



Australian Government



**Consumer
Data Right**

Accredited Data Recipient Technical Guidance Material v4.3.0

Conformance Test Suite

Table of Contents

1	Document Control	4
1.1	Test Plan Revision History	4
2	Overview	6
2.1	Document Purpose	6
2.2	Background	6
2.3	CTS Scope for ADR Testing	6
2.3.1	Test plan alignment to the Consumer Data Standards	7
2.4	Technical Considerations	9
2.4.1	Register API Version Support	9
2.4.2	Authentication Flows	9
3	ADR Test Plan Competencies	10
3.1	CTS Entry Criteria	10
3.1.1	Before you start:	10
3.2	CTS Exit Criteria	10
3.3	Dynamic Client Registration	11
3.3.1	Purpose	11
3.3.2	Competency Conditions	11
3.3.3	Endpoints	11
3.3.4	Test Results	12
3.3.5	High-Level Test Steps	12
3.4	Establishing Consent	15
3.4.1	Purpose	15
3.4.2	Competency Conditions	15
3.4.3	Endpoints	15
3.4.4	Test Results	16
3.4.5	High-Level Test Steps	16
3.5	ADR to DH Consent Arrangement Revocation	17
3.5.1	Purpose	17
3.5.2	Competency Conditions	17

3.5.3	Endpoints.....	18
3.5.4	Test Results	18
3.5.5	High-Level Test Steps.....	18
3.6	DH to ADR Consent Revocation	21
3.6.1	Purpose	21
3.6.2	Competency Conditions.....	21
3.6.3	Endpoints.....	21
3.6.4	Test Results	22
3.6.5	High-Level Test Steps.....	22
4	Endpoints used in the CTS ADR Test Plan.....	24
5	Glossary	28

1 Document Control

Document Version	1.0
Document Status	Approved
Issued Date	21 March 2024
Owner	ACCC

1.1 Test Plan Revision History

Test Plan Version	CDS Version	Issued Date	Description of Changes
4.0.0	1.20.0	19 January 2023	<ul style="list-style-type: none"> Renamed the Get Accounts competency to Establishing consent. Removed test steps that called the banking Get Accounts endpoint in the Establishing consent competency.
4.1.0	1.22.0	20 April 2023	<p>This test plan has been updated to conform with version 1.22.1 of the Consumer Data Standards, notable the FAPI 1.0 Phase 3 obligations. As part of these changes the test plan has:</p> <ul style="list-style-type: none"> Added support for the conformance testing of the Authorisation Code Flow (ACF) Added support for JARM

Test Plan Version	CDS Version	Issued Date	Description of Changes
4.2.0	1.25.0	7 September 2023	<p>This test plan has been updated to conform with version 1.25.0 of the Consumer Data Standards, notable the private_key_jwt authentication obligations. As part of these changes the test plan has:</p> <ul style="list-style-type: none"> • Changed client_id to optional in token requests
4.3.0	1.29.0	21 March 2024	<p>This test plan has been updated to conform with version 1.29.0 of the Consumer Data Standards, notable the FAPI 1.0 Phase 4 obligations. As part of these changes the test plan has:</p> <ul style="list-style-type: none"> • CTS Simulated Data Holder has retired support for Hybrid Flow • CTS Simulated Register has been updated to improve consistency across ACCC CDR implementations.

2 Overview

2.1 Document Purpose

The purpose of this document is to provide technical information about the Consumer Data Right (CDR) Conformance Test Suite (CTS). It will provide an in-depth understanding of the following:

- the scope of the CTS
- the purpose of each CTS ADR competency
- what is being tested to ensure technical conformance
- pass and fail conditions for each CTS ADR competency
- how to react correctly to valid requests.

2.2 Background

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 more 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 new test scenarios as standards are updated or their software evolves.

The CTS is **not designed** to:

- test the internal workings and validations of a Data Holder (DH) brand or an Accredited Data Recipient's (ADR) software products
- test compliance to **all** CDR Rules (the Rules) and CDS
- be a sandbox or assisted development tool. It will not help participants design and build a product that conforms to the CDS. Before undertaking the CTS, participants require a production-ready DH brand or ADR software product that is built in accordance with the CDS.

For the steps you need to complete before you can use the CTS, please consult the 'On-boarding for data recipients' page on the [CDR website](#).

2.3 CTS Scope for ADR Testing






The CTS interacts with the ADR's software product and assesses the ADR's technical competency in conforming to the CDS. To achieve this, the CTS simulates the Register and a DH, testing that the ADR's software product can safely interact with a DH brand.


In Scope	Out of Scope
<p>The CTS will conduct a series of tests to determine the technical competency of the ADR software product and whether it conforms to the CDS. The following core competencies are tested in the CTS:</p> <ol style="list-style-type: none"> 1. Dynamic Client Registration 2. Establishing consent 3. ADR to DH consent arrangement revocation 4. DH to ADR consent revocation 	<p>The CTS does not test the internal workings and validations of an ADR's software products. The CTS will not cover how:</p> <ul style="list-style-type: none"> • consent is managed within an ADR's software product • an ADR's software product correctly handles certain consent flow attack vectors • an ADR removes consent and consumer data in their software product.
<p>The CTS includes only those endpoints that are detailed in this document.</p>	

2.3.1 Test plan alignment to the Consumer Data Standards

This version of the test plan aligns with v1.29.0 of the CDS. Within each version of the CDS, there are dated standard changes that are independent of the CDS version. The below table details which dated standard changes have been applied to this test plan.

