# Data Standards Body

## Technical Working Group

## Decision 356 – Maintenance Iteration 21

*Contact: Mark Verstege, Nils Berge, Amy Nussbaumer, Eunice Ching, Hemang Rathod*

*Publish Date: 4 December 2024*

*Decision Approved By Chair: 12 December 2024*

## Context

This decision relates to the issues consulted on in Maintenance Iteration 21 of the Data Standards.

Maintenance iterations may include change requests related to Information Security, CX, Banking, Energy, Common, Admin, NFR and CDR Register Standards.

The details for this iteration can be found at:

- Decision Proposal 356 - Maintenance Iteration 21
- DSB Maintenance Iteration 21 Agenda & Notes

Additionally, an overview of the maintenance operating model and processes can be found at: https://github.com/ConsumerDataStandardsAustralia/standards-maintenance.

## Decision To Be Made

Changes related to the Standards arising from the issues consulted in the Maintenance Iteration.

## Feedback Provided

Below is a summary list of the issues considered or addressed in this iteration. Each issue has a link to the issue thread containing the public consultation relating to the issue:

| Iss. # | Sector | Issue | Decision | Change Type | Obligation Date |
|---|---|---|---|---|---|
| **666** | Security | Retirement of OIDC Hybrid Flow | Change Recommended | **Breaking change** | **Y25 #2: 12th May 2025** |
| **667** | Security | Clean up of Refresh Token requirements | Change Recommended | **Breaking change** | **Y25 #2: 12th May 2025** |
| **664** | Banking | New Enums for Voluntary disclosure of additional service overlays | Change Recommended | **Breaking change** | **FY25 #3: 14th July 2025** |

| Iss. # | Sector | Issue | Decision | Change Type | Obligation Date |
|---|---|---|---|---|---|
| **657** | Banking | Addition of LVR in the enumerated values list for constraintType | Change Recommended | **Breaking change** | **FY25 #3: 14th July 2025** |
| **655** | Admin | Get Metrics V5 error metrics documentation | Change Recommended | **Non-breaking** | **Y25 #2: 12th May 2025** |
| **663** | MI21 | Maintenance Iteration 21 Holistic Feedback | Change Recommended | **Non-breaking** | **N/A** |
| **661** | General | Obligation milestones for 2026 and 2027 | Change Recommended | **Non-breaking** | **N/A** |
| **654** | Security | Clarify Transaction Security requirements | Change Recommended | **Non-breaking** | **N/A** |
| **473** | Documentation | Add RFC8174 to list of normative references and update the use of Requirements Levels | Change Recommended | **Non-breaking** | **N/A** |
| **675** | Documentation | PAR/RFC9126 in Normative references appears twice | Change Recommended | **Non-breaking** | **N/A** |
| **659** | CX and Technical | Enhancing CDR Adoption: Streamlining Account Selection and Improving Data Transparency | CX Guidelines | **Non-breaking** | **N/A** |
| **674** | CX Guidelines | CX Guidelines: Updates stemming from 2024 Consent Review changes | CX Guidelines | **N/A** | **N/A** |
| **540** | Security | Data Recipient Software Product unable to indicate optional idtoken encryption requirement | No change | Related to issue #666. Issue will be closed once changes from #666 are implemented. | |
| **229** | Banking | Service field in the Get Transaction Details API | Duplicate | Related to issues #664. Issue will be closed. | |
| **660** | NFRs | Revise the Availability Requirements NFRs | No change | Carry over to next MI | |
| **656** | Banking | A status of POSTED should indicate the final update for a transaction | No change | Carry over to next MI | |

| Iss. # | Sector | Issue | Decision | Change Type | Obligation Date |
|---|---|---|---|---|---|
| **553** | Banking | Running balance available under transaction detail | No change | Carry over to next MI | |
| **649** | Security | Inconsistent JARM error responses | No Change | Carry over to next MI | |
| **650** | Security | Weaken JARM Encryption Requirements for ADRs | No change | Carry over to next MI | |
| **8** | Security | Adoption of detached signatures | No change | Revert to backlog for future consideration | |

# Decisions For Approval

## Issue 663 – Maintenance Iteration 21 Holistic Feedback

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/663

Change Type
**Non-Breaking Change**

Decision
To make the following minor changes to the Standards to correct defects or clarify intent:

- Update URLs in non-normative examples to make them clearer
- Remove outdated reporting detail and update link to Get Metrics endpoint from Reporting Requirements section
- Fix broken link in 'section 3' of the Holder of Key Mechanism section
- Clarified 'CDR Arrangement JWT method' details by removing duplicate lines and improving language
- In the FDO table, update the retirement statements for Get Generic Plan Detail v2, Get Energy Account Detail v3, Get Billing For Account v2, Get Bulk Billing v2, Get Billing For Specific Accounts v2 and Get Metrics v3, to clarify that they may be retired “from” (after), rather than “by” (before) the specified date.

