Data Standards Body

Technical Working Group

Decision 209 - Transition to FAPI 1.0 Advanced Profile

Contact: Mark Verstege
Publish Date: December 13th 2021
Decision Approved By Chairman: December 16th 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.

This decision presents a set of recommendations as a series of transition steps.

Decision To Be Made

1. 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.

Feedback Received

The Data Standards Chair welcomes the feedback of all participants in response to the Decision Proposal. The feedback provided strong consensus for a preferred target state in line with the proposal presented.

Feedback was in response to several questions and the proposed phasing schedule. The feedback is summarised against each question below.

Design questions

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

- Feedback supported removing refresh token cycling.
- The feedback indicated that refresh token cycling is not required for confidential clients and it has caused consumer-facing impacts due to technical issues.
- Further, feedback indicated that refresh token cycling will not be recommended in the final FAPI 2.0 profile specification and it is not in common use in other jurisdictions.

1. (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?

- Feedback supported retaining the claims as-is until the Data Standards support the Rich Authorization Requests (RAR) specification as part of the FAPI 2.0 target state.
- In principle feedback supported standardisation without registering the CDR-specific claims internationally.

1. (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?

- Feedback identified that the "sharing_expires_at" and "refresh_token_expires_at" claims can be retired once refresh token cycling has been deprecated. This would simplify the token response and remove redundant claims. The normative "exp" claim would represent the expiry time of the authorisation and consequently the sharing arrangement.
- Feedback indicated that the "sharing_duration" and "cdr_arrangement_id" can be moved into the RAR response as part of the FAPI 2.0 target state but not before.
- Feedback indicated the "grant_id" from Grant Management could replace the "cdr_arrangement_id" longer term.

2. (a) Should the CDS explicitly define the request_uri must only be used once and cannot be replayed?

- Feedback indicated that single use Request URI was supported.
- Feedback also supported an explicit statement be made in the Consumer Data Standards to that affect for both Data Recipient relay and Data Holder validation.

2. (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)?

- Feedback supported a short expiry time for the Request URI
- Respondents indicated a minimum of 10 seconds and a maximum of 90 seconds would be an acceptable lifespan for the Request URI.

2. (c) Should the Data Standards make requiring PAR mandatory for all Data Holders and Data Recipients?

- Feedback was consistent in support of a PAR-only end state for the lodgement of the authorisation request.
- This would allow for the deprecation of the request object being sent in the front channel to the Authorization end point in preference for a PAR only lodgement of the request object.

- Feedback indicated this would improve security and reduce the potential front channel attack surface.

3. (a) Should JARM be supported when response_type is "code"?

- Feedback indicated that JARM must be supported if the response type of "code" is adopted as defined and required in FAPI 1.0 Final.
- Feedback indicated that the support of JARM is not a high implementation impact but could be a phased target state to allow Data Recipients to transition from the OIDC Hybrid Flow (response type "code id_token").

3. (b) Should the Data Standards require JARM when response_type is "code"?

- As above, the use of JARM s required where the response type "code" is supported. Therefore, it must be required and the FAPI 1.0 Final normative reference can be relied upon.

3. (c) Should the CDS mandate that the same "kid" is not allowed to be used by multiple keys within a JWKS?

- Respondents supported the Consumer Data Standards explicitly requiring a unique "kid" and prohibiting re-use.

Transition approach

- One Data Holder supported a single phase with a cutover date for supporting FAPI 1.0 Final
- Respondents supported Data Holders the discretion to adopt FAPI 1.0 Final enhancements ahead of the mandatory obligation dates.
- Some respondents supported fewer phases
- Some feedback indicated a longer delivery time of October 2022 for final obligation dates.
- One participant supported a shorter delivery time of May 2022 for final obligation dates.