CDS Section	Description	Date	v4.3.0
Revised Profile Scopes	<p>For new and amended consents and authorisations only, CDR participants SHOULD comply with the following standards from 1 February 2022, but MUST comply by 1 July 2022:</p> <ul style="list-style-type: none"> • Technical Standards: Revised Claims • CX Standards: Profile Scope - Data Language Standards <p>Note: These standards changes do not apply to existing consents and authorisations unless they are amended on or following the compliance dates.</p>	<p>July 1st 2022</p>	<p>✓</p>
Revoke consent using 'CDR Arrangement JWT' method	<p>From July 31st 2022, Data Holders MUST revoke consent using "CDR Arrangement JWT" method. Data Holders SHOULD use the "CDR Arrangement JWT" method from March 31st 2022</p>	<p>July 31st 2022</p>	<p>✓</p>

CDS Section	Description	Date	v4.3.0
Self-Signed JWT Client Authentication	Until July 31st 2022, Data Recipients MUST accept the Resource Path for the endpoint and the <code><RecipientBaseURI></code> as a valid audience value. From July 31st 2022, Data Holders MUST use an audience value matching the Resource Path for the endpoint and the Data Recipient MUST verify the audience matches the Resource Path for the endpoint.	July 31st 2022	
FAPI 1.0 Phase 2	FAPI 1.0 adoption is introduced across three phases. Phase 2: FAPI 1.0 Final (Baseline & Advanced) includes, amongst other changes: <ul style="list-style-type: none"> Enforces additional requirements for authorisation code, token and request object use Enforces PAR-only authorisation request data submission Refresh token cycling is not permitted Data Holders and Data Recipients MUST support FAPI 1.0 Final including [RFC9126], [RFC7636] and [JARM] Data Holders SHOULD support of Authorization Code Flow in conjunction with Hybrid Flow 	September 16th 2022	
Validate cdr_arrangement_id within the 'CDR Arrangement JWT'	From November 15th 2022, Data Recipients MUST validate the <code>cdr_arrangement_id</code> , if presented, is the same as the value included in the "CDR Arrangement JWT".	November 15th 2022	
FAPI 1.0 Phase 3	FAPI 1.0 adoption is introduced across three phases. Phase 3: Support Authorization Code Flow includes, amongst other changes: <ul style="list-style-type: none"> Data Holders MUST support Authorization Code Flow Data Holders MUST support Hybrid Flow 	April 7th 2023	
FAPI 1.0 Phase 4	FAPI 1.0 adoption is introduced across four phases. Phase 4: Retire Hybrid Flow: <ul style="list-style-type: none"> Data Holders MAY retire Hybrid Flow 	July 10th 2023	

CDS Section	Description	Date	v4.3.0
Private Key JWT Client Authentication	Change to support [RFC7521] such that, until November 13th 2023, clients authenticating using Private Key JWT are recommended to provide the client_id, but no longer required. From November 13th 2023, it is then optional to provide the client_id. This applies to ADRs and the CDR Register authenticating with Data Holders and ADRs authenticating with the CDR Register.	November 13th 2023	

2.4 Technical Considerations

2.4.1 Register API Version Support

The CTS ADR Flexi Test Plan v4.3.0 supports the latest endpoint versions as outlined in the [CDS endpoint version schedule](#) and detailed in the section [Endpoints used in CTS ADR Test Plan](#).

Register API versions supported in this version of CTS ADR Flexi Test Plan v4.3.0 are listed in the table below.

API	Version Supported
Get Data Holder Brands	2
Get Software Statement Assertion	3
Get Data Recipients	3
Get Data Recipients Statuses	2
Get Software Product Statuses	2
Get Data Holder Brands Statuses	1

2.4.2 Authentication Flows

The CTS Simulated DH now only supports the OpenID Connect (OIDC) Authorization Code Flow in line with FAPI 1.0 Phase 4.

3 ADR Test Plan Competencies

This section provides step-by-step instructions on how to start your CTS test run and initiate a specific test. The CTS ecosystem simulates the Register with a Simulated Register and the Data Holder (DH) with a Simulated Data Holder. Subsequent references to the Register and the Data Holder refer to the CTS Register and the CTS Simulated Data Holder respectively.

After the Participant ADR has been activated in the CTS ecosystem, CTS waits for the Participant ADR to engage in 4 core competencies to determine if the ADR's software product can conform to the Consumer Data Standards (CDS).

After completion of the Dynamic Client Registration, the remaining 3 test competencies can be completed in any order.

The 4 competencies are as follows:

1. **Dynamic Client Registration (DCR)** - the software product must demonstrate an ability to register with a Simulated DH successfully.
2. **Establishing consent** - the software product must demonstrate an ability to securely obtain authorisation and consent by means of Pushed Authorisation Request (PAR), request_uri and Proof of Key Code Exchange (PKCE).
3. **Participant ADR to CTS Simulated DH consent arrangement revocation** - the software product must demonstrate an ability to revoke a consumer consent arrangement from the software product dashboard.
4. **DH to ADR consent revocation** - the software product must demonstrate an ability to allow the revocation of a consumer consent arrangement when a request is received from a CTS Simulated DH.

3.1 CTS Entry Criteria

For a Participant ADR, each software product needs to pass the CTS separately. You should enrol in the CTS when your software product is ready for production release or close to being ready. After receiving your enrolment confirmation, you can start your CTS competencies.

3.1.1 Before you start:

1. Apply the CTS certificates to your software product.
2. If necessary, configure your software product to interact with the CTS. Infrastructure changes, such as firewall rules or IP allowlisting, may need to be configured.
3. Create a mock client in your software product to simulate a consumer.

Consult the [on-boarding guide](#) and the [CTS Connection Datasheet](#) for more information on the steps and actions.

3.2 CTS Exit Criteria

1. You must pass all the tests mandatory on your CTS enrolment form to successfully complete the CTS.
2. The CTS should be completed within 3 months of starting your first test run.

3. Tests can be run multiple times, the final submitted test plan will be included in the test run report for the CTS outcome assessment.
4. Submit the test result via the [CTS Participant Portal](#) after finishing all mandatory tests. You must inform the On-boarding Officer via email, when you submit your test results so that an On-boarding Officer can start reviewing your results.