*Background*
This is the regular Maintenance Iteration Holistic Feedback Change Request that is created at the beginning of each maintenance iteration to capture trivial changes to the standards that do not warrant a dedicated Change Request.

## Issue 666 – Retirement of OIDC Hybrid Flow

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/666

Change Type
**Breaking Change**

Decision
To set the retirement for OIDC Hybrid with a planned future retirement date after which ONLY Authorization Code Flow shall be supported.

The change includes the following in the Authentication Flows section:

**Replace**:

| |
|---|
| Specifically the OIDC Hybrid Flow outlined at section 3.3 of **[OIDC]**. |

**with:**

| |
|---|
| Authorization Code Flow outlined at section 3.1 of **[OIDC]** is supported. |

**Replace:**

| |
|---|
| From July 4th 2022, Authorization Code Flow outlined at section 3.1 of **[OIDC]** is supported. |

**with:**

| |
|---|
| **Until May 12th 2025**, Data Holders **MAY** support OIDC Hybrid Flow outlined at section 3.3 of **[OIDC]**. |

Following changes in the Authentication Flows -> Baseline Security Provisions -> Data Holders section:

**Replace:**

| |
|---|
| **From July 10th 2023 (FAPI 1.0 Migration Phase 4)**<br>• Data Holders **MAY** retire support for the OIDC Hybrid Flow. |

**with:**

| |
|---|
| **From 12th May 2025**,<br>• Data Holders **SHALL** require the value of response_type described in **[RFC6749]** to be code |

**Remove:**

| |
|---|
| Data Holders **MUST** support the OIDC Hybrid Flow. |

Following changes in the Authentication Flows -> Baseline Security Provisions -> Data Recipient Software Products section:

**Add:**

| |
|---|
| **Until 12th May 2025,** Data Recipient Software Products **SHOULD** use Authorization Code Flow.<br>**From 12th May 2025**, Data Recipient Software Products **SHALL** only use Authorization Code Flow. |

**Future Date Obligation: Y25 #2: 12th May 2025**.

*Background*

OIDC Hybrid Flow was deprecated during the FAPI 1.0 transition however no retirement date for its removal was set. This was intentional to facilitate transition of the ecosystem. Now that all data holders support Authorization Code Flow, this change specifies a retirement date after which neither ADR or Data Holder may support the authorisation flow. This change progresses the transition to FAPI 2.0 by removing the support of OpenID Connect Hybrid Flow authentication flow, which is not supported by FAPI 2.0. This reduces ecosystem complexity, reduces costs to achieve interoperability and provides better upstream alignment to international specifications. This change proposes the retirement of OIDC Hybrid Flow with a planned future retirement data after which ONLY Authorization Code Flow shall be supported.

The future dated obligation date for complete retirement of Hybrid Flow authentication support is proposed to be **Y25 #2: 12th May 2025**.

## Issue 667 – Clean up of Refresh Token requirements

### Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/667

### Change Type
**Breaking Change**

### Decision
Clarify the Refresh Token requirements in Security Profile -> Tokens -> Refresh Tokens section by **replacing:**

> **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 **MUST NOT** cycle refresh tokens (rotation). In other words, Refresh Tokens **SHOULD** be issued with an "exp" equal to the sharing duration authorised by the Customer.

**with:**

> **Refresh Token**
>
> Refresh Tokens **MUST** be supported by Data Holders in accordance with section 12 of [OIDC].
>
> In addition Data Holders:
>
> - **MUST NOT** cycle refresh tokens (rotation).
> - **MUST** issue Refresh Tokens with an "exp" equal to the sharing duration authorised by the Customer.