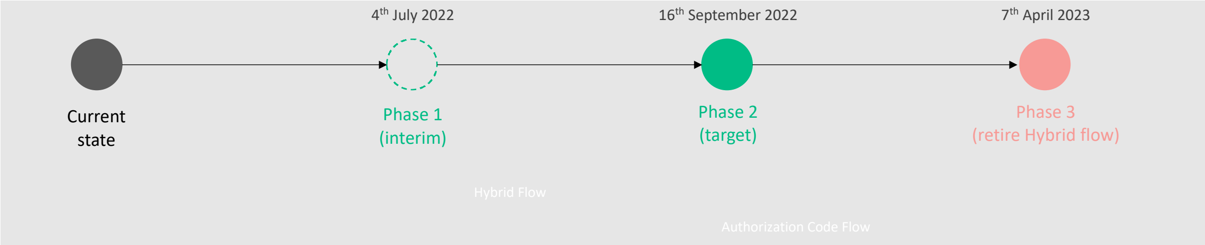
Additional feedback

- Some respondents indicated that long-term support for message integrity was supported and recommended. When Code Flow is supported, respondents supported retaining message integrity.
- Some respondents supported the removal of encrypted ID tokens to reduce technical issues and increased system latency
- Feedback strongly supported CDR conformance testing adopting the FAPI conformance test suite as an input of technical compliance.

Decision for Approval

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 deterministic changes with high impact and low implementation effort that are universally supported in the feedback received. These changes improve the robustness and certainty of behaviour for Data Recipients integrating with Data Holders.

Phase 1 changes *should* be supported by Data Recipients and Data Holders as soon as possible but no later than the obligation date. Data Recipients may immediately use PAR only authorisation request and may use PKCE where data holders support PKCE.

The obligation date for Phase 1 is 4th July 2022.

The following changes are recommended in Phase 1:

- **Request URI Replay (PAR) is not permitted**
  - The Request URI is a single-use reference to the request object.
  - Data Recipient Software Products MUST only use a Request URI value once in accordance with [PAR-RFC9126] section 4.
  - Data Holders SHOULD make the request URIs one-time use and reject the reuse of the request URI.
- **Authorization Code Reuse**
  - Data Holders MUST reject the reuse of authorisation codes in token requests
- **x-fapi-customer-ip-address**
  - Data Holders MUST NOT reject requests with a "x-fapi-customer-ip-address" header containing a valid IPv4 or IPv6 address.
- **Request Object Expiry**
  - Data Holders SHOULD reject "exp" claim which has a lifetime of more than 60 minutes after the "nbf" claim value.
- **Request URI Expiry**
  - The Request URI MUST expire between 10 seconds and 90 seconds
- **Unique "kid" for JWK set**
  - Data Holders and Data Recipients MUST NOT us the same "kid" for multiple keys within a JWK set.
- **Multi-Brand Support (Separate Issuers For Data Holder Brands)**
  - Where a Data Holder has multiple brands, each brand MUST have a separate issuer
- **Optional Require Pushed Authorization Requests Support**
  - Data Holders MAY support [PAR-RFC7636] only authorisation requests using the [OIDD] "require_pushed_authorization_requests" parameter set to "true". Defaults to "false".
  - Data Recipients MUST support [PAR-RFC7636] for authorisation requests
- **Optional PKCE Support**

  - Data Holders MAY support PKCE
  - Data Holders MUST NOT reject clients sending PKCE claims including "code" and "code_verifier"
  - Data Holders MUST support [OIDD] "code_challenge_methods_supported" metadata parameter if they support [PKCE-RFC7636]
- **Optional Authorization Code Flow Support**
  - Data Holders MAY support Authorization Code Flow in addition to OIDC Hybrid Flow
  - If Data Holders support Authorization Code Flow they MUST also support [JARM] and [PKCE] for Authorization Code Flow in accordance with FAPI 1.0 Advanced

Phase 2

Phase 2 introduces mandatory FAPI 1.0 Baseline and Advanced support using the OIDC Hybrid Flow.
Data Holders MAY optionally support Authorization Code Flow.
Data Recipients MAY use Authorization Code Flow if offered by the Data Holder.
Phase 2 requires Data Holders and Data Recipients to support PAR RFC9126 and PKCE RFC7636.

The obligation date for Phase 2 is 16th September 2022.

