Data Standards Body

Technical Working Group

Decision Proposal 209 - Transition to FAPI 1.0 Advanced Profile

Contact: Mark Verstege

Publish Date: 18th October 2021

Feedback Conclusion Date: 16th November 2021

Context

As with all normative standards the Consumer Data Standards relies upon, these change over time. Maintaining and uplifting the Consumer Data Standards in line with the changes to the normative standards is important to maintain vendor support, lower cost of ownership for participants and ensure the security of the Consumer Data Standards is kept strong and current.

The Consumer Data Standards Information Security profile currently leverages Financial-Grade API (FAPI) Implementer's Draft v06 (ID2 Draft 06) and Pushed Authorization Request (PAR) Draft 01. Since the finalisation of version 1.0 of the Consumer Data Standards, the FAPI 1.0 standards have also been finalised and PAR has been finalised as RFC 9126. This has introduced a small set of significant changes that impact existing implementations.

Recommendation 1 in Decision 182 approved migration of the Consumer Data Standards to the FAPI 1.0 Advanced Profile and PAR Draft 10. This decision proposal considers the changes required within a transition timeframe that supports the Energy sector's entry into the CDR. As such, it is proposed that uplift for existing Data Holders and Data Recipients be completed before October 2022 obligations for data sharing in Energy.

A gap analysis of the current Consumer Data Standards against FAPI 1.0 and PAR Draft 10 have been conducted. This analysis defines the changes required.

- FAPI Part 1 Analysis
- FAPI Part 2 Analysis
- Pushed Authorization Requests (PAR) analysis

This decision proposal presents a recommendation as a series of transition steps. It further poses a set of questions for design consideration. Feedback is sought on the key design questions, the phasing scope and obligation dates proposed.

Decision To Be Made

- The changes required to adopt FAPI 1.0 for Data Recipients and Data Holders as well as the migration plan for phased introduction that de-risks implementation within timeframes for Energy data sharing.

Design questions

1. **General questions**

   (a) Should Refresh token expiry time be pegged to consent duration?

   The current refresh token expiry time, expressed using the "refresh_token_expires_at" claim, is tied to the consent's sharing duration on token issuance. Each time a new refresh token is issued, the Data Holder must set the expiry time to be the lesser of the Data Holder's default refresh token cycle time or the duration of the sharing arrangement.

   > *Refresh Token expiration MAY be any length of time greater than 28 days but MUST NOT exceed the end of the duration of sharing consented to by the Consumer.*

   Coupling security and business logic may lead to increased complexity and customisation at the security layer. Should this requirement be decoupled such that the consent's sharing arrangement status is verified independently of refresh token status?

   Doing so would introduce a breaking change for Data Recipients and Data Holders.

   (b) Should CDR authorisation input parameters be registered or otherwise moved out of the authorisation request object? If so, where should they be moved to for better Identity & Access Management (IAM) software supportability?

   The Consumer Data Standards define jurisdictional input parameters including:

   - cdr_arrangement_id (Authorisation request object JWT claim)
   - sharing_duration (Authorisation request object JWT claim)

   Should international registration of these claims and/or moving these claims to a different location be considered in the migration to FAPI 1.0? Alternatively, is it preferrable that this be addressed as part of Decision Proposal 210 (transition to support FAPI 2.0) where specifications such as Rich Authorization Requests (RAR) would provide facilitate the technical solution?

   (c) Should CDR token response parameters be registered or otherwise moved out of the parent token endpoint response JSON / ID token JWT? If so, where should they be moved to for better Identity & Access Management (IAM) software supportability?

   The Consumer Data Standards define jurisdictional claims/ input parameters including:

   - cdr_arrangement_id (Token response JSON)
   - sharing_expires_at (ID Token JWT)
   - refresh_token_expires_at (ID Token JWT)

   Should the migration be considered in the transition to FAPI 1.0? Alternatively, is it preferrable that this be addressed as part of Decision Proposal 210 (transition to support FAPI 2.0) where specifications such as Rich Authorization Requests (RAR) would provide facilitate the technical solution?

2. **Phase 1**
    (a) **Should the CDS explicitly define the request_uri must only be used once and cannot be replayed?**
    Refer to s 4. of the RFC9126 (PAR) specification.

