Data Standards Body
Technical Working Group

Decision Proposal 135 – November Consent Obligations

Contact: Mark Verstege
Publish Date: 30th July 2020
Feedback Conclusion Date: To be confirmed

Context

Since version 1.2.0, the Consumer Data Standards have included standards to support concurrent consent. Based on community feedback, the solution included in version 1.2.0 was revisited and further community feedback was incorporated to address security concerns. These changes were incorporated into version 1.3.0 release in April 2020. This version incorporated a set of changes to support concurrent consent along with the introduction of some of the foundations required to enable amending consent and fine-grained consent in future. With these changes, care was given to allow for discoverability of the new capability as a mechanism for Data Holders and Data Recipients to smoothly transition current implementations.

Based on further feedback from the community via GitHub as well as an ABA workshop in July 2020, the DSB has further described how the transition of the ecosystem should take place. In addition to this, there was valid feedback that some statements in the CDR are ambiguous and clarification could assist with the transition from November 2020.

Decision To Be Made

Decide changes required to describe the transition to concurrent consent and November 2020 obligations for consent.

Current Recommendation

The following changes are recommended:

1. Fix CDR Arrangement End Point table. This end point requires Client Authentication for Data Recipients calling Data Holders.
2. Fix Pushed Authorisation Request (PAR) End Point table. This end point requires Client Authentication for Data Recipients calling Data Holders.
3. Clarify that a Data Recipient can use PAR to initiate authorisation when a Data Holder supports PAR. It is not limited to the presence of the “cdr_arrangement_id”. In fact, it is encouraged that Data Recipients use PAR when it is supported by a Data Holder. The Data Recipient MAY initiate authorisation by calling using the PAR End Point.
4. Change the deprecation date of the Data Recipient Token Revocation End Point to February 2021 to ensure Data Holders can reliably notify Data Recipients of consent withdrawal

5. Change CDR Arrangement End Point to be a POST to correctly support "`private_key_jwt`" Client Authentication.
6. Change the CDR Arrangement End Point to be the CDR Arrangement Revocation End Point because of HTTP method change to POST

Changes to current standards

Identifiers and Subject Types

CDR Arrangement ID

The CDR Arrangement ID is a unique string representing a consent arrangement between a Data Recipient and Data Holder for a given consumer.

The identifier MUST be unique per customer according to the definition of customer in the CDR Federation section of this profile.

The Data Holder MUST provide the CDR Arrangement ID as the claim "cdr_arrangement_id" in the Token End Point response and Token Introspection End Point response.

A Data Holder MUST only return the "cdr_arrangement_id" in the Token and Token Introspection End Point responses if they also support concurrent consent. This ensures that Data Recipients have a reliable way to determine whether a given Data Holder supports concurrent consent.

Statements related to the CDR Arrangement ID:

- The CDR Arrangement ID MUST be unique to a Data Holder
- The CDR Arrangement ID MUST be non-guessable and must not identify a consumer
- A CDR Arrangement ID SHOULD be generated using an algorithm that reduces the chances of collision
- A CDR Arrangement ID MUST be static across consents within the one sharing arrangement (e.g. across consent renewal and re-authorisation)

Retrospectively obtaining a CDR Arrangement ID

For any existing consents, Data Holders must retrospectively generate a "cdr_arrangement_id" such that from November 2020, Data Recipients can obtain a valid "cdr_arrangement_id" for all active consents they hold.

A Data Recipient can call either the Token or Token Introspection End Points at any point post-consent to obtain the CDR Arrangement ID in the response JSON as the claim "cdr_arrangement_id".

Request Object

Specifying an existing arrangement

Provided a Data Holder supports PAR, they MUST also support the “cdr_arrangement_id” claim provided in the Request Object sent to the PAR End Point. The Data Recipient MAY provide the “cdr_arrangement_id” claim in the Request Object sent to the PAR End Point.

The “cdr_arrangement_id” claim MUST be handled as follows:

Until November 2020 data holders are not required to take any action if “cdr_arrangement_id” is supplied but MUST NOT respond with an error.

Until November 2020 data recipients MUST NOT implement scenarios that support concurrent consent. Only single, extant consent scenarios should be implemented until this date.

If a data recipient provides the “cdr_arrangement_id” claim in the request object to the data holder's PAR End Point, the data holder MUST revoke any existing tokens related to the arrangement once the new consent is successfully established and a new set of tokens has been provided to the data recipient.

For data recipients seeking to replace consent where the Data Holder does not support PAR, data recipients MUST actively revoke previously supplied refresh tokens, immediately after receiving the tokens for a newly established consent, using the appropriate revocation end point.

End Points

OpenID Provider Configuration End Point

- cdr_arrangement_revocation_endpoint: The URL of the CDR Arrangement Revocation End Point for consent revocation

Token Revocation End Point

Description	Value
Hosted By	Data Holder and Data Recipient
Transport Security	MTLS for Data Holders, TLS for Data Recipients
Client Authentication Required	Yes (for verifying Data Recipients)
Bearer Token Required	Yes (for verifying Data Holders)

Requirements for Data Recipient implementations

The Token Revocation End Point, when implemented by the Data Recipient allows a Data Holder to notify the Data Recipient of the revocation of a sharing arrangement by the Customer in totality as required by the ACCC CDR Rules. This revocation will have been actioned by the Customer via the Data Holder's consent dashboard as described in the ACCC CDR Rules.

Revocation of Access Tokens MUST not be supported.

