Market Interface Technology Enhancements Working Group (MITE WG)

Wednesday 27 November 2024

(1:00pm to 5:00pm AEDT)

This meeting will be recorded for minute taking purposes.

We acknowledge the Traditional Custodians of the land, seas and waters across Australia. We honour the wisdom of Aboriginal and Torres Strait Islander Elders past and present and embrace future generations.

We acknowledge that, wherever we work, we do so on Aboriginal and Torres Strait Islander lands. We pay respect to the world's oldest continuing culture and First Nations peoples' deep and continuing connection to Country; and hope that our work can benefit both people and Country.

'Journey of unity: AEMO's Reconciliation Path' by Lani Balzan

AEMO Group is proud to have delivered its first Reconciliation Action Plan in May 2024. 'Journey of unity: AEMO's Reconciliation Path' was created by Wiradjuri artist Lani Balzan to visually narrate our ongoing journey towards reconciliation - a collaborative endeavour that honours First Nations cultures, fosters mutual understanding, and paves the way for a brighter, more inclusive future.

Read our RAP

Housekeeping

1. This meeting will be recorded for minute taking purposes
2. Please mute your microphone, this helps with audio quality as background noises distract from the conversation.
3. Use the ‘Raise hand’ function should you wish to speak to an item.
4. Use the ‘Chat’ function for any other questions or comments you may have.
5. In attending this meeting, you are expected to:
    - Not only represent your organisation’s interests but also the interests of Industry and its customers
    - Have an open mindset
    - Contribute constructively
    - Be respectful, both on the call and in the chat

1. Welcome

Blaine Miner

Objective of today's session

The MITE WG has been established to define and develop Technical Procedures/guides for IDAM, IDX and Portal Consolidation. These initiatives seek to deliver foundational capability supporting interactions between participants and AEMO and based on the agreed scope to transition or enable decisions on transitioning of existing business services

This workshop aims to cover:

- IDX Large File Share (FG recap)
- IDX Payloads (FG recap)
- IDX and IDAM Future Topics
- Forward Plan

The ask of participants:

- Invite and share this pack with your technical experts who will support the MITE WG / FG process to provide context and background
- Provide your inputs on the outcomes, polls and results as presented – in and out of session is fine
- Engage in the workshop – questions are welcome

Link to the target state pack established in consultation with the industry stakeholders

Agenda

#	Indicative Timings	Topic	Presenter
1	1:00pm-1:10pm	Welcome	Blaine Miner
2	1:10pm-2:40pm	IDX – Large File share Focus Group Recap	Udaya Uppalapati
3	2:40pm-4:10pm	IDX – Payload Focus group Recap	Selwyn Sequeria / David Freeman
4	4:10pm-4:15pm	IDX Future Topics	David Freeman
5	4:15pm-4:20pm	Forward Plan	Blaine Miner
6	4:20pm-4:25pm	General Business and Next Steps	Blaine Miner
	Appendix	Appendix A: AEMO Competition Law - Meeting Protocol Appendix B: IDAM FG Session outlines	

Notes

Blaine spoke to the Agenda.

AEMO highlighted that some focus group references may not align with the November 15th updates, so it will note the updated timings to ensure coordinators and the working group have accurate dates

2. IDX - Large Fileshare Focus group Recap

Udaya Uppalapati

Objective of the Focus Group

The MITE FG was established to discuss in detail specific topics for IDX. This working group session will focus on recaps of focus group content for Large File and Payload.

This focus group aims to..

- Review and discuss drafted Definitions, Pain Points and Reference Model.
- Recap of Decision Tree and Large File share examples.
- Review and discuss drafted Large File Share capabilities.
- Review and discuss drafted Large File Share orchestration and seek recommendation on File deletion control.
- Review and discuss current and proposed structure of folders/directories.
- Review and discuss Stop File principles.

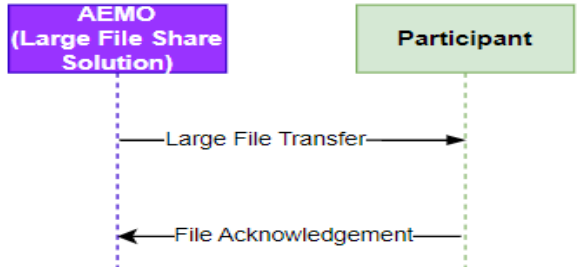
The ask of participants...

- **Participate** in highly technical discussions, including engaging within their business prior, to provide detailed responses to matters under discussion
- **Champion** technical discussions with their peers and within own organisations.
- **Review** draft documentation prepared by the Focus Group and provide input

Call Out's

- Protocols, Authentication and Authorization aspects of the large file transfers will be discussed in a future IDAM Focus Group.
- Message sizes and size thresholds are out of scope and are handled as part of different workshops.
- Payload transformations will be discussed in the Payload Focus Group session.
- Object versus file-based storage will be discussed in a future Focus Group.
- Stop file details will be discussed in a future Focus Group.
- Non-repudiation of messages via Large File Share will be covered in the Payload Focus Group.
- File naming conventions will be discussed in a future Focus Group.
- Event notifications (i.e.. via websocket, or polling) will be discussed in the Async and Event Notification Focus Group.

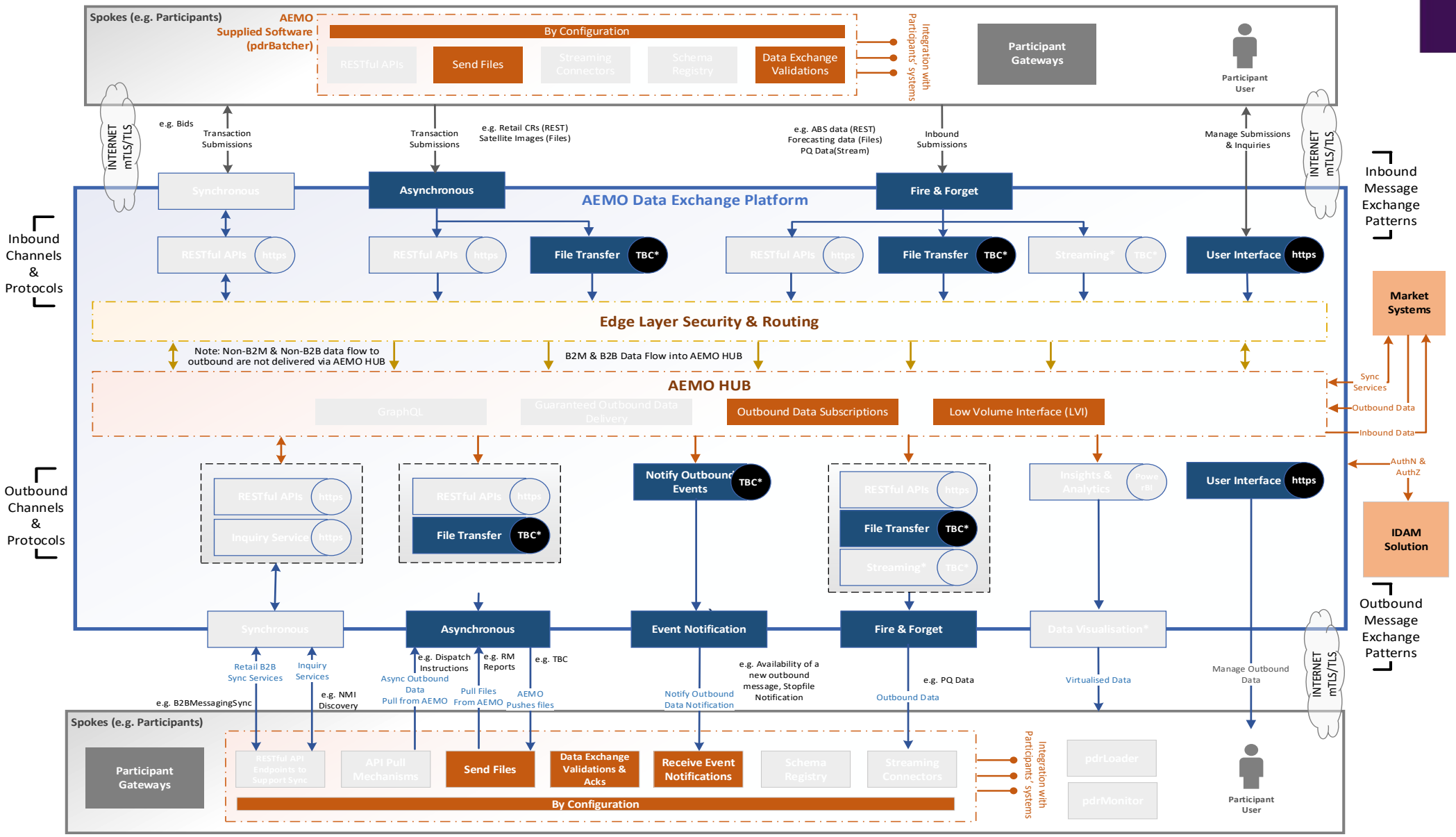
Large File Share – Data Exchange

Pain points	Proposed Principle(s)	Target State Concept
Industry raised pain-point: • Protocols, formats and standards are inconsistent and unnecessarily convoluted. • Lack of consistent standards across Systems / Fuels / Jurisdictions. *AEMO's reading of Industry pain points:* • AEMO exchanges a large volume of files (structured and unstructured) with Participants that doesn't follow consistent patterns or proper industry defined file transfer mechanisms. • Participants do not have a secure mechanism for transferring files in the data exchange.	• A standard set of Industry agreed on channels, protocols, patterns, and capabilities to meet the Large file share needs across all Participants, Markets and Domains. • Applying security best practices (in transit and at rest) in the transfer of large file shares. • Apply standardisation across interfaces and processes in the large file share exchange mechanism. • Applying speed and efficiency techniques (like compression, parallel processing, etc.) in the large file transfer mechanism. • Adopting scalable and flexible infrastructure in the implementation of large file share exchanges.	• AEMO-hosted Large File Share solution shall be the foundation for any large file data exchanges between participants and AEMO.  • Ability to support consistent patterns (Async Inbound, Async Outbound and Fire & Forget Outbound) for services that require large file transfer through one platform while meeting SLA's. • Execution of security and comprehensive monitoring for end-to-end large file transfer operations allows for the early mitigation of risks that could adversely affect essential business processes.

Why Large File Share?

Data Safety	• Integrity and security of data while at rest and in-transit
Eliminate complexity	• Standardisation (Storage, Interfaces, Orchestrations, Processes) helps in removing business and technical complexities
Mitigate Risks proactively	• By actively monitoring end-to-end file transfer activities, risks that can impact critical business process are mitigated earlier than later
Highly performant platform	• Large file transfers require more resources and a dedicated highly performing infrastructure and application architecture, therefore it is recommended to have a dedicated platform
Support B2B and B2M models	• Ability to support different models of files transfer in one platform while meeting different SLAs/SLRs

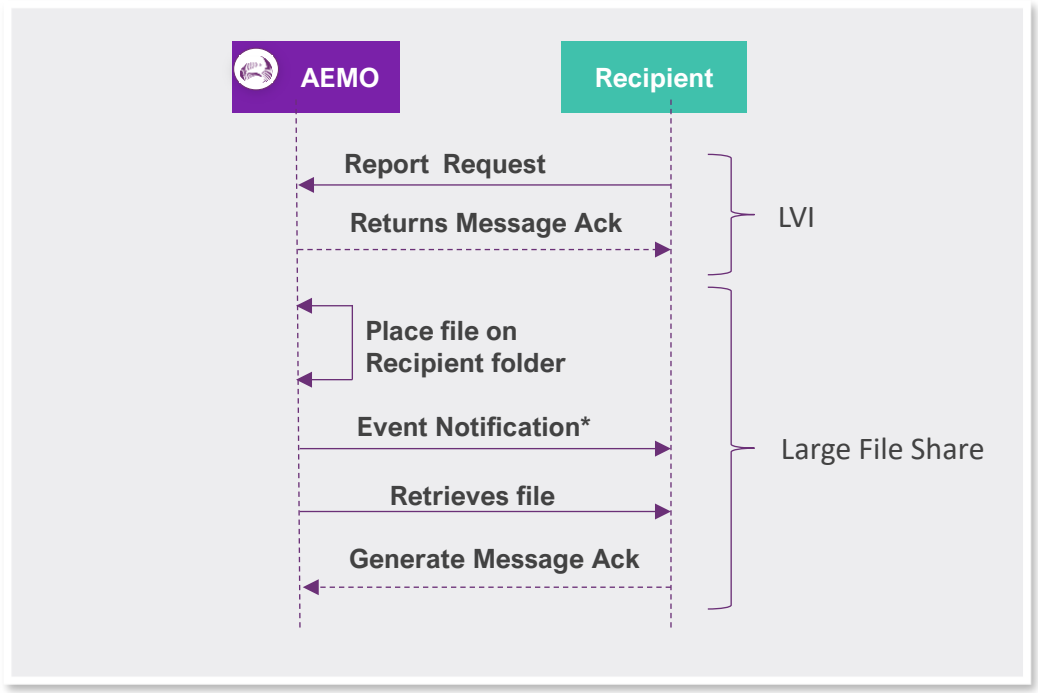
Reference Model



Decision Tree Recap

Async Message Sequence Example: Large File Transfer - Energy Settlement Report(RM16)

Using Energy Settlement reports (RM16) as an example, we will walk through the decision tree to demonstrate how a use case fits into the Asynchronous Large File transfer scenario. The below is a representation of the message flow for this use case.

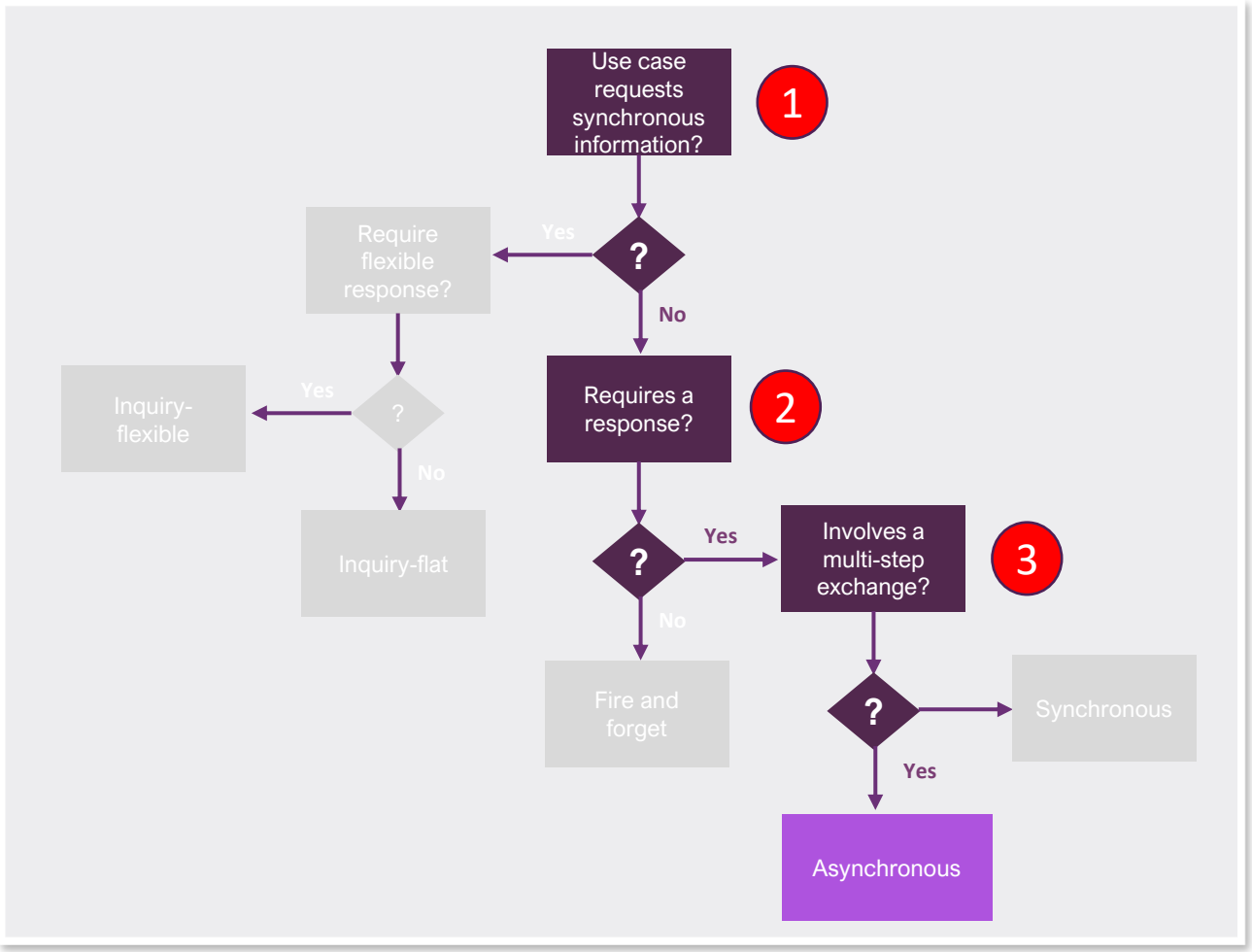


Sequence flow :

1. **Report Data is requested by the recipient.**
2. **AEMO generates the report and places in the recipient folder.**
3. **AEMO generates event notification*.**
4. **Participant downloads the report file and acknowledges back to AEMO.**

**** Upcoming Focus Group*** **-** a detailed conversation on Event Notifications is reserved in the Async and Event Notification FG on 25th Nov

STEP 1: Determine the Message Pattern - Energy Settlement Report(RM16)

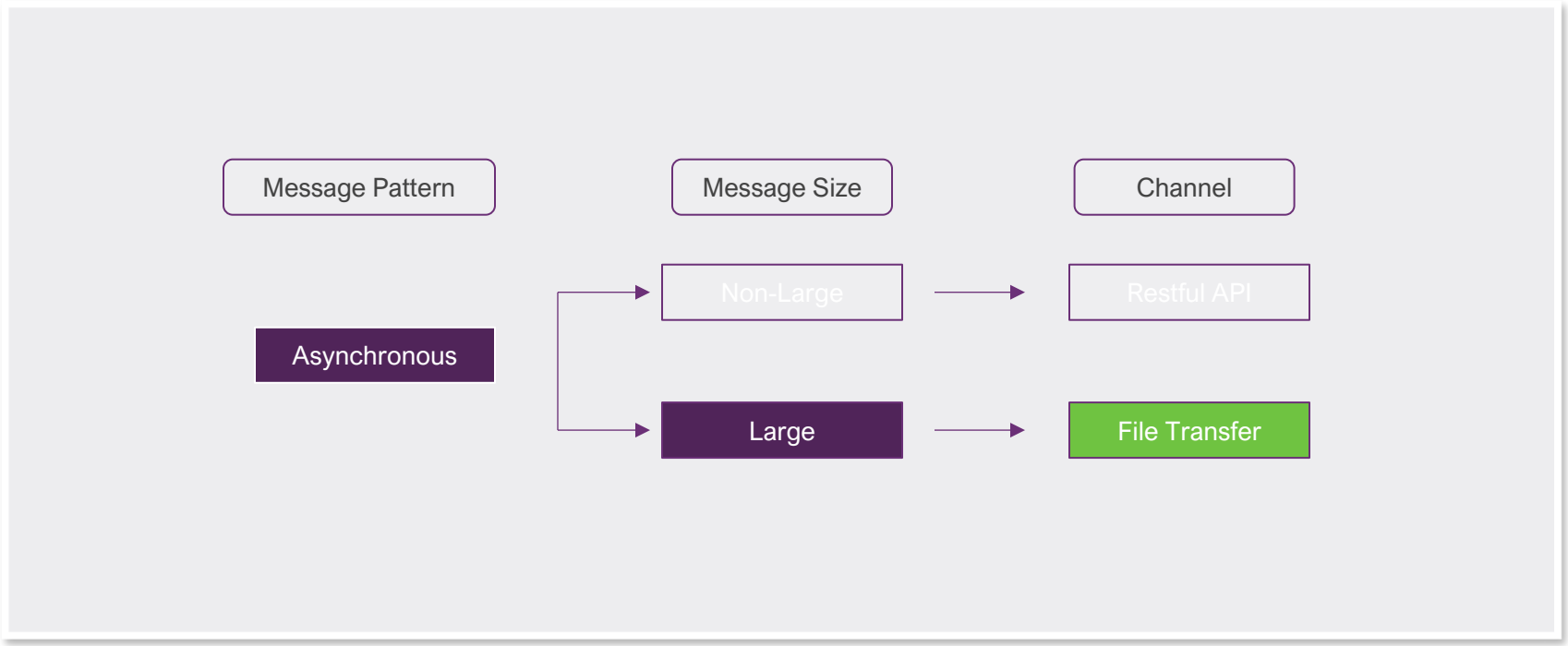


Use Case: Participant Request for Settlement Report(RM16) to AEMO

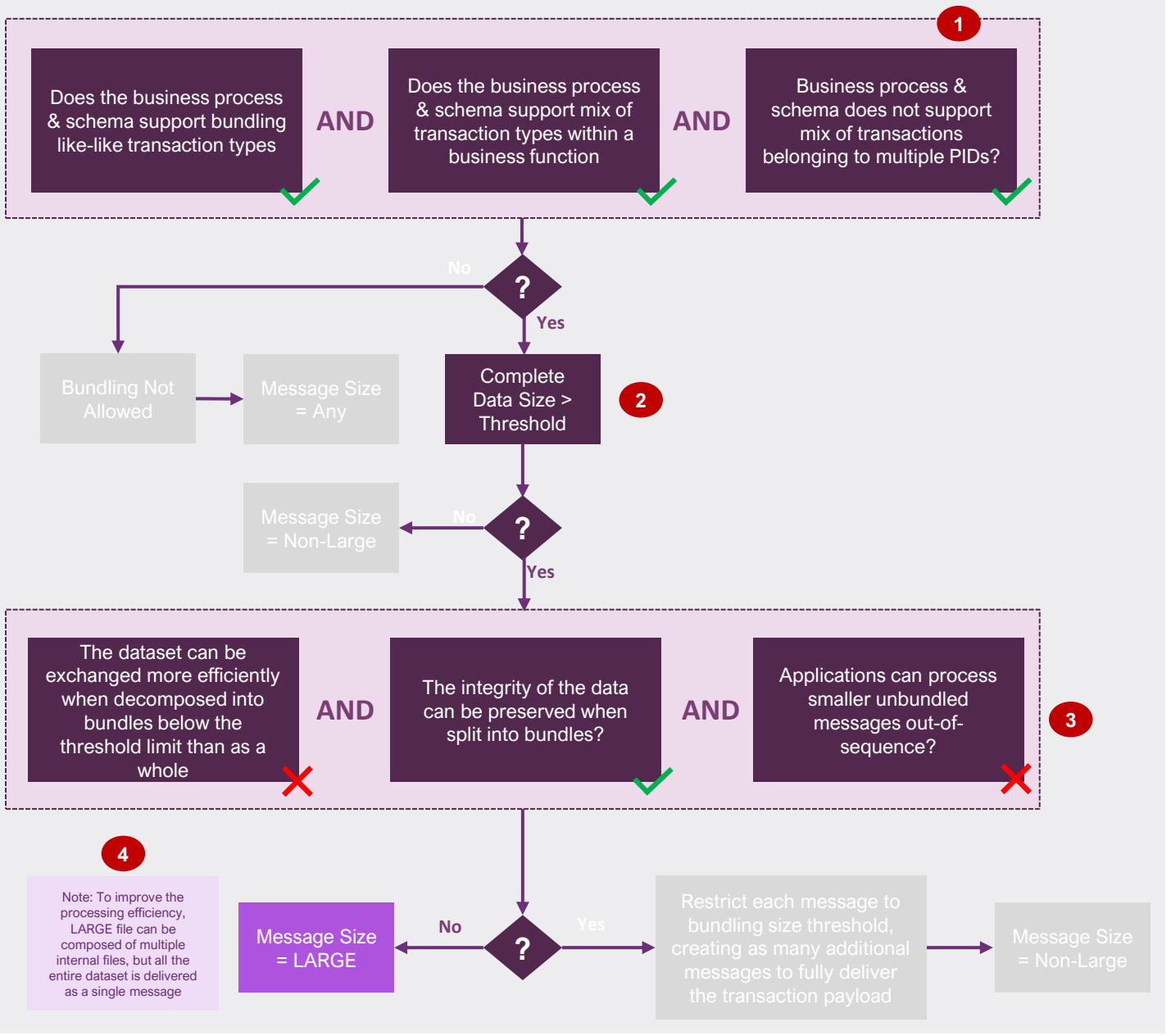
Decision tree applied criteria:

1. **Report Data is being requested**
2. **A business response (Report Response) is required**
3. **The business response is not passed immediately, as it has further steps in the process to be completed for the report to be generated.**

Decision tree – Asynchronous



Step 2: Determine the message Size - NEM Reports - Energy Settlement Report(RM16)



Use Case Description

Use Case: AEMO delivering NEM Reports (Energy Settlements) to Participants

For illustration: Message size threshold = 5MB

Report Name: Level1SettlementReconciliation

Average Zipped Report Size: ~10MB

Energy Settlements report has got the CSV Data sent as part of the report file.

