Target State discussion

- Industry Data Exchange (IDX)
- Identity Access Management (IDAM)
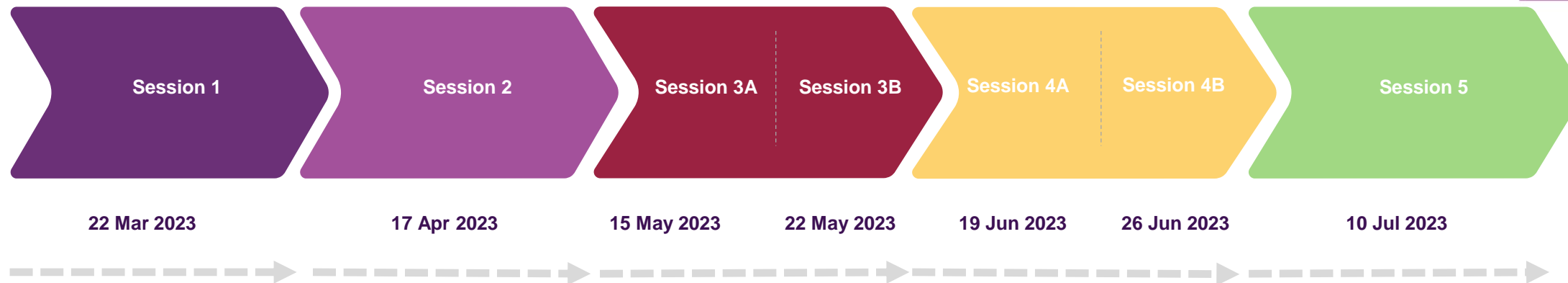- Portal Consolidation (PC)

15 May 2023

1. Introduction

We acknowledge the Traditional Owners of country throughout Australia and recognise their continuing connection to land, waters and culture.

We pay respect to their Elders past and present.

Industry Consultation

	Session 1	Session 2	Session 3A	Session 3B	Session 4A	Session 4B	Session 5
	22 Mar 2023	17 Apr 2023	15 May 2023	22 May 2023	19 Jun 2023	26 Jun 2023	10 Jul 2023

Session	Introduction – IDX, IDAM & PC	Discovery Workshops – IDAM and PC	Target State Discussion	Transition Strategy	Conclusions and Business Case
Agenda*	• Introduce initiatives • Outline workshop plan	• Pain points and benefits • Survey	• Concept walkthrough	• Transition Strategy • Impacts & Benefits	• Summary • Options
Audience	👥	🔦 🔦	🔦 🔦	🔦 🔦	👥

Legend: 🔦 Business Focus Group   🔦 Technical Focus Group   👥 All interested stakeholders who nominated to Focus Groups

Objective of today's session

Agree in principle an Industry and AEMO aligned position on key principles and concepts to define Target State for Foundational and Strategic initiatives that:
- Supports existing services while providing flexibility to support future services
- Addresses key pain points workshopped with participants

To this end, this workshop aims to:

- Present AEMO's thinking on candidate target state
- Seek input and guidance from Focus Group members

- Identify key inputs for transition principles and roadmap
- Identify further inputs into benefits and impacts

- Confirm updates and or outstanding elements for Target State
- Validate in principle alignment across industry

Agenda

#	Time	Topic	Presenter
1	9:30am – 10:00am	**Introduction** • Consultation recap • Objectives & agenda	Andrew Bell (AEMO)
		Vision for Strategic & Foundational initiatives	Gordon Dunsford, EGM Digital (AEMO)
2	10:00am – 12:15pm	**Proposed Target State – Industry Data Exchange** • IDX foundation • IDX Target State concepts • Conceptual Target State & Potential Flows • Next steps	Satheesh Kumar, Sri Gundu, Simon Tu (AEMO)
	12:15pm – 1:30pm	**Lunch**	
3	1:30pm – 3:30pm	**Proposed Target State – Identity & Access Mgmt** • IDAM foundation • Conceptual Target State • Example workflows • Next steps	Satheesh Kumar, Phil Hayes, Sivaraj Ganesan (AEMO)
	3:30pm – 3:45pm	**Afternoon Tea**	
4	3:45pm – 4:15pm	**Proposed Target State – Portal Consolidation** • PC foundation • Conceptual Target State • Next steps	Phil Hayes, Ben Friebel (AEMO)
5	4:15pm – 4:45pm	**Summary & close** • Ask of the Focus Group • Proposed actions	Andrew Bell (AEMO)