**Future Date Obligation: Y25 #2: 12th May 2025**.

#### *Background*
Refresh tokens act like master keys for an active authorisation. They are issued by the data holder and securely held by the data recipient. They allow the data recipient to present this key for a short lived access token granting them access to data sets (resources). The Data Standards don't permit the cycling of refresh tokens (which is aligned upstream to the FAPI profile) and so aligning the

expiry date of the refresh token to the authorised sharing duration ensures the refresh token remains valid for the duration the consumer gave authorisation to the data recipient to collect data on their behalf.

The current Refresh Token requirements include a legacy reference to an expiration date of 28 days or longer from when refresh token cycling was permitted. This change removes the requirement and makes the standards clear to understand.

No feedback has been received from Data Holders that they are not currently setting refresh token expiry to anything but the length of the sharing duration, however out of caution it is proposed this change be attached to a future dated obligation date of **Y25 # 2: 12th May 2025**.

## Issue 664 – New Enums for Voluntary disclosure of additional service overlays

### Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/664

### Change Type
**Breaking Change**

### Decision
Update the standards to support the range of New Payments Platform (NPP) service overlays including newer versions. It involves making the following updates to the *BankingTransactionDetail.extendedData* object:

- Update the allowed ENUM value of *extensionUType* to be "nppPayload"
- Change the *x2p101Payload* object to *nppPayload*
- Update the *service* ENUM field to allow the following values*:*
    - ["X2P1", "BSC", "CATSCT", "IFTI"]
- Add the following new fields to the *nppPayload* object:
    - *serviceVersion:* ExternalRef field referring to the versions as defined by NPP

This change will result in new version of the Get Transaction Detail API, incrementing from v1 to v2.

**Future Date Obligation: Y25 #3: 14th July 2025.**

### *Background*
Since version 1.0.0 of the data standards, NPP service overlays have undergone changes which include Osko version increments and the introduction of new service types.

This means that the data standards do not currently allow for the breadth of designated transaction history thus preventing data holders from sharing all required data. This change request was raised to update the standards to accommodate the additional NPP service overlays and new versions of the Osko service overlay.

This change updates the current *BankingTransactionDetail.extendedData* structure with a common extended message format, taking advantage of the common fields across the NPP service overlays. With this option, the fields in the existing *x2p101Payload* are extracted out into a common *nppPayload* object which includes:

- Overlay service code

- Overlay service version
- Any specialisations for a specific overlay service as required

This option would also allow transaction detail to be extended to non-NPP extended data included Data Holder defined extensions in future. Further this change minimises ongoing implementation costs by supporting the service version being defined by the upstream NPP specification without requiring ongoing endpoint version updates to the data standards.

An example highlighting the detail of the change is below:

```
"extendedData": {
    "payer": "string",
    "payee": "string",
    "extensionUType": "nppPayload", //new ENUM value “nppPayload”
    "nppPayload": {  //replace x2p101Payload with nppPayload
      "extendedDescription": "string",
      "endToEndId": "string",
      "purposeCode": "string"
      "service": [“X2P1”, “BSC”, “CATSCT”, “IFTI”], //new ENUM values
      "serviceVersion": "01" //new ExternalRef field referring to the versions as
defined by NPP
    }
  }
```

## Issue 657 – Addition of LVR in the enumerated values list for constraintType

### Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/657

### Change Type

**Breaking Change**

### Decision

Add the following new ENUM values to *BankingProductConstraint*.*constraintType* field to allow sharing of minimum and maximum Loan to Value Ratio (LVR) limits that may be applicable to relevant banking products:

| Value | Description | Use of additionalValue Field |
|---|---|---|
| **MAX_LVR** | A maximum LVR (Loan to Value Ratio) exists | The maximum LVR in RateString format |
| **MIN_LVR** | A minimum LVR (Loan to Value Ratio) exists | The minimum LVR in RateString format |

This change will result in new version of the Get Product Detail endpoint, incrementing from v4 to v5.

**Future Date Obligation: Y25 #3: 14th July 2025.**

### *Background*

The change request was raised to allow data holders to accurately reflect LVR product constraints within the CDR framework. This would help align the information shared via the standards to what

DHs provide on their website and allow ADRs to understand the application constraints on home loan products.