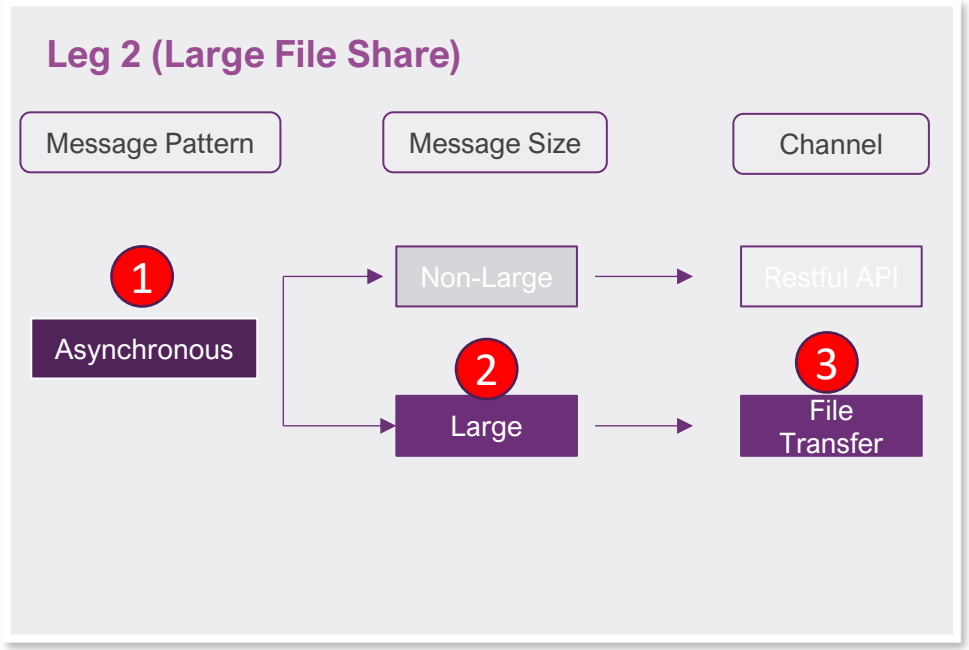
Applying Decision Tree for the Use Case

1a. NEM energy settlement report allow bundling of like-like transactions
1b. NEM energy settlement report .
1c. It does not allow transactions belonging to multiple participants. Hence message size is large.

2. Bundling not allowed

3. Message size for this use case is 10MB > Threshold (5MB for this example). So, message classification is LARGE.

Step 3: Determine the Channel - Worked example: Energy Settlement Report(RM16)



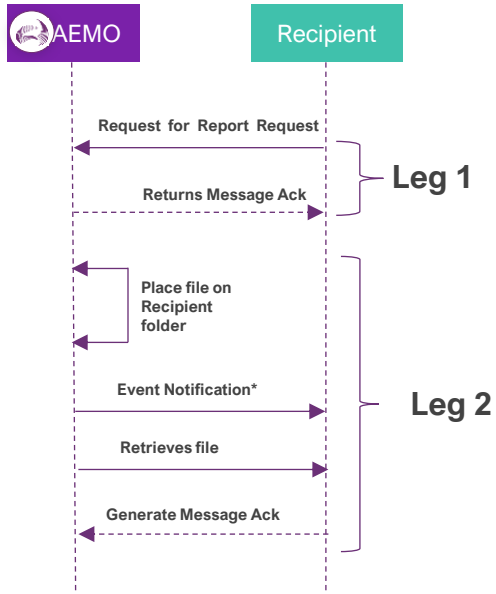
- In this service the overall Asynchronous pattern is used
- Message size = 'Large', as files are over 10MB in size and cannot be decomposed.
- Channel to be used is File Transfer.

Leg 1 (LVI)

1. Recipient requests the report from AEMO.
2. AEMO Acknowledges.

Leg 2 (Large File Share)

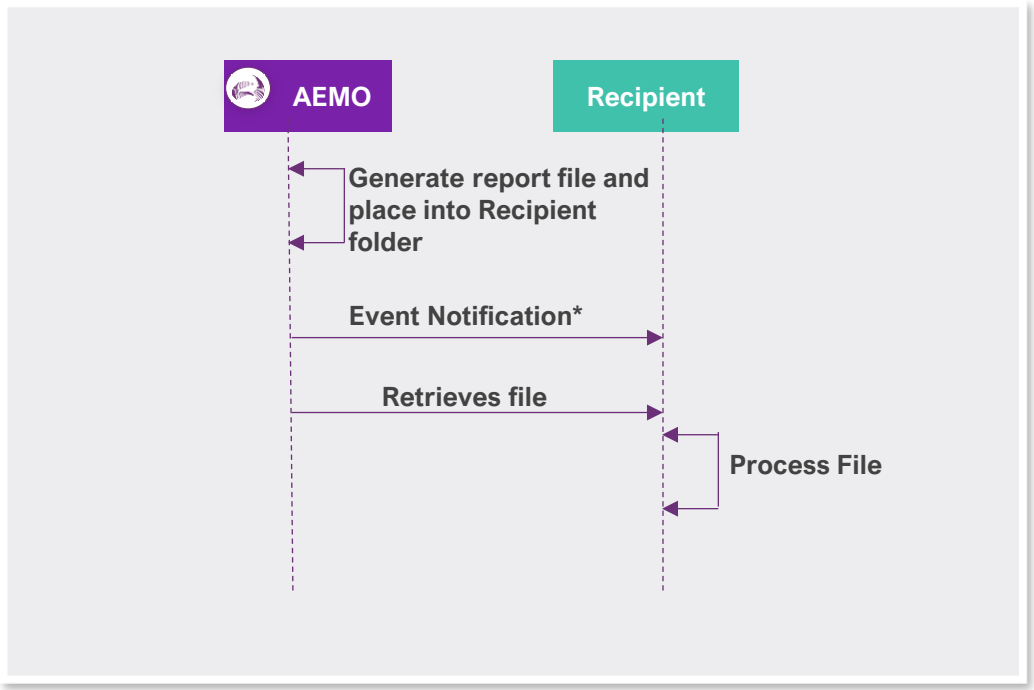
3. AEMO generates the report.
4. Once report is complete, the Recipient is notified. (this may occur over the Event Notification channel or through polling*).
5. Recipient retrieves the report from the appropriate folder.
6. Recipient Acknowledges the receipt of the file.



Upcoming Focus Group - a detailed conversation on Event Notifications is reserved in the Async and Event Notification FG on 25th Nov

Fire & Forget - Large File Transfer Example - Monthly Snapshot Reports

Using Monthly Snapshot reports as an example, we will walk through the decision tree to demonstrate how this use case fits into the Fire and Forget Large File transfer scenario. The below is a representation of the message flow for this use case.

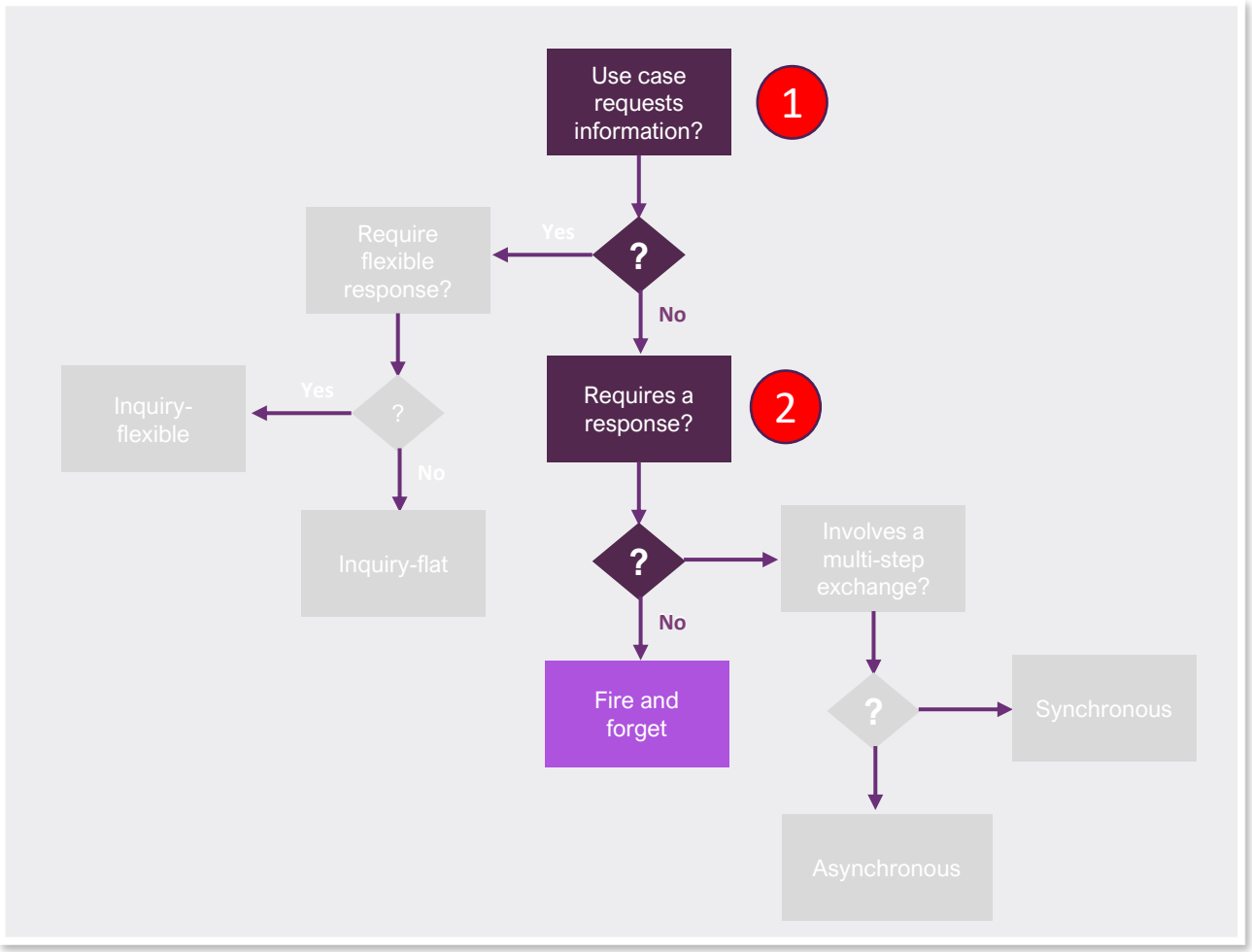


Sequence flow :

1. **Monthly snapshot report is generated by AEMO and placed into the Recipient folder.**
2. **Event notification* to the recipient.**
3. **Recipient downloads and processes the report file.**

**** Upcoming Focus Group*** **-** a detailed conversation on Event Notifications is reserved in the Async and Event Notification FG on 25th Nov

STEP 1: Determine the Message Pattern - Monthly Snapshot Reports

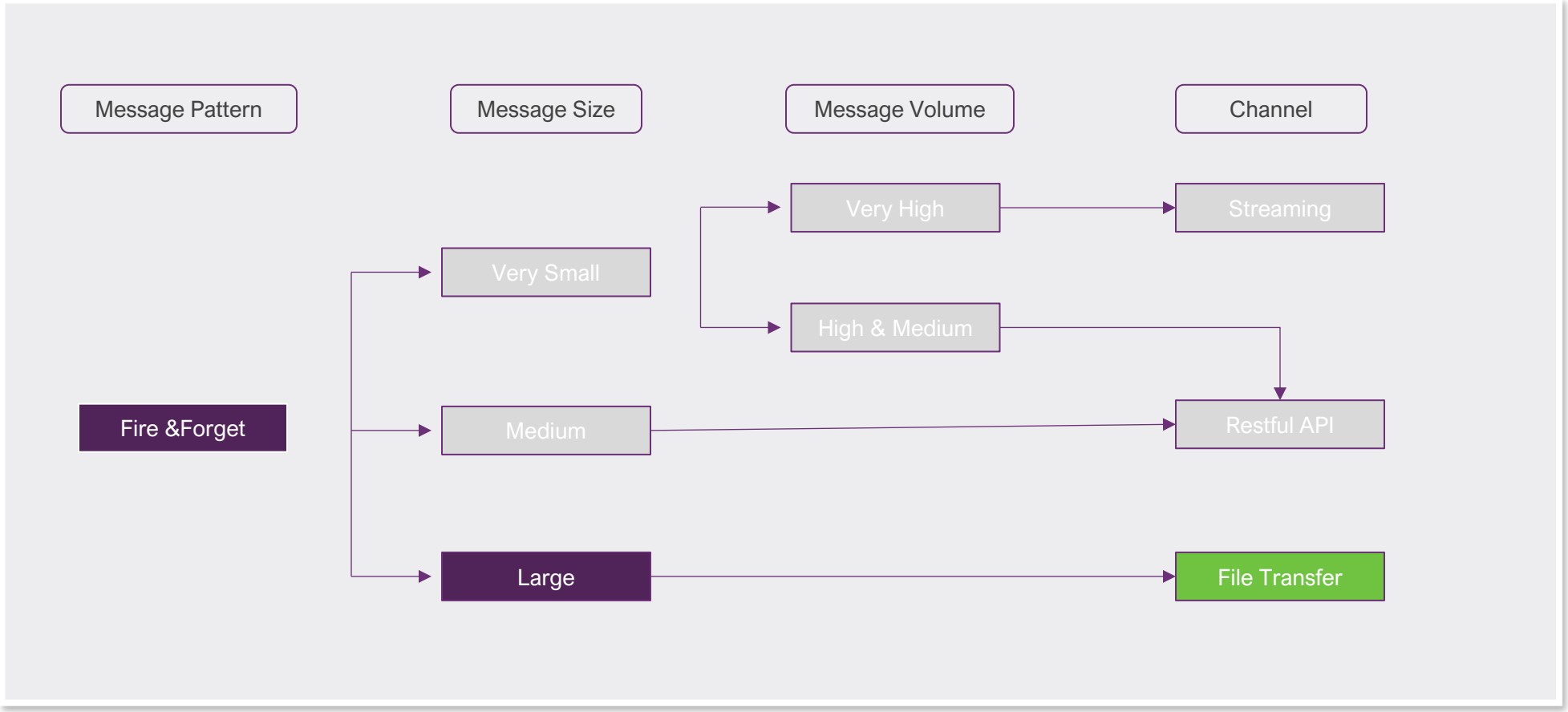


Use Case: Monthly Snapshot from AEMO

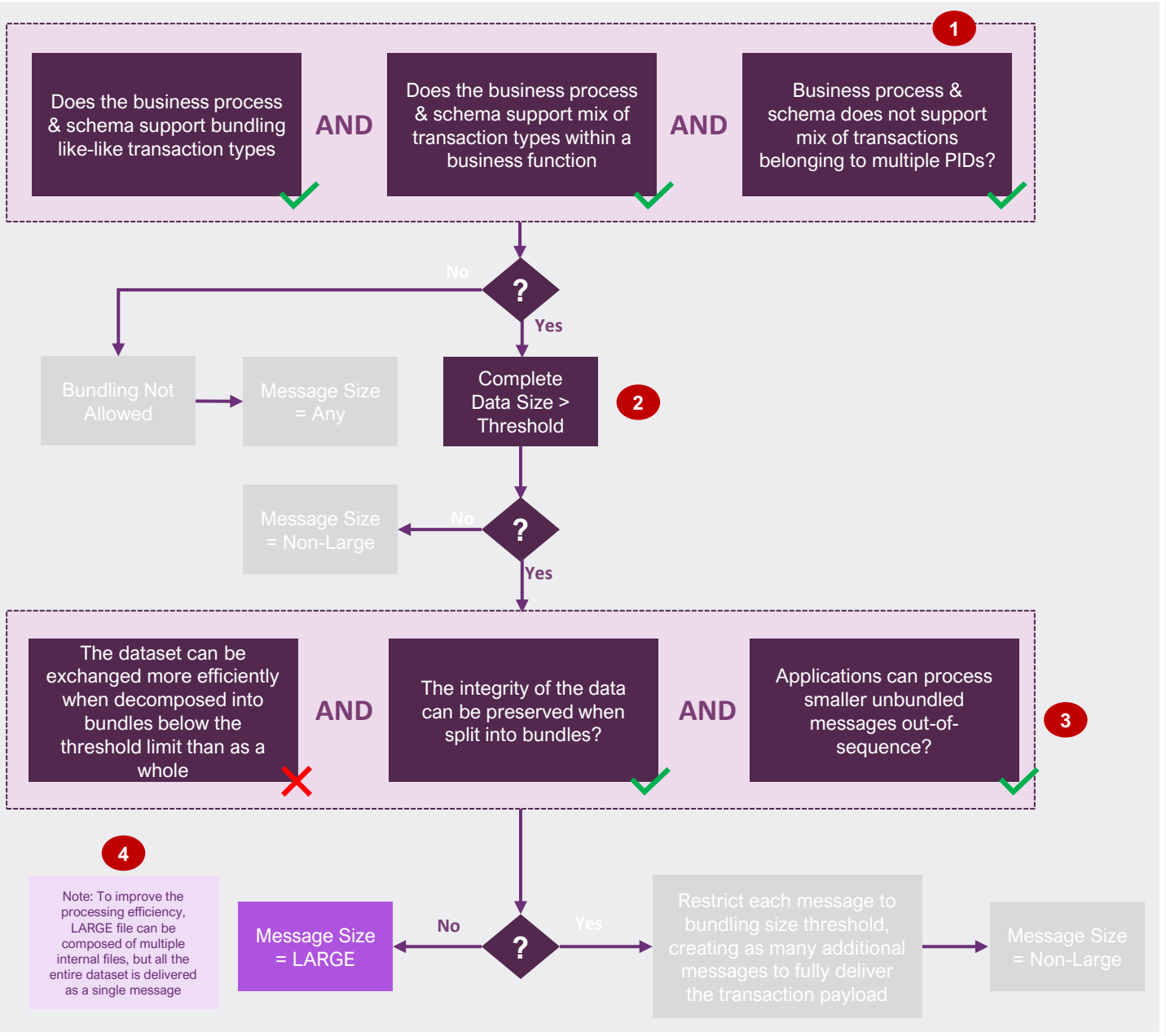
Decision tree applied criteria

1. **Data is being supplied by AEMO to participants**
2. **A response is not required, as there is no expectation of validation or acknowledgement for receiving the Monthly Snapshot Report**

Decision tree – Fire & Forget



Step 2: Determine the message Size - Monthly Snapshot Reports



Use Case Description

Use Case: Monthly Report Snapshot Reports

For illustration: Message size threshold = 1MB

Report Name: Daily Snapshot Report

Average Zipped Report Size: ~100MB – 1GB

Payload has data from multiple Standing Data tables – CATS_NMI_DATA, CATS_NMI_PARTICIPANT_RELATIONS, CATS_METER_REGISTER, CATS_REGISTER_IDENTIFIER, CATS_NMI_DATA_STREAM

Applying Decision Tree for the Use Case

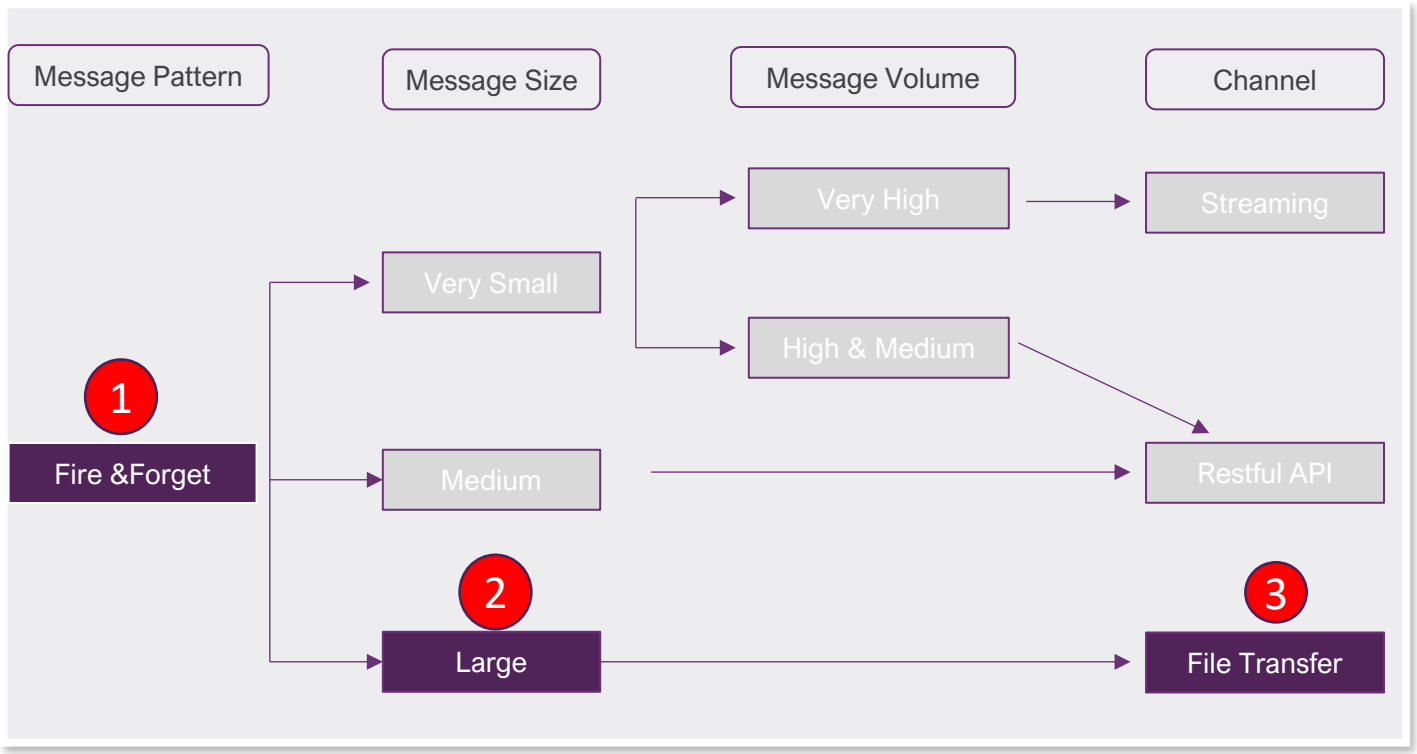
1a. Snapshot reports support bundling of like-like transactions
1b. Snapshot reports allow mix of transaction types (e.g. CND, CRI, CMR, CNDS & CNPR data) within a business function
1c. Snapshot reports are run for a ParticipantID

2. Complete Data Size (~100MB to 1GB) > Threshold (1MB for this example)

3a. Dataset is efficiently processed by Participants when the entire dataset is sent as one message
3b. Integrity of the data can be preserved when split into smaller bundles
3c. Applications can process smaller unbundled messages out-of-sync

4. The Large file can be composed of multiple internal files (say 25MB each) to improve the efficiency of processing these large files

Step 3: Determine the Channel - Use Case: Monthly Snapshot Reports



Use Case: Delivery of Monthly Snapshot Reports

1. **When AEMO provides the Monthly Snapshot report there is no expectation of a business response, so it is Fire & Forget pattern.**
2. **Message payload size is 'Large'**
3. **Channel to be used is File Transfer**

Background - Message Size Threshold – Recommendation Made

AEMO requested Focus group members to share their feedback on the option that should be used to assign the threshold value. AEMO asked the Focus group to consider their organisation needs and provide inputs on how these options will improve their pain points and/or minimise the capex-opex costs.

Criteria	Option 1: Global Value	Option 2: @ Business Function Level	Option 3: @ Schema Type Level
Minimises operational & governance overhead in managing the threshold value	●	◐	●
Minimises the impacts to performance of the message exchange e.g. (not limited to) schema validations, transformation, applying business & technical validations	◐	◔	◔
Minimises the impacts to Participants' infrastructure capacity uplifts. Ability to localise the uplifts only when consuming the business function / service	◐	◔	◐
Minimises the overhead to establish new business services	●	◐	●

The Focus group discussed these options in detail and the recommendation was that **Option 3 – Schema type level** provided the right balance factoring in flexibility and complexity

Background - Approach to determining message size thresholds – Recommendation Made

Two potential approaches to determining message size thresholds were put forward in the Decision Tree Focus Group for consideration by the broader Working Group:

1. **Academic** – reference best practice / technical standards where available to determine thresholds

2. **Test & tune** – use best practice / technical standards to establish a target range, test and tune by measuring performance to confirm an optimal threshold
   - Performance testing could be performed internally by AEMO or in concert with industry as part of the pilot phase

The previous MITEWG selected Test & Tune as the poll outcome.

Large File Capabilities

Capabilities and Features Overview

Large File Transfer is planned to provide the following capabilities and features. The following slides will provide more detail on these capabilities and features.

Security

- AuthN and AuthZ [1]
- Restrictions and Policy Enforcement [1]
- Malware Protection
- Non-Repudiation

Access

- Network Access
- Interfaces Available
- AEMO Gateway Software

Payload and Structure

- B2B File Transfers [2]
- File Delivery Orchestration [2]
- Folder / Directory Structure [2]
- Audit Logs
- Event Notifications [2]
- Technical Documentation
- Fan-out

Industry Key Pain Points

[1] ***Enhanced security*** *for data exchange and centralised access management*

[2] **Protocols, formats and standards are inconsistent** and unnecessarily convoluted

Capabilities - Securing Large File Transfers

Today, AEMO provides very limited security on file transfers. As part of IDX, we will uplift our security on large file transfers.

File Transfer Security (AuthN and AuthZ)	Currently AEMO uses FTP for NEM file transfers. Since FTP is a non-secure way to transfer data, it is recommended to use more secure protocols like SFTP, FTPS, HTTPS, etc. for large file transfers. Further we expect to deliver fine-grained access to Large File services and folders through the IDAM solution
Restrictions and Policy Enforcement	Throttling, maximum supportable file sizes, file compression, file chunking, encryption, bandwidth checks, flow control, masking.
Malware Protection	As part of the large file solution, AEMO will implement more robust virus and malware security scans of files.
Non-Repudiation	AEMO recommends digitally signing the files for non-repudiation purposes (done today on Gas FRC ebXML messages). This will be discussed in a future Focus Group session on Payloads, where the outcome will be applied to all channels.

Upcoming Focus Group - a detailed conversation on this is reserved in a future IDAM Focus Group

File compression will be reviewed in a further slide

Upcoming Focus Group - the Payload Focus Group on 15th Nov will discuss this capability

Capabilities - Access

AEMO will provide various access methods to participants in using Large File Services.