    (b) **Should the CDS explicitly define the upper lifetime of the PAR request_uri? If yes, what is the acceptable lifespan (e.g., 60 minutes)?**
    Refer to s 2.2 "expires_in" of the RFC9126 (PAR) specification.

    (c) **Should the Data Standards make requiring PAR mandatory for all Data Holders and Data Recipients?**
    Refer to s 5. "require_pushed_authorization_requests" of the RFC9126 (PAR) specification.

3. **Phase 3**
    (a) **Should JARM be supported when response_type is "code"?**
    Refer to s 5.1.2 of the FAPI 1.0: Advanced profile.

    (b) **Should the Data Standards *require* JARM when response_type is "code"?**
    Refer to s 5.1.2 of the FAPI 1.0: Advanced profile.

    (c) **Should the CDS mandate that the same "kid" is not allowed to be used by multiple keys within a JWKS?**
    Refer to s 8.9 of the FAPI 1.0: Advanced profile.

Identified Options

Transition approach

The transition options impact existing Data Recipient and Data Holder implementations as well as any entrants within the CDR before final transition to FAPI 1.0.

Phase 1

Phase 1 introduces PAR and FAPI 1.0 changes with minimal impacts to Data Recipients and Data Holders.

The proposed obligation date for Phase 1 is 1st March 2022. Because changes may have some impact in a many-to-many ecosystem, a future dated obligation is proposed. If feedback indicates an early obligation date or immediate adoption of Phase 1, this will be considered.

Request URI Replay (PAR)
PAR: § 4.

Change	Request URI replay is not permitted. Data Holders must reject the reuse of the request_uri.
Requirement	Mandatory
Description	• The request_uri is provided in exchange for a Data Recipient staging their authorisation request using PAR • Data Holders must reject Data Recipients that attempt to re-use the request_uri more than once. • If the Data Recipient's authorisation request fails for whatever reason (be it technical or consumer denies the authorisation), the Data Recipient needs to stage a new authorisation request via the PAR endpoint • The Data Holder will then issue a new request_uri which the Data Recipient can use to commence authorisation
Impacts	• Data Holders must reject authorisation requests where the request_uri has already been presented • Data Recipients should not reuse the same request_uri. If they do, the authorisation request will be rejected.

Require Pushed Authorization Requests (PAR)
PAR: § 5.

Change	Data Holders MAY choose to support PAR only and require all request object submissions to be done in the back channel using the PAR lodgement process. In other words, Data Holders may support the "require_pushed_authorization_requests" equal to "true". This is at the discretion of the Data Holder.
Requirement	Optional
Description	• Data Holders may elect to support request object submission only using the PAR submission process. • If they do so, they can advertise this to Data Recipients using the "require_pushed_authorization_requests" OIDD parameter. • This can simplify the Data Holder's implementation • Increases security • Allows Data Holders to move towards the target state of PAR only authorisation requests as soon as is practical for the Data Holder
Impacts	• Data Recipients must verify the value of "require_pushed_authorization_requests" in the Data Holder's OIDD (default to False). • If True, Data Recipients must pass Request Objects to the PAR endpoint,

	• If True, Data Holders must reject Request Objects passed to the Authorization endpoint. • The Data Holder must also appropriately populate Dynamic Client Registration response metadata with the "require_pushed_authorization_requests" value set to "true" in line with PAR s "6. Client Metadata"

PKCE Support (PAR, RFC 7636)
FAPI 1.0: Advanced, § 5.2.2. (18)

Change	Data Holders MAY optionally support PKCE (response_type of "code" only).
Requirement	Optional
Description	The Data Holder publishes supported PKCE code challenge methods in their OpenID Provider Metadata Discovery Document using the "code_challenge_methods_supported" metadata parameter. If published, the Data Holder supports PKCE. If the Data Recipient determines that the PKCE is supported, they may initiate an authorisation request with a code verifier and response_type of "code". If the Data Holder elects to require PAR only request object submission via "require_pushed_authorization_requests"
Impacts	• No breaking changes. Data Holders may choose to support PKCE. If so, Data Holders must not refuse clients that do not support PKCE. Specifically, Data Holders must not refuse clients that support response_type "code id_token". • Data Holders that support PKCE must accept clients presenting response_type "code". • Data Holders that do not support response_type "code" may reject such requests (in other words, the Data Holder only supports response_type "code id_token"). • If Data Holders do not support PKCE they must not reject clients presenting code verifiers. Instead, code_verifier should be ignored. • Similarly, Data Recipients may optionally implement PKCE support.