## Issue 661 – Obligation milestones for 2026 and 2027

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/661

Change Type
**Non-Breaking Change**

Decision
Add the following future obligation dates for 2026 and 2027:

| Obligation Milestone | Milestone Date |
|---|---|
| **Y26 #1** | 16/03/2026 |
| **Y26 #2** | 11/05/2026 |
| **Y26 #3** | 13/07/2026 |
| **Y26 #4** | 14/09/2026 |
| **Y26 #5** | 09/11/2026 |
| **Y27 #1** | 15/03/2027 |
| **Y27 #2** | 10/05/2027 |
| **Y27 #3** | 12/07/2027 |
| **Y27 #4** | 13/09/2027 |
| **Y27 #5** | 08/11/2027 |

*Background*
The change request extends the Milestone Dates in the Obligation Dates Schedule to 2026 and 2027. To provide the CDR participants with forward notice of when obligations *may* apply in future, a schedule of obligation dates for 2026 and 2027 was proposed, to extend upon the existing obligation schedule. As a result, this gives participants forward notice for resource planning. Participants agreed that milestone dates for 2026 and 2027 be published in advance, to allow any upcoming changes to be assigned to them.

## Issue 659 – Enhancing CDR Adoption: Streamlining Account Selection and Improving Data Transparency.

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/659

Change Type
**CX Guidelines Update (No Standards Change)**

Decision
- **CX Guidelines**: Update CX guidelines demonstrating how data holders may, under the existing CX standards, voluntarily implement a 'select all' functionality for account selection and implement additional functionality where a large number of accounts are presented at this step

- **CX Standards**: No change is currently proposed as further assessment of the issue is required with more community input
- **Technical standards:** No change is proposed to technical standards

This request will remain open to progress the assessment on CX standards change

*Background*

This CR was raised by an ADR participant requesting changes to the standards to encourage consumers to share data from all available accounts, while also providing oversight to ADRs when consumers do not share data from specific accounts. This would enable ADRs pause the lending application process and hand off to a manual process for more thorough affordability assessment, in alignment with responsible lending practices.

The request sought changes across CX and technical standards, and CX guidelines which are described below.

**CX Standards and Guideline Changes:**

- The request sought to standardise the presentation of a "select all" functionality by DHs for account selection in the consent flow
- The DSB noted the existing CX standard (Authorisation: Account selection functionality) and CX guidelines (Authorisation to disclose, Default example) already allow and show a basic "select all" functionality.
- The DSB will publish further CX Guidelines demonstrating how data holders may, under the existing CX standards, voluntarily implement a 'select all' functionality for account selection, and include reference to the Authorisation: Account selection functionality standard, in response to the original request for CX changes.
- Making the "select all" functionality mandatory would require further assessment alongside other consent drop-off concerns. To help monitor the progress of this, the CR will be left open for future MIs

**Technical Standards Changes**

- The request proposed the introduction of a new field "*availableRecords"* field to the Get Accounts API which would indicate the number of accounts that were available for sharing, allowing the ADR to know if all the accounts were shared or not
- The DSB consulted with OAIC who advised it does not satisfy the rules for privacy considerations. Disclosing the fact that the consumer did not share all of their accounts, and additionally disclosing how many accounts they did not share could result in consumer harm.
- As a result of the above, the decision is to not support the technical change component

## Issue 655 – Get Metrics V5 error metrics documentation

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/655

Change Type
**Non-Breaking Change**

### Decision

Update the description of the following fields to provide clarity on the expected and compliant responses:

| Field Name | New Description |
|---|---|
| **»» additionalProperties** | This is a placeholder field to be substituted with each respective HTTP error code in the 4xx and 5xx range recorded by the Data Holder. It is represented by *property1* and *property2* in the *Non-normative Examples* section. Note that the property name **MUST** be the three-digit HTTP error code as per the adjacent *500* example. All possible property names have not been defined as the range is expected to vary across participants. Examples would include, but are not limited to: *400, 404, 405, 406, 415, 422, 429, 500, 503, 504*. |
| **»» 500** | Reflecting the description provided in the adjacent *additionalProperties* field, this is an example demonstrating the structure for reporting the number of calls resulting in HTTP error code 500. Each error code recorded by the Data Holder in the 4xx and 5xx range **MUST** be provided in this format against the respective property name. |

The fields appear in the following schemas of Get Metrics API:

- *ErrorMetricsV2.unauthenticated.currentDay*
- *ErrorMetricsV2.unauthenticated.previousDays*
- *ErrorMetricsV2.authenticated.currentDay*
- *ErrorMetricsV2.authenticated.previousDays*

For the authenticated schemas, error codes 410 and 403 are also included in the example list.