Network Access	Large file message exchange is available over both MarketNet and the Internet.
Interfaces Available	Accessible via both machine-to-machine and Low Volume Interface (LVI).
AEMO Gateway Software	The AEMO gateway software will support large file transfers with the IDX large file solution.

Would participants see a need to access large file share services across both **MarketNet and the Internet**?

The Focus group suggested we retain both access methods

Upcoming Focus Group **-** the AEMO Gateway Software Focus Group on 5th Dec will discuss this capability

Capabilities – Payload and Structure

Other features and capabilities associated with Large File Transfers include the following

B2B File Transfers	The large file solution should be able to manage the transfer of large file transfers between participants.
File Delivery Orchestration	The large file solution will be able to orchestrate a series of files / messages / acknowledgements into a single process for traceability.
Logical Hierarchy Structure	A Hierarchy (e.g. folders) will be segregated by market, by business function and per registered participant. There will be corresponding inbound, outbound and archive locations.
Audit Logs	The large file solution will have the ability to track and audit all legs of large file transfers and log them to the Technical and Audit logs.
Event Notifications	The large file solution should have the ability to generate and send events/notifications through a common channel.
Technical Documentation	A technical guide for machine-to-machine integration (to explain how to integrate, access and use large file services) should be available on a developer portal, or similar portal for technical documentation.
Fan-out	Ability of single large file message to be delivered to multiple recipients.

Logical hierarchy structure will be discussed in more detail in following slides

Upcoming Focus Group – the Async Focus Group on 25th Nov will discuss this channel

File Delivery Orchestration

File Delivery Orchestration

Currently there are different ways in which markets manage file-based message exchanges. IDX looks to develop a common pattern where practical to ensure consistency across markets and data exchanges. Key areas for discussion are:

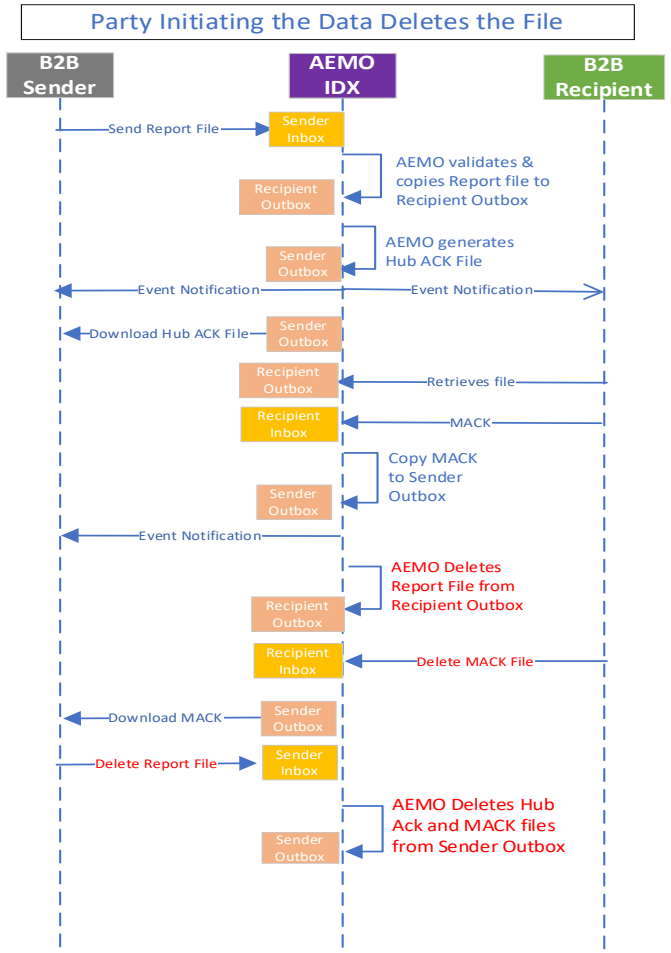
- **Orchestration:** The large file solution will be able to orchestrate a series of files / messages / acknowledgements into a single process for traceability across Asynchronous and Fire and Forget Pattens.

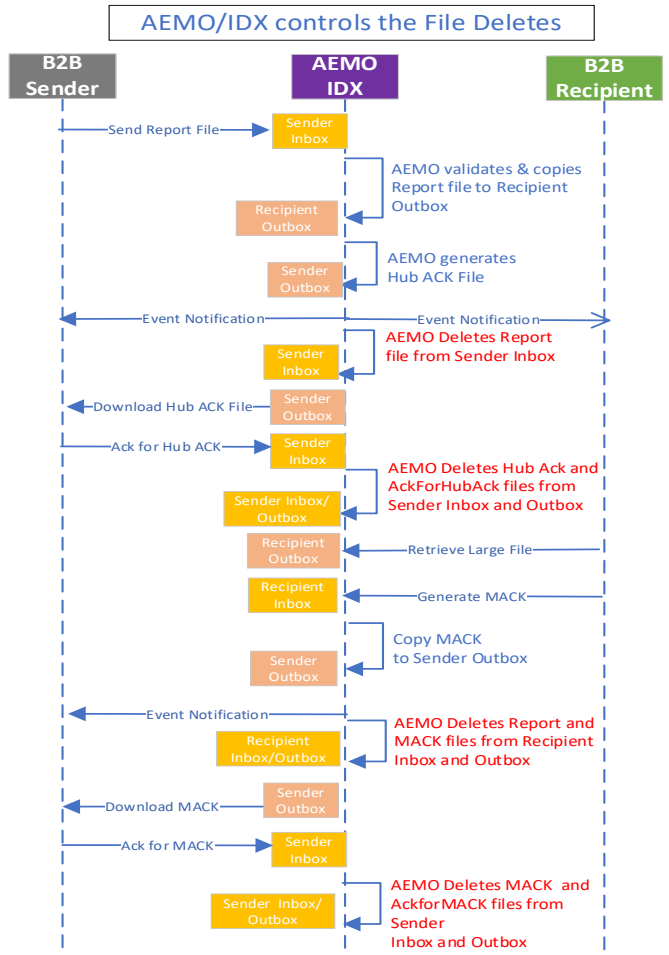
- **File deletion:** Wholesale and Retail have different approaches to file deletion:
  - In Wholesale the recipient deletes the files.
  - In Retail the initiator deletes the files.

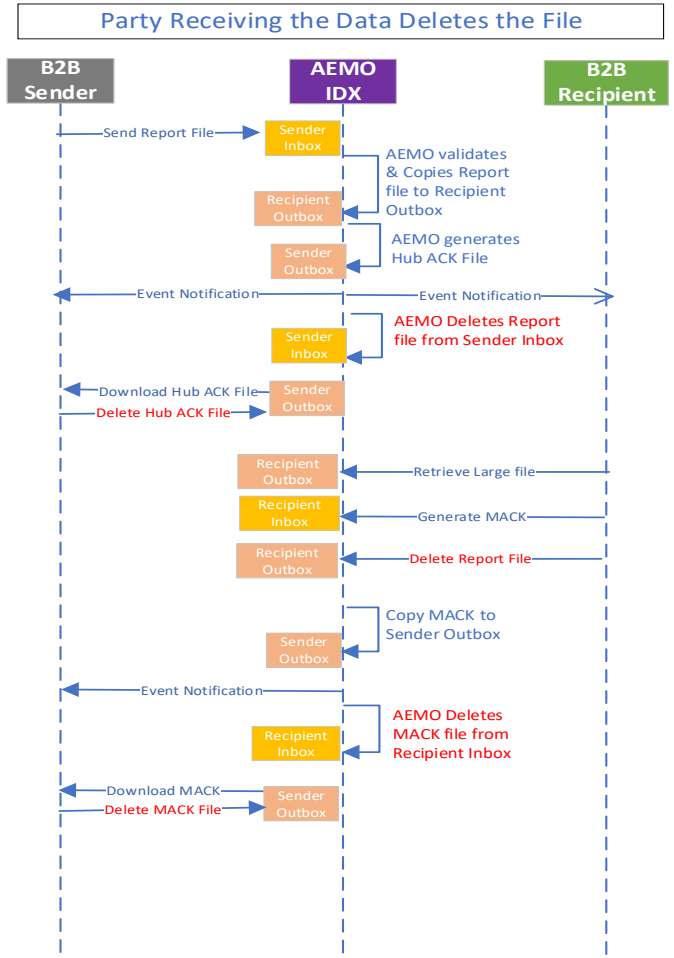
- **Establishing a common Pattern**: The IDX platform looks to establish a common pattern across markets and will seek focus group feedback on the preferred option for file deletion.

Async File Delivery Orchestration – File delete control options

The below flows outline the file orchestration and options on who controls the deletion of files in the Async model (Sender, IDX or the Recipient). There are pros and cons of each method. AEMO will adopt a common standard file deletion standard.

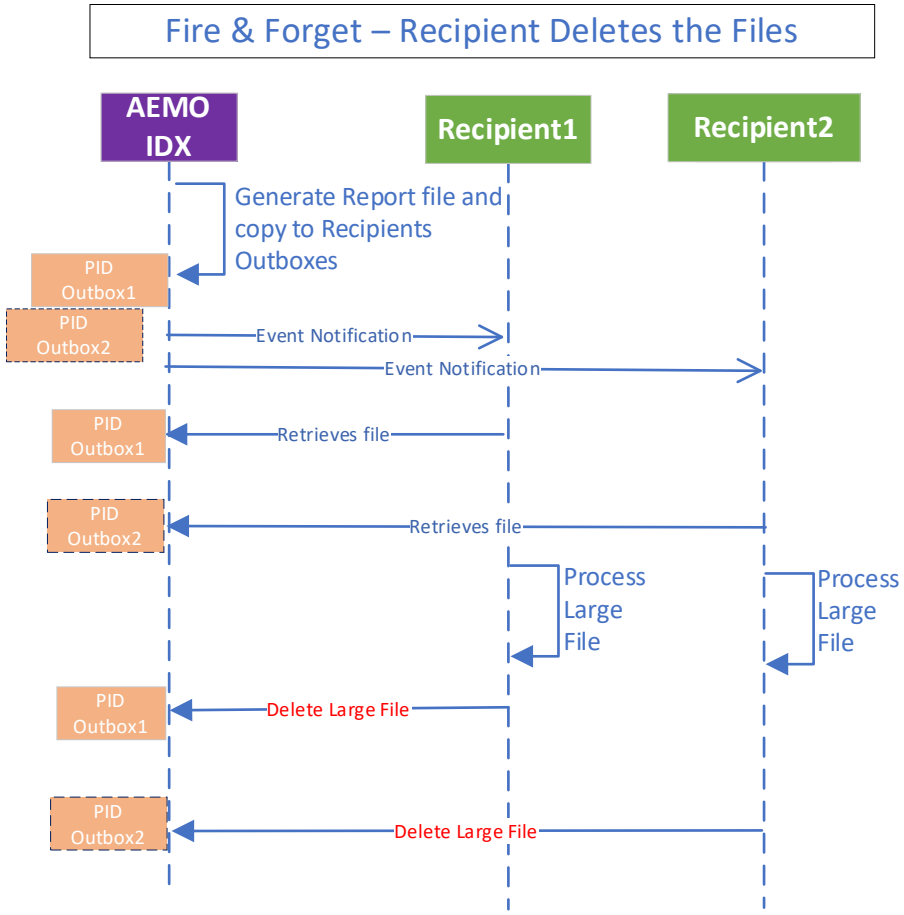


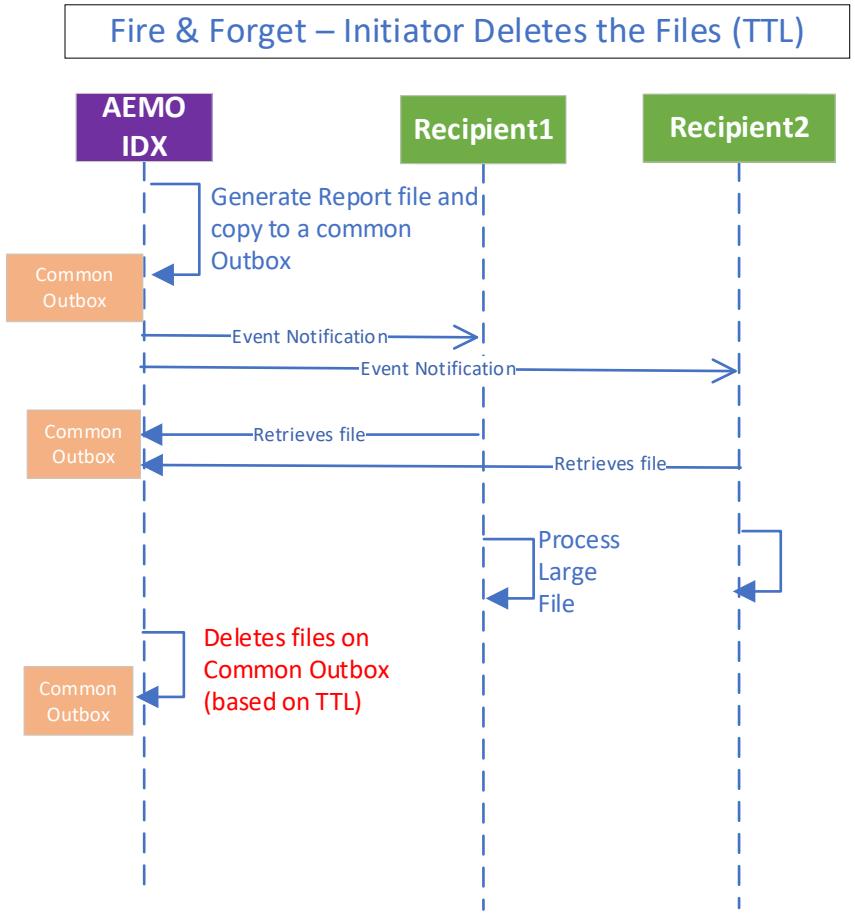




Fire & Forget - File Delivery Orchestration

Below flows outlines the file orchestration and options on who controls the deletion of files in the Fire & Forget model (Initiator/IDX and Recipient). Both these options will be available for F&F services, but a service can't have both these options at once. For e.g., Public Reports are TTL whereas Monthly Snapshot Reports are the ones that recipient controls the delete.



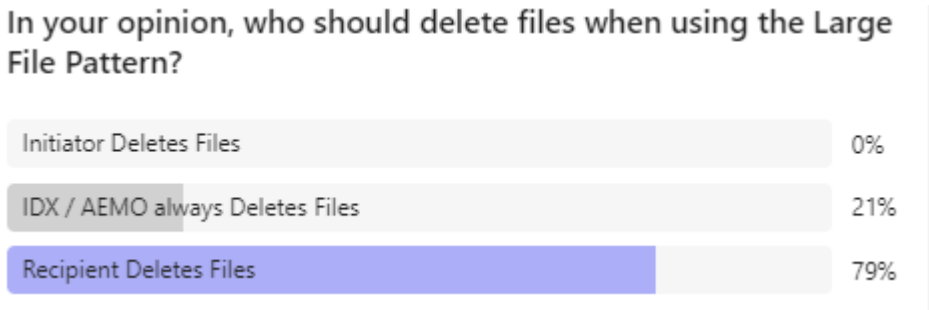


File Delivery Orchestration – Async File Deletion Options

AEMO asked the Focus group to consider their organisation needs and provide inputs into the option that should be used as a basis for the recommendation to the MITE Working group.

Criteria	Option 1: Initiator Deletes	Option 2: IDX Deletes	Option 3: Recipient Deletes
Level of effort required on the participant side	◐	◐	◐
Guaranteed delivery (related to non-repudiation)	◐	◐	●
File integrity (recipient file is incorrupt)	◐	◐	●
Folder control (AuthZ security)	●	◔	◐
Orchestration complexity(knowing when to delete)	◔	◐	●
Fire & Forget friendly (no Acknowledgements required)	◔	◔	●

The Focus Group recommendation based on the POLL conducted in the Focus group was to recommend Option 3 : Recipient Deletes with 79% of the Poll results.



Compression

Today, AEMO uses Zip compression on all files.

AEMO recommends:

- **Committing to Zip as a single compression format for all file transfers.**
- **Compressions of all files by default.**

Format	Pros	Cons
Zip	• Can compress multiple files. • Can be password protected • Wide range of support • CRC file check to verify file integrity	• Less efficient compression ratios

The Focus group Identified no additional compression formats

Are there other compression formats that participants need?

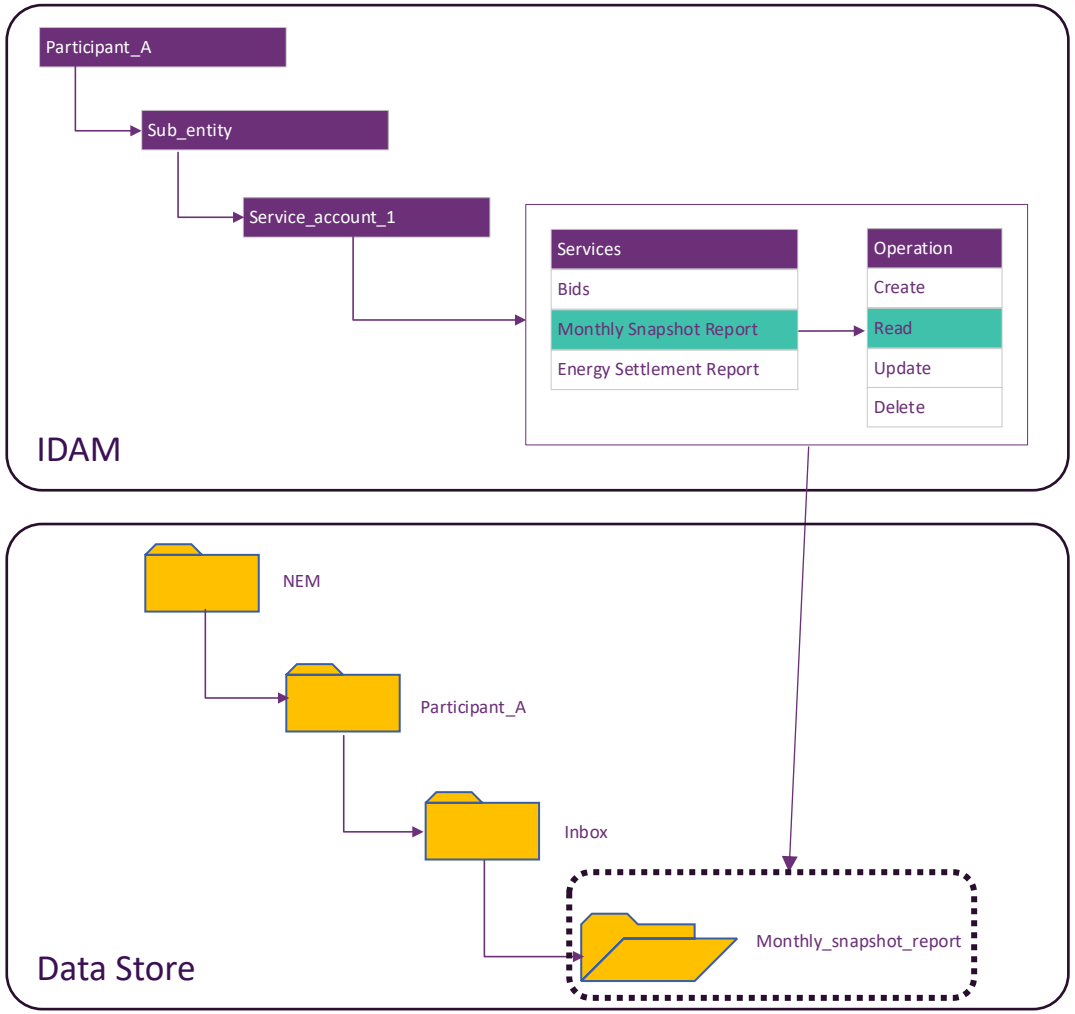
Are there any objections to compressing files by default?

The Focus group had no objections to compressing files by default

Logical Hierarchy

Proposed Structure - Principles

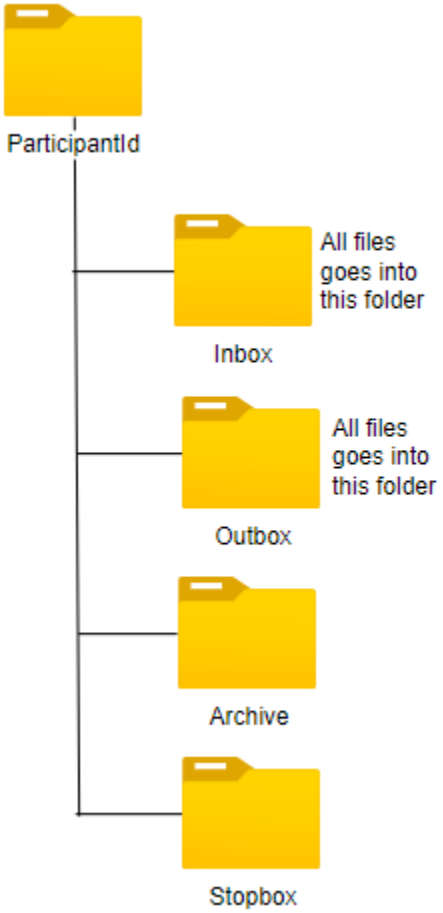
- A unified single structure the supports all business functions
- For each market participant, a hierarchy of structures shall be provisioned (for object, or file-based storage).
- Each market participant is granted fine-grained access rights for the hierarchy (IDAM). Authentication details will be discussed at a future IDAM Focus Group.
- AEMO's Applications and Participants MUST not overwrite, lock out each other at the file level.



For illustrative purposes only, an example of fine-grained access to be provided from Participant accounts to Large File Share folders

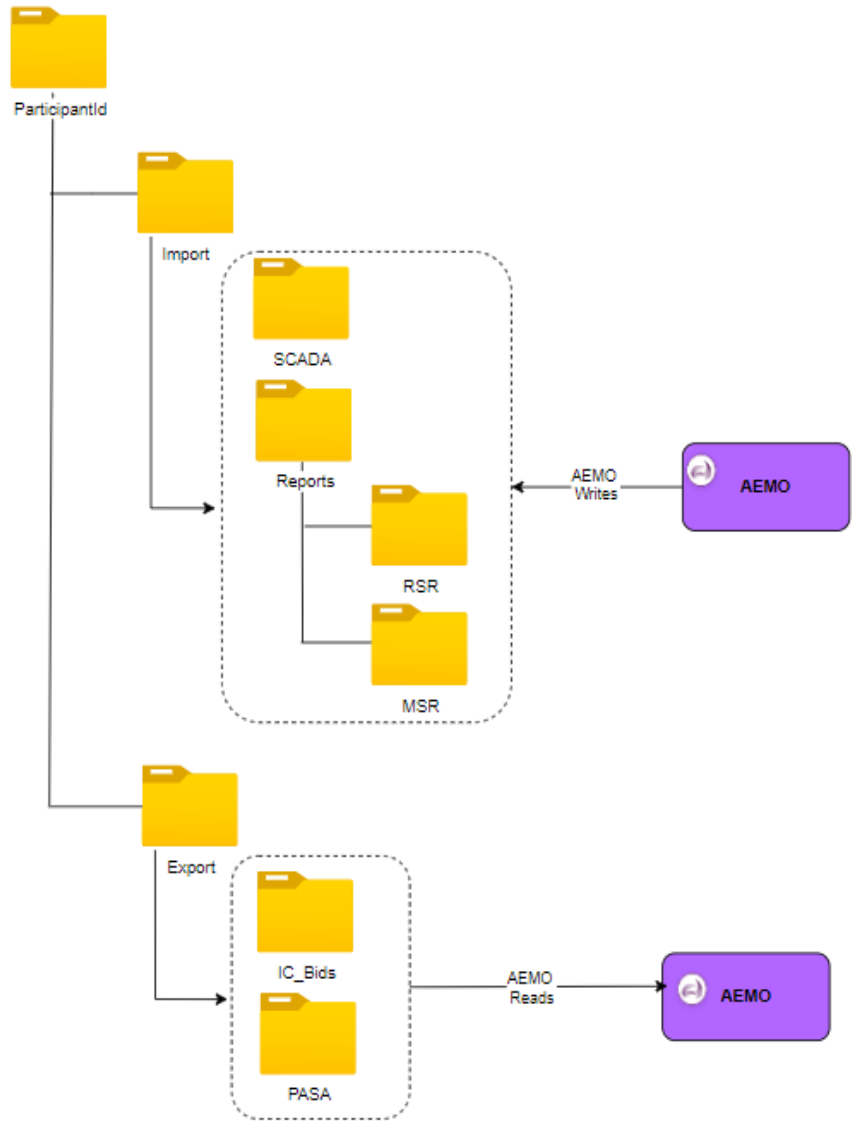
Current Hierarchy of Folders - Retail

- Current folder structure used in **retail** file transfers.