Supporting materials:
• Appendix A: Competition law meeting protocol
• Appendix B: Indicative workshop schedule
• Appendix C: IDX proposed principles summary
• Appendix D: IDAM example workflows for the Conceptual Target Solution

2. Proposed Target State

Industry Data Exchange

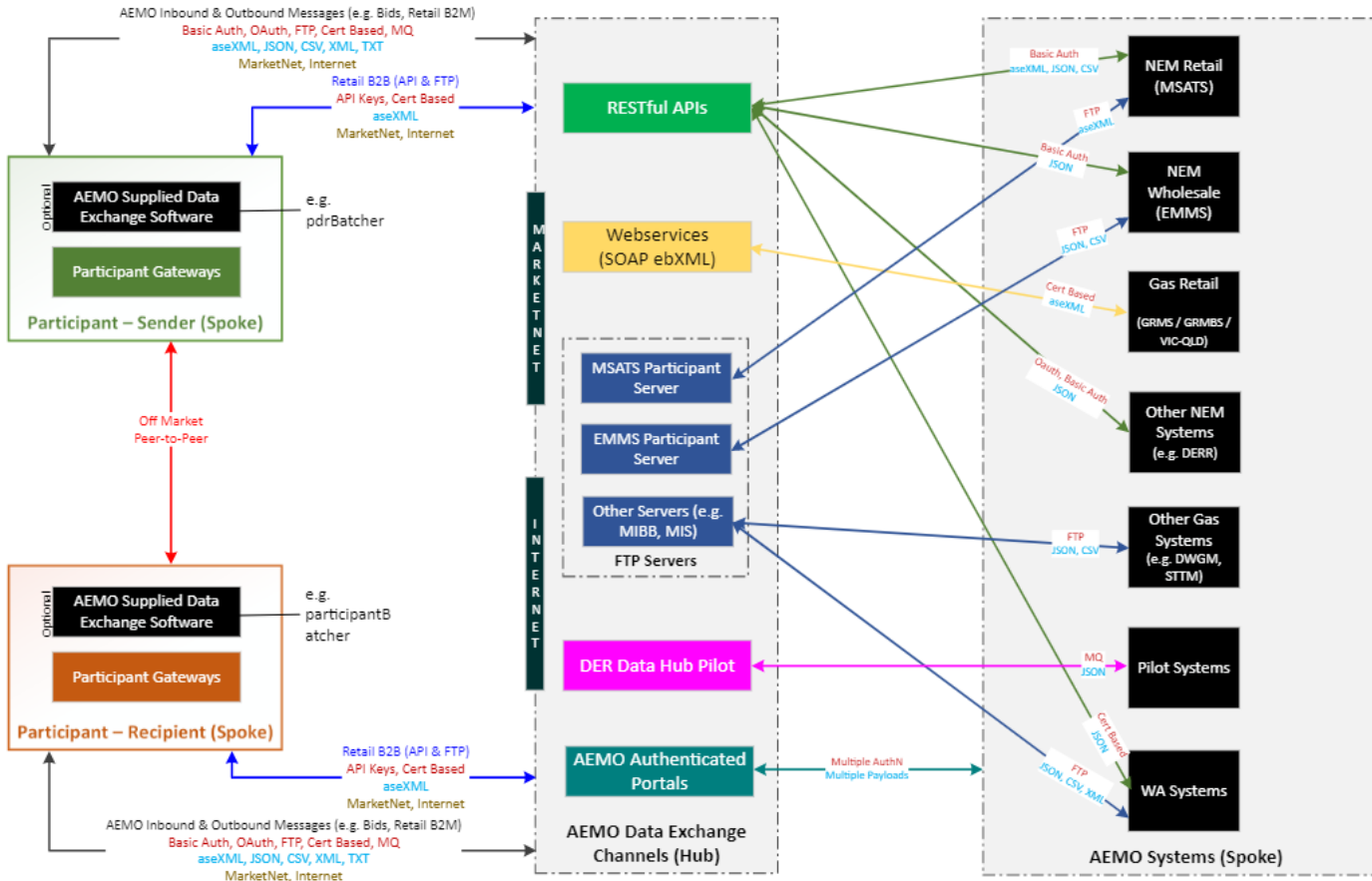# Industry Data Exchange foundation

- Scope
- IDX 2021 workshops summary
- Objectives
- Concepts

Industry Data Exchange (IDX) Scope

Industry Data Exchange: A unified data exchange mechanism to support exchanging data between energy stakeholders and AEMO.