Authorisation Code Reuse (*FAPI 1.0 Baseline)*
FAPI 1.0: Advanced, § 5.2.2. (13)

Change	Require Data Holders to enforce protections against reuse of authorisation codes
Requirement	Mandatory
Description	Data Holders upon receipt of an authorisation code which has previously been used by the Data Recipient client to obtain authorisation tokens must reject subsequent reuse of the authorisation code.
Impacts	• Data Recipients cannot attempt to obtain authorisation tokens using an authorisation code they have previously used • Data Holders must reject attempts to reuse an authorisation code

Scope Request Support (*FAPI 1.0 Baseline)*
FAPI 1.0: Advanced, § 5.2.2. (15)

Change	Data Holders may implement FAPI 1.0 scope requirements in the token response such that the scope value is not mandated where scopes requested are equivalent to scopes authorised.
Requirement	Optional
Description	• In all other scenarios, the scopes value must still be returned in the authorisation response • Data Holders may continue to support the scope response value as-is and always return the scope value (hence no impact to existing implementations) • Data Recipients must update their software products to check if the scope list is returned • Behaviour aligns to RFC6749 s 5.1 such hat the scope value is only "OPTIONAL, if identical to the scope requested by the client; otherwise, REQUIRED.
Impacts	• Data Recipients must check for the absence of the scope value. If not present, all requested scopes were granted • Data Recipients must check the list of scopes returned (granted) against the list requested. Where the list differs, the Data Recipient should not make a request to data endpoints that require one of the unauthorised scopes. If they do, the request will be denied. • At the discretion of the Data Holder if they optionally return scope in this scenario or continue to always return the list of scopes granted

Multi-Brand Support (Separate Issuers For Data Holder Brands) (*FAPI 1.0 Baseline)*
FAPI 1.0: Baseline, § 7.7.

Change	Where a Data Holder has multiple brands, each brand must have a separate issuer
Requirement	Mandatory
Description	• This provides greater flexibility in future rather than tightly coupling multiple brands to the one issuer context.
Impacts	• Any Data Holders currently representing multiple brands under one issuer must change to separate issuers immediately

x-fapi-customer-ip-address (*FAPI 1.0 Baseline)*
FAPI 1.0: Baseline, § 6.2.1. (13)

Change	Data Holders shall not reject requests with a "x-fapi-customer-ip-address" header containing a valid IPv4 or IPv6 address.
Requirement	Mandatory
Description	• If a Data Holder is actively rejecting Data Recipient requests based on the contents of the "x-fapi-customer-ip-address" it must not reject a request where the value is a valid IPv4 or IPv6 addresses
Impacts	• Minimal impact. It is expected that few, if any, Data Holders are rejecting requests based on the contents of this header • Currently this header is not defined in the FAPI 2.0 Implementer's Draft. • This header is no longer included in the core FAPI 2.0 specification, moving into advice documentation. The long-term benefit or implementation of this field is limited.

Request Object Expiry
FAPI 1.0: Advanced, § 5.2.2. (13), § 5.2.3. (10, 11, & 14),

Change	Data Holders must reject "exp" claim which has a lifetime of more than 60 minutes after the "nbf" claim value. **NOTE:** Refer to Phase 1 design question 4. (a)
Requirement	Mandatory
Description	Data Holders must validate that the "exp" is no longer than 60 minutes *after* the value provided in the "nbf" claim value. Further, request objects must contain "nbf" and "aud" claims in line with s 5.2.3 (10, 11, & 14).

Impacts	• Data Holders may require an update to their authorisation request and PAR request implementations to correctly reject request objects that do not meet the expiry lifetime requirements • Data Recipients must not send a request object to a Data Holder where the "exp" is beyond the accepted lifetime after the "nbf", else their authorisation request will be rejected.

Phase 2

The proposed obligation date for Phase 2 is 1st May 2022.