Current Hierarchy of Folders - Wholesale

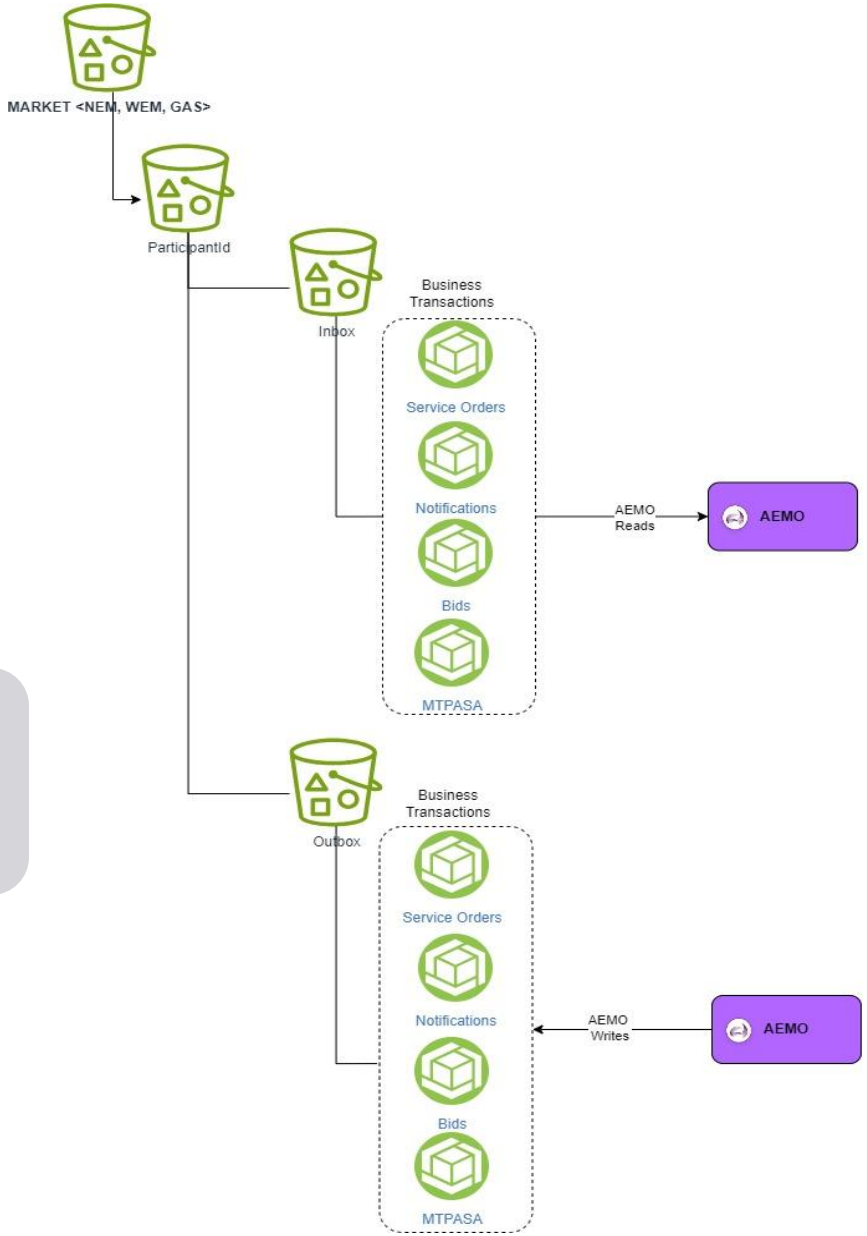
- Current folder structure used in **wholesale** file transfers.



Proposed Logical Hierarchy – Wholesale and Retail

- For each market participant, a logical hierarchy to be provisioned.

- Key Requirement:
  - Each market participant is granted fine-grained access rights for the logical hierarchy.
  - AEMO's Applications and Participants MUST not overwrite, lockout each other.
  - AEMO is exploring more sophisticated logical hierarchy storage mechanisms like Object store, S3, etc., which will simplify the logical hierarchy and control structures.



The Focus group had no objections to compressing files by default

Do participants support the above logical hierarchy across Large File Share services?

Flow Control (Stop Files)

Flow Control Principles

The current stop file process used in NEM Retail applies across B2B and B2M services for Participants. The challenge with this approach is that message volumes span across all message priority and Transaction types, potentially impacting participants ability to send high priority messages.

IDX is looking to define / update flow control measures to support equivalent Stop file capabilities by defining a set of principles across both Large File and API channels to allow more fine-grained controls. While this is to be discussed in another Focus group a few things to note are:

- IDX will look to enforce flow control at the Business Function and is Channel specific.
  - E.g. if there's a stop on Service Orders, this will only impact the Service Orders service for the Participant.
- Applicable based on message pattern (e.g. applicable to Asynchronous, not Fire and Forget)
- Flow control processes will need to be considered across both Large File and API channels

Upcoming Focus Group - a detailed conversation on flow control will be covered in a future Focus Group

Notes

Udaya spoke to the IDX Large File topic with lots of great questions and feedback.

Participants asked if the system would support splitting large files into multiple chunks for outbound delivery if the file is too large to process or transfer as a whole? AEMO responded by saying yes, bundling and unbundling mechanisms will be supported, with decisions guided by the decision tree framework to ensure data integrity, efficiency, and consistency. The approach will balance technical feasibility and practicality while maintaining a consistent process across energy markets.

Participants asked if the decision has been made that who will delete the file? AEMO responded that in last meeting many of the participants agreed via poll that the recipient will delete the file. AEMO also reiterated that the goal is to establish a consistent approach across energy markets, with a preferred mechanism where the receiving party deletes the file, ensuring they have control and confidence in its receipt and consumption.

Participants raised the risk of files accumulating in case of option 3, but AEMO responded by saying that this risk exists in case of option1 as well and reminded that the flow control mechanisms will mitigate the risk by prompting participants to delete files to continue processing data in both options one and three.

Participants asked about how data management, folder handling, access options, and structural consistency will be addressed during the transition from FTP to the new system, to which AEMO responded by saying that the approach is to transition users to the new framework while maintaining parallel operation for backward compatibility, but with plans to phase out compatibility where it limits progress, such as moving from folder-based to object-based models for improved technology adoption. AEMO also mentioned that the framework balances unbundling for functionality, flow control, and security without overcomplicating or limiting industry value.

AEMO also addressed questions about stopfile and explained the benefits of having flow control limits per business function instead of a global limit.

3. IDX - Payload Focus group Recap

Selwyn Sequeira

Objective of the Focus Group

The MITE FG was established to discuss in detail specific topics for IDX. This focus group discussed Payloads.

The focus group covered..

- Re-Cap the pain points for payloads that exist today.
- Review and discuss drafted different payloads options considered, including payload Decision Tree.
- Review and discuss proposed Payload schema; versioning, validation and transformation (target state)
- Review and discuss payload compression.
- Review and discuss non-repudiation of payloads and target-state principles.

The ask of participants...

- **Participate** in highly technical discussions, including engaging within their business prior, to provide detailed responses to matters under discussion
- **Champion** technical discussions with their peers and within own organisations.
- **Review** draft documentation prepared by the Focus Group and provide input.

Out of Scope

- Payload formats for Scada and Direct device messaging will be out of scope for IDX.
- The detailed specification of each payload will be covered in a future Focus Group.
- The detailed and confirmed non-repudiation method and process.

Payloads Pain Points

Pain Points	Proposed Principle(s)	Target State Concept
Industry raised pain points: • Inconsistent protocols, formats and standards across systems, fuels and jurisdictions • Mandatory schema updates are costly • Slow implementation of business and regulatory changes when it affects the schema *AEMO's reading of industry pain points:* • With many payload formats this brings about complexity and cost • Adding new transactions in aseXML requires changing a schema version • Schema updates take time (typically 2-3 months) and schema breaking changes are usually bundled together reducing speed to market of business and regulatory changes • Lack of Enumeration versioning can lead to outdated participant versions	• A standard set of Industry agreed payloads across all Participants, Markets and Domains. • Applying security best practices in the transmission and store of payloads. • Applying best-practice non-repudiation as a standard on payloads. • Applying speed and efficiency techniques (like compression) in the payload transmission mechanism. • Adopting scalable and flexible infrastructure in the handling of payloads.	• Unify to JSON and AEMO_CSV Payload Formats. • Schemas will be per business function per payload format. Allowing for schema updates only on part of a business function for that payload format, allowing for more quicker version updates and significantly limiting participant impacts.

Payload types - JSON

JSON


```
{
    "transactionId": "296432aa-7cc6-43e5-b611-0c8cbd092748",
    "data": {
        "CallSuccessful": true,
        "CallResponseMessage": "GSH Physical Gas Future Data Request completed.",
        "ItemList": [{
            "MarketId": "GSH",
            "RecordId": 33983,
            "ParticipantId": "2012",
            "GasFutureId": "ASX-AEMO-DEMO-344",
            "ProductGroupCode": "GAS-WAL",
            "ProductTypeCode": "Gas - NG Months",
            "DeliveryPoint": "WAL HP Trade Point",
            "StartDate": "2022-07-01T00:00:00Z",
            "EndDate": "2022-07-31T00:00:00Z",
            "TradeType": "BUY",
            "Price": 3,
            "Volume": 4,
            "TradeValue": 12,
            "Status": "PENDING",
            "ValidationMsg": "",
            "SubmittedTime": "2022-06-07T22:56:37Z",
            "LastChanged": "2022-06-07T22:56:37Z"
        }, {
            "MarketId": "GSH",
            "RecordId": 33982,
            "ParticipantId": "2012",
            "GasFutureId": "ASX-AEMO-DEMO-344",
            "ProductGroupCode": "GAS-WAL",
            "ProductTypeCode": "Gas - NG Months",
            "DeliveryPoint": "WAL HP Trade Point",
            "StartDate": "2022-07-01T00:00:00Z",
            "EndDate": "2022-07-31T00:00:00Z",
            "TradeType": "BUY",
            "Price": 3,
            "Volume": 4,
            "TradeValue": 12,
            "Status": "OVERRIDE",
            "ValidationMsg": "",
            "SubmittedTime": "2022-06-07T12:20:07Z",
            "LastChanged": "2022-06-07T22:56:37Z"
        }]
    },
    "errors": []
}
```


Features:

- Simplified data parsing and easy readability.
- Modern programming languages have built in libraries that natively support JSON
- Greater support for different data types like strings, numbers, arrays, Boolean

Current use case:

- GSH Physical Gas Futures Data

Payload types - aseXML

aseXML

```
<?xml version="1.0" ?>
<ase:aseXML xmlns:ase="urn:aseXML:r44" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:aseXM
http://www.nemmco.com.au/aseXML/schemas/r44/aseXML_r44.xsd">
  <Header>
    <From description="Australian Energy Market Operator Limited">NEMMCO</From>
    <To description="Australian Energy Market Operator Limited">NEMMCO</To>
    <MessageID>NEMMCO-MSG-1339293967</MessageID>
    <MessageDate>2024-10-22T19:34:55+10:00</MessageDate>
    <TransactionGroup>CATS</TransactionGroup>
    <Priority>Medium</Priority>
    <SecurityContext>NEMMCOBATCH</SecurityContext>
    <Market>NEM</Market>
  </Header>
  <Transactions>
    <Transaction transactionID="CATS-1339293967" transactionDate="2024-10-22T19:34:55+10:00" initiatingTransactionID="2726
      <ReplicationNotification version="r10">
        <ReplicationParameters>
          <TableName>CATS_ERROR_CODES</TableName>
          <CreationFromDate>1970-01-01T00:00:00+10:00</CreationFromDate>
          <CreationToDate>2024-10-22T23:59:59+10:00</CreationToDate>
          <LastSequenceNumber>0</LastSequenceNumber>
          <MaximumRows>1000</MaximumRows>
        </ReplicationParameters>
<ReplicationBlock tableName="ErrorCodes">
  <Row xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ase:ErrorCodeRow">
    <SequenceNumber>1</SequenceNumber>
    <CreationDate>2001-01-01T00:00:00+10:00</CreationDate>
    <MaintenanceDate>9999-12-31T00:00:00+10:00</MaintenanceDate>
    <RowStatus>A</RowStatus>
    <FromDate>2001-01-01T00:00:00+10:00</FromDate>
    <ToDate>9999-12-31T00:00:00+10:00</ToDate>
    <Code>1000</Code>
    <Description>Fatal Error</Description>
  </Row>
  <Row xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ase:ErrorCodeRow">
    <SequenceNumber>2</SequenceNumber>
    <CreationDate>2001-01-01T00:00:00+10:00</CreationDate>
    <MaintenanceDate>9999-12-31T00:00:00+10:00</MaintenanceDate>
    <RowStatus>A</RowStatus>
    <FromDate>2001-01-01T00:00:00+10:00</FromDate>
    <ToDate>9999-12-31T00:00:00+10:00</ToDate>
    <Code>1001</Code>
    <Description>Success: Changes saved</Description>
  </Row>
```


Features:

- Can be validated using a defined schema
- Uses a tree-based structure
- Allows for enumerations to be defined

Current use case:

- Cats C1 Report

Payload types - aemoCSV

aemoCSV

```
C,NEMP.WORLD,TRADINGIS_LEGACY,AEMO,PUBLIC,2024/10/01,00:10:10,0000000434723082
,TRADINGIS,0000000434723080
I,TRADING,INTERCONNECTORRES,2,SETTLEMENTDATE,RUNNO,INTERCONNECTORID,PERIODID,M
ETEREDMWFLOW,MWFLOW,MWLOSSES,LASTCHANGED
D,TRADING,INTERCONNECTORRES,2,"2024/10/01
00:15:00",1,N-Q-MNSP1,3,1.9,9,0.6,"2024/10/01 00:10:03"
D,TRADING,INTERCONNECTORRES,2,"2024/10/01
00:15:00",1,NSW1-QLD1,3,330.9,340.4,12.45,"2024/10/01 00:10:03"
D,TRADING,INTERCONNECTORRES,2,"2024/10/01
00:15:00",1,T-V-MNSP1,3,500.5,501.49,24.18,"2024/10/01 00:10:03"
D,TRADING,INTERCONNECTORRES,2,"2024/10/01
00:15:00",1,V-S-MNSP1,3,50,50,1.95,"2024/10/01 00:10:03"
D,TRADING,INTERCONNECTORRES,2,"2024/10/01
00:15:00",1,V-SA,3,498.96,499.46,33.42,"2024/10/01 00:10:03"
D,TRADING,INTERCONNECTORRES,2,"2024/10/01
00:15:00",1,VIC1-NSW1,3,1049.45,1079.9,122.97,"2024/10/01 00:10:03"
I,TRADING,PRICE,2,SETTLEMENTDATE,RUNNO,REGIONID,PERIODID,RRP,EEP,INVALIDFLAG,L
ASTCHANGED,ROP,RAISE6SECRRP,RAISE6SECROP,RAISE60SECRRP,RAISE60SECROP,RAISE5MIN
RRP,RAISE5MINROP,RAISEREGRRP,RAISEREGROP,LOWER6SECRRP,LOWER6SECROP,LOWER60SECR
RP,LOWER60SECROP,LOWER5MINRRP,LOWER5MINROP,LOWERREGRRP,LOWERREGROP,PRICE_STATU
S
D,TRADING,PRICE,2,"2024/10/01 00:15:00",1,SA1,3,94.48,0,0,"2024/10/01
00:10:03",94.48,0.36,0.36,0.36,0.36,0.97,0.97,4.73,4.73,0.1,0.1,0.15,0.15,0.01
,0.01,0.01,0.01,FIRM
D,TRADING,PRICE,2,"2024/10/01 00:15:00",1,NSW1,3,103.59,0,0,"2024/10/01
00:10:03",103.59,0.36,0.36,0.36,0.36,0.97,0.97,4.73,4.73,0.1,0.1,0.15,0.15,0.0
1,0.01,0.01,0.01,FIRM
D,TRADING,PRICE,2,"2024/10/01 00:15:00",1,QLD1,3,110.43,0,0,"2024/10/01
00:10:03",110.43,0.36,0.36,0.36,0.36,0.97,0.97,4.73,4.73,0.1,0.1,0.15,0.15,0.0
1,0.01,0.01,0.01,FIRM
D,TRADING,PRICE,2,"2024/10/01 00:15:00",1,TAS1,3,0.17,0,0,"2024/10/01
00:10:03",0.17,0.36,0.36,0.36,0.36,0.97,0.97,3.45,3.45,0.98,0.98,0.98,0.98,0.0
1,0.01,3.72,3.72,FIRM
D,TRADING,PRICE,2,"2024/10/01 00:15:00",1,VIC1,3,84.06,0,0,"2024/10/01
00:10:03",84.06,0.36,0.36,0.36,0.36,0.97,0.97,4.73,4.73,0.1,0.1,0.15,0.15,0.01
,0.01,0.01,0.01,FIRM
C,"END OF REPORT",15
```


Features:

- Contains C – Comment fields , I – Header information , D-Data rows
- Reports on number of records and has an end of report indicator

Current use case:

- NEM Wholesale Reports

Payload types - ebXML

ebXML

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:eb="http://www.ebxml.org/namespaces
xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
file:packages/WmebXML/config/init/schemas/msg_1_0/envelope.xsd http://www.ebxml.org/namespaces/messageHeader
file:packages/WmebXML/config/init/schemas/msg_1_0/messageHeaderv0_99.xsd">
    <SOAP-ENV:Header>
        <eb:MessageHeader SOAP-ENV:mustUnderstand="1" eb:version="1.0">
            <eb:From>
                <eb:PartyId eb:type="urn:frchub.net">FBS</eb:PartyId>
            </eb:From>
            <eb:To>
                <eb:PartyId eb:type="urn:frchub.net">VENCORP</eb:PartyId>
            </eb:To>
            <eb:CPAId>FBS VENCORP 00:05 2 PT60M PT180M</eb:CPAId>
            <eb:ConversationId>FBS VENCORP FBS e28506a2-0962-4811-b0f8-ec6cbfe1a37f</eb:ConversationId>
            <eb:Service eb:type="fbs">MediumPriorityAseXMLDocument</eb:Service>
            <eb:Action>CATS</eb:Action>
            <eb:MessageData>
                <eb:MessageId>FBS e28506a2-0962-4811-b0f8-ec6cbfe1a37f</eb:MessageId>
                <eb:Timestamp>2024-09-17T15:47:44+10:00</eb:Timestamp>
                <eb:TimeToLive>2024-09-17T18:47:44+10:00</eb:TimeToLive>
            </eb:MessageData>
            <eb:QualityOfServiceInfo eb:deliverySemantics="OnceAndOnlyOnce"/>
        </eb:MessageHeader>
        <eb:TraceHeaderList SOAP-ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1" eb:version="1.0">
            <eb:TraceHeader>
                <eb:Sender>
                    <eb:PartyId eb:type="urn:frchub.net">FBS</eb:PartyId>
                    <eb:Location>[redacted]:5619/invoke/relay/inbound</eb:Location>
                </eb:Sender>
                <eb:Receiver>
                    <eb:PartyId eb:type="urn:frchub.net">RELAY</eb:PartyId>
                    <eb:Location>[redacted]:5319/invoke/relay/inbound</eb:Location>
                </eb:Receiver>
                <eb:Timestamp>2024-09-17T15:47:45+10:00</eb:Timestamp>
            </eb:TraceHeader>
        </eb:TraceHeaderList>
        <eb:Via SOAP-ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1" eb:ackRequested="Signed" eb:version="1.0"/>
        <ds:Signature Id="WmEbXML-Signature-[redacted]" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                <ds:Reference URI="">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                        <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
                            <ds:XPath>not(ancestor-or-self::eb:TraceHeaderList or ancestor-or-self::eb:Via)</ds:XPath>
                        </ds:Transform>
                        <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <ds:DigestValue>[redacted]=</ds:DigestValue>
                </ds:Reference>
                <ds:Reference URI="cid:aseXML">
```


Features:

ebXML is strictly not a payload type. It is an envelope that wraps aseXML to provide the below features:

- reliable delivery
- once and only once delivery
- message time to live
- message integrity
- Non-repudiation

Current use case:

- Gas Retail

Unstructured Payload types

Images / PDF's

Portable Document Format – E.g.: Settlement Statement Report
Power System Simulation for Engineering files – E.g.: PSSE files
Graphs – E.g.: jpg, bmp

AEMO sought feedback on the data exchange of other unstructured formats

The Focus group identified no specific additional unstructured formats

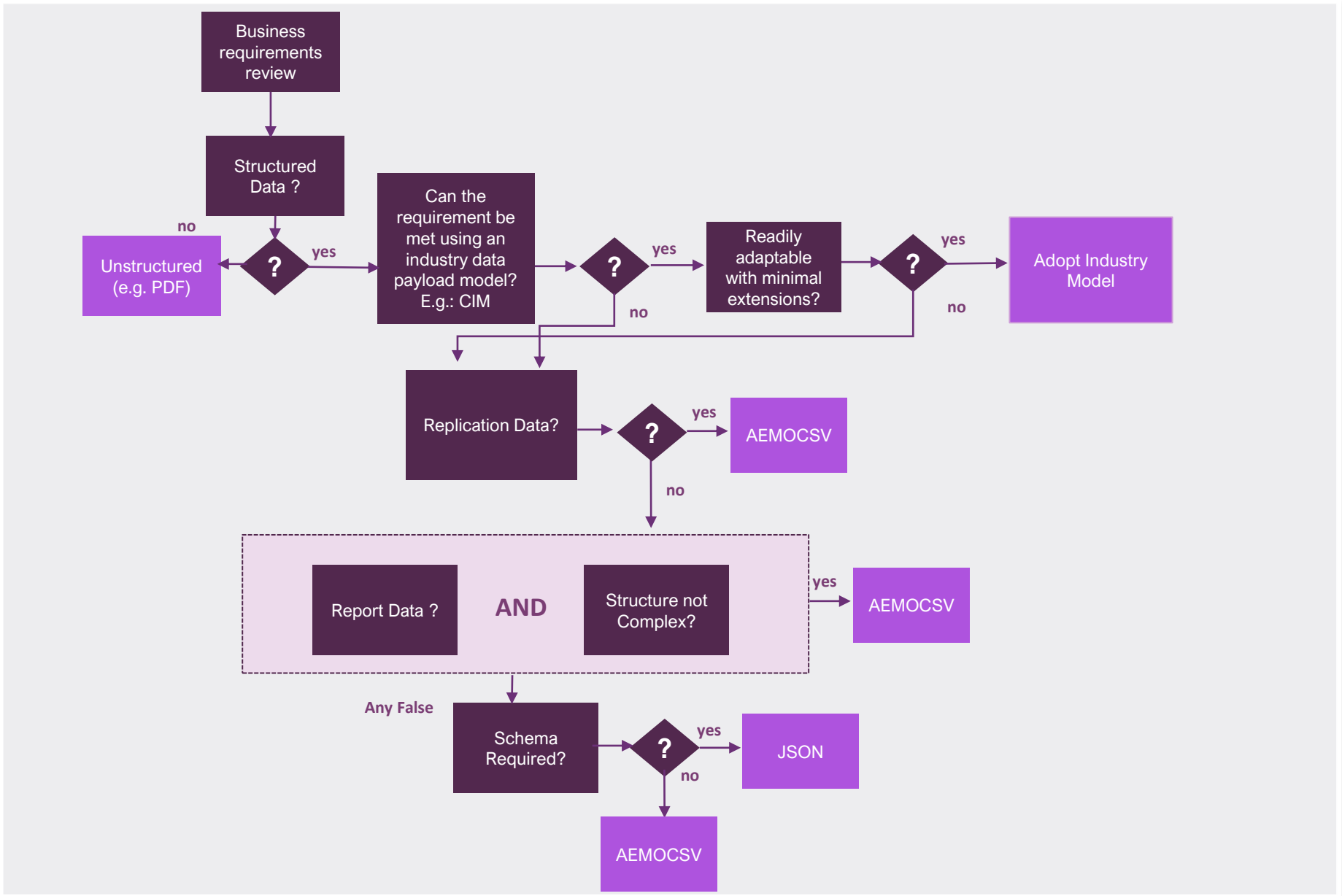
Payload Decision Tree

How the payload format for an IDX service is selected

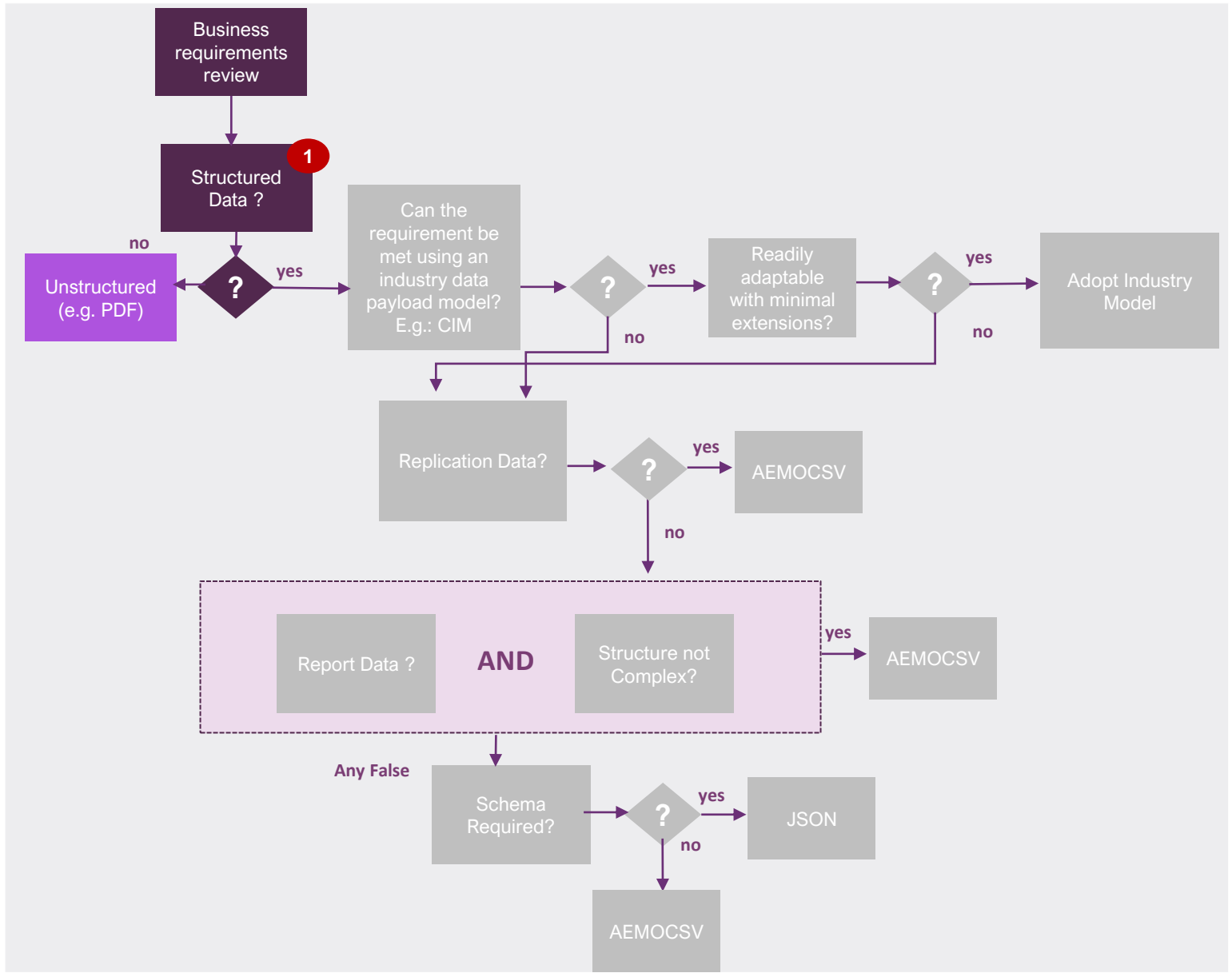
Payload Decision Tree - Definitions

Industry Standards	Where data has an industry standard defined for exchange of information. Examples include IEC CIM (61968) , IEC CIM (61970) ,Consumer Data Standards (CDR/CDP)
Replication Data	Where the data will be consumed for ingestion into a system using replication tools like PDR batcher, AEMO gateway software etc.
Structural complexity	Where data has hierarchical structures (E.g., Nesting, tree structures etc) the complexity of the data is higher than flat structures
Adopt Industry Model	New Industry Model payload formats are reviewed for adoption.
Schema required	If a payload needs to be using a defined schema. AEMO provides a schema definition for participants to validate the payload exchanged.

Payload Decision Tree



Payload Worked Example: Settlement PDF Reports



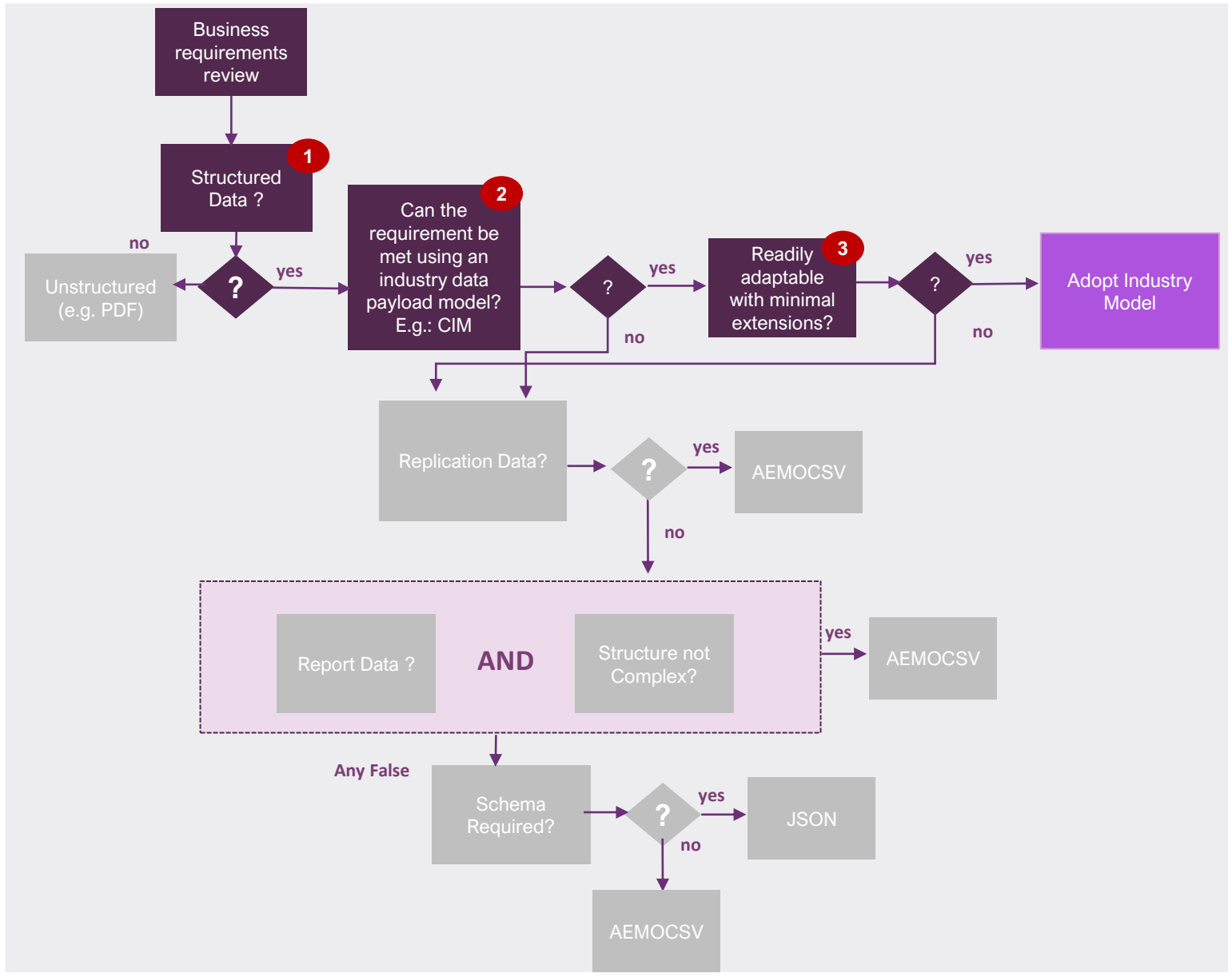
Use Case: Participant settlement reports generated by AEMO in PDF format

Decision tree applied criteria

1. **Data output is structured? - No**

Decision tree output = Unstructured payload format

Payload Worked Example: Consumer Data Right



Use Case: Consumer Data Right – Get DER for Service Point

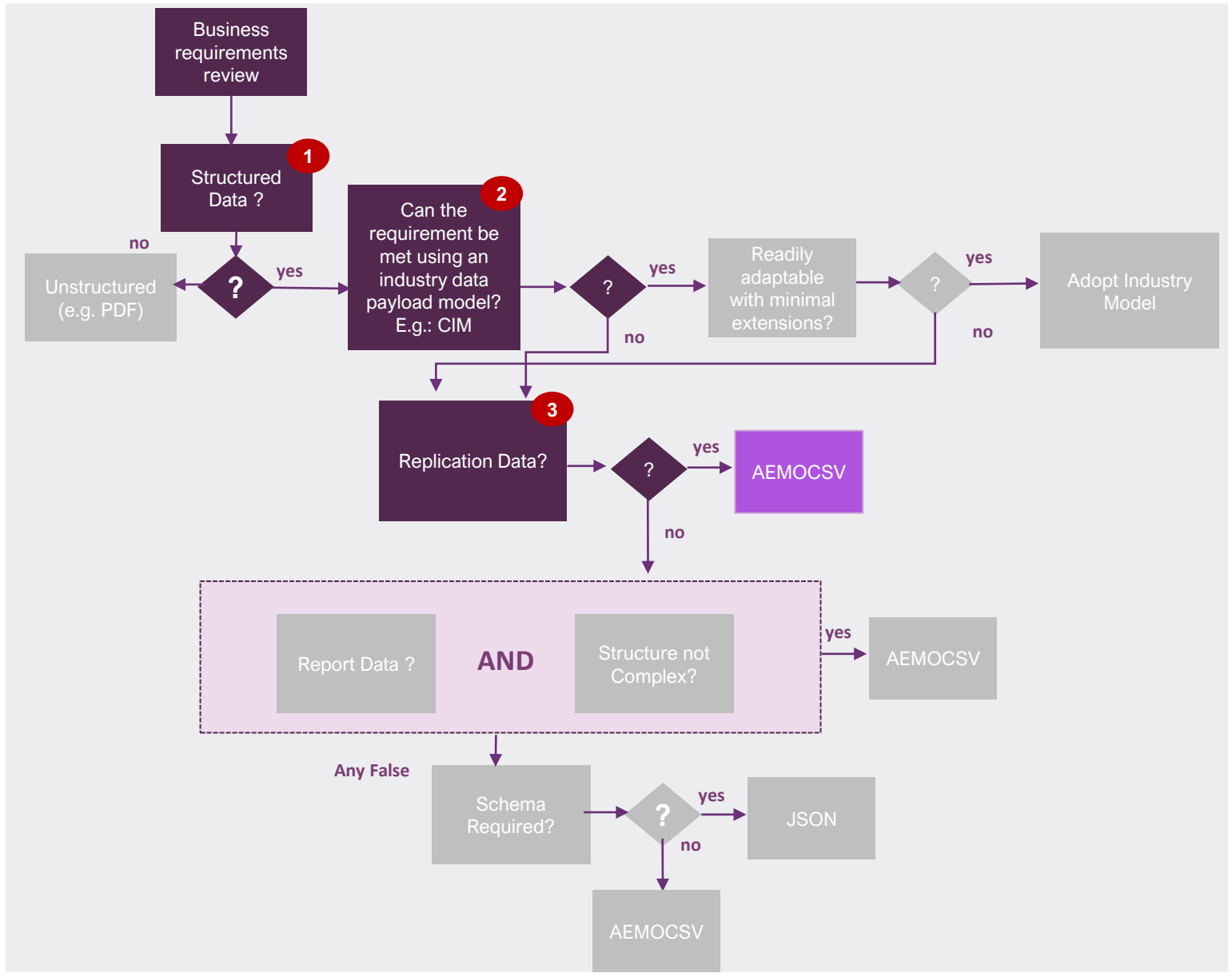
https://consumerdatastandardsaustralia.github.io/standards/#cdr-energy-api_get-der-for-service-point

Decision tree applied criteria

1. Data output is structured? – Yes
2. Can the requirement be met using an industry data payload model? – Yes
3. Readily adaptable with minimal extensions – Yes

Decision tree output = Adopt Industry Model

Payload Worked Example: NEMReports Next Day Public Reports



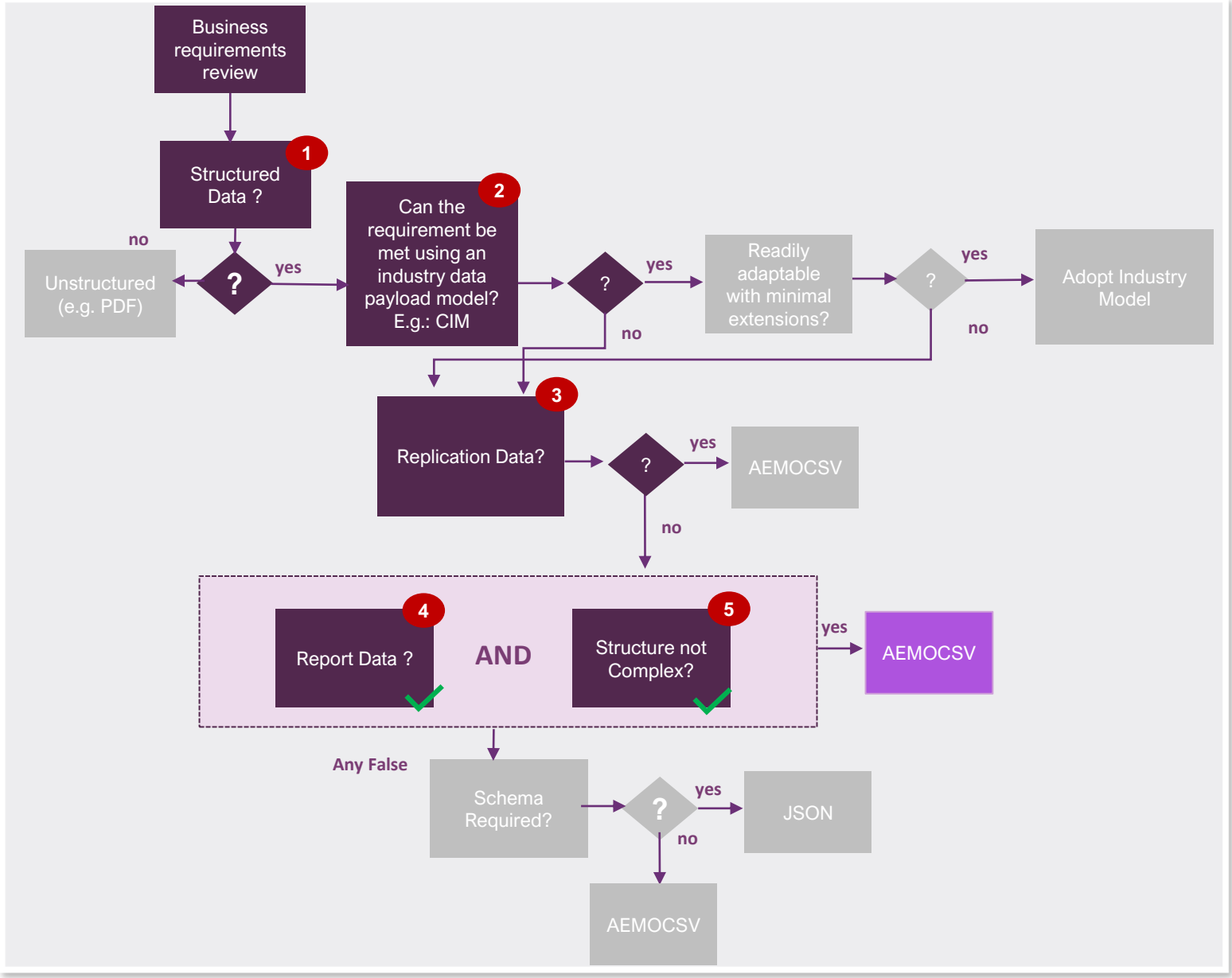
Use Case: NEMReports Next Day public Reports (Dispatch outputs to Participants)
Report Name: Next_Day_Dispatch

Decision tree applied criteria

1. **Data output is structured? – Yes**
2. **Can the requirement be met using an industry data payload model? – No**
3. **Replication Data– Yes**

Decision tree output = AEMOCSV

Payload Worked Example: RM16 reports (Level 2 Settlement report)



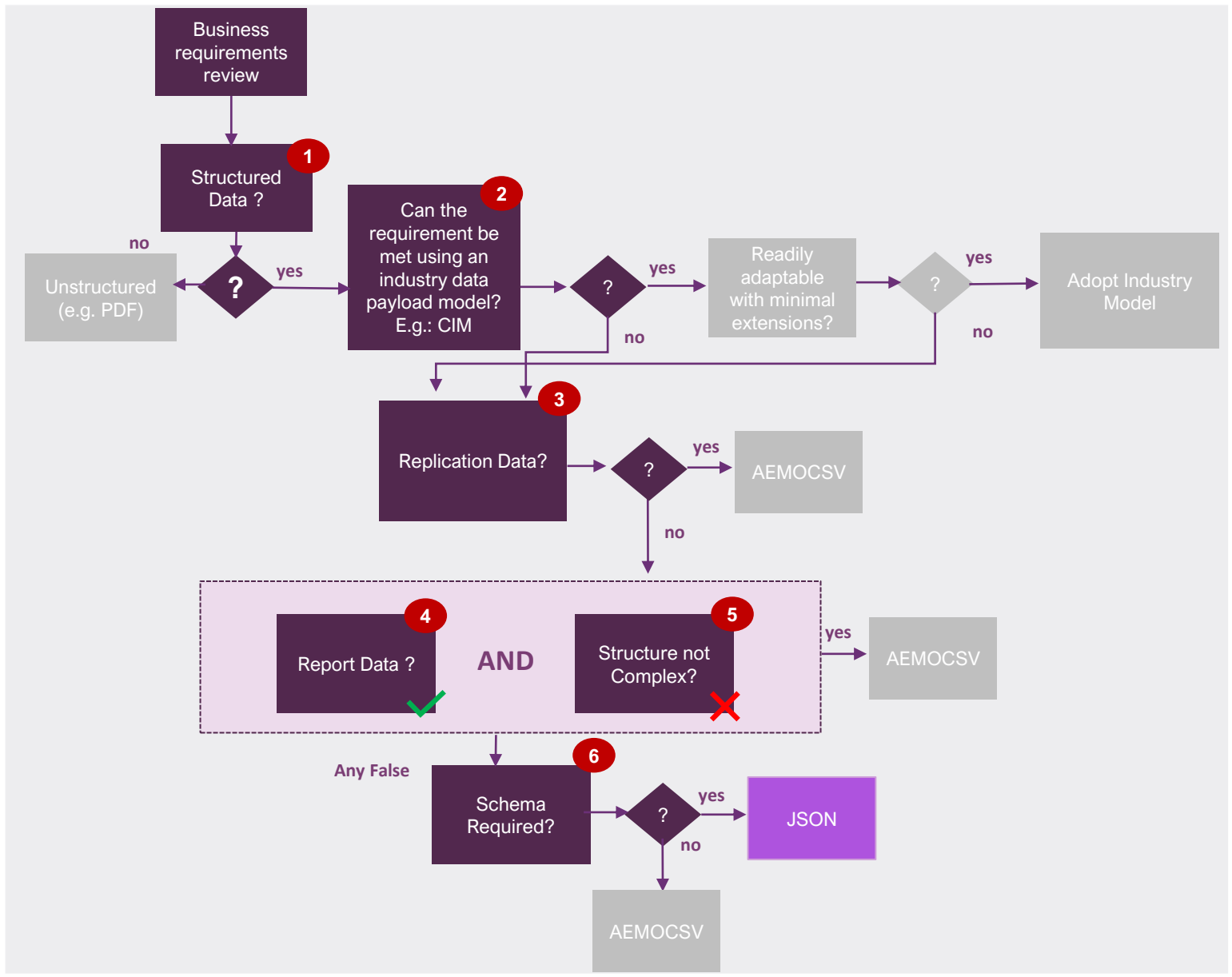
Use Case: RM16 – Level 2 Settlement Aggregated Report

Decision tree applied criteria

1. Data output is structured? – Yes
2. Can the requirement be met using an industry data payload model? – No
3. Replication Data– No
4. Report Data – Yes
5. Structure Not Complex - Yes

Decision tree output = AEMOCSV

Payload Worked Example: Retail Snapshot Report



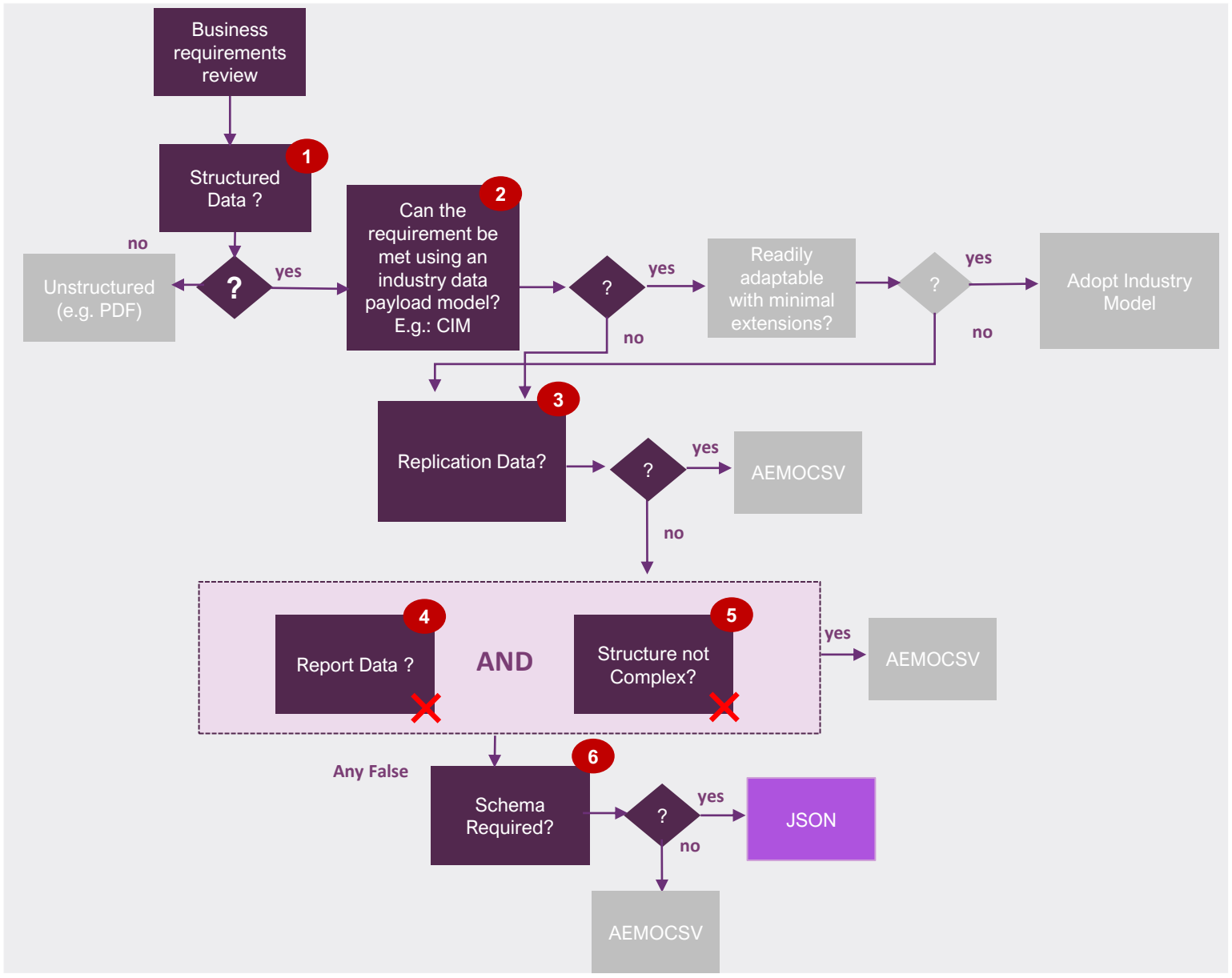
Use Case: Retail Snapshot Report

Decision tree applied criteria

1. Data output is structured? – Yes
2. Can the requirement be met using an industry data payload model? – No
3. Replication Data– No
4. Report Data – Yes
5. Structure Not Complex – No
6. Schema Required - Yes

Decision tree output = JSON

Payload Worked Example: Bidding API - submit Bids



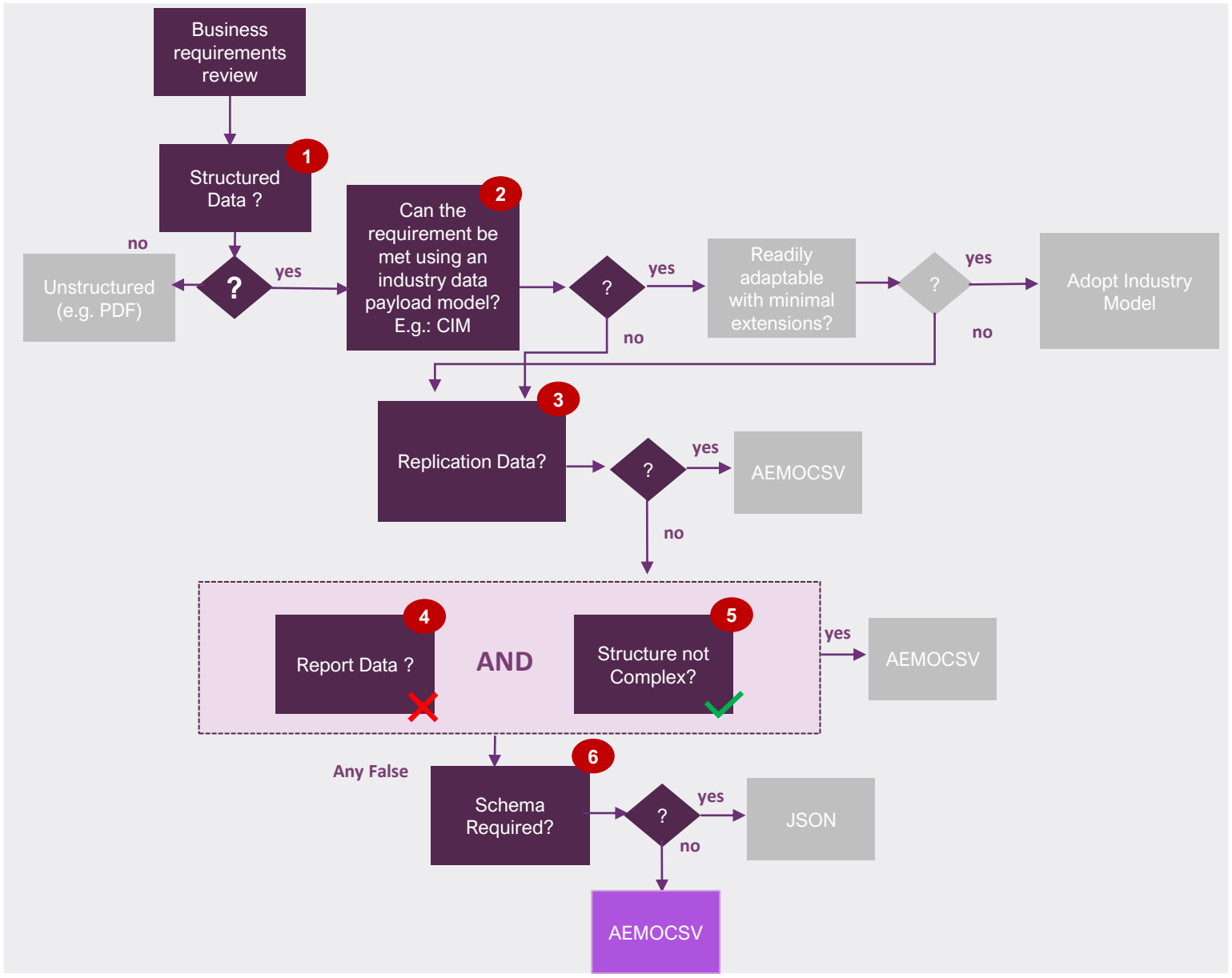
Use Case: Bidding API –Submit Bids

Decision tree applied criteria

1. Data output is structured? – Yes
2. Can the requirement be met using an industry data payload model? – No
3. Replication Data– No
4. Report Data – No
5. Structure Not Complex – No
6. Schema Required - Yes

Decision tree output = JSON

Payload Worked Example: Blind Update Tool Submission



Use Case: Blind Update Tool submission

`https://api-prd.aemo.local/NEMRetail/BlindUpdate/v1/submission`

Decision tree applied criteria

1. Data output is structured? – Yes
2. Can the requirement be met using an industry data payload model? – No
3. Replication Data– No
4. Report Data – No
5. Structure Not Complex – Yes
6. Schema Required - No

Decision tree output = AEMOCSV

Payloads and Schemas

Schema validation, versioning and transformation

Payloads and Schemas

Schema Validation	Versioning	Transformation
• Schema validation allows a check if the payload data conforms to the correct structure, reducing errors and ensures data integrity.	• Versions of schemas are created to allow for change management of schemas.	• Transformation is where a payload needs to be transformed from one schema version to another (e.g. n to n-1).
• Our approach will be to use JSON Schema validation. Where a schema has been defined for a service, all data relating to that schema will be validated.	• A proposed structure for schemas and schema versioning will be articulated in this pack.	• Our approach to transformation is proposed to change and is outlined in further slides.

Validation

Validating payloads

Validation

What is validation?

Schema Validation

Schema validation confirms a message in its entirety complies with a structural definition and can be read. Schema validation failure results in the entire message being rejected at the message level (via a message acknowledgement, MACK).

The IDX Hub (including the AEMO Gateway Software) supports schema validation.

Both JSON and aseXML support the creation of schemas to validate the expected structure and data types. CSV has no formal schema validation mechanism, although custom tools can be used to validate a CSV structure.

Business Validation

Business validation occurs at the transaction level and results in individual acceptance or rejection of each transaction (via a transaction acknowledgement).

The IDX Hub does not support business validation.

NOTE: Participants could extend the AEMO Gateway Software to support their own validations.

How we do schema validation today

Schema Type	NEM Retail and B2B	NEM Wholesale
aseXML	• Hub - AEMO validates the aseXML schema on the hub. It provides basic validation of the aseXML schema. • Participant – AEMO provides the XSD to Participants to allow them to validate inbound and outbound messages. AEMO provides validation extensions beyond XSD through the B2B Validation Module (aka EVM). This is a schema validation application embedded in participants' B2B systems allowing them to validate an XML file before it is deployed to the MSATS B2B e-Hub. Its purpose is to decrease the amount of invalid XML files sent to the MSATS B2B e-Hub. This provides in depth and service-specific schema validation, allowing for a rich-set of validation checks and errors for a particular service (e.g. Service Order Request) beyond the XML schema validation.	• Not Applicable
JSON	• Consumer Data Rights API and DER APIs are examples of JSON-based APIs with some JSON-level schema validation.	• Bidding API (NEM Dispatch Bidding) has JSON-level schema validation.
CSV	• In general, no validation is provided. As an exception, AEMO provides a custom validation of the Blind Update Tool CATS Standing data.	• No services are CSV validated

Validation Level

What validation capabilities will AEMO provide?

IDX Hub:

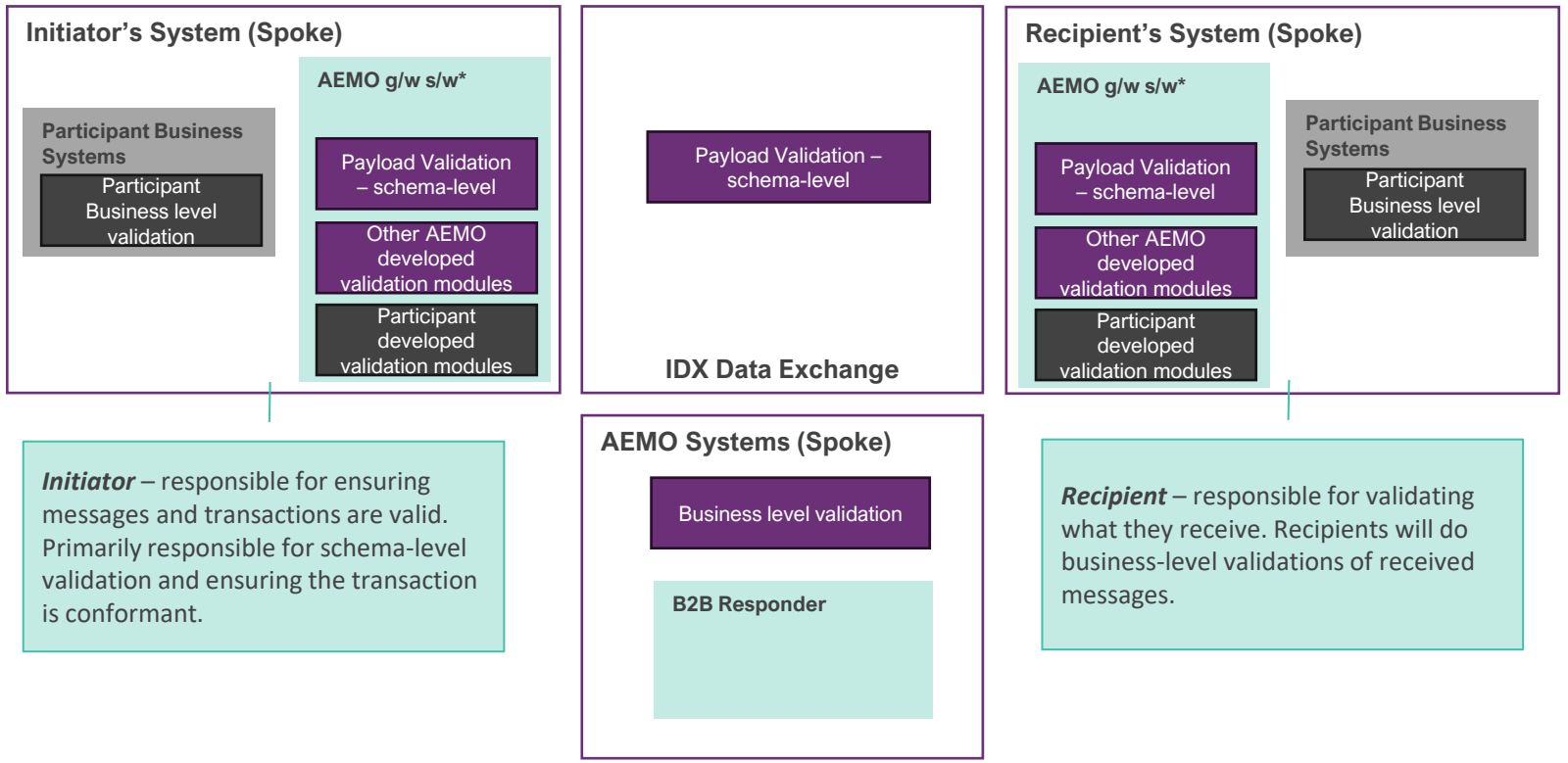
- Will be limited to schema level validation.
- Will only generate MACKs, therefore MACKs associated with schema-level validation (Hub MACK for B2B and MACK for B2M).
- **B2B Responder:**
  - The B2B Responder is a tool that simulates a participant to enable responses in B2B. This also provide schema validation.
  - On a case-by-case basis, additional transaction validations may be done for specific services above the schema level (e.g. what EVM provides today), to enable negative-transaction responses where transactions don't conform to message validity.
  - The B2B Responder will be made available via the LVI and as a validation module.

Participant Spoke:

- **Validation modules:**
  - AEMO will consider providing validation logic beyond the schema-level on a case-by-case basis. For example; if there is a wide industry need for a particular validation on a service that assists the industry.
  - Validation modules will generally only be available for structures that allow for schema-validation (e.g. JSON).
  - Participants can deploy their own validation configuration at the transaction level. (Technically possible at the message-level although no use-cases are known, typically used at the transaction-level).
  - Validation modules will be pluggable into the AEMO Gateway to allow the further extension of validation. Participants and AEMO can develop modules to be used for further validity checks.
  - Any validation module beyond schema-level will be constrained to B2B.
  - We will provide the specification for how to interact with a validation module if a participant decides to include in their own gateway.
- **AEMO Gateway Software:**
  - Can deploy validation schema to the gateway for inbound and outbound for schema validation.

IDX Hub and Spoke Validation

Validation capabilities on IDX Hub and the Spokes



IDX Elements	Description
IDX Data Exchange	The IDX Hub will provide payload validation at the schema-level and provide Hub MACK responses for B2B and MACK responses for B2M
AEMO Systems (Spoke)	AEMO systems will be considered a spoke. AEMO Systems will be acting as a Recipient spoke, and also as an Initiator for B2M. The AEMO spoke will ensure business-level validation of received payloads.
Initiator's System (Spoke)	Sender's system initiating B2M or B2B messages to the AEMO's Data Exchange Platform. Responsible for ensuring messages and transactions are valid at a schema-level and a business level.
Recipient's System (Spoke)	Recipient's system accepting B2M or B2B messages from the AEMO's Data Exchange Platform. Responsible for ensuring business-level validation.

Schema Validation Equivalency and benefits of JSON

Feature	XSD (aseXML Schema Definition)	JSON Schema
Data Types	✓	✓
Required Properties	✓	✓
Property Constraints	✓	✓
Format Validation	✓	✓
Enum	✓	✓
Pattern Constraints	✓	✓
Array Constraints	✓	✓ *
Nested Structures	✓	✓
Dependencies	✓	✓
Default and Fixed Values	✓	✓
Element Order	✓	NA
Namespace Validation	✓	✓

Are Participants comfortable with the above assessment?

The Focus group were comfortable with the above assessment. A question was raised about XPath, AEMO will investigate.

Other benefits of JSON and JSON Schemas

Simplicity and Readability
- JSON and JSON-schemas are easier for people to read than XML and XSD, which also makes them easier to write and maintain.

Parsing
- Faster and simpler with JSON.

Growing tools and support
- JSON is native to JavaScript, the most commonly-used web development language.
- Although there is great support for XML, it is an older standard and is less favoured than JSON, which has a growing list of tools and is expected to have more supportability into the future.

Data Interchange Friendly
- JSON has been designed for data interchange, ideally suited for APIs.

Native Support in OpenAPI Specifications
- Modern APIs typically use the OpenAPI Spec 3 standard for documenting APIs and how they are used. This standard natively supports JSON schema, with the ability to provide detailed examples for success and error conditions. This allows API users to understand the service and get to a quicker time-to-first-hello-world.

See Appendix – for a detailed analysis of XSD versus JSON schema validation capabilities.

* The array constraint of `<xsd:all>` is not supported in JSON schema. This is not used in any current AEMO XSD. Note: This can be achieved with similar results using `object`, `properties` and `required` fields in a JSON schema.

CSV Payload Validation

The CSV format does not have a formal schema validation mechanism like XML and JSON, however a custom solution can validate a CSV to a custom defined schema.

Today, AEMO provides CSV validation by exception. AEMO provides a Blind Update Tool through API, or the MSATS LVI, which checks the submitted CSV against a defined structure for CATS Standing Data fields.

CSV Validation is not proposed to be provided by IDX. This means that for payloads with AEMO_CSV this will not be validated by AEMO Gateway Software, or the IDX Hub.
Apart from the exception above, this conforms to today's validation principles.

Does this align with Participants expectations?

The Focus group was largely aligned, however there was a question that AEMO is investigating.

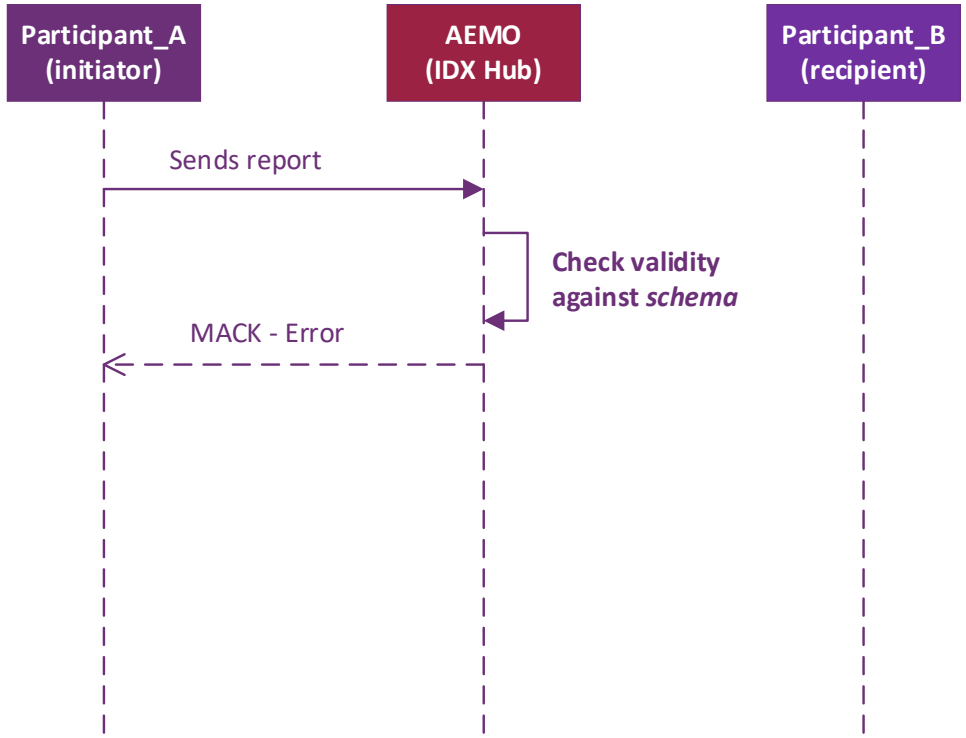
IDX Principle – CSV validation will not be done in IDX

JSON Validation against schema

AEMO will provide JSON validation of all B2M and B2B messages prior to delivery. Failure at the schema-level will result in the message being gracefully rejected. Procedural errors, handled outside of the schema, are handled differently. Below outlines how AEMO handles validation outcomes in two scenarios.

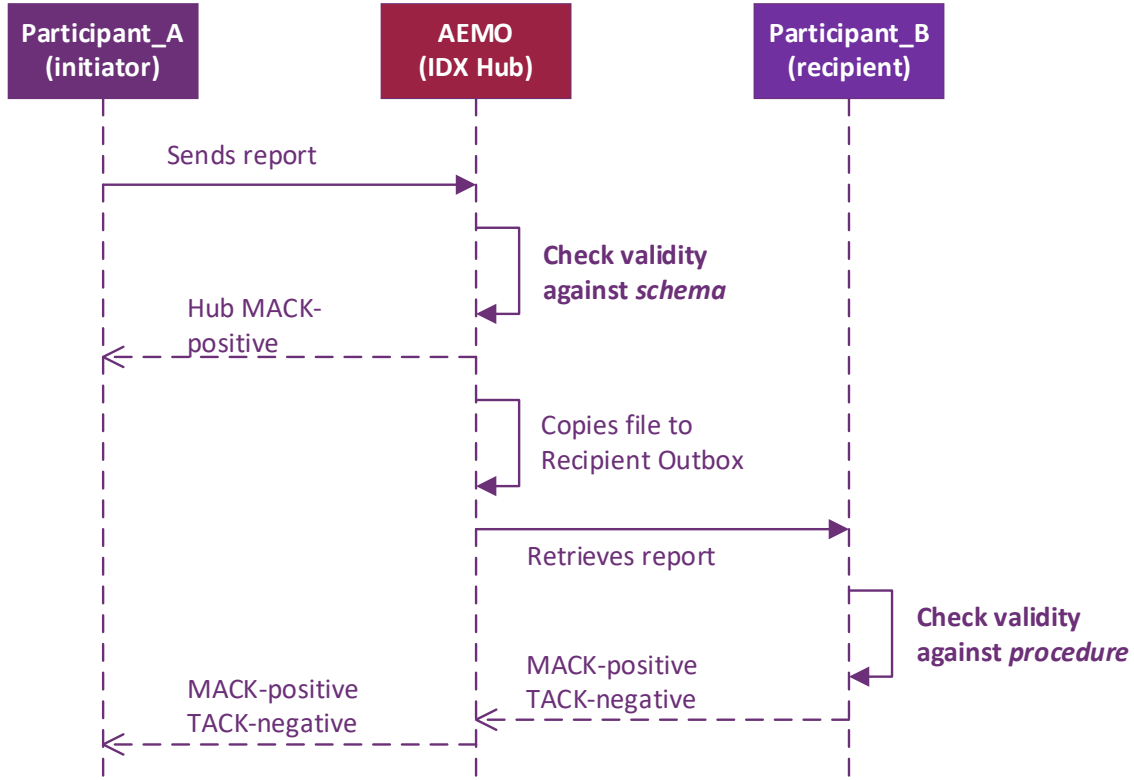
Schema errors – IDX Hub rejects via negative-MACK.

The message is schema-invalid, Participant_A will receive a negative-MACK. Participant_B would be unaware of the attempt to send an invalid payload by Participant_A.



Business errors - IDX accepts via positive-MACK, Participant_B rejects via negative-TACK.

The message is schema-valid, Participant_B will check the message, which will fail procedurally in their back-end and they generate a negative-TACK.



Versioning

As schemas are updated, new versions are required to be published

Payloads and Versioning

Recap from Business function Endpoints

Guiding Principle: A business function must only support a distinct schema for each payload type. Multiple transactions belonging to a business function and sharing the same payload type are bundled under one schema.

Market: NEM Retail
Business Function: Meter Reads (MTRD Transaction Group)
Business Function API: https://.../NEMRetail/v1/B2BMeterReads/<resource group>/<resources>
Supported functionalities required:

Use Case	API Method	API Definition	Proposed Payload Format
Send meter reads to the B2B Recipient (messages & TACKs)	POST	NEMRetail/V1/**B2BMeterReads**/transactions/meterDataNotification	AEMOCSV / MDFF
Retrieve meter reads from the B2B Sender (messages & TACKs)	GET	NEMRetail/**B2BMeterReads/**v1/transactions/meterDataNotification	AEMOCSV / MDFF
Send Provide Meter Data Request or Response (messages & TACKs)	POST	NEMRetail/**B2BMeterReads/**v1/transactions/provideMeterData	JSON
Retrieve Provide Meter Data Request or Response (messages & TACKs)	GET	NEMRetail/**B2BMeterReads/**v1/transactions/provideMeterData	JSON
Send Verify Meter Data Request or Response (messages & TACKs)	POST	NEMRetail/**B2BMeterReads/**v1/transactions/verifyMeterData	JSON
Retrieve Verify Meter Data Request or Response (messages & TACKs)	GET	NEMRetail/**B2BMeterReads/**v1/transactions/verifyMeterData	JSON

NEM_MTRD_AEMOCSV_r1

NEM_MTRD_JSON_Schema_r1

Payload Schema versioning

Versions for Schemas are mapped to the business function and payload type.

Today	Challenges with all versions	Proposed