- **Adopt FAPI 1.0: Baseline**
  - Change the [FAPI-R] normative reference to FAPI 1.0: Baseline (Final)
- **Adopt FAPI 1.0: Advanced**
  - Change the [FAPI-RW] normative reference to FAPI 1.0: Advanced (Final)
- **ID Token Encryption changed from MUST to MAY**
  - ID Tokens MUST be signed and MAY be encrypted when returned to a Data Recipient Software Product from both the Authorisation End Point and Token End Point.
- **Mandatory Require Pushed Authorization Requests Support**
  - Data Holders MUST support [PAR-RFC9126] only authorisation requests and MUST set the [OIDD] "require_pushed_authorization_requests" parameter set to "true".
  - Data Recipients MUST only send authorisation request objects using [PAR-RFC7636]
- **Adopt PAR RFC 9126**
  - Data Holders MUST support RFC9126
- **Adopt PKCE RFC 7636**
  - Data Holders MUST support Authorization Code Flow
  - Data Recipients MUST use PKCE
- **Authorization Code Flow**
  - Data Holders MAY support the Authorization Code Flow in accordance with FAPI 1.0 Advanced. This requires JARM and PKCE.
- **OIDC Hybrid Flow**
  - Data Holders MUST support the OIDC Hybrid Flow
- **Retire Sharing Expires At and Refresh Token Expiry claims**
  - Data Holders MAY "sharing_expires_at" and "refresh_token_expires_at" claims.
  - Data Holder MUST continue to support "exp" claim for refresh token expiry
- **Refresh Token Cycling**
  - Data Holders MUST NOT cycle refresh tokens. In other words, Refresh Tokens should be issued with an expiry equal to the sharing duration authorised.

- **Request URI Replay (PAR) is not permitted**
  In addition to Phase 1,
    - Data Holders MUST make the request URIs one-time use and reject the reuse of the request URI.
- **Request Object Expiry**

  In addition to Phase 1,

    - Data Holders MUST reject "exp" claim which has a lifetime of more than 60 minutes after the "nbf" claim value.

Phase 3

Phase 3 retires the OIDC Hybrid Flow in preference for an end state of Authorization Code Flow only. During this phasing, ADRs can continue to use the OIDC Hybrid Flow for banking data holders.

The obligation date for Phase 3 is 7th April 2023.

- **Retirement of OIDC Hybrid Flow**
    - Data Holders MAY retire OIDC Hybrid Flow (response_type of "code id_token")
- **Authorization Code Flow**
    - Data Holders MUST support Authorization Code Flow (response_type of "code" only)
    - JARM and PKCE MUST be used
    - Response Mode of "jwt" MUST be used as defined by FAPI 1.0 Advanced
    - Data Recipients MUST support Authorization Code Flow with JARM and PKCE in accordance with FAPI 1.0 Advanced
- **Retire Sharing Duration and Refresh Token Expiry claims**
    - Data Holders MUST NOT provide "sharing_expires_at" and "refresh_token_expires_at" claims in the ID Token.

Security Review

The Data Standards Chair recommends a security review be performed to independently assert the changes outlined to uplift the Data Standards to be aligned to FAPI 1.0 Final. The scope of this review will be considered in consultation with community stakeholders.

Summary

The phasing of changes presented above has been summarised in the following table[1]:

	Current State	Phase 1	Phase 2	Phase 3
		4th July 2022	16th September 2022	7th April 2023
FAPI 1.0: Baseline (Final) support	Implementer's Draft 2 (Draft 06)	Partial	**FAPI 1.0: Baseline fully supported**	FAPI 1.0: Baseline 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**	MUST support
FAPI 1.0: Advanced (Final) support	Implementer's Draft 2 (Draft 06)	Partial	**FAPI 1.0: Advanced fully supported**	FAPI 1.0: Advanced fully supported
Cipher Support	Draft 06	Draft 06	**FAPI 1.0**	FAPI 1.0
JARM Support	No	Optional (must be supported for Authorization Code Flow)	Optional (must be supported for Authorization Code Flow)	**MUST support JARM (for Code Flow)**

