Australian Government

Consumer Data Right

Participant Conformance Approach*

Version 1.0

*The Participant Conformance Approach replaces the Participant Test Strategy that was published in December 2020

Table of contents

Table of figures

1. References

Table 1: References

#	Title	Location
R1.	CDR Rules	https://www.legislation.gov.au/Series/F2020L00094
R2.	CDR Consumer Data Standards	https://consumerdatastandardsaustralia.github.io/standards/
R3.	CDR Register design	https://cdr-register.github.io/register/#introduction
R4.	CDR Consumer Experience Guidelines and Standards	https://consumerdatastandardsaustralia.github.io/standards/#consumer-experience
R5.	CDR Website	https://www.cdr.gov.au/
R6.	CDR On-boarding guide	https://www.cdr.gov.au/sites/default/files/2021-06/CDR-participant-on-boarding-guide_v1-2.pdf
R7.	CDR CTS guidance material	https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-conformance-test-suite
R8.	Mock Register	https://github.com/ConsumerDataRight/mock-register
R9.	Mock Register	https://github.com/ConsumerDataRight/mock-register

2. Introduction

A critical element of the Consumer Data Right (CDR) ecosystem is the successful operation of all participants' technology solutions. The Australian Competition and Consumer Commission (ACCC) manages the Conformance Test Suite (CTS), which is a key input into activation requests and on-going security and stability of the ecosystem. The CDR CTS confirms the technical conformance of participant's production-ready solution using a range of test scenarios targeting a limited subset of high-risk areas. Each new participant must complete the CTS before they can be made active on the CDR Register.

The CTS has two test suites – one for each participant type: data holders and data recipients. For data holders, the tests provide simulated data recipient interactions and a CTS Mock Register to support the test scenarios. For data recipients, the tests provide simulated data holder interactions and a CTS Mock Register to support the test scenarios. Testing must take place in isolation against the simulated providers and the CTS Mock Register without interfering with live consumer data.

Participants are expected to have completed internal testing, including security testing, prior to commencing CTS. After the completion of CTS, the Registrar can request evidence of a participants' internal test results as part of the activation process. Participants are expected to ensure their implementation aligns to the Consumer Data Standards (herein the Standards) and CDR Register Design. While CTS conforms to the CDR Standards, its role is not to validate a participant's solution is compliant with those standards. Participants are accountable for compliance with the Standards and must address any alignment issues prior to commencing CTS testing.

This Participant Conformance Approach (PCA) provides guidelines for participants who are seeking to enter the ecosystem (new participants) and participants who are already part of the ecosystem (active participants). It will discuss activities participants are expected to have completed prior to CTS and provides guidance on CTS related activities. The PCA has been drafted with consideration of future CDR sectors.

3. Participant internal testing approach

As outlined in section 4, the CTS is not designed to test the internal workings and validations of a data holder brand or data recipient software products. CTS serves as a final checkpoint and relies on appropriate internal participant testing to be completed prior to commencing CTS. One of the final steps in the on-boarding process requires participants to provide an attestation confirming they have completed appropriate internal testing and their solution is ready to enter the ecosystem.

3.1 Participant internal testing guidelines

The ACCC expects that new and active participants complete all build and internal participant testing prior to testing against CTS. Participants are expected to follow an established testing process in conjunction with formal software release and risk management practices. This could include activities such as unit, system, and integration testing as well as user acceptance testing (UAT), performance testing and penetration testing.

New and active participants are expected to ensure that their solutions correctly incorporate the relevant CDR release scope. In addition, active participants should perform regression testing on previously tested code to ensure no defects have been introduced and are confident that their CDR solution operates as intended.

Part of the Registrar's functions include requesting an Accredited Person or a Data Holder to do specified things (r 5.30(c)) in order for the Registrar to perform its function to maintain the security, integrity and stability of the Register of Accredited Persons and associated database (herein the Register) (rule 5.30(b)). In this context, this means that the CDR Registrar may request information and evidence from participants on their internal testing and outcomes.