Inbound: AEMO Supports **all** versions of the schema. Although some business transactions may get rejected if older than n-1 version Outbound: AEMO supports n and n-1 only	• Large testing cycles • Increased complexity with additional logic to handle version specific processing , validation and compatibility • Participants may be uncertain on which version to use and when to upgrade	Inbound: AEMO will **only** support n and n-1 versions, within a defined transition window. On IDX we will reject any messages that are n-2 and below. Outbound: As per today, AEMO supports n and n-1 only, within a defined transition window.

AEMO sought feedback on the proposed support for n and n-1 schemas for ***both*** inbound and outbound

The focus group discussed the proposed versioning approach, a concern was raised around only supporting n and n-1 however AEMO believes due to the business service level schemas the risk of non-beneficial (to participants) schema change is mitigated

Payload versioning - Enumerations

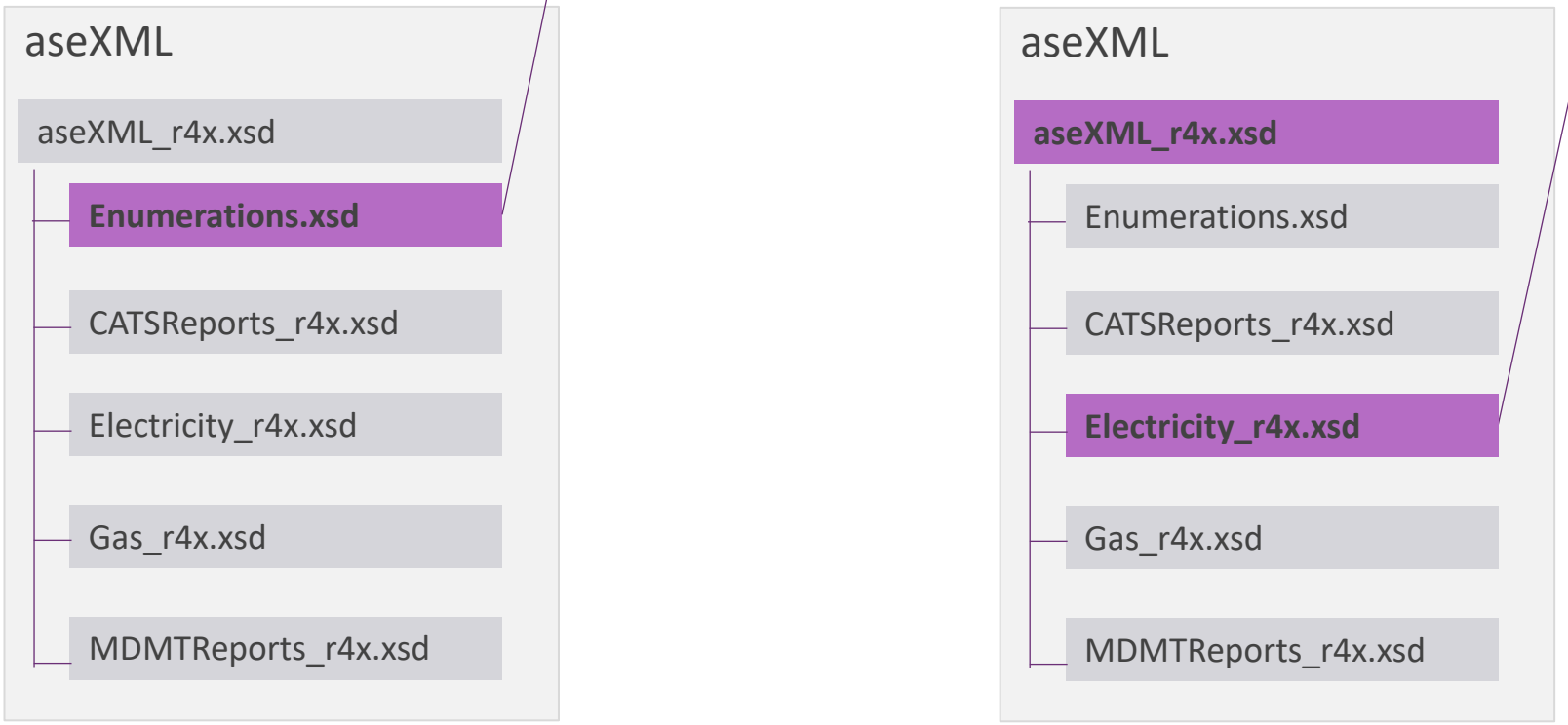
Pain Points	IDX Principle

• Today, Enumerations exist in multiple locations
  • Versioned schema files at the transaction level
  • Non versioned schema files
  • Non schema enumerations where applications enforce validations
• With an un-versioned enumeration file updates are posted to the AEMO website, but a participant's copy can get out of sync
• Updates to Enumerations in the schema forces everyone to update even if they do not use the enumerated value
	• Enumerations will be defined in AEMO provided schemas.
	• Enumerations will be defined at the schema level will be validated by the IDX Hub.
	• Enumerations specific to a business function is implemented within a business function schemas.
	• Enumerations common across multiple business functions is implemented in the common enumeration schema, which is inherited by the business function schemas.

Payload versioning – Example Today

AustralianFlatOrUnitType maxLength value change from “4” to “15”

Add a new Life Support type for Electricity



Implications:

- Entire schema is affected
- Changes are usually delayed and bundled with other schema related changes
- Functions not related to Life Support are forced to take on the new schema

Payload versioning – IDX Example

Adding a new Life Support Type for Electricity

Option 1

- CommonEnumerations.json.schema
- ServiceOrder_v1.json.schema
- CUST_v1.json.schema
- CATS_v1_.json.schema
- Gas_Change_Request_v1.json.schema
- CATS_Elec_Reports_v1.json.schema

These schemas include "CommonEnumerations.json.schema"

Option 2

- CommonEnumerations.json.schema
- ElectricityEnums.json.schema
- GasEnums.json.schema
- ServiceOrder_v1.json.schema
- CUST_v1.json.schema
- CATS_v1.json.schema
- Gas_Change_Request_v1.json.schema
- CATS_Elec_Reports_v1.json.schema

These schemas include "ElectricityEnums.json.schema"

Option 3

- ServiceOrder_**v2**.json.schema
- CUST_**v2**.json.schema
- CATS_v1_.json.schema
- Gas_Change_Request_v1.json.schema
- CATS_Elec_Reports_v1.json.schema

In this option a new schema is published for each business function affected

Legend

- Schema that is changing
- Referencing business schema that is impacted by change
- Referencing business schema that is not impacted by change
- Unaffected Schema

Payload versioning – IDX Example

Adding a new Life Support Type

Wide ⟷ Narrow

Option 1	Option 2	Option 3
• A common enumeration schema has elements that are common across multiple schemas (e.g. Addresses). An update to the common item, would update the common schema and will be referenced by the business functions that use that schema. • Enumeration schema update is too impacting on the Participants compared to other options.	• Common schemas defined outside of the business function schema that can be inherited. • There may be multiple common schemas that cover various markets, or domains, that are focussed on sets of enumerations for that domain. This reduces the blast radius of common enumeration updates. • Business function specific schemas can extend the common schema	• In this proposal, an update to common items would be updated in the schemas that have that enumeration. Everything sits in the business function schema. • There are no un-versioned schemas to manage
✕	?	?
Not Considered	**72% (8)**	27% (3)

Participants were asked to provide feedback on Options 2 and 3 through a Poll.
Option 2 was preferred with 72% (8) and Option 3 received 27% (3) of the vote.
Some Participants would like to gather some internal feedback and then respond back to AEMO.

Transformation

Supporting Participants moving from an old version to the current version

Payload Transformation – Current state

Today, Payload version is pre-nominated by Participants. Data received is transformed to the version pre-nominated. Below we explore the mechanics of how Participants pre-nominate schema versions between markets.

NEM Retail	NEM Wholesale
• Participants nominate the schema version – Latest, Current, Superseded • When a new schema is added Participants on Latest get the new schema (schema n) automatically. • Participants who were on Current become Superseded and get the n-1 schema • Participants who were previously on Superseded (n-2), remain on Superseded and now get schema n-1 • Changing of schema versions is facilitated by the MSATS browser and has a time bound transition window • Participants can only choose 1 version	• Participants nominate the schema version – Current , Legacy • Participants nominate report subscriptions via the markets portal • When a new schema is released, the version that was previously n becomes n-1. The released schema becomes n. • Previously existing n-1 is dropped off • Participants can choose to subscribe to n and n-1 concurrently and it is only for a limited time. After 5 days they are automatically unsubscribed from n-1 (unless Participants go back in, unsubscribe and resubscribe). • Changing of schema versions is facilitated by the markets portal.

Payload Transformation – Today API and FTP (NEM Retail Only)

Today's process - Pre-nomination on API and FTP
How Transformation works during a schema change

- Participants nominate the version required for both API and FTP services.
- When changing versions any files to be delivered are held in a 'parkbox'.
- Participants are required to process any transactions that were delivered prior to initiating the schema change and are timebound (currently 30 min).
- If this is exceeded, then the process resets.
- If completed, the Participant can update to the new schema.
- Files that were in the parkbox are now delivered in the schema selected by the participant.

Payload version for B2B outbound payload transformation Large file options

Principle – For Non-API channels (i.e. Large File) the Payload version will be Pre-Nominated. This is how it is done today. The transformation service is only available for payloads that can be defined in a schema.

When a Participant is trying to update to the latest schema version, there are two options:

Option 1

- During schema upgrade send both n and n-1 versions of the file.
- Participant chooses which version of file to process.
- Participants would delete both n and n-1 files after processing.

0% (0)

Option 2

- During the change window, no files are delivered. We will only send version n after the upgrade is complete and prior to upgrade n-1 files.
- The Gateway software will handle both n and n-1 file versions.

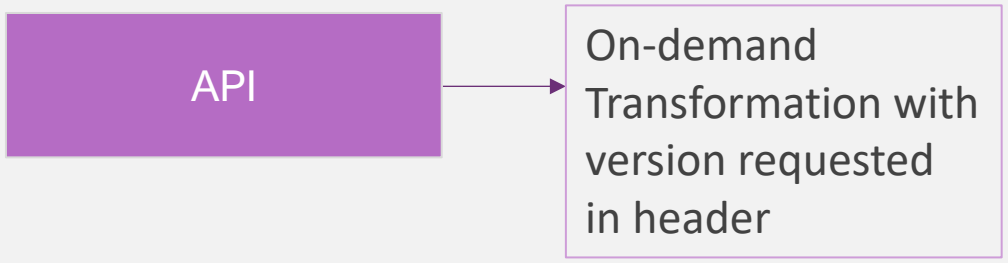
100% (10)

Participants voted in poll. 100% of Participants voted for Option 2 – where during a version change window for a particular participant, no files are delivered to that participant until the version change is complete.

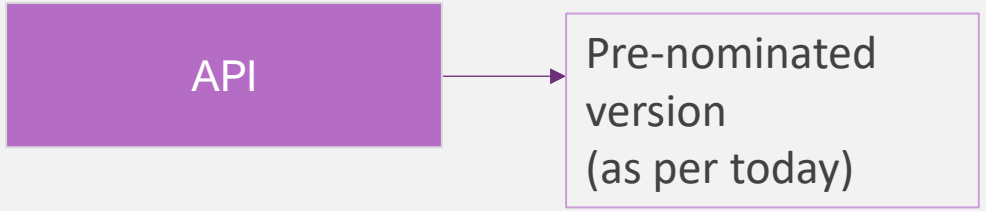
Payload Transformation – Proposed API options (outbound only)

For API there are two options on how to handle transformations

API option 1



API option 2



Benefits of On-demand

- No Park box process required
- Offers Flexibility between versions

Benefits of Pre-nominated

- Will be the same as large-file process

Issues:

- We will not deliver 2 messages. This will bring in the Park box pain-points, which will need to be resolved.

Payload Transformation - options

Channel	Option 1 : Unification	Option 2 : Mixed
API	Pre-Nominated	On-Demand
Large File	Pre-Nominated	Pre-Nominated
	50% (5)	**50% (5)**

Participants voted in a poll between having a Unified experience of Pre-Nomination between API and Large file or a Mixed Experience where API was On-Demand and Large File was Pre-Nominated. The response were evenly split with 50% favouring Unification and 50% supporting the Mixed experience.

AEMO recommends option 2 as it provides the most flexibility and control to Participants with receiving on-demand versions through API

File Naming conventions

Principle – Participants and AEMO gateways should be able to route file based content accurately by inspecting filenames alone – without the need to open the file.

Why Structure matters?

- To enable this principle a level of structure in the filename naming is required.
- It allows for routing capabilities and identification of meta data like market, version, business function, priority, etc
- This ensures operational efficiency and consistency.

Linking to non file-based transactions

- When API transactions are placed in the archive, similar naming convention will be adopted ensuring uniformity across data exchange channels.
- There will be a correlation between API and file naming (for example; in API providing a Message Context ID header, and in Large File providing the Message Context ID in the file-name.

Workshop Assumptions

- For the remainder of the workshop let's assume that essential meta data elements are included in the filename
- Details will be explored during technical specification consultation with industry.

Compression - Payload

- **Compression of payloads reduces the data size, optimising use, especially for large payloads.**
- **Compression also allows for the payload to be checked for completeness and verification using CRC32 checks**

	API	Large Files
Inbound / Outbound	**Raw JSON / Uncompressed CSV File** • No payload compression will be done on services over the API channel (however transport-level compression will be in place)	**ZIP** • All Large files will be compressed in zip as default for both inbound and outbound

Compression - Transport-level

Transport-level compression is a technique used to reduce the size of data transmitted over a network, which can improve performance by reducing bandwidth usage and transmission time. In the context of an API, compression parameters are specified in the header.

	API
Inbound	**GZIP** • Where participants POST data to AEMO, the gateway will support inbound compression if specified in the header using header type: `Content-Encoding`. • The AEMO gateway will support GZIP compression type only. • E.g.: `Content-Encoding: gzip` • Content-Encoding is optional
Outbound	**GZIP** • Where participants get data from AEMO, the gateway will support a request to specify an outbound compression type using header type: `Accept-Encoding` • The AEMO gateway will support GZIP compression type only • E.g.: `Accept-Encoding: gzip` • Weighted Accept-Encoding values is not supported • Content-Encoding is optional

Principle **–** AEMO will only accept and send with compression using ***gzip*** for inbound and outbound. Participants using API channel services will need to support this transport-level compression type. Other compression types will not be supported.

Recommendation **-** AEMO recommends to use `content-encoding` and `accept-encoding` of gzip to reduce transport bandwidth

Principle **-** Outbound delivery compression - the default will be gzip. Content-Type as gzip and Accept-Encoding as gzip.

Non-Repudiation

Ensuring the authenticity of messages

Non-Repudiation

What is non-repudiation?

Non-repudiation is where the sender of a message cannot deny the sending of a particular message by virtue of the message integrity (is intact) and the message being authenticated by the sender.

For a message to fit the definition of non-repudiation it must fulfill the following core principles.

Authentication	The identity of the parties involved, and particularly the sender of the message is known and is who they claim to be.
Integrity	The message has not been altered or tampered with in any way.
Digital Signature	A unique and unforgeable cryptographic signature that verifies the integrity of the message. The digital signature also provides proof of the sender of the message is who they claim to be.
Audit trail	A record of the transactions and communication path of the message so it's delivery can be traced end-to-end.
Timestamping	A record of the exact time the message was sent or received.

IDX Non-Repudiation Target State Principles

Principle – Universal method for all markets. The same method for non-repudiation will be used for all markets and will apply to B2B and B2M.

Principle – Non-repudiation for all services, unless by exception. Services will by default have non-repudiation.

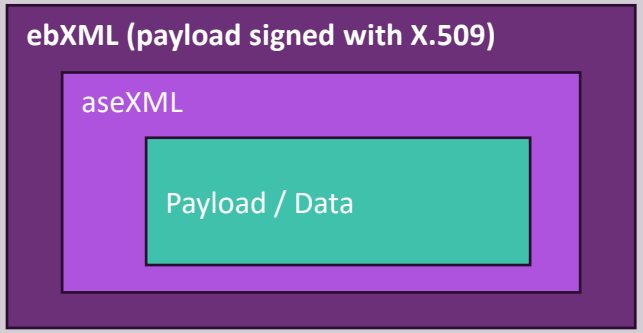
Principle – Available in M2M and LVI channels. Non-repudiation will be available in both M2M interfaces and LVI services.

Considering the above, are these principles reasonable?
Will this be achievable for smaller participants using LVI?

The Focus group identified no other options to consider

What we do today

AEMO provides minimal non-repudiation services today across the markets.

Market	Non-Repudiation Mechanism
NEM Retail	Archive files are used for non-repudiation today.
NEM Wholesale	There is no formalised non-repudiation method today.
Gas FRC Hub	Uses participant-specific TLS certificates. Payloads are signed with the participants' private key, and the participants' matching public TLS certificate is stored in the FRC Hub. The payload integrity is checked by the FRC Hub with the participants' public TLS certificate. The FRC Hub then re-signs the payload with it's FRC Hub private key. The recipient then checks the payload integrity with the FRC Hub public TLS certificate. All formal aseXML acknowledgements of messages (MACKs) are also wrapped in a signed ebXML envelope. 

Non-Repudiation and Transformation

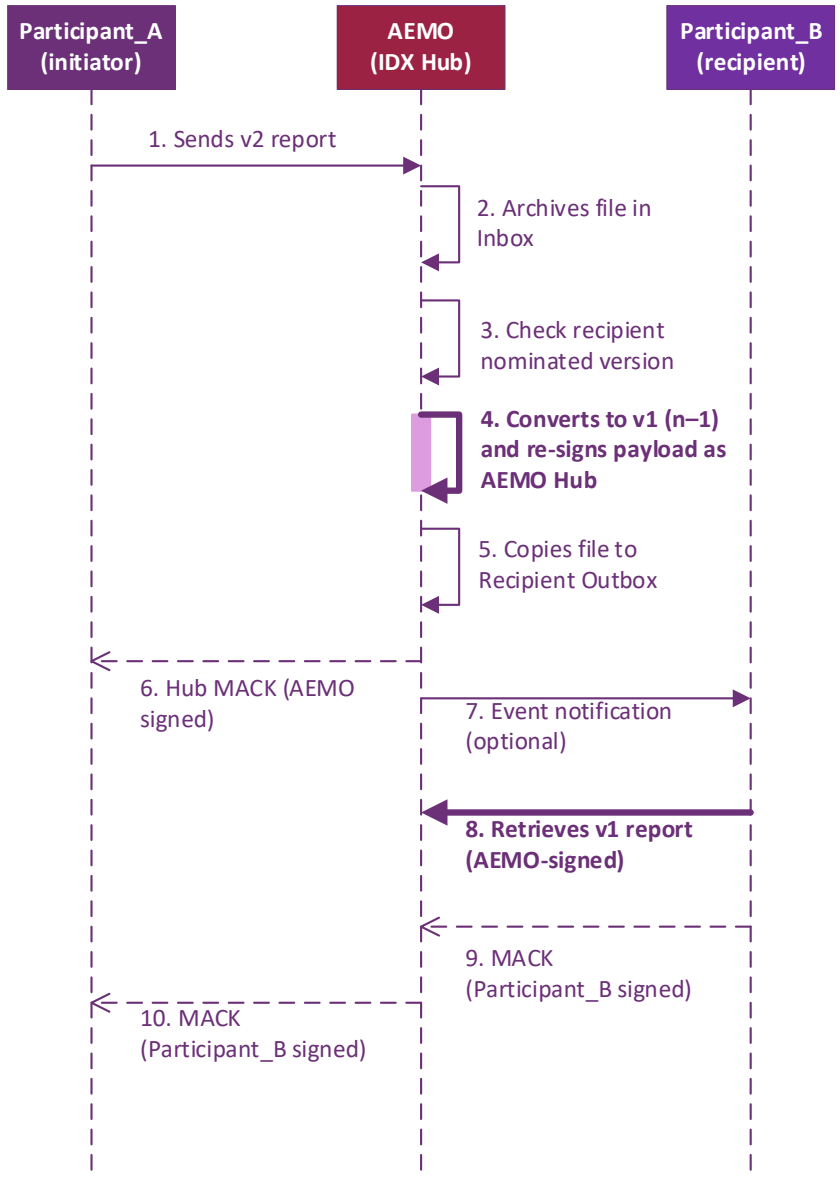
In B2B, how can we ensure non-repudiation when a payload needs to be transformed?

To support the transformation of payloads, where a transformation needs to occur for B2B messages, the original signed payload integrity must be broken.

The resulting transformed payload will be re-signed by the IDX Hub. In transformation scenarios, Participants will need to trust payloads that are signed by the IDX Hub.

This is how the Gas FRC Hub works today.

The archiving process will enable Participants to view the sender's originally-signed payload prior to transformation to verify the chain of authenticity and to provide an audit trail of the message.



Step	Description
1	Participant_A send a B2B report in v2 schema format to IDX Hub
2	IDX Hub archives the v2 report in the Inbox. This is makes available the original signed payload.
3	IDX Hub checks Participant_B nominated version, which is n-1 (a v1 report)
4	**IDX Hub converts a copy of the report to v1 schema format. In doing so this new payload must be signed by IDX (as Participant_A signature will not match the converted payload)**
5	IDX Hub copies the file to the Participant_B Outbox
6	IDX Hub sends a Hub MACK
7	IDX Hub notifies Participant_B of a new Message in their Outbox (optional, this may also be a poll method)
8	Participant_B retrieves the v1 report, signed by AEMO
9	Participant_B send a signed MACK to IDX Hub
10	Participant_A retrieves the MACK signed by Participant_B

B2B Options - Signing Payloads for non-repudiation

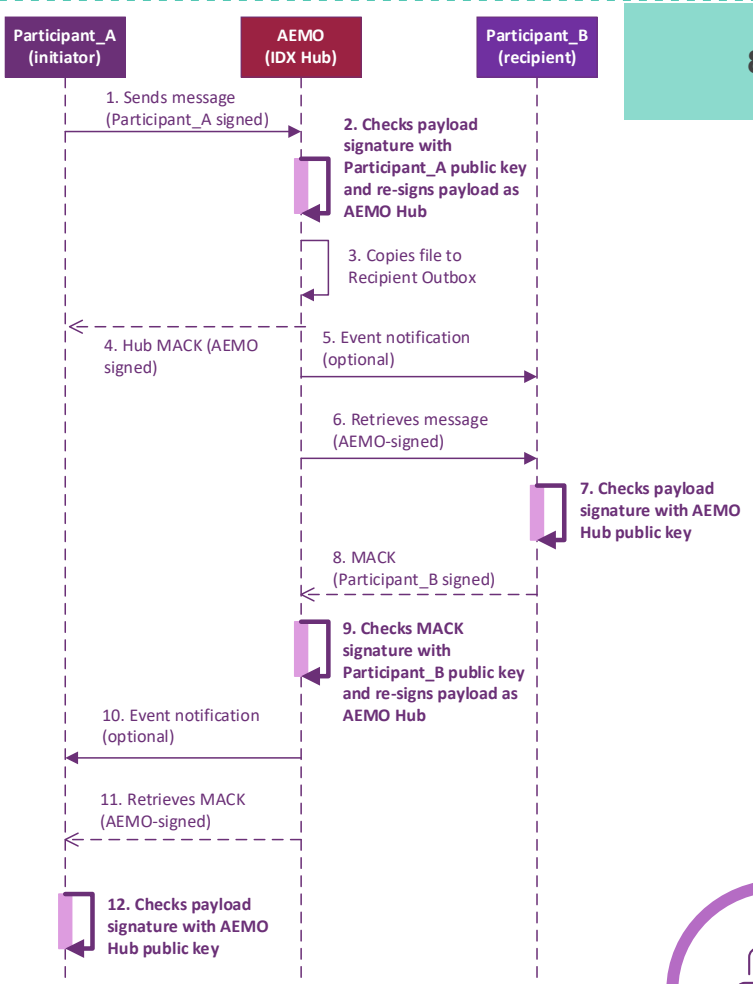
Option	Description
AEMO Hub forced re-sign **(e.g. as per today on the Gas FRC Hub)**	Today, the Gas FRC Hub process uses ebXML envelopes that contain the participants digital signature based on their FBS private key. Inside the envelope is the aseXML payload (which was signed using their private key). The participant's public FBS certificate is stored on the Hub, and is verified by the Hub before it is re-signed with the FBS Hub private key and sent to the receiving Participant. The public FBS Hub certificate can be accessed by receiving Participants to verify the aseXMl payload. The same mechanism using X.509 certificates for signing can be applied to JSON payloads.
Participant sticky signing **(using JWS Asymmetric Key)**	Like the existing Gas FRC Hub, the payload is signed by the Participant (using JWS RFC 7515), resulting in a JSON Web Signature, which is then attached to the payload. The JWS can be included in a header (e.g. *X-Payload-Signature*, or *x-jws-signature*) or in the JSON body. However, the originating signature from the Participant sending the message into the IDX Hub is intact and is only re-signed by the Hub when transformation is required. The receiving Participant checks the signature with the initiating Participant's public key.

For noting: **JWS Symmetric Key**	Requires both client and server to have a shared secret, i.e.. HMAC. This key is used to sign the payload to ensure its integrity. This is not a suitable mechanism for non-repudiation as the shared secret needs to be held by the initiator and the recipient, meaning one party cannot conclusively prove they have sent the message.

For discussion purposes - Example Flows: JWS Signing

OPTION 1: AEMO Hub Re-signs Everything

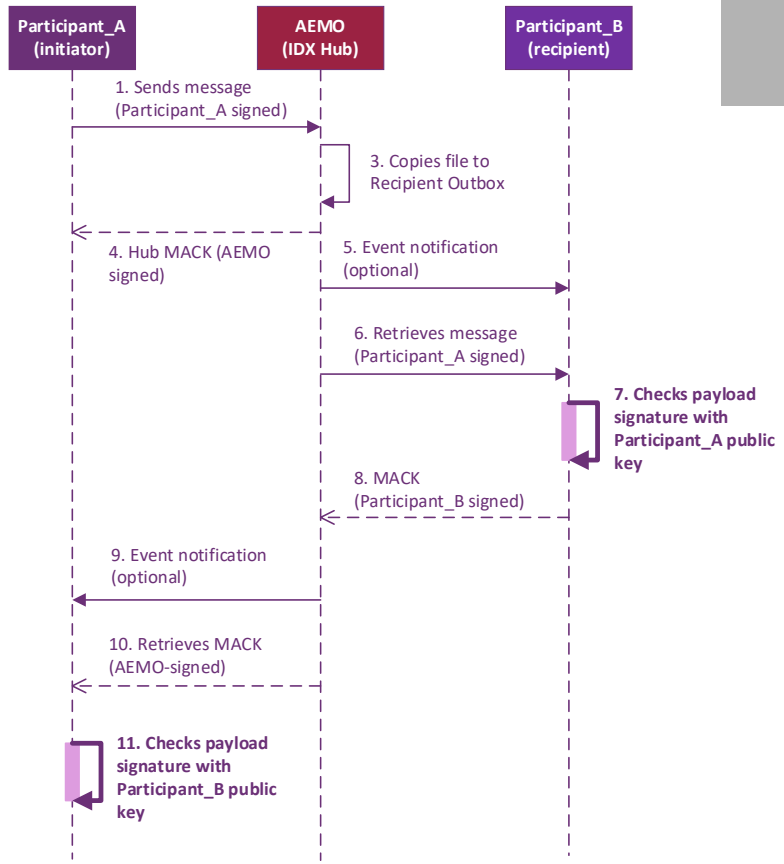
As per FRC Hub today. AEMO re-signs all payloads (regardless of those payloads needing transformation or not).



88% (8)

OPTION 2: Participant Signing Preserved

Proposed - Wherever possible, the original signed payload is preserved and delivered to the recipient as signed by the initiator.*



11% (1)

Through a poll, Participants were in favour of AEMO re-signing all payloads through the IDX Hub for non-repudiation.

API Channel - JWS Payload Signature

A JWS can be provided in an API header, or within the API body. Each option has implications.

OPTION 1: Signature in Header

Example1: using a **HTTP request header** with the signature