Revocation of Refresh Tokens MUST be supported and will be used to notify the Data Recipient of sharing revocation.

If consent is withdrawn by a Customer in writing or by using the Data Recipient's dashboard the Data Recipient MUST revoke consent using Data Holder's implementation.

Revoking consent

If the Data Holder **does not** support a CDR Arrangement Revocation End Point, Data Recipients MUST use the Data Holder's Token Revocation End Point with the current Refresh Token to notify the Data Holder.

If the Data Holder **does** support the CDR Arrangement Revocation End Point, Data Recipients MUST use the Data Holder's CDR Arrangement Revocation End Point with a valid "cdr_arrangement_id" to notify the Data Holder.

NOTE: Data Recipients MUST continue to support this Token Revocation End Point until February 2021.

CDR Arrangement Revocation End Point

Description	Value
Hosted By	Data Holder & Data Recipient
Transport Security	MTLS for Data Holders, TLS for Data Recipients
Client Authentication Required	Yes (for Data Holders verifying Data Recipients)
Bearer Token Required	Yes (for Data Recipients verifying Data Holders)

HTTP Method: POST

Data Holder Path: The "cdr_arrangement_revocation_endpoint" defined using OIDC Discovery

Data Recipient Path: /arrangements/revoke

From November 2020, Data Holders and Data Recipients MUST implement a CDR Arrangement Revocation End Point that can be used to revoke an existing sharing arrangement.

The request MUST include the following parameters using the “application/x-www-form-urlencoded” format in the HTTP request entity-body:

“cdr_arrangement_id”: The ID of the arrangement that the client wants to revoke.

This end point will be implemented according to the following:

- Data Recipients and Data Holders MUST revoke consent by calling the CDR Arrangement Revocation End Point with a valid CDR Arrangement ID
- Data Holders MUST publish their CDR Arrangement Revocation End Point using their OpenID Provider Metadata Discovery End Point
- Data Recipients MUST expose their CDR Arrangement Revocation End Point under their Recipient Base URI published in their Software Statement Assertion
- Consent revocation MUST also revoke associated refresh and/or access tokens
- For Data Recipients, Data Holder must be authenticated when they call this end point according to the guidance in the Client Authentication section.
- If the “cdr_arrangement_id” is not related to the client making the call it MUST be rejected

Response Codes

The following responses are in addition to error responses covered by normative references. Error scenarios is the following table MUST use the error structure defined in the Payload Conventions.

Response Code	Situation	Description
204 No Consent	Success	The sharing arrangement has been revoked successfully
422 Unprocessable Entity	Invalid Arrangement ID	The client submitted an invalid arrangement identifier or the identifier could not be found

Data Holders calling Data Recipients

Data Holders may discover that a given Data Recipient supports the CDR Arrangement Revocation End Point by the presence of the Recipient Base URI in the Software Statement Assertion (SSA). If a Data Recipient does not support the CDR Arrangement Revocation End Point, the Data Holder MUST call the Data Recipient Token Revocation End Point.

Data Recipients SHOULD update their client registration with each Data Holder as soon as is practical once they support the CDR Arrangement Revocation End Point .

Data Recipients MUST continue to support their Token Revocation End Point until February 2021.

Updating Register Meta Data and Client Registration

When a Data Recipient supports the CDR Arrangement Revocation End Point, they MUST:

1. Update their meta data with the CDR Register to include their “recipient_base_uri”.

2. Update their client registration with each Data Holder.

If the Data Recipient does not support the CDR Arrangement Revocation End Point, the Data Holder MUST instead revoke consent using the Data Recipient Token Revocation End Point.

Data Recipients calling Data Holders

Data Recipients may discover that a given Data Holder supports the CDR Arrangement Revocation End Point by the presence of the ”cdr_arrangement_revocation_endpoint” in the Data Holder's OpenID Provider metadata.

If a Data Recipient does not support the CDR Arrangement Revocation End Point , Data Holders must notify Data Recipients when consent is withdrawn by calling the Data Recipient Revocation End Point.

Pushed Authorisation Request End Point

Description	Value
Hosted By	Data Holder
Transport Security	MTLS
Client Authentication Required	Yes
Bearer Token Required	No

From November 2020, Data Holders MUST support Pushed Authorisation Requests (PAR) via the pushed authorisation end point according to [PAR].

Data Recipients MAY send authorisation requests using [PAR] if supported by the Data Holder. Request objects which contain the “cdr_arrangement_id” claim MUST only be sent using [PAR]. If a Data Holder does not support [PAR], a Data Recipient SHOULD NOT provide the “cdr_arrangement_id” claim in the request object.

The Data Holder response provides the Data Recipient with a Request URI in the response. The Request URI is then passed to the Data Holder’s Authorisation End Point to initiate an authorisation flow.

In addition:

- Request Object references SHALL NOT be supported in any mode of use other than Pushed Authorisation Requests (PAR). If a Data Holder does not support Pushed Authorisation Requests (PAR), it MUST NOT support Request Object references.
- The Request URI MUST expire between 10 seconds and 90 seconds
- Data Recipients MAY provide an existing “cdr_arrangement_id” claim in an authorisation request object to establish a new consent under an existing arrangement

- Data Holders MUST revoke existing refresh tokens and access tokens when a “cdr_arrangement_id” is provided in the Request Object but only after successful authorisation
- If the “cdr_arrangement_id” is not related to the consumer being authenticated it MUST be rejected
- If the “cdr_arrangement_id” is not recognised by to the Data Holder it MUST be rejected