4. CDR conformance testing

4.1 CTS introduction

The CTS is a final checkpoint for participants of key elements of a participant's solution before activation in the ecosystem. The primary focus of the CTS is to provide the ACCC as the CDR Registrar, performing its function to maintain the security, integrity, and stability of the Register, with a level of confidence that:

- a participant has delivered to the security standard required for CDR
- a participant is able to share consumer data in the CDR ecosystem without significant disruption
- key capabilities have been built, unless an exemption has been granted

The CTS is designed to verify a limited subset of standards alignment against security profile and consent components as well as other high-risk areas. The CTS will continue to evolve and further test scenarios will be added as ecosystem requirements change. The execution of CTS is not a one-time event for a participant, it is expected that active participants will complete the new test scenarios. This is described in more detail in section 4.3.

In order to test or retest conformance, a participant must have a set of endpoints different to their production endpoints, with which the CTS can interact. Mutual Transport Layer Security (mTLS) endpoints must be configured to use a certificate that has been provisioned by the ACCC from the Test Certificate Authority infrastructure. Consumer data must not be communicated or used when interacting with the CTS via these endpoints as the consumer cannot provide consent. As per the Consumer Data Sharing obligations, Active participants will be required to continue sharing consumer data via their production solution while CTS testing is completed.

The CTS is ***not designed*** to:

- Test the internal workings and validations of a data holder brand or data recipient software products
- Confirm for data holders and data recipients:
    - how they manage consent within their brand / software product
    - their brand / software product correctly handles certain consent flow attack vectors
- Test compliance to ***all*** CDR Rules (the Rules) and Standards
- Be a sandbox or assisted development tool. It will not help participants design and build a product that conforms to the Consumer Data Standards (CDS) and the Register design. Before undertaking the CTS, participants require a production-ready data holder brand or data recipient software product that is built in accordance with the CDS and the Register design

The ACCC has published the following guidance material relating to the CTS:

- An up to date list of the available test scenarios on the CDR Support Portal
- An overview of CTS test plan versions on the CDR Support Portal, which includes the test plan release date, an overview of the different test scenarios, and the high-level scenario changes between different versions.

! Note

A participant must complete CTS with each individual brand or software product.

Passing all CTS tests does not guarantee compliance with the Rules [R1], Consumer Data Standards [2] and Register design [3] obligations.

Participants who are preparing to meet a compliance milestone should allow sufficient time in their plans to execute CTS. While the CTS can be completed in a few hours, the duration required to execute CTS is participant dependent, it is not unusual for completion of CTS to take between 4 and 8 weeks in elapsed time.

! Note

For security reasons, Public Key Infrastructure (PKI) test certifications will expire after 1 month. Participants will be reminded to renew their certificate(s) three times prior to the expiry date. Test plan renewal does not impact on the test plan progress, participants are able to proceed with their existing plans after their new certificate has been successfully installed in their infrastructure.

4.2 Conformance testing for new participants

The conformance testing for new participants where they do not have an 'Active' status for their software product and/or brand is based on the following:

- Participant solutions should be fully developed and quality assured by the participant before CTS testing commences. See *section 3 Participant internal testing approach* for further details
- New participants must confirm the technical conformance of their production-ready solution using a range of test scenarios targeting a limited subset of high-risk areas by completing test scenarios through the CTS as part of the On-boarding process. This and all other on-boarding requirements are explained in more detail in the Participant On-boarding Guide.
- New participants will need to complete all relevant CTS tests within the assigned test plan, as well as the other on-boarding steps, which are outlined in the Participant On-boarding Guide, before the activation assessment can be sent to the Registrar to make a decision if the participant can be made active on the Register. The Registrar can also request further evidence of conformance. If a participant is unable to execute all applicable tests (e.g. if certain tests are not relevant for an ADR offering or the participant has an active exemption), they are required to inform the ACCC, as outlined in the CTS guidance material.