```
POST /api/v1/transactions HTTP/1.1
Host: example.com
Content-Type: application/json
Authorization: Bearer <access_token>
X-Payload-Signature: RSA-SHA256;BtSqbj4KuQX7Y/lz64OuSbMy8=
{
  "Transactions": {
            "Transaction": {
                        "CATSChangeRequest": {
                                    "ChangeReasonCode": "5054",
                                    "ProposedDate": "2009-03-09",
                        }
            }
  }
}
```

RECOMMENDED

Implication:

- Simple - allows API payload to be sent as Content-Type application/json or application/csv.

OPTION 2: Signature in JSON body

Example2: using signature objects in the **JSON body**

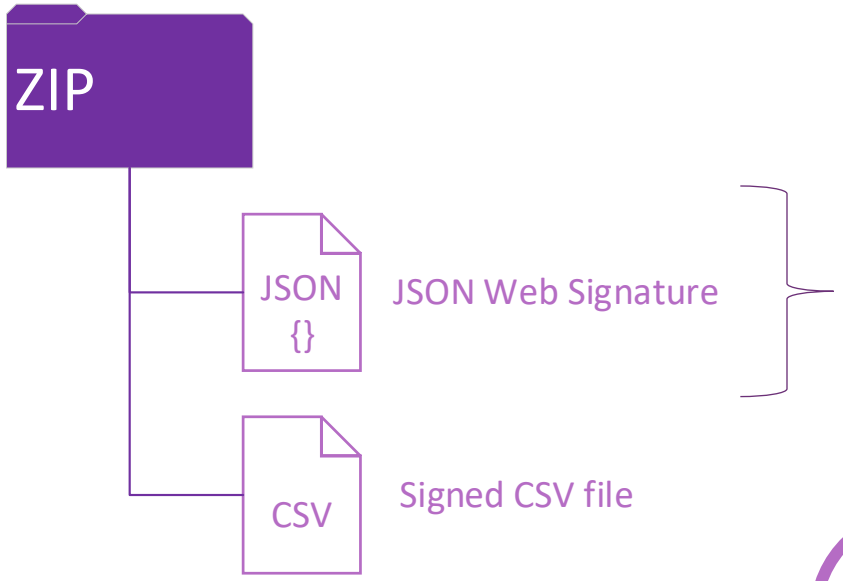
```
{
  "header": "RSA-SHA256",
  "payload": {
    "Transactions": {
            "Transaction": {
                        "CATSChangeRequest": {
                                    "ChangeReasonCode": "5054",
                                    "ProposedDate": "2009-03-09"
                        }
                        }
    }
  },
  "signature": "BtSqbj4KuQX7Y/lz64OuSbMy8="
}
```

Implication:

- More complex – Requires embedding of payload with the signature objects. For CSV, will require either base64-encoding or Content-Type multipart/form.

Large File Channel - JWS Payload Signature

Large file transfer will always be transferred as a ZIP file. AEMO proposes the signature to be added as a *signature.json* file to the ZIP, accompanying the signed payload file.



Example: signature objects in the **signature.json** file