3.3 Dynamic Client Registration

3.3.1 Purpose

The software product must demonstrate the ability to dynamically register with the CTS Simulated Data Holder (DH) using [DCR](#).

When successful, the Participant ADR’s software product is registered with the CTS Simulated DH. The CTS Simulated DH will return a client ID to your software product.

3.3.2 Competency Conditions

Not Applicable.

3.3.3 Endpoints

See also [Endpoints used in the CTS ADR Test Plan](#)

Endpoint	Description	Method
Get OpenId Provider Config	Participant ADR requests the Discovery Document from the CTS Register via the Get OpenId Provider Config	GET
Token	Participant ADR requests a token from the CTS Register via the Register Token endpoint	POST
Get Data Holder Brands	Participant ADR requests a list of Data Holder brands from the CTS Register via the GET Data Holder Brands endpoint	GET
Get Software Statement Assertion	Participant ADR requests an SSA from the CTS Register for the purposes of registering with a CTS Simulated DH from the above list of Data Holder Brands via the GET Software Statement Assertion endpoint	GET

OpenID Provider Configuration End Point	Participant ADR requests a Discovery Document from the CTS Simulated DH via the Discovery endpoint	GET
DH JWKS	Participant ADR requests JWKS from the CTS Simulated DH via the Discovery JWKS endpoint	GET
Dynamic Client Registration	Participant ADR sends their DCR request to the CTS Simulated DH via the Dynamic Client Registration endpoint	POST

Link to specifications

- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#security-endpoints>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#client-registration>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#get-data-holder-brands>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#dcr-apis>
- <https://www.rfc-editor.org/rfc/rfc7591>

3.3.4 Test Results

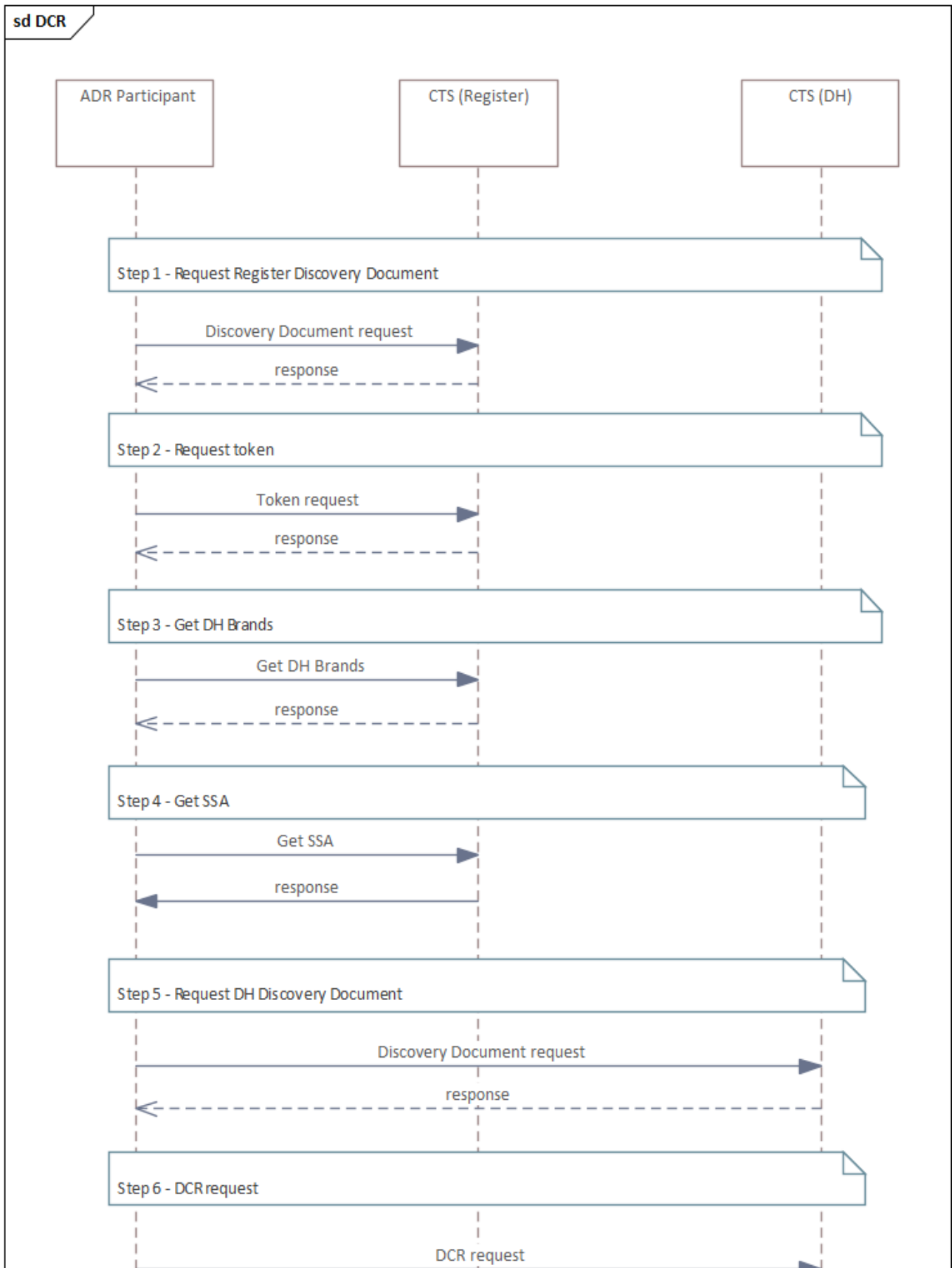
You have achieved a successful registration when you **can**:

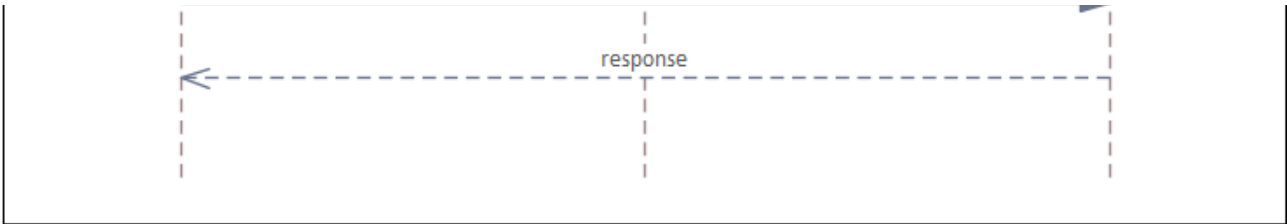
- receive a client ID from the CTS Simulated DH.