Figure 1 outlines the high level steps for internal participant testing in relation to conformance testing activity, and the sequence of the CTS in relation to when new participants can commence live data sharing. CTS conformance testing is step 7 of the on-boarding process for new participants as outlined in the Participant On-boarding Guide.

Figure 1: Internal participant testing in relation to conformance testing

Internal participant testing for new participants can be conducted prior to and in parallel to Steps 1 to 6 of the On-boarding process.

4.3 Conformance testing for active participants

The ACCC may require participants who are already active in the CDR ecosystem to retest against CTS in response to changing ecosystem requirements. In some instances this will be voluntary and in others retesting will be mandated as outlined below.

4.3.1 Voluntary testing

The CTS will be readily accessible for active participants to use on a voluntary basis. Access to CTS can be requested via the participant portal by requesting a new PKI test certificate and submitting a new CTS enrolment form. The ACCC encourages active participants to retest through the latest version of the CTS:

- If they make a significant change to their solution/technology
    - Participants are strongly encouraged to retest through the CTS prior to the production release of the changes to their solution / technology / use case. This is to ensure the interactions of the solution within the CDR ecosystem continue to work as expected and to reduce critical points of failure.
- When there is a significant change in the Rules or Standards
    - Participants are strongly encouraged to revisit CTS before a change in the Rules or Standards comes into effect. This is to ensure that active participants remain in sync with new participants joining the ecosystem. The ACCC intends to announce changes to CTS resulting from changes to the Rules and Standards at least 4 months before new Rules or Standards come into force and intends to make new CTS scenarios available for testing 3 months prior to this date.
- Even if there is no material impact to the CTS, regular retesting through the latest version of CTS can be an effective form of regression testing areas covered by CTS. The ACCC encourages participants to revisit CTS at least once every 3 months.

Figure 2 outlines the anticipated sequence of a participant's internal testing in relation to the CTS, when active participants update their solution.

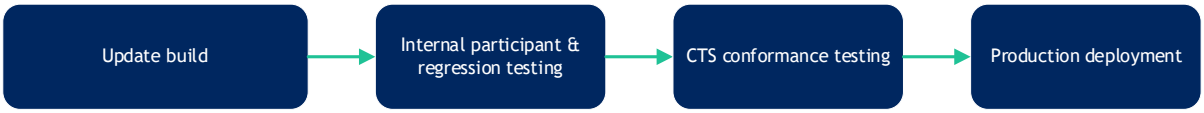

Figure 2: Active participants - update in participant solution

4.3.2 Mandatory testing

Under certain circumstances, the Registrar may mandate active participants to retest their solution through the CTS, to reduce broader ecosystem risk. This may include a sub-set or all of the CTS test scenarios in a test plan. Examples that might form part of the consideration for such a request could include, but are not limited to, the following:

- the stability of the ecosystem (e.g. due to information security concerns)
- volume and severity of incidents in the ecosystem

Figure 3 outlines the anticipated sequence for conformance testing in relation to production deployments when active participants are notified of ACCC expectations regarding retest.

Figure 3: Active participants - retest as requested by the ACCC

5. Updates to CTS test plans and test plan retirement

The CTS plays a key role in ensuring the interactions of a participant solution against the Register interactions are working as expected and to reduce critical points of failure. The CTS will evolve over time in response to changing ecosystem requirements. This may result in new test plans and scenarios being introduced over time. An up to date list of test plans and scenarios is available on the CDR Support Portal.

As stated in section 4.3.1, the ACCC intends to announce major CTS releases 4 months in advance and publish any new test cases 3 months prior to the date the changes will take effect. Note that in some circumstances (e.g. if required to protect the quality, security and stability of the CDR ecosystem) scenarios might be added closer to the date new Rules and Standards are effective.