Adopt FAPI 1.0: Baseline (Final)
Full adoption of Baseline specification

Content-Type Header Requirement (*FAPI 1.0 Baseline)*
FAPI 1.0: Baseline, § 6.2.1. (9)

Change	Charset is no longer required. Data Holders must not reject Content-Type headers without charset. Equally, Data Holders must not reject Content-Type headers with a valid charset specified.
Requirement	Mandatory
Description	• Data Holders must validly accept Content-Type without charset specified (equivalent to charset=UTF-8)
Impacts	• No impact to existing implementations

Require Pushed Authorization Requests (PAR)
PAR: § 5.

Change	Data Holders MUST only support request object submission using PAR. In other words, Data Holders MUST support the "require_pushed_authorization_requests" equal to "true" and reject request object submission via the authorization endpoint.
Requirement	Mandatory
Description	• Changes the optional enforcement of PAR to be required by all Data Holders • Request object submission is only supported via reference whereby the Data Recipient stages the authorisation intent using the Data Holder's PAR endpoint
Impacts	• Any Data Recipient currently passing request objects by value must switch to using the PAR request object submission pattern exclusively • **Because Data Holders currently support PAR, it is recommended that Data Recipients switch to only use PAR lodgement of the request**

	object as soon as is practicable. This can occur at any time with immediate effect. • Data Holders must reject request object submission passed by value to the authorisation endpoint • Data Holders must require PAR requests and set "require_pushed_authorization_requests: to true in their OIDD document.

PKCE Support (PAR)
FAPI 1.0: Advanced, § 5.2.2. (18)

Change	Data Holders must support PKCE (response_type of "code" only). Data Recipients must support PKCE.
Requirement	Mandatory
Description	Data Holders must support PKCE. Similarly, Data Recipients must send PKCE code verifiers and support all client aspects of the PKCE specification
Impacts	• Data Holders must reject non PKCE client requests • Data Recipients must implement PKCE client requirements

Phase 3

Phase 3 full aligns to final upstream specifications.

The proposed obligation date for Phase 3 is 1st July 2022.

Adopt FAPI 1.0: Advanced (Final)
Full adoption of Advanced specification. Both FAPI 1.0: Baseline (Final) and FAPI 1.0: Advanced (Final) are now completely mandated.

Cipher support
FAPI 1.0: Advanced, § 8.5.

Change	Defer to additional cipher support introduced in FAPI 1.0: Advanced section 8.5 permitting the use of ciphers defined by BCP 195.
Requirement	Mandatory
Description	As part of the full adoption of FAPI 1.0: Advanced, cipher support is extended to recommendations presented in BCP 195 for TLS 1.2. If the Data Holder supports TLS 1.2, the four mandatory ciphers defined in s 8.5 are still required
Impacts	• Data Holders have wider discretion of cipher support. • Data Recipients must update cipher library support to any and all BCP 195 recommended TLS 1.2 ciphers.

Ignore Claims Outside The Request Object
FAPI 1.0: Advanced, § 5.2.2. (10)

Change	Parameters shall be included in the request object and any parameters provided outside the request object shall be ignored.
Requirement	Mandatory
Description	Where the client presents claims outside the request object, the Data Holder must ignore those values. This is simply an alignment to the upstream FAPI specification and should present minimal impact. It is recommended, but not necessary, that Data Recipients should not send claims outside the request object unless required by the normative standards to do so.
Impacts	• Data Holders must ignore any claims presented outside the request object • Data Holders must still verify claims outside the request object are the same value as those presented in the request object to prevent mix up attacks • Data Recipients should not present claims outside the request object

Adopt PAR RFC 9126
Full adoption of Pushed Authorization Request specification.

Summary

The phasing of changes presented above has been summarised in the following table:

	Current State	Phase 1	Phase 2	Phase 3 (FAPI 1.0 Target State)
		1st March 2022	1st May 2022	1st July 2022
FAPI 1.0: Baseline (Final) support	Implementer's Draft 2 (Draft 06)	Partial	**Fully supported**	Fully supported
Scope Request Support	Always	Optional FAPI 1.0	FAPI 1.0	FAPI 1.0
Ignore Claims Outside The Request Object	Not specified	Not specified	SHALL ignore	SHALL ignore
Authorization Code Reuse	SHOULD refuse	MUST refuse (Not Allowed)	MUST refuse (Not Allowed)	MUST refuse (Not Allowed)
Content-Type Header Requirement	SHOULD support	SHOULD support	MUST support (FAPI 1.0)	MUST support (FAPI 1.0)
FAPI 1.0: Advanced (Final) support	Implementer's Draft 2 (Draft 06)	Partial	Partial	**Fully supported**
Cipher Support	Draft 06	Draft 06	Draft 06	FAPI 1.0
JARM Support	No	No	No	No
PAR version	Draft 01	Draft 01	Partial RFC 9126	**RFC 9126**
Require Pushed Authorization Requests	Not supported	Optional	Mandatory	Mandatory

