues to evolve and change over its life cycle, you may need to revisit certain aspects of the on-boarding process, such as CTS, to ensure new features meet conformance requirements, and the ACCC, in its capacity as the Registrar, may issue requests for further information or further testing.

Appendix A: 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 testing focuses on critical risk points for the ecosystem. It does not include all possible scenarios relevant to CDR.

Consult the CTS guidance material 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 testing.
 - 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 completing CTS testing 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 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.

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 B: Getting help

The key resources available to support participants through the on-boarding process and their commencement in the ecosystem are outlined below.

CDR Support Portal

The [CDR Support Portal](#) (the Support Portal) is maintained by both the 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.

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

CDR website

The [CDR website](#) provides prospective participants with general information on the process of getting on-boarded to the CDR ecosystem. It also includes a [CDR information map](#) which provides a topic-based listing of CDR information published by the CDR agencies.

CDR implementation call

The [CDR implementation call](#), co-facilitated by the ACCC and the DSB, takes place weekly every Thursday at 3pm-4:30pm (AEDT). 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 data holder and data recipient obligations, while getting access to important updates on CDR. These meetings offer an opportunity to better understand how to interpret and implement the Rules, the Standards and CX Guidelines.

<https://github.com/ConsumerDataStandardsAustralia/standards/wiki/ACCC-&-DSB-Consumer-Data-Right-Implementation-Call>

Questions related to the on-boarding process can be raised during the weekly call, though questions submitted via [CDR Support Portal](#) or the CDR Support Portal before the call will be discussed first.

Seeking assistance from the CDR Participant Engagement team

You may need to reach out to the CDR Participant Engagement team with questions and clarifications as you work through the steps of the on-boarding process. The Participant Engagement team is on hand to help and answer your queries.

The Participant Engagement team can be contacted by email at CDRONboarding@accc.gov.au.

Appendix C: 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).

Where there is a single data holder for a white label product (whether that is the white labeller or the brand owner) in partnership with a non-data holder, that data holder may be subject to CDR obligations in relation to the product.

In some instances, both the white labeller and the brand owner may be data holders. In this scenario, the data holder that has the contractual relationship with the consumer may be subject to obligations under the CDR Rules for CDR data they hold in respect of the white label product. However, the data holder that has the contractual relationship with the consumer may agree with the other data holder, that the other data holder will be subject to those obligations instead.

There are two options for brand owners to be recorded on the Register or associated database.

Table 6: Options for brand owners

Option	Description
1	<p>The brand owner is a data holder:</p> <ul style="list-style-type: none">• The brand owner will be responsible for adding and managing their data holder brand/s on the associated database. They will work with the white labeller to determine the configuration of the brand identity.• Both parties must work together and with the Participant Engagement team to ensure the brand identity is optimised for consumer experience.
2	<p>The white labeller is a data holder, the brand owner is not a data holder:</p> <ul style="list-style-type: none">• The white labeller will be responsible for adding and managing brands on the associated database.• Both parties must work together and with the Participant Engagement team to ensure the brand identity is optimised for consumer experience

The ACCC understands there is a wide variety of white label arrangements, and the above options may not cover all potential scenarios. We are not seeking to mandate any commercial model and are seeking to enable flexibility for parties in how they comply with the rules. If a data holder has any compliance concerns regarding its white label arrangements, especially those with complex white labelling arrangements, please contact acc-cdr@acc.gov.au.

For further information on white labelling see the ACCC's guidance on the [approach to disclosure of consumer data for white label products](#), [the approach to disclosure of product data for white label products](#), [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 Register or associated database with a white label product, contact CDR Technical Operations via CDRTechnicalOperations@acc.gov.au.

Appendix D: Use of the CDR logo

Participants need to accept the CDR Trade Mark Licence Agreement (TMLA), which sets out the terms and conditions of the logo's use, to use the CDR logo (the logo) in their solution.

The latest version of the Trade Mark Licence Agreement is available on the [ACCC website](#). Other than Commonwealth agencies, only entities that have been authorised by the ACCC through a TMLA (Licensees) can use the CDR logo, and entities may only use the CDR logo for the Licensed Purpose specified in the TMLA. The Licensed Purpose in the TMLA limits use of the CDR logo to data holders and accredited persons only.

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 accredited persons when asking a consumer to give consent to collect and use CDR data, and by a data holder 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.

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

Please refer to the [CDR logo fact sheet](#) for further information on what the CDR logo is, who can use it, and how it is authorised to be used under the Trade Mark Licence Agreement.

Confirming your intention to use the CDR Logo

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

Figure 15: Agreements list

The screenshot shows the CDR Participant Portal interface. At the top, there is a navigation bar with icons for Home, Applications, Organisation (highlighted with a red box), and Profile, along with a Sign out button. Below the navigation bar, the breadcrumb trail reads 'Home > Organisation details > Agreements'. The main heading is 'Agreements'. A message below the heading says 'Hi David, you're acting as a Primary Business Contact for Kenoby.' On the left side, there is a sidebar with a section 'Explore this section' containing links for 'Organisation details', 'Update addresses', 'User list', 'Change request', and 'Agreements' (highlighted with a red box). Below this are links for 'DR participation' and 'Banking sector'. The main content area is titled 'Agreements list' and contains a table with the following data:

Reference	Agreement	Version	Status	Accepted on ↑	Actions
AGR004814	Subscriber agreement				View
AGR004945	Relying party agreement				View
AGR005076	Trademark licence agreement				View

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

Figure 16: View and read 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:

Figure 17: Agreed Trademark license agreement

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

- See the CDR Participant Portal User Guide for more information on viewing and accepting the Agreements within the Participant Portal.
- In response, you will receive the CDR logo in various formats.
- The primary lockup consists of the exact arrangement and design of the CDR logo mark and the wordmark. This lockup should be the favoured orientation whenever possible. Refer to the master assets for the source files. See also the [Brand Guidelines for Participants](#) and [CDR logo - fact sheet](#) for further information on the appropriate use of the CDR logo.

Table 7: CDR Logo Styles

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
PNG	Short	Black	1413	2076
PNG	Short	Colour	1439	2137
PNG	Short	White	1412	2076
SVG	Monogram	Black		
SVG	Monogram	Colour		
SVG	Monogram	White		
SVG	Primary	Black		
SVG	Primary	Colour		Scalable
SVG	Primary	White		
SVG	Short	Black		
SVG	Short	Colour		
SVG	Short	White		

Appendix E: Participant Contacts

The ACCC will need to communicate with your organisation both prior to and once you are active on the Register or associated database. Each communication purpose tabled below explains who will be contacted and where contacts for your organisation can be maintained.

Table 9: Participant contacts

Communication Purpose	Contact	System Nominated/ Maintained in	Communication method	Comments
CDR ecosystem incidents	Agent licence	Service Management Portal (SMP)	System notification (SMP) / 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	System notification (SMP) / 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	System notification (SMP) / Email / Phone Letter	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	System notification (SMP) / Email / Phone	Communication likely from on-boarding commencement through to activation and ongoing participation.
Get Metrics	Primary IT Contact	CDR Participant Portal User Guide	System notification (SMP) / Email / Phone	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 prior to activation on the Register and associated database.
Update information on the Register or associated database	Primary Business Contact	CDR Participant Portal User Guide	Email / Phone	Completion of production readiness confirmation for activation on the Register or associated database. Request for removal or name change on the Register or associated database.

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 to 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 to Rule 5.34
Temporary restriction on use of Register and associated database (data holder)	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 to Rule 5.33