[1] Green shading indicates the first obligation of the target state

	Current State	Phase 1	Phase 2	Phase 3
		4th July 2022	16th September 2022	7th April 2023
PAR version	Draft 01	Draft 01	**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
Request Object Expiry	Not specified	"exp" no more than 60 minutes after "nbf". Else SHOULD be rejected	**"exp" no more than 60 minutes after "nbf". Else MUST be rejected**	"exp" no more than 60 minutes after "nbf". Else MUST be rejected
PKCE Support (RFC 7636)	Not specified	Optional	**Mandatory**	Mandatory
Request URI Replay	SHOULD refuse	SHOULD refuse (Not Allowed)	**MUST refuse (Not Allowed)**	MUST refuse (Not Allowed)
Request URI Expiry	**10 – 90 seconds**	10 – 90 seconds	10 – 90 seconds	10 – 90 seconds
General security enhancements				
Multi-Brand Support (Separate Issuers For Data Holder Brands)	**Separate issuer**	Separate issuer	Separate issuer	Separate issuer
Refresh Token Cycling	Allowed	Allowed	**No Refresh Token Cycling**	No Refresh Token Cycling
Retire Sharing Duration and Refresh Token Expiry claims	MUST support	MUST support	**MAY retire**	**MUST NOT return**

	Current State	Phase 1	Phase 2	Phase 3
		4th July 2022	16th September 2022	7th April 2023
Unique "kid" for JWK set	Not specified	**MUST be unique**	MUST be unique	MUST be unique
Access Token Revocation	**Mandatory**	Mandatory	Mandatory	Mandatory
Authorisation Flow				
Hybrid Flow	Mandatory	Mandatory	Mandatory	**Retire**
Authorization Code Flow		Optional	Should support	**Mandatory**

Implementation Considerations

General considerations

Feedback supported fewer phases with longer lead times to adopt FAPI 1.0 Baseline and Advanced profiles. This feedback has been reflected in the phasing. High impact changes with low implementation effort have been prioritised for Phase 1. These changes sought to improve implementation certainty and consistency across all data holders. The second phase provides a longer timeframe for data holders and data recipients to implement FAPI 1.0 Baseline and Advanced that

Consideration has also been given to key shutdown periods including Christmas / New Year and End of Financial Year to avoid obligation dates that would clash. In some instances, this has led to longer phase in periods. This may result in overlap of FAPI 2.0 migration with the FAPI 1.0 migration schedule. Most notably, Rich Authorization Requests (RAR) functionality, is likely to be phased in during 2022 and overlap the phasing out of the OIDC Hybrid Flow. These changes are independent and do not cause dependency issues. Consideration of FAPI 2.0 dependencies have been factored into this decision document.

Energy sector

The Energy sector data sharing obligation dates were considered in this transition to FAPI. Of priority was providing the Energy sector with a stable Information Security profile that provided a high level of international standards alignment and vendor support. 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).

Further to this, the retirement of the OIDC Hybrid Flow in favour of the Authorization Code Flow has a longer phase out period. This provides more time for Data Recipients to update their existing software products collecting banking data. Having this reliability and a longer retirement date for the OIDC Hybrid Flow allows for Data Recipients to plan changes whilst ensuring that Data Holders continue to provide dual authorisation flow support.

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 first phase 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 which do not break or impair client implementations.

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.

Whilst no feedback was received regarding conformance testing lead times, the adoption of FAPI 1.0 Baseline and Advanced profiles have a longer lead time than originally proposed which also supports CTS development.

We note that strong feedback indicated the CDR Conformance Test Suite adopt or augment technical compliance using the FAPI conformance test suite. Respondents argued that this would improve security compliance and reduce technical issues experienced in production. Respondents also argued for the CDR conformance test suite to be updated in line with the phasing of obligations for both Data Holders and Data Recipients.

Whilst the Data Standards Chair notes this feedback, the Data Standards do not specify or require any conformance testing. The role of onboarding and continual conformance testing is the role of the CDR regulator and as such, it is recommended that participants provide this feedback directly to the regulator in seeking an uplift to ecosystem testing and technical quality.

Security Review

Additional time has been provided in the phasing obligations to allow for an independent security review. If changes were to arise from this review, the additional time would allow the changes to be considered within the Data Standards maintenance process and incorporated as changes to the standards where supported.