```
{
  "header": "RSA-SHA256",
  "signature": "BtSqbj4KuQX7Y/lz64OuSbMy8="
}
```

For the non-repudiation of file transfer, are there other options we should be considering?

The Focus group identified no other options to consider

Payload Encryption- in transit and rest

- Payloads will always be encrypted in transit and at rest.
- This will apply to both API and Large File Transfer channels.
- In transit – payloads are encrypted in transit via TLS, (MTLS) with AEMO-provided certificates.
- At rest – AEMO's data stores will provide encryption of all files/payloads by default.

Notes

Selwyn and David spoke to the IDX Large File topic with lots of great questions and feedback.

AEMO requested feedback for any additional unstructured formats, but participants didn't provide any feedback.

Participants asked how AEMO is classifying payload structure as not complex and that schema is required, to which AEMO responded by saying that the schema requirement is a procedural, not technical need, focusing on whether enforceable data models add value, as in cases like blind updates where validation occurs at the endpoint, making schema enforcement less relevant. Participants also asked specifically about NEM12 and NEM13 payload formats, to which AEMO responded that industry doesn’t have the appetite to change NEM13 but NEM12 could be a candidate for AEMOCSV.

Participants enquired about the validation module and its availability to the participants, to which AEMO responded that it will be available through the LVI as well as a module. AEMO also assured that it will preserve existing useful features, like EVM capabilities, and offer higher-level validation where needed and valuable to the market, which will also be integrated into the AEMO gateway software.

AEMO acknowledged the participants feedback around version management of Unenumerated schema files and JSON not having the ability to add comments.

AEMO asked for feedback on the recommended option of having on-demand transformation for API but nomination for large file channels, but there was no objection to option 2.

Participants asked if the data which is encrypted at rest will be available to them via the markets portal and will be automatically decrypted before viewing, to which AEMO responded yes.

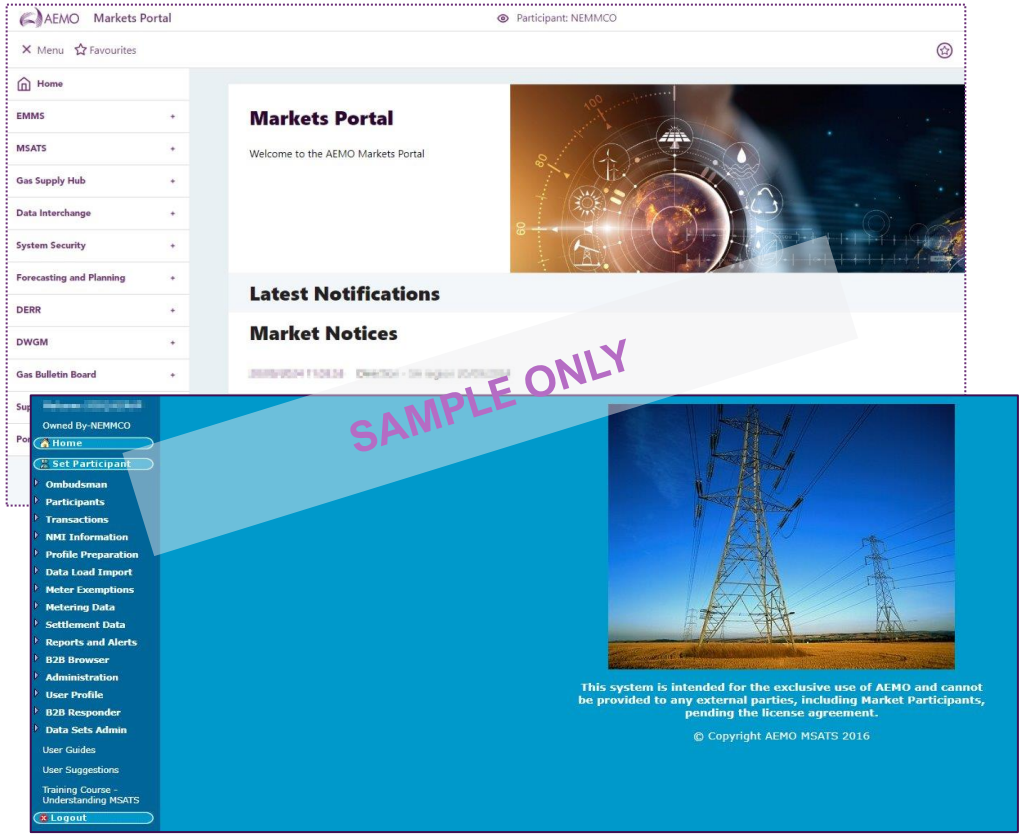
4. IDX Future Topics

IDX Working Group Session: "Low Volume Interface"

Thursday 12 December, 1:00pm – 4:00pm AEDT

Nominations closed

The objective of this working group session is to discuss capabilities to be delivered in the IDX Low Volume Interface (LVI).



The **Low Volume Interface** is a user interface mechanism to allow participant to manage aspects of data exchange without the requirement of having a system-to-system interface.

Sample business drivers for consideration in the focus group are:

- Contingency (e.g. when participant systems fail)
- Operating small business without the need for system-to-system integration
- Accreditation

Audience Skill Set

- Users of existing market interfaces to input and receive market data.
- Technical/business leads who understand the use cases for existing User Interfaces

Topics for discussion

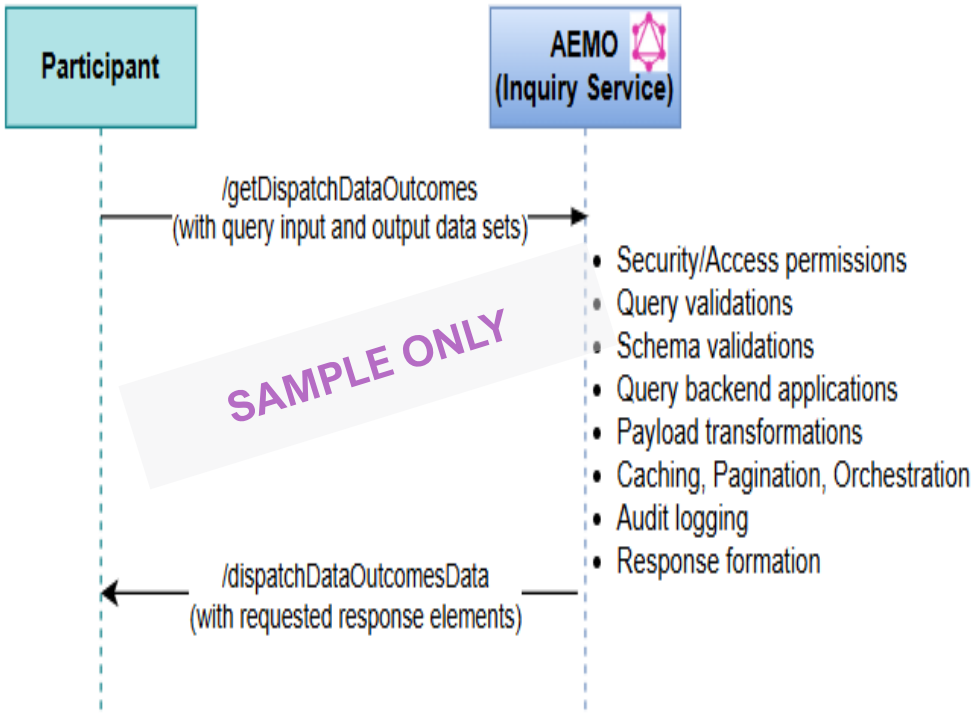
- Scope of the LVI
- Current user interface pain-points (e.g. as per the MSATS and Market Portal interfaces today)
- Capabilities required by the LVI e.g.:
  - Dashboards
  - Create, view and acknowledge transactions
  - Reports, analytics and insights.

This focus group discussion will be relevant to all stakeholders who participate in exchanging data between AEMO and energy stakeholders via user interfaces

IDX Focus Group Session: "Inquiry Service"

Friday 31 January, 2025, 1:00pm – 4:00pm AEDT

The objective of this focus group session is to discuss capabilities to be delivered in the IDX Inquiry Service.



This focus group discussion will be relevant to all stakeholders who participate in exchanging data between AEMO and energy stakeholders via user interfaces

The **Inquiry Service** uses a query language framework for APIs, such as GraphQL, enables clients only retrieve data they are interested in, removing the dependencies on new data introduced.

Sample business drivers for consideration in the focus group are:

- The capability for clients to define the structure of their response by customising the request query.
- To addresses over-fetching challenges where a large dataset is returned by an API, but only a subset of the fields may be of interests to the client.

Audience Skill Set

- Technical Leads
- Integration Architecture Teams (Market Interface Specific)

Topics for discussion

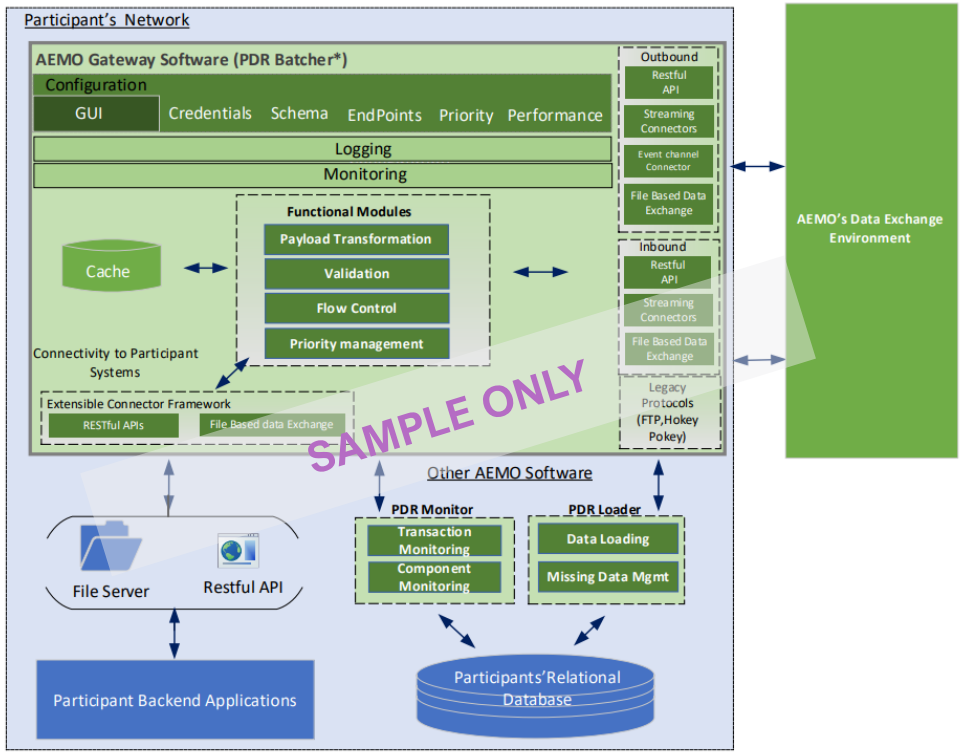
- Demonstrate current use case(s) that require the over fetching of data.
- A draft end to end business use case for Inquiry Service flow.
- Sequence diagram demonstrating the Inquiry Service to support the end-to-end business case.
- Interface requirements for implementing the Inquiry Service.
- Discuss on the Proof-of-concept outcomes.

IDX Focus Group Session: AEMO Gateway Software

Friday 14th February – Time TBC

Nominations closed

The objective of this focus group session is to discuss capabilities to be delivered by the AEMO Gateway Software, which is proposed to combine the Participant Batcher, pdrBatcher capabilities and is extended to support the target state AEMO IDX Environment.



This focus group discussion will be relevant to all stakeholders who currently use pdrBatcher, and participants who may look to use AEMO Gateway Software to integrate with services transitioned to the new IDX platform.

The **AEMO Gateway Software** will be participant-side software, developed by AEMO, to allow participants to easily interface with new services on the IDX platform. Primarily the AEMO Gateway Software will offer the same services as pdrBatcher does today and allow the translation of existing integration to the new IDX patterns.

Sample business drivers for consideration in the focus group are:

- As part of transition, reduce or remove the need for participants to "recode" their integrations to AEMOs new IDX patterns.
- Support participants using the existing pdrBatcher software.
- Allow 3rd party integrators a cost-effective mechanism to integrate their applications into IDX.

Audience Skill Set

- Technical leads from participants using pdrBatcher.
- Technical/business leads who wish to use existing integration patterns during transition.

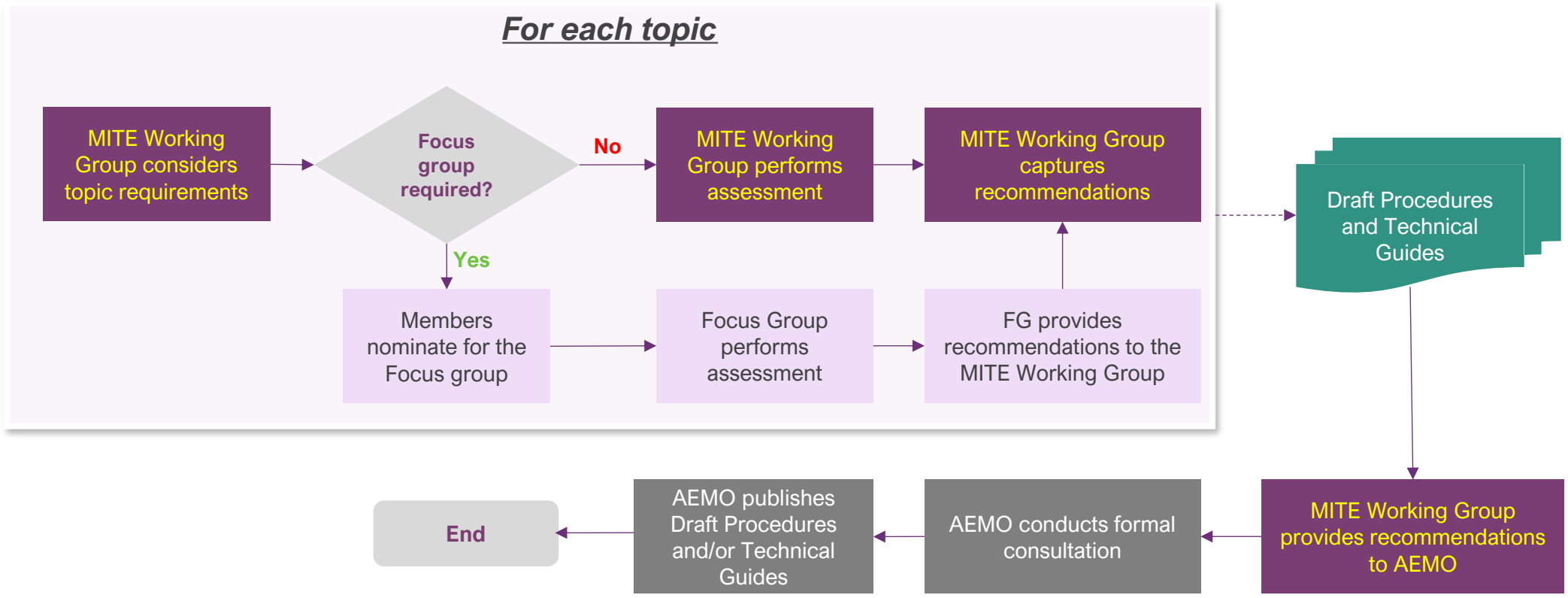
Topics for discussion

- Scope of the AEMO Gateway Software
- Existing pdrBatcher features
- Capabilities required by the AEMO Gateway Software e.g.:
  - Connectivity and integration services
  - Data handling and Transformation
  - Flow and priority management
  - Configuration and monitoring
  - Logging and error management

5. Forward Plan

Blaine Miner

Consultation Workshop Structure



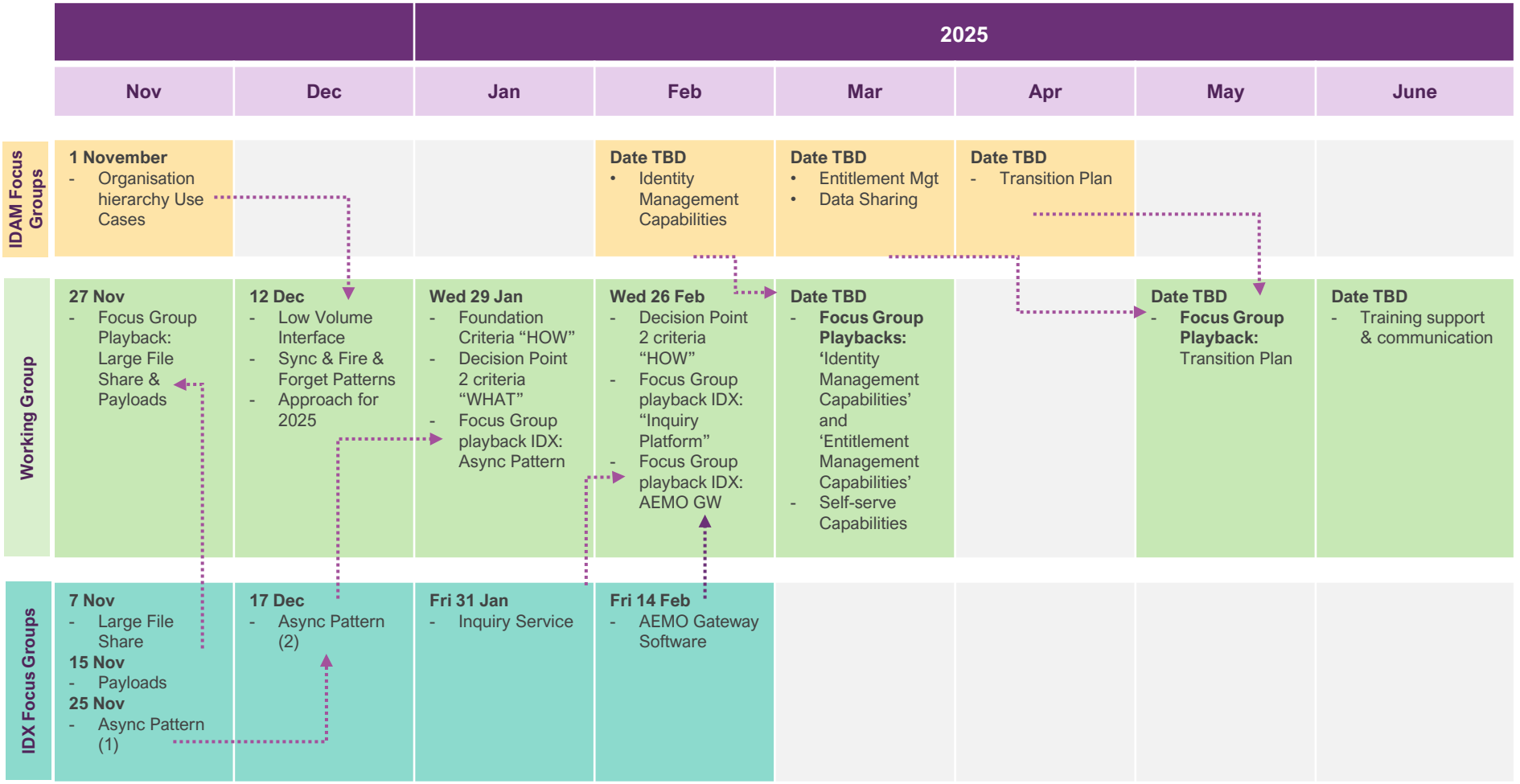
MITE Working Group

- **Actively participate** in highly technical workshop discussions to assess options, co-design draft deliverables.
- **Review key drafts** of documentation prepared by the Focus Group.
- **Consult** internally within own organisation to test, socialise and ultimately champion.

Focus Group (as required)

- **Co-design** draft deliverables for consultation with working group members
- **Actively participate** in the Focus Group workshops and activities
- **Participate** in **highly technical discussions**, including engaging within their business prior, to provide detailed responses to matters under discussion
- **Champion** technical discussions with their peers and within own organisations

Indicative Timeline for Upcoming Sessions
(as at Fri 15 Nov 2024)



- ***Fri 15 Nov updates:***
  - ***'Async and Event Notifications':***
    - *This topic has been determined to be too complex for a single session, therefore, a second session has been proposed for 17 Dec 2024.*
  - ***'AEMO Gateway Software':***
    - *This FG is being deferred to Fri 14 Feb 2025 to allow for the second session of the 'Async and Event Notifications' FG.*
  - ***'Low Volume Interface':***
    - *This FG is not proceeding as AEMO believes it can be presented directly to the working group on 12 Dec 2024.*
  - ***'Large File Share' and 'Payloads'** will now be the focus of the MITE WG on 27 November.*

6. General Business and Next Steps

NEMReform@aemo.com.au

General Business and Next Steps

MITE Working Group Forward Plan

Stream	Content	Timing

IDX	**IDX**
	• Focus Group Playbacks:
	  • Large File Share
	  • Payloads
		27 November

IDAM and IDX	• Focus Group Playbacks:
	  • IDX - Async and Event Notifications
	  • IDAM - Organisation hierarchy
	IDX
	• Sync and Fire & Forget Patterns
	• Low Volume Interface
	• Approach for 2025
		12 December

IDX	• Focus Group Playbacks: • IDX - Async and Event Notifications **IDX** • Foundation Criteria – "HOW" discussion & AEMO proposals • Decision Point 2 Criteria – "WHAT" discussion	**29 January '25**

Focus Group Forward Plan

Stream	Topic	Timing
IDX	Asynchronous Pattern Focus Group – Session 1	**25 November**
IDX	Asynchronous Pattern Focus Group – Session 2	**17 December**
IDX	Inquiry Service	**31 January '25**
IDX	AEMO Gateway Software	**14 February '25**

AEMO | Market Interface Technology Enhancements

For more information visit

aemo.com.au

Appendix A

AEMO Competition Law - Meeting Protocol

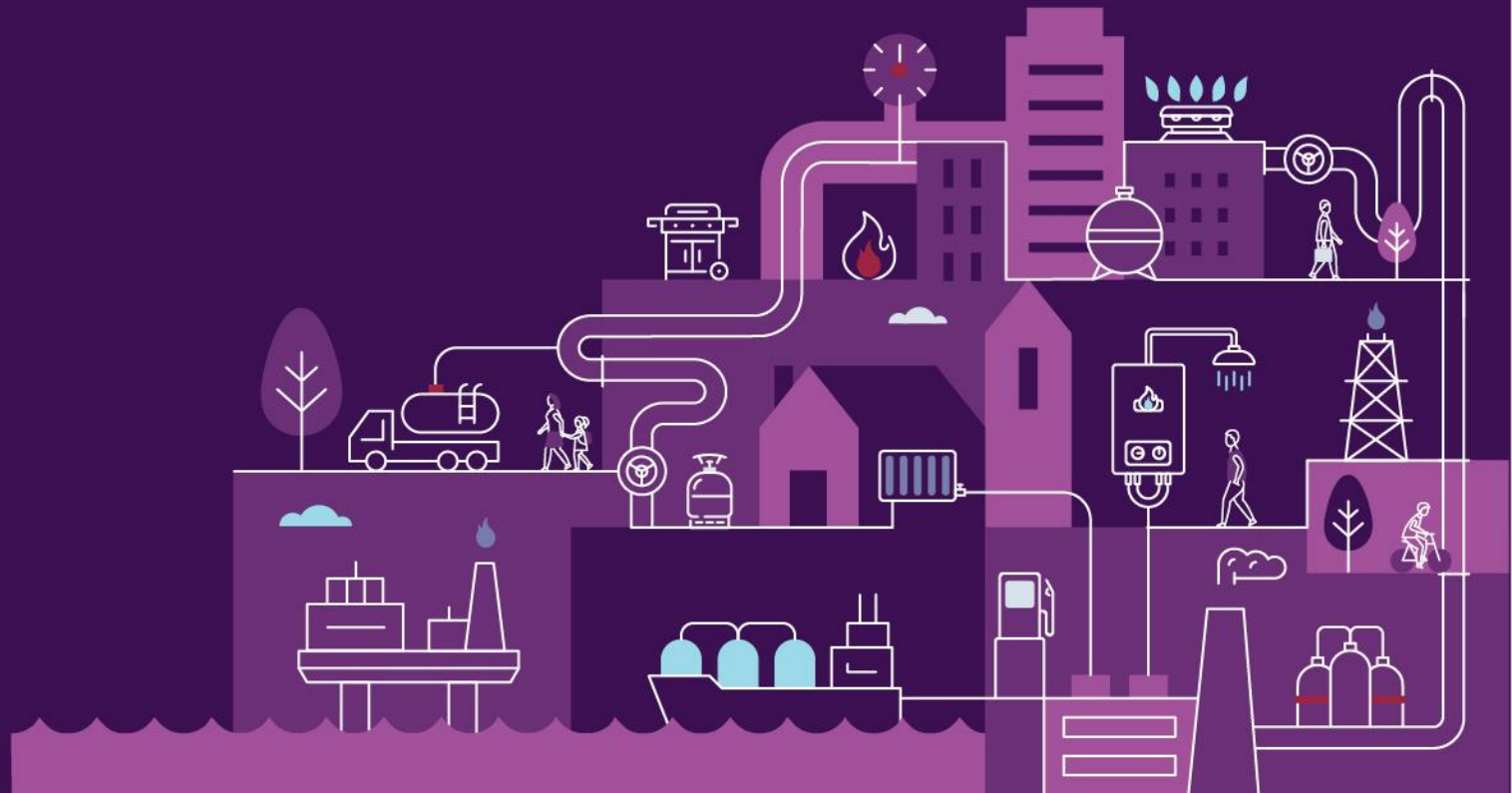
AEMO Competition Law Meeting Protocol

AEMO is committed to complying with all applicable laws, including the Competition and Consumer Act 2010 (CCA). In any dealings with AEMO, all participants agree to adhere to the CCA at all times and to comply with appropriate protocols where required to do so.

AEMO has developed meeting protocols to support compliance with the CCA in working groups and other forums with energy stakeholders. Before attending, participants should confirm the application of the appropriate meeting protocol.

To access the full protocol at AEMO's website, visit: https://aemo.com.au/en/consultations/industry-forums-and-working-groups

IDAM FG Session Outlines



Organisation Hierarchies and Enhanced Data Sharing

The objective of this focus group meeting is to thoroughly explore the technical capabilities introduced as part of the new Organisation Hierarchy and Enhanced Data Sharing Capabilities.

In the target state for Entitlements Management AEMO proposed a new set of capabilities known as Organisation Hierarchy and Enhanced Data Sharing, which will enable participants to more accurately model their corporate group structures within AEMO systems. These capabilities will facilitate the management of complex data sharing and user entitlements scenarios in a structured manner, including those involving third-party service providers.

The focus group will discuss the application flows and would seek inputs on design decisions regarding the Organisational Hierarchies and Data Sharing Framework.

Audience Skill Set for Focus Group Discussion

- Business leads who coordinate multiple PIDs arrangements
- Service Provider leads who support data sharing configurations
- Technical leads / Architects supporting multiple PID solutions and data sharing solutions

Topics for discussion

- New and enhanced Entitlements Management capabilities due to the Organisation Hierarchies
- Enhanced Data Sharing Framework.

Note: This focus group discussion will be relevant to the organisations with multiple participants Ids and all stakeholders who leverage data sharing capabilities.