Background: AEMO's existing data exchange systems have been variously acquired over the last 10-15 years, and use inconsistent standards, protocols and formats. AEMO's markets are also undergoing significant transformation, resulting in new data exchange needs. AEMO is introducing new data exchange patterns without a target state and roadmap which is inhibiting participants from modernising their systems and quantifying the benefits of their investments.
This Initiative will conceptualise unified data exchange standards, patterns, protocols, payload formats and channels to support market and domain-agnostic, streamlined, secure, reliable, scalable centralised data exchange platform.

IDX Context Diagram:

Following areas will be explored during the IDX feasibility phase.

In Scope	Out of Scope
✓ Data Exchange between AEMO and energy stakeholders across NEM, WEM and Gas	✗ Control systems communications and interactions
• Inbound and Outbound transactions	✗ Direct device communications and interactions
• Connectivity methods	
• Protocols to connect to AEMO systems	
• Payload formats	
• AEMO data exchange systems that Participants connect to	
• Data exchange standards & patterns	
✓ Interactions via all supported channels (current & future)	

Note: Data Exchange Scenarios, Channels, Protocols & Patterns illustrated in this slide are indicative only and not the finite list

IDX 2021 Workshop Summary

Methodology:

- Discovery workshops: 19 responses from 27 organisations attended an IDX workshop on 24 March 2021.
- 100% response in a Post-workshop survey in March 2021 with complete support for AEMO to initiate an IDX Project Discovery phase, including:
    - Investigate the costs and benefits of uplifting our current NEM market-facing systems.
    - Definition of a data exchange roadmap (target & transition states).
    - Investigation of the costs and benefits of introducing alternative data exchange.
    - Mechanisms for current & future Markets.
- Below is a summary of the key pain points from Business and Technical focus group discussions, classified into themes according to the challenges they pose to IDX services.