3.3.5 High-Level Test Steps

- 1. ADR retrieves Discovery Document from the CTS Register**
 - a. Participant ADR requests the Discovery Document from the CTS Register via the Register Get OpenId Provider Config endpoint.
 - b. CTS Register responds with the Discovery Document.
- 2. ADR retrieves a Token from the CTS Register**
 - a. Participant ADR requests a token from the CTS Register via the Register Token endpoint.
 - b. CTS Register responds with an Access Token, Token Type of Bearer and Token Expiry.
- 3. ADR retrieves DH Brands from the CTS Register**
 - a. Participant ADR requests a list of CTS Simulated DH brands from the CTS Register via the Get Data Holder Brands endpoint.
 - b. CTS Register responds with a list, containing one multi-sector DH Brand (the CTS Simulated DH).
- 4. ADR retrieves a Software Statement Assertion (SSA) from the CTS Register**

- a. Participant ADR requests an SSA from the CTS Register for the purposes of registering with the CTS Simulated DH from the above DH Brands list via the GET Software Statement Assertion endpoint.
 - b. CTS Register responds with an SSA.
- 5. ADR retrieves Discovery Document from the CTS Simulated DH**
- a. Participant ADR requests a Discovery Document from the CTS Simulated DH via the OpenID Provider Configuration endpoint.
 - b. CTS Simulated DH responds with the Discovery Document.
- 6. ADR requests DCR with the CTS Simulated DH**
- a. Participant ADR creates their DCR request to the CTS Simulated DH via the DH Registration endpoint.
 - b. CTS Simulated DH returns a valid Registration response.





1 - Dynamic Client Registration

3.4 Establishing Consent

3.4.1 Purpose

The Software Product must demonstrate an ability to securely obtain authorisation and consent by means of Pushed Authorisation Requests (PAR), request_uri and Proof Key for Code Exchange (PKCE).

Note: This test can be run multiple times during the test run. The result of the last attempt of the test will be included in the test run report for the CTS outcome assessment.

3.4.2 Competency Conditions

Successful completion of the DCR Competency.

3.4.3 Endpoints

See also [Endpoints used in the CTS ADR Test Plan](#)

Endpoint	Description	Method
Pushed Authorisation	Participant ADR sends request object to the CTS Simulated Data Holder (DH), via Pushed Authorisation endpoint for request_uri	POST
Authorisation	Participant ADR requests authorisation with the CTS Simulated DH via the Authorisation endpoint	GET
Token	Participant ADR exchanges their code for a Token from the CTS Simulated DH via the Token endpoint	POST

Link to specifications

- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#authentication-flows>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#request-object>

- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#consent>
- <https://tools.ietf.org/html/draft-ietf-oauth-par-01>
- <https://datatracker.ietf.org/doc/html/rfc7636>