Request Object Submission	Authorisation endpoint and PAR	Authorisation endpoint and PAR	PAR only	PAR only
PKCE Support (RFC 7636)	Not specified	Optional	Mandatory	Mandatory
response_type	code id_token	code id_token (unless supporting PKCE)	code	code
Request URI Replay	SHOULD refuse	MUST refuse (Not Allowed)	MUST refuse (Not Allowed)	MUST refuse (Not Allowed)
Multi-Brand Support (Separate Issuers For Data Holder Brands)	Separate issuer	Separate issuer	Separate issuer	Separate issuer
Access Token Revocation	Mandatory	Mandatory	Mandatory	Mandatory

Current Recommendation

It is recommended that the transition to FAPI 1.0 (Final) and PAR (RFC 9126) adoption within the CDR is conducted over three phases with obligation dates of 1st of March 2022, 1st of May 2022, and 1st July 2022. These transitions will increase alignment to FAPI 1.0 (Final) and PAR (RFC 9126).

As part of the transition, it is recommended that an independent security review is conducted on the target state drafts to the Information Security profile.

Implementation Considerations

Energy sector

The Energy sector has a planned go-live of consumer data sharing in October 2022. To meet this date, implementation certainty of the Information Security profile is required to allow energy Data Holders confidence to build against a stable specification. By aligning to the FAPI 1.0 (Final) profile for energy obligations this reduces customisation for energy Data Holders and accelerates implementation.

Furthermore, Data Recipients seeking to provide cross-sector use cases can implement software products that can reliably interoperate across banking and energy Data Holders.

Data Recipients

Phasing has considered a progressive approach that reduces change impact to Data Recipients and minimises the risk of a single cutover date. Instead, the phasing has sought to resolve minor low-hanging fruit that will have little to, no, impact to Data Recipients in Phase 1 towards progressive support of PKCE and client enhancements before fully supporting FAPI 1.0 (Final).

Banking sector

As the only sector currently live within the CDR, careful consideration has been given to the transition of the banking sector Data Holders to minimise build impact in the early phases whilst progressively moving towards increased vendor support as the final version of FAPI 1.0 is adopted. Phasing has considered mechanisms that support Data Holders progressing enhancements early where possible, whilst keeping larger changes to later phases of the transition.

Conformance Testing

Sufficient time needs to be provided where breaking changes also impact tests included in the ACCC Conformance Test Suite. As a quality release gate for Data Recipients and Data Holders, participants require sufficient lead time to complete additional testing required by the Registrar before release.

Additionally, in consideration of breaking changes, the Registrar requires time to update or add new test cases where required.

Security Review

After collation of community feedback and drafting of all changes, it is recommended that the Data Standards Chair conducts an independent security review of the Consumer Data Standards Information Security profile. This review, like previous reviews conducted against the Information Security profile, will review the controls defined by the standards. This review is sought against the draft target state such that the proposed FAPI 1.0 target state is stable, and any changes recommended by the review can be incorporated as required.

A second independent security review will be conducted on completion of the draft FAPI 2.0 target state after community consultation.

Existing Consumer Data Standards FAPI statements

The following section details the existing statements in the CDS that define variations to the baseline FAPI specifications.

OIDC Hybrid Flow

Only a response_type (see section 3 of **[OIDC]**) of code id_token SHALL be allowed.
The request_uri parameter is only supported if the Data Holder supports PAR.

OIDC Client Types

Only Confidential Clients SHALL be supported under this profile. Therefore, Public clients SHALL NOT be supported.
In reference to the client types referenced in section 2.1 of **[OAUTH2]**:

- Confidential Clients MUST be supported under this profile.
- Public clients MUST NOT be supported.