This clarification will be applicable from the FDO **Y25 #2: 12th May 2025**. The Get Metrics version remains unchanged.

### *Background*

This CR was raised as a documentation change to update the field descriptions in the ErrorMetricsV2 schema to ensure the requirements are clear in providing error codes. Specifically, to indicate that errors are to be reported against each respective error code in the 4xx and 5xx series where the example **additionalProperties** and *property1* and *property2* fields currently appear.

This is not a breaking change. However, participant feedback and DSB analysis indicated that approximately half of all Data Holder brands have incorrectly implemented the requirements for the above fields. Based on discussion with ACCC, an FDO is proposed to allow DHs time to correct their implementations, which was agreed by participants.

## Issue 473 – Add RFC8174 to list of normative references and update the use of Requirements Levels

### Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/473

### Change Type
**Non-Breaking Change**

### Decision
Replace "must" with "**MUST**" in all occurrences of following statements to align with RFC8174 - Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words:

- An [RFC4122] UUID used as a correlation id. If provided, the data holder **MUST** play back this value in the *x-fapi-interaction-id* response header. If not provided a [RFC4122] UUID value is required to be provided in the response header to track the interaction.
- If all versions requested are not supported then the data holder **MUST** respond with a `406 Not Acceptable`.
- If all versions requested are not supported then the Register **MUST** respond with a `406 Not Acceptable`.

### *Background*
This change was raised to consider the options for inclusion of RFC8174 as a normative reference and standardisation of requirements level usage in the Data Standards to be capitalised.

The request proposed the following changes:

- Update all usage of requirements levels to adopt the capitalised form.
- Update normative references with [RFC8174] *in addition to* [RFC2119]
- Update the Data Standards introduction with respect to requirements levels as appropriate with reference to [RFC8174]

The change proposed focuses on capitalisation of the key word "must" in alignment with RFC8174. The remaining changes will be carried over to separate CRs in preparation of inclusion of RFC8174 as normative reference.

## Issue 654 – Clarify Transaction Security requirements

### Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/654

### Change Type
**Non-Breaking Change**

### Decision
Update the documentation in Security Profile section to improve requirements clarify by making the following changes:

- In the **Transaction Security** -> **Use of MTLS** section, **replace:**

End points for transferring CDR Data that are classified as not requiring authentication do not require the use of [MTLS].

**with:**

| |
|---|
| Endpoints for transferring CDR Data that are classified as not requiring authentication (i.e. public endpoints) or those specified as TLS, MUST NOT use [MTLS]. |

- In the **Certificate Management** -> **Issued by the Register for Data Holders** section, **replace**:

| |
|---|
| Server Certificate(s) \| Certificate is issued to a FQDN Secures the following endpoints: - Resource endpoints - InfoSec endpoints - Admin endpoints. |

**with:**

| |
|---|
| Server Certificate(s) \| Certificate is issued to a FQDN. Secures the endpoints as detailed in [Participant endpoints] |

- In the **Certificate Management** -> **Issued by the Register CA for Data Recipients** section, **replace:**

| |
|---|
| • Server Certificate(s) \| Certificate is issued to a FQDN. Secures the following: - CDR Arrangement Revocation endpoint - JWKS endpoint<br>• ADRs may choose to secure their [endpoints] with the Register CA issued certificate or a certificate issued by a public CA |

**with:**

| |
|---|
| Server Certificate(s) \| Certificate is issued to a FQDN. Not currently required by Data Recipients. |

- In the **Security Endpoints** -> **Dynamic Client Registration Endpoints** section:
  In the table heading row, **replace**:

| |
|---|
| TLS-MA |

**with:**

| |
|---|
| MTLS |

- In the **Participant Endpoints** section, **add the following**:

| |
|---|
| • Endpoints specified as MTLS MUST be configured according to the [Certificate Trust Model] in the [Certificate Management] section.<br>• Endpoints specified as TLS MUST be configured with a certificate issued by a public CA accepted by major web browsers. |