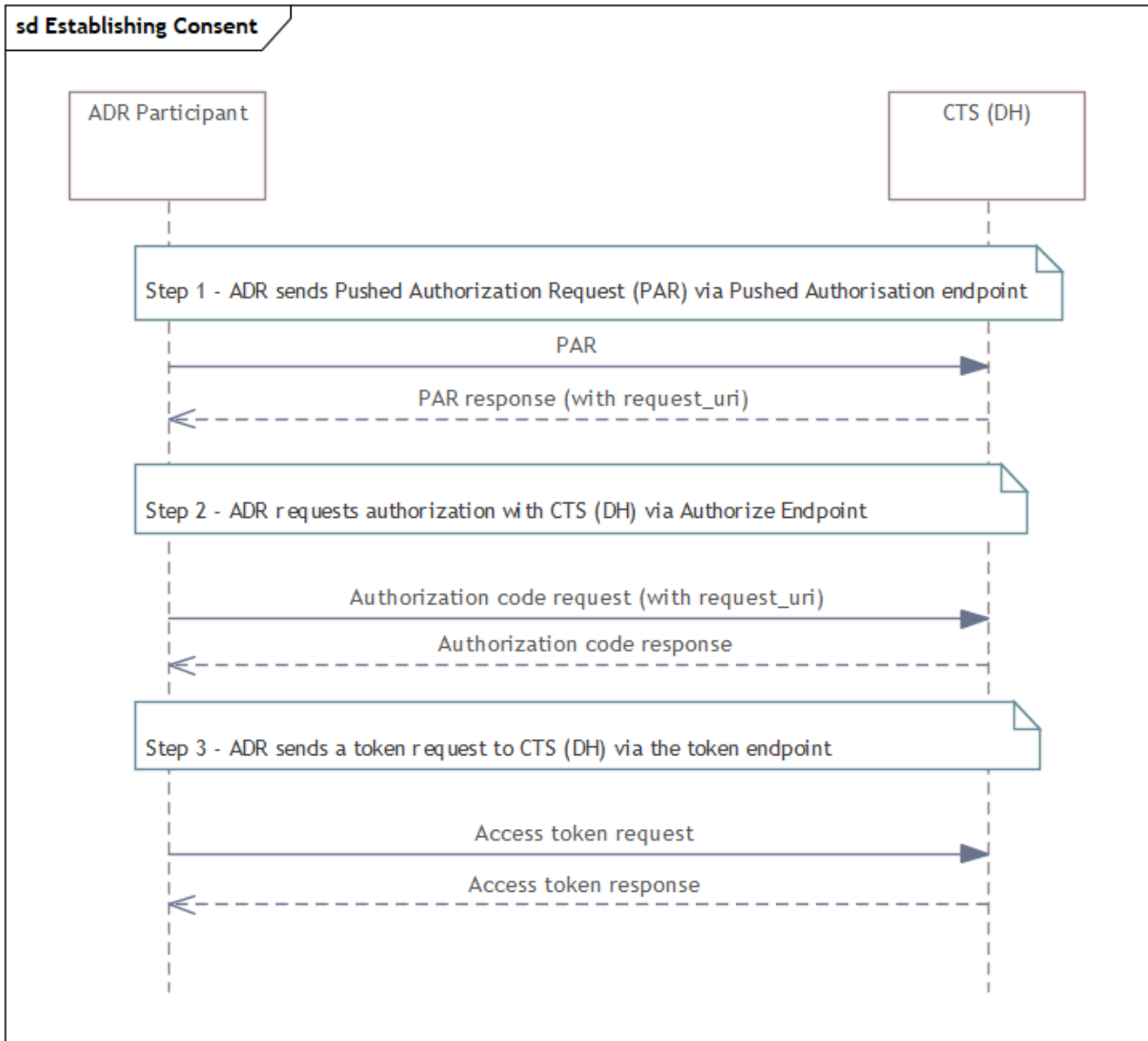
3.4.4 Test Results

You have passed the test when you **can**:

- receive a valid Access Token.

3.4.5 High-Level Test Steps

- 1. ADR sends Pushed Authorisation Request (PAR) via Pushed Authorisation endpoint**
 - a. Participant ADR sends a PAR with the request object to the CTS Simulated DH via the Pushed Authorisation endpoint.
 - b. CTS Simulated DH validates the Participant ADR PAR and responds with request_uri.
- 2. ADR sends an authorisation request to the CTS Simulated DH via the Authorisation endpoint**
 - a. Participant ADR sends an authorisation request, with the request_uri, using their DCR Client ID to the CTS Simulated DH via the Authorisation endpoint.
 - b. CTS Simulated DH validates the ADR authorisation request, verifying that the ADR software product is registered with the CTS Simulated DH and responds via the Redirect URI with an Authorization Code.
- 3. ADR sends a token request to the CTS Simulated DH via the Token endpoint**
 - a. Participant ADR sends a Token request to the CTS Simulated DH via the Token endpoint, exchanging their Authorization Code for a Token.
 - b. CTS Simulated DH validates the token request and returns an Access Token.



2 - Establishing Consent

3.5 ADR to DH Consent Arrangement Revocation

3.5.1 Purpose

The software product must demonstrate an ability to revoke a consumer consent arrangement from the software product dashboard.

Note: This test can be run multiple times during the test run. The result of the last attempt of the test will be included in the test run report for the CTS outcome assessment.

3.5.2 Competency Conditions

A `cdr_arrangement_id` was issued to the Participant ADR by the CTS Simulated Data Holder.

3.5.3 Endpoints

See also [Endpoints used in the CTS ADR Test Plan](#)

Endpoint	Description	Method
Pushed Authorisation	Participant ADR sends request object to the CTS Simulated DH via PAR endpoint for request_uri	POST
Authorisation	Participant ADR requests authorisation with the CTS Simulated DH via the Authorize endpoint	GET
Token	Participant ADR exchanges their code for a Token from the CTS Simulated DH via the Token endpoint	POST
Arrangement Revocation	Participant ADR sends an arrangement revocation request, using their cdr_arrangement_id, to the CTS Simulated DH (Auth Server) to withdraw consent	POST

Link to specifications

- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#cdr-arrangement-revocation-end-point>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#authentication-flows>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#request-object>
- <https://tools.ietf.org/html/draft-ietf-oauth-par-01>
- <https://datatracker.ietf.org/doc/html/rfc7636>