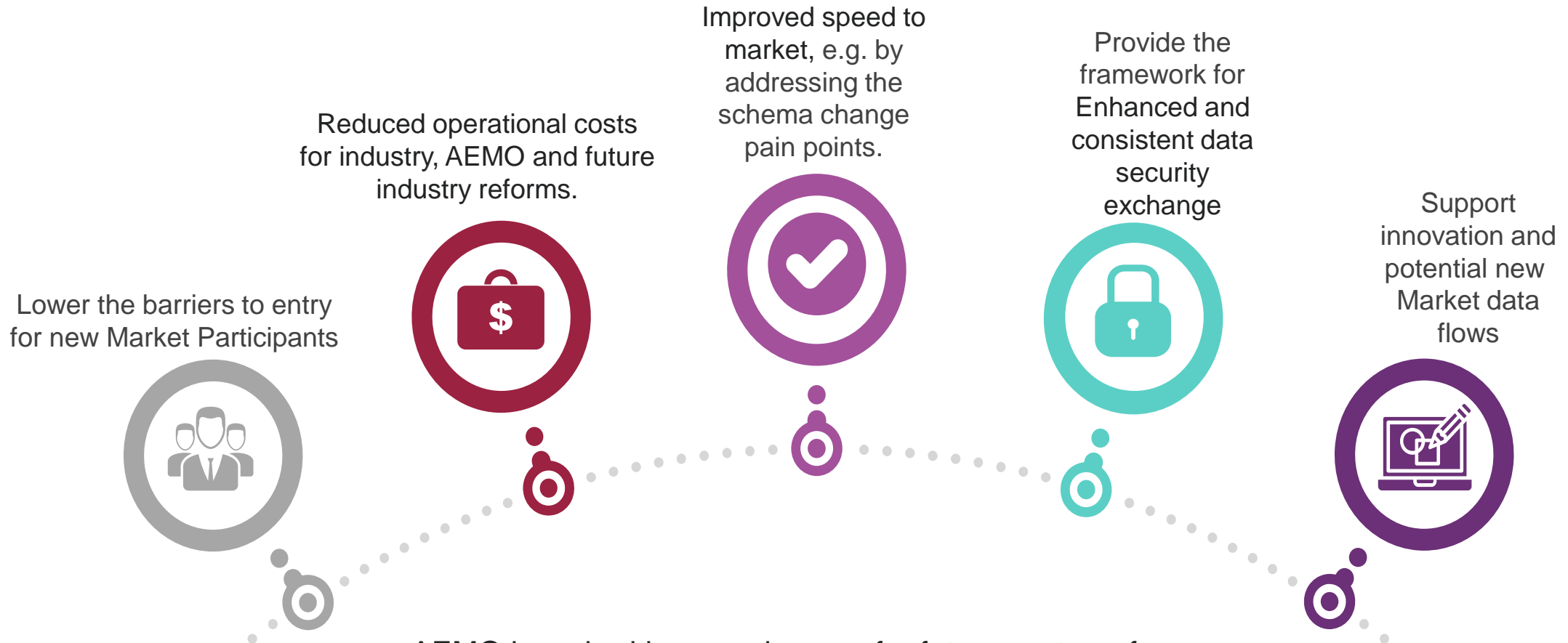| Complexity and inconsistency	• Protocols, formats and standards are inconsistent and unnecessarily convoluted. • Lack of consistent standards across Systems / Fuels / Jurisdictions
Define Roadmap	• There is no clear data exchange roadmap for future capabilities. • Legacy exchange methodologies & need for data exchange roadmap definitions (target & transition state)
Manage Cost-Effective Change	• Provide cost effective centralised services to reduce industry cost • Mandatory schema updates are costly, aseXML schema version change mandates industry to upgrade the aseXML schema even if the Participants do not have any procedural impact to the changes.
Opportunities in the Future	• Near real-time visibility of critical market transactions. • Enhanced security for data exchange and centralised access management. • Improved speed to market of business and regulatory changes. • Improved management of higher volumes of market data. • Improve developer experience. • Harmonised data exchanges between participants and AEMO market systems • Improved customer outcomes. • Better transparency of future maintenance costs for data exchange systems • Unified data exchange standards across markets, fuels and jurisdictions.
For AEMO to consider	• Event-based solution - Markets using AEMO-provided integrated data model (NEM) incur less cost than those not using (Gas or WEM). • Alternate data consumption pattern - Consumption of queryable & interoperable data in a simple & standard way. • B2M and B2B systems integrated to provide operational and industry efficiency, reducing resources, time and cost involved in delivering the service.

IDX Objectives

Lower the barriers to entry for new Market Participants

Reduced operational costs for industry, AEMO and future industry reforms.

Improved speed to market, e.g. by addressing the schema change pain points.

Provide the framework for Enhanced and consistent data security exchange

Support innovation and potential new Market data flows

AEMO is embarking on a journey for future sector reforms, which will entail the introduction of new integration channels, patterns, protocols and payload formats to simplify and uplift the way data is exchanged between Market Participants and AEMO

IDX Concepts

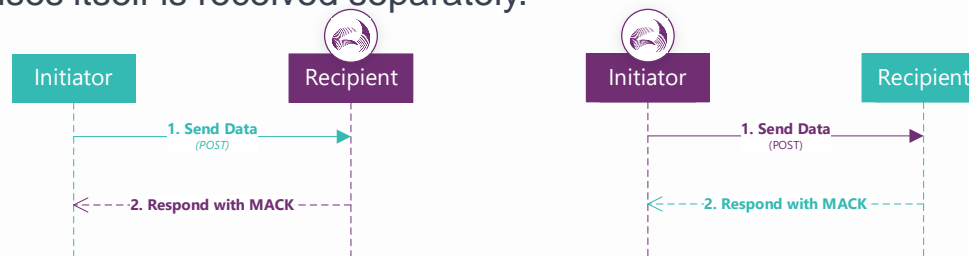**Inbound:** From the standpoint of AEMO, AEMO is the data recipient

Initiator → Recipient
1. Send Data *(POST)*
2. Respond with MACK
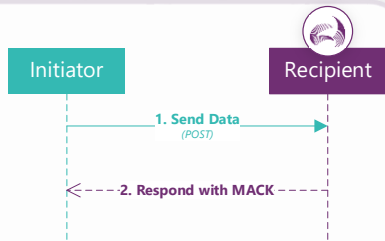
Outbound: From the perspective of AEMO, AEMO is Responsible for delivering the data to a recipient.

Initiator → Recipient
1. Send Data *(POST)*
2. Respond with MACK