The ACCC strongly recommends and may mandate active participants to retest through CTS in conjunction with the introduction of any new Rules or Standards to reduce critical points of failure. New participants will be allocated to the test plan that is most relevant to their projected activation date.

A new test plan could be released when minor changes to existing scenarios are required or as new scenarios are added. Participants will be notified when a new test plan is published.

- New participants (i.e. those who are not yet activated on the CDR ecosystem) should be testing against the Register design they will go live against. This means that, depending on a participant's planned activation date, a participant might have to be moved to a new test plan. Note that minor releases are introduced to better support participants and will not affect the test scenarios deployed

- Active participants (i.e. participants who are active on the CDR ecosystem) who wish to revisit CTS after activation will be allocated to the latest available test plan that includes future changes to the Rules or Standards or the version prior to that one if they wish to test against the latest current obligations in the ecosystem

While new test plans are created in response to changing ecosystem requirements, older test plans will retire over time. Until the date new Rules and Standards are in force, two test plans will be available:

- A test plan that supports future changes to the ecosystem prior to the new compliance date
- A test plan that reflects the current state of the ecosystem. Participants can be allocated to this plan only prior to the future compliance date

! Note

When new Rules come into force the old test plan will be retired once the last participant allocated to this plan completes CTS or three months after the compliance date. This is to ensure that new participants test scenarios that are relevant to the Rules and active participants remain in sync with new participants joining the ecosystem.

6. Mock Register

The CTS is available to participants as part of the final steps of the on-boarding process. The ACCC recognises Participants' desire to have access to ecosystem components during their development stage. In addition to the comprehensive documentation that is available, the ACCC has developed a tool designed to operate within and integrate with participants' own technology environments.

In June 2021, the ACCC released a free and open source Mock Register. The Mock Register is a simulation of the production CDR Register. It helps businesses to explore and understand the CDR regime before they join. It also gives them the ability to prove potential solutions in the early development phase.

Interested parties can download and run the Mock Register in an environment of their choice. Test data is pre-loaded but participants have the ability to load their own metadata to test specific solutions.

Participants can download the source code, make changes and run their own modified versions of the Mock Register. They can choose to contribute any modifications back to the main codebase, subject to ACCC review and approval.

The ACCC is also developing a Mock Data Holder and Mock Data Recipient, which together with the Mock Register, will provide a complete CDR ecosystem of mock components for use by the community. Both the Mock Data Holder and Mock Data Recipient solutions will follow the same approach as the Mock Register. The source code and artefacts will be published to an open source repository, with community contributions reviewed and vetted by the ACCC. These solutions will also be available for download and are designed for participants to run in an environment of their choice.

The ACCC will continue to work on new and enhanced tooling for participants to help understand the CDR ecosystem's technical requirements and facilitate and support the development and implementation of CDR solutions by participants.

Appendix A: Terminology

Shortened Form	Extended Form
ACCC	Australian Competition and Consumer Commission
CDR	Consumer Data Right
CDR Rules	Competition and Consumer (Consumer Data Right) Rules 2020
CDS	Consumer Data Standards
CTS	Conformance Test Suite
Data holder (DH)	A Legal Entity (participant) that is a data holder subject to CDR data sharing obligations (data sharing obligations) under the CDR Rules.
Accredited data recipient (ADR)	A Legal Entity (participant) who has been granted accreditation by the DR Accreditor and is able to receive CDR data.
Participant	In this context, a participant is an entity that has been accredited (data recipient) or registered (data holder) and is preparing or currently undertaking on-boarding in order to participate in the CDR regime
New participant	A participant entering the CDR ecosystem for the first time
Active participant	A participant already part of the CDR ecosystem
CDR Registrar	The person or entity appointed as the Accreditation Registrar under the CDR legislation, currently the ACCC.
Mock Register	A simulation of the production CDR Register
Mock Data Holder	A simulation of a data holder
Mock Data Recipient	A simulation of a data recipient