3.5.4 Test Results

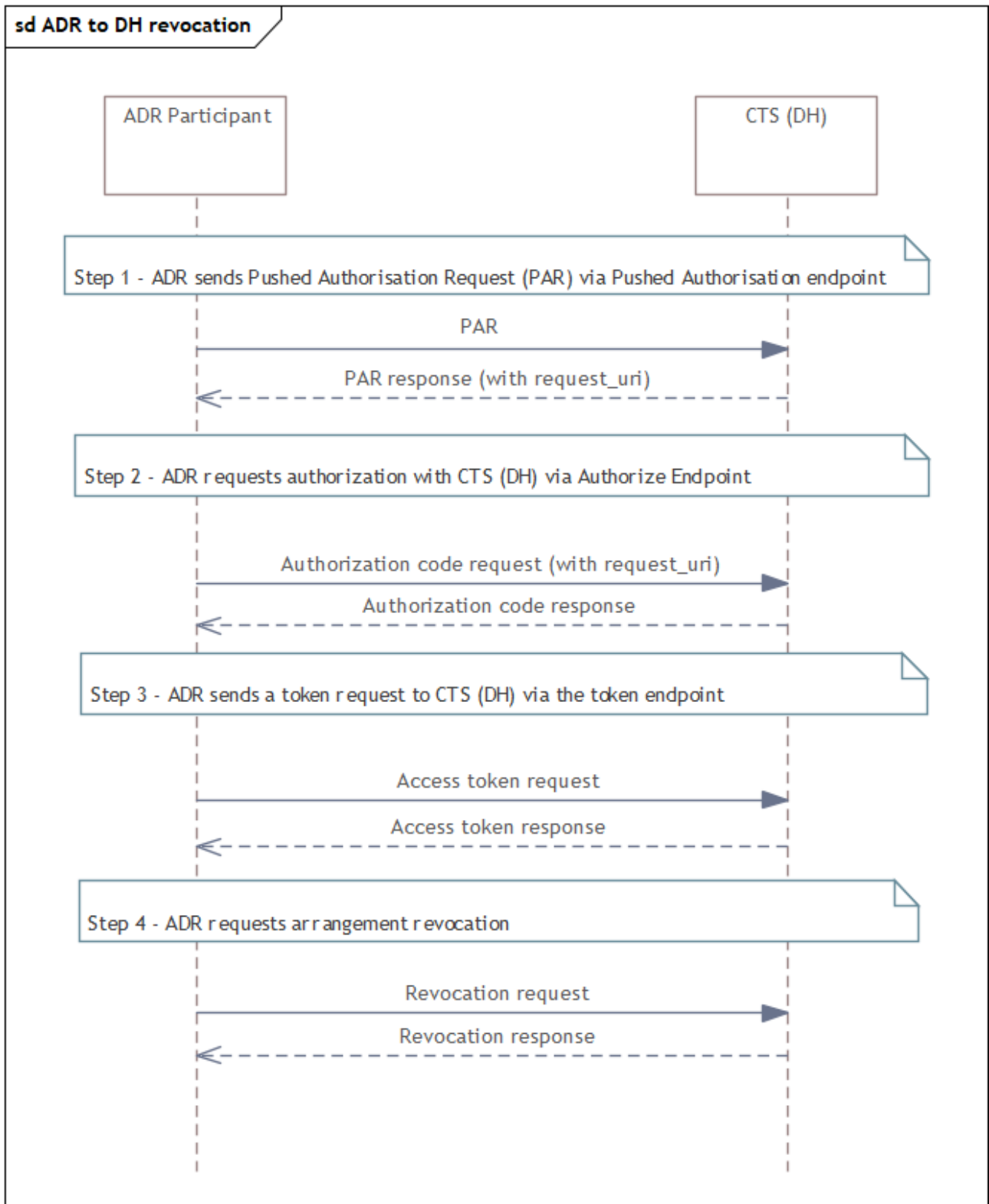
You have passed the withdrawal of consent flow when you can:

- call the CTS Simulated DH Arrangement Revocation endpoint and receive a success code response.

3.5.5 High-Level Test Steps

1. **ADR sends Pushed Authorisation Request (PAR) via Pushed Authorisation endpoint**
 - a. Participant ADR sends a PAR with the request object to the CTS Simulated DH via the Pushed Authorisation endpoint.
 - b. CTS Simulated DH validates the Participant ADR PAR and responds with request_uri.
2. **ADR sends an authorisation request to the CTS Simulated DH via the Authorize endpoint**

- a. Participant ADR sends an authorisation request with the request_uri using their DCR client ID to the CTS Simulated DH via the Authorize endpoint.
 - b. CTS Simulated DH validates the ADR authorisation request, verifying that the ADR software product is registered with the CTS Simulated DH and responds via the Redirect URI with an Authorization Code.
3. **ADR sends a token request to the CTS Simulated DH via the Token endpoint**
- a. Participant ADR sends a token request to the CTS Simulated DH via the Token endpoint, exchanging their Authorization Code for a Token.
 - b. CTS Simulated DH validates the token request and returns an Access Token, a Refresh Token and a cdr_arrangement_id.
4. **ADR sends an arrangement revocation request to the CTS Simulated DH with the cdr_arrangement_id**
- a. Participant ADR sends an arrangement revocation request to the CTS Simulated DH via the Arrangement Revocation endpoint, with their cdr_arrangement_id.
 - b. CTS Simulated DH validates the arrangement revocation request, revoking the consent and returns a response.



3 - ADR to DH Consent Revocation

3.6 DH to ADR Consent Revocation

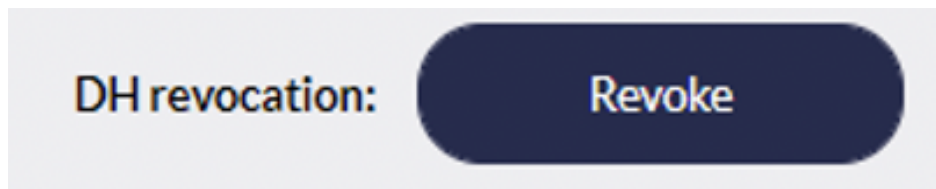
3.6.1 Purpose

The software product must demonstrate an ability to support the revocation of a consumer consent arrangement when a request is received from a CTS Simulated Data Holder (DH).

Note: This test can be run multiple times during the test run. The result of the last attempt of the test will be included in the test run report for the CTS outcome assessment.

3.6.2 Competency Conditions

- A `cdr_arrangement_id` was issued to the Participant ADR by the CTS Simulated DH.
- The `cdr_arrangement_id` be sent within the `cdr_arrangement_jwt`
- This competency test is triggered by clicking on the "Revoke" button shown on the footer of the CTS ADR test plan in the Participant Portal:



3.6.3 Endpoints

See also [Endpoints used in the CTS ADR Test Plan](#)

Endpoint	Description	Method
Pushed Authorisation	Participant ADR sends request object to the CTS Simulated DH via Pushed Authorisation endpoint for <code>request_uri</code>	POST
Authorisation	Participant ADR requests authorisation with the CTS Simulated DH via the Authorize endpoint	GET
Token	Participant ADR exchanges their code for a Token from the CTS Simulated DH via the Token endpoint	POST
Arrangement Revocation	CTS Simulated DH sends an arrangement revocation request to the Participant ADR Arrangements Revocation endpoint Participant ADR validates the request and returns a success code response	POST

[Link to specifications](#)

- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#cdr-arrangement-revocation-end-point>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#authentication-flows>
- <https://consumerdatastandardsaustralia.github.io/standards-archives/standards-1.29.0/#request-object>
- <https://tools.ietf.org/html/draft-ietf-oauth-par-01>
- <https://datatracker.ietf.org/doc/html/rfc7636>

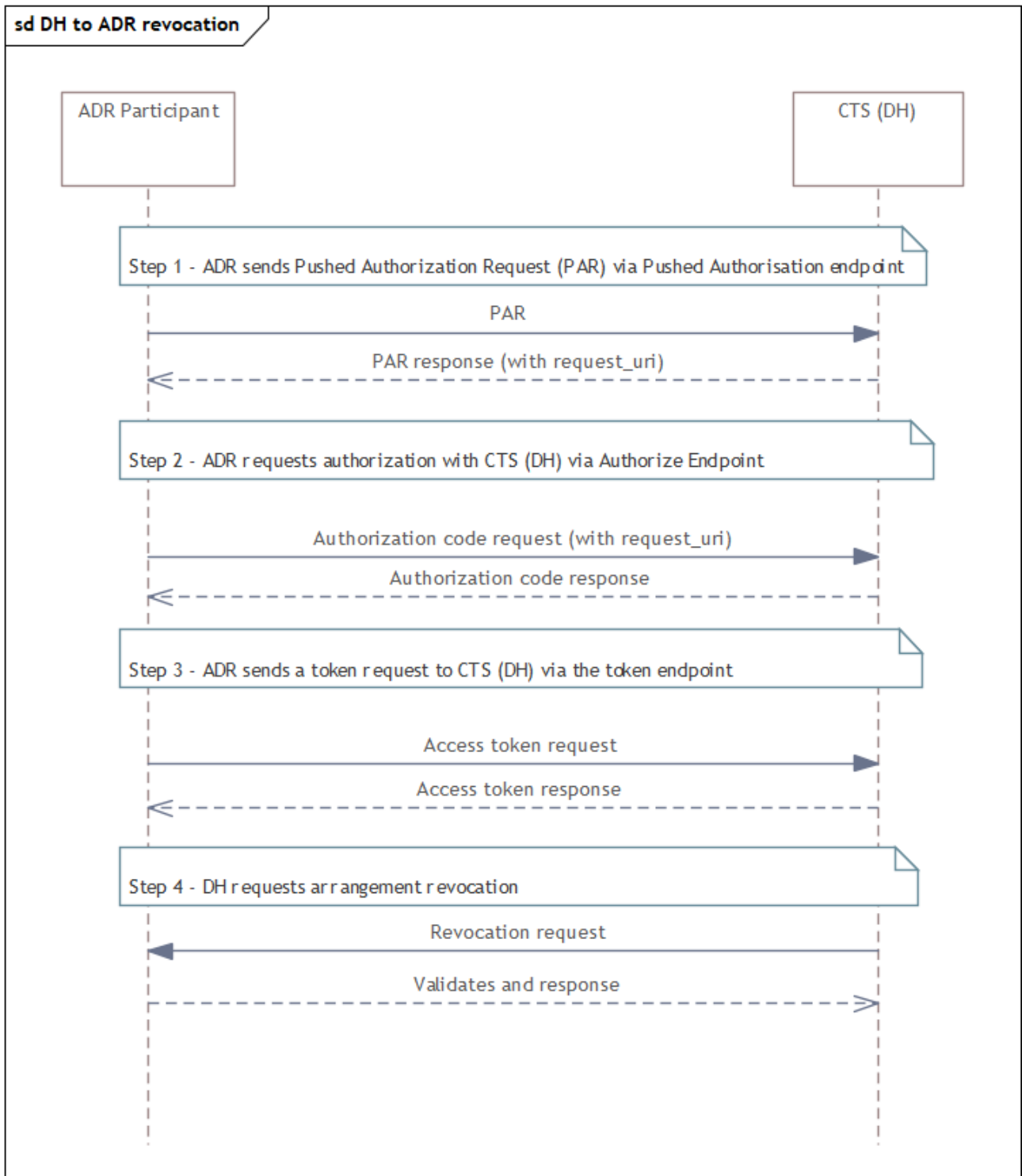
3.6.4 Test Results

You have passed the test when you can:

- receive an arrangement revocation and respond with an appropriate response [HTTP Status code 204].

3.6.5 High-Level Test Steps

- 1. ADR sends Pushed Authorisation Request (PAR) via Pushed Authorisation endpoint**
 - Participant ADR sends a PAR with the request object to the CTS Simulated DH via the Pushed Authorisation endpoint.
 - CTS Simulated DH validates the Participant ADR PAR and responds with request_uri.
- 2. ADR sends an Authorisation to the CTS Simulated DH via the Authorize endpoint**
 - Participant ADR sends an authorisation request, with the request_uri, using their DCR Client ID to the CTS Simulated DH via the Authorize endpoint.
 - CTS Simulated DH validates the ADR authorise request, verifying that the Participant ADR's software product is registered with the CTS Simulated DH and responds via the Redirect URI with Authorization Code.
- 3. ADR sends a Token request to the CTS Simulated DH via the Token endpoint**
 - Participant ADR sends a Token request to the CTS Simulated DH via the Token endpoint, exchanging their Authorization Code for a Token.
 - CTS Simulated DH validates the token request and returns an Access Token, a Refresh Token, and a cdr_arrangement_id.
- 4. ADR waits for an arrangement revocation request from the CTS Simulated DH with the cdr_arrangement_jwt**
 - CTS Simulated DH sends an arrangement revocation request to the Participant ADR via the ADR Arrangement Revocation endpoint, with their cdr_arrangement_jwt and Client Assertion sent as a Bearer Token.
 - Participant ADR validates the arrangement revocation request and returns a response [HTTP Status code 204].
 - CTS Simulated DH validates the arrangement revocation response received from the Participant ADR.