Claims

- refresh_token_expires_at: indicates the date-time at which the most recently provided refresh token will expire. Its value MUST be a number containing a NumericDate value, as specified in section 2 of section 2 **[JWT]**. If no refresh token has been provided then a zero value should be returned.
- sharing_expires_at: indicates the date-time at which the current sharing arrangement will expire. Its value MUST be a number containing a NumericDate value, as specified in section 2 of **[JWT]**. If consent is not complete or a sharing_duration was not requested in the authorisation request object then a zero value should be returned.

Refresh Token

Refresh Tokens MUST be supported by Data Holders.
The usage of Refresh Tokens is specified in section 12 of **[OIDC]**.
The expiration time for a Refresh Token MUST be set by the Data Holder.
Refresh Token expiration MAY be any length of time greater than 28 days but MUST NOT exceed the end of the duration of sharing consented to by the Consumer.
Data Holders MAY cycle Refresh Tokens when an Access Token is issued. If Refresh Token cycling is not performed then the Refresh Token MUST NOT expire before the expiration of the sharing consented by the Customer.

Token Expiry

The expiry time for issued access tokens and refresh tokens must be deterministic for the Data Recipient.
In order to achieve this:

- The Data Holder MUST indicate the lifetime in seconds of the access token in the expires_in field of the JSON object returned by the token end-point (see section 4.2.2 of **[OAUTH2]**).

- The Data Holder MUST indicate the expiration time of the refresh token using the refresh_token_expires_at claim.

Request Object

Requesting Sharing Duration

To facilitate the specification of the duration for consent to share CDR data that is approved by the consumer, a mechanism for the Data Recipient to specify a sharing duration to the Data Holder is required.

To accomplish this, the Data Holder MUST support an additional claim in the authorisation request object named sharing_duration. The sharing_duration claim MUST be handled as follows:

- The sharing_duration parameter is a number
- The value of the sharing_duration parameter will contain the requested duration for sharing, in seconds.
- If the sharing_duration value exceeds one year then a duration of one year will be assumed.
- If the sharing_duration value is less than or equal to 24 hours, then one-time collection will be assumed, and a Refresh Token should be provided by the Data Holder
- If the sharing_duration value is zero or absent then once off access will be assumed and only an Access Token (without a Refresh Token) will be provided on successful authorisation.
- If a Refresh Token is issued for one-time collection the Data Recipient must call the Data Holder's revocation endpoint after successful collection of the CDR data.
- If the sharing_duration value is negative then the authorisation should fail.

Note that the period of one year in the above statements should be interpreted as 365, 24 hour days (or 31,536,000 seconds).

The Data Recipient is able to obtain the expiration of sharing via the sharing_expires_at claim.

CDR Arrangement ID

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.

Obtaining a CDR Arrangement ID

For any existing consents, Data Holders must retrospectively generate a cdr_arrangement_id such that 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.

Ciphers

Only the following cipher suites SHALL be permitted in accordance with section 8.5 of **[FAPI-RW]**:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Introspection End Point

Data Holders MUST implement an Introspection End Point to allow Data Recipients to determine the status and expiry date of Refresh Tokens. The requirements for an Introspection End Point are described in section 2 of **[RFC7662]**.

Introspection of Refresh Tokens MUST be supported.

Introspection of Access Tokens and ID Tokens MUST NOT be supported.

A Token Introspection End Point Response SHALL include, at least, the following fields:

- active: Boolean indicator of whether or not the presented token is currently active.
- exp: A JSON number representing the number of seconds from 1970-01-01T00:00:00Z to the UTC expiry time.
- scope: A JSON string containing a space-separated list of scopes associated with this token.
- cdr_arrangement_id: A unique identifier of the CDR arrangement related to the authorisation.

A Token Introspection End Point Response MAY include claims defined in Section 2.2 of **[RFC7662]** but username SHALL NOT be allowed.

Token Revocation End Point

Requirements for Data Holder implementations

Data Holders MUST implement a Token Revocation End Point as described in section 2 of **[RFC7009]**.

The Revocation End Point serves as a revocation mechanism that allows a Data Recipient to invalidate its tokens as required to allow for token clean up.

Revocation of Refresh Tokens and Access Tokens MUST be supported.