- The following changes to the table in **Participant Endpoints** section:
  1. Add a Transaction Security column to specify the high-level requirement for each Base URI
     1. PublicBaseUri: TLS
     2. ResourceBaseUri: MTLS
     3. InfoSecBaseUri: TLS
     4. AdminBaseUri: MTLS
     5. ExtensionBaseUri: TLS/MTLS (depending on extension requirements)
     6. RevocationUri: TLS

7. RecipientBaseUri: TLS
8. JwksUri: TLS (for both DH and ADR)

2. For *ResourceBaseUri* and *RecipientBaseUri*, change 'This should' to 'This **MUST**'
3. Clarify that the *InfoSecBaseUri* only provides reference to the OIDC Discovery endpoint over TLS
4. Provide references to usage of the different *JwksUri* values for Data Holders and Data Recipients

*Background*

This change was raised to improve the documentation regarding transaction security and CDR certificate requirements in the Security Profile sections related to Transaction security, Certificate management and Partcipant endpoints.

## Issue 674 – CX Guidelines: Updates stemming from 2024 Consent Review changes

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/674

Change Type
**CX Guidelines Update (No Standards Change)**

Decision
Update the CX Guidelines where necessary to align with changes resulting from the consent and operational enhancement amendments to the CDR Rules.

*Background*

In August 2024, the Treasury conducted a consultation on proposed consent and operational enhancement amendments to the CDR Rules. The DSB simultaneously consulted on Decision Proposal 350 to outline the expected changes to the standards to support the proposed rules. The amended rules were made by the Minister and commenced on 12 November 2024. Decision 350 was made by the Chair on 15 November 2024 with future dated obligations.
This CR outlines the anticipated updates to the CX Guidelines that will be required to reflect these rules and standards changes and was raised as a means to allow the community to provide any feedback.

**Note:**
The CX Guidelines provide optional implementation examples for key rules, standards, and best practice recommendations. Changes to the guidelines are not considered standards changes. This issue is captured here for noting purposes only.

## Issue 675 – PAR/RFC9126 in Normative references appears twice

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/675

Change Type
**Non-Breaking Change**

### Decision

Combine two rows referring to the PAR and RFC9126 Normative References into a single row as it is the same specification.

### *Background*

References to the [PAR] and [RFC9126] standards respectively had been included in the Standards, however they now refer to the same version of RFC9126.

## Standards staging documentation and schema changes

The following change requests are for minor changes to correct formatting and spelling issues, and support consistent interpretation:

| Issue # | Change Type | Change Description |
|---|---|---|
| #443 - Apply consistent styling in the Transaction Security section | Documentation change | Apply consistent styling in the Transaction Security section |
| #442 - Apply consistent styling to the Common Field Types table | Documentation change | Apply consistent styling to the Common Field Types table |
| #435 - Maintenance Iteration 21 - typos and formatting | Documentation change | Miscellaneous typos and formatting changes noted in the CR |
| #431 - Fix spelling, grammar and punctuation | Documentation change | Apply various documentation corrections continuing from #527 - Fix spelling, grammar and punctuation errors across the API specification. |
| #429 - Refer to components in Banking API spec | Standards publishing | Remove repetition of various common details in every endpoint definition of Banking API specifications by referencing them instead |
| #463 - Remove redundant generated 'additional' file | Standards publishing | Remove the generation of a timestamped 'additional' file (e.g. additional20241021-8236-1xvavno for the 'Additional Standards' section) during Standards build process which affects managing, merging and building development branches, when the file has not actually changed. |

# Implementation considerations

When possible, consideration and preference to non-breaking change has been prioritised with community consultation. Where breaking changes have been recommended, future dated obligations have been proposed in consultation with participants during the course of the Maintenance Iteration to ensure sufficient lead time for implementation.

Implementation considerations for each change request have been considered and detailed within each change request summary.

In relation to the breaking changes for the Security Profile, these changes reduce or simplify the obligations on data holders and thus reduce ongoing cost whilst improving alignment to the upstream FAPI profile.

For banking transaction history changes, the DSB considered alternative options and sought to reduce the need for ongoing changes to the detail transaction payloads to reduce long-term costs for Data Holders. Whilst other consumer data was identified within the change, this shall be consulted on in a future maintenance iteration to unlock value for ADRs faster and help prioritise support of high value use cases including better borrowing decisions and accounting services for business consumers.