4 - DH to ADR Consent Revocation

4 Endpoints used in the CTS ADR Test Plan

A CTS Conformance ID is assigned to a Data Recipient's Software Product upon enrolment in the CTS. This ID serves as a unique identifier during CTS execution and must be included in the CTS Simulated Register and CTS Simulated DH URLs to identify the Software Product being tested. These URLs can be accessed through the domains `api.cts.cdr.gov.au` or `secure.api.cts.cdr.gov.au`.

The endpoints and URLs used in the ADR test plan are listed in the table below:

Function	Endpoint	Hosted By	Description	Relative Path
Discovery	Get OpenId Provider Config	Register	Participant ADR requests the discovery document from the CTS Simulated Register via the Get OpenId Provider Config endpoint	<code>/cts/{conformanceId}/register/idp/.well-known/openid-configuration</code>
DCR	Token	Register	Participant ADR requests a token from the CTS Simulated Register via the Register Token endpoint	<code>/cts/{conformanceId}/register/idp/connect/token</code>
	Get Data Holder Brands	Register	Participant ADR requests a list of DH brands from the CTS Simulated Register via the Get Data Holder Brands endpoint	<code>/cts/{conformanceId}/register/cdr-register/v1/{industry}/data-holders/brands</code>

	Get Software Statement Assertion	Register	Participant ADR requests an SSA from the CTS Simulated Register for the purposes of registering with a DH from the above list of DH brands via the Get Software Statement Assertion endpoint	/cts/{conformanceId}/register/cdr-register/v1/{industry}/data-recipients/brands/{dataRecipientBrandId}/software-products/{softwareProductId}/ssa
	OpenID Provider Configuration	Data Holder	Participant ADR requests a Discovery Document from the CTS Simulated DH via the OpenID Provider Configuration endpoint	/cts/{conformanceId}/dh/.well-known/openid-configuration
	JWKS	Data Holder	Participant ADR requests JWKS from the CTS Simulated DH via the JWKS endpoint	/cts/{conformanceId}/dh/.well-known/openid-configuration/jwks
	Dynamic Client Registration	Data Holder	Participant ADR sends their DCR request to the CTS Simulated DH via the Dynamic Client Registration endpoint	/cts/{conformanceId}/dh/connect/register
Consent	Authorisation	Data Holder	Participant ADR requests authorisation from the CTS Simulated DH via the Authorization endpoint	/cts/{conformanceId}/dh/connect/authorize

	Token	Data Holder	Participant ADR exchanges their code for a Token from the CTS Simulated DH via the Token endpoint Participant ADR requests a Refresh Token from the CTS DH via the Token endpoint	<code>/cts/{conformanceId}/dh/connect/token</code>
	Pushed Authorisation	Data Holder	Participant ADR sends a PAR, with Client Authentication and Replacement Claims, to the CTS Simulated DH via the Pushed Authorisation endpoint	<code>/cts/{conformanceId}/dh/connect/par</code>
Revocation	Arrangement Revocation DH to DR	Data Recipient	The CTS Simulated DH sends a request, using their cdr_arrangement_id, to the Participant ADR to withdraw arrangement consent	<code>/arrangements/revoke</code>
	Arrangement Revocation DR to DH	Data Holder	Participant ADR makes an arrangement revocation request to the CTS Simulated DH Revocation endpoint (registered uri)	<code>/cts/{conformanceId}/dh/connect/arrangements/revoke</code>

Token Revocation DR to DH	Data Holder	Participant ADR makes a Token Revocation request to the CTS Simulated DH Token Revocation endpoint (registered uri)	<code>/cts/{conformanceId}/dh/connect/revocation</code>
------------------------------	-------------	---------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------

5 Glossary

This section provides a list of CTS-specific terms and their meanings.

Term	Meaning
ADR	Accredited Data Recipient
Authenticate / authentication	When a consumer verifies themselves with a DH. For more information see: https://consumerdatastandardsaustralia.github.io/standards/#authentication-flows
Authorise / authorisation	A consumer confirming to the disclosure of their CDR data from a DH. For more information see: https://openid.net/specs/openid-connect-core-1_0.html#Overview .
Brand	A DH's system that is designed to interact with an ADR's software product.
CDR	Consumer Data Right
CDS	Consumer Data Standards
Consent	Technically used to refer to when a consumer agrees to share their CDR data with an ADR for a specific purpose (i.e. collect and use); technically distinguished from the final affirmative action (i.e. authorise) in the consent flow. Consent is also used as a term in consumer-facing interactions to refer to data sharing arrangements. Consent requirements will be communicated between the ADR and DH via the authorisation request object. The primary mechanism for capturing consent will be scopes and claims under Open ID connect. Other patterns for the establishment of consent may be considered in the future, including the incorporation of fine-grained consent for specific use cases. For more information see: https://consumerdatastandardsaustralia.github.io/standards/#consent

CTS	Conformance Test Suite
CTS Simulated Data Holder	The DH built within CTS. Used to test an ADR's software product during conformance testing.
CTS Simulated Data Recipient	The ADR built within CTS. Used to test a DH's brand during conformance testing.
CTS system	The components of the CTS that an ADR and DH will interact with during conformance testing.
CTS Simulated Register	CDR Register functionality that has been replicated within CTS. Used for testing ADR software products and DH brands during conformance testing.
DH	Data Holder
Revoke / revocation	DHs and ADRs MUST implement a CDR Arrangement Revocation endpoint as described in the Consumer Data Standards endpoints. The CDR Arrangement Revocation endpoint is used to revoke an existing sharing arrangement. DHs MUST implement a Token Revocation endpoint as described in section 2 of [RFC7009] . The revocation endpoint serves as a revocation mechanism that allows an ADR to invalidate its tokens as required to allow for token clean up. Revocation of refresh tokens and access tokens MUST be supported.
Software product	A software product developed by an ADR that is designed to interact with a DH's brand to facilitate the consent and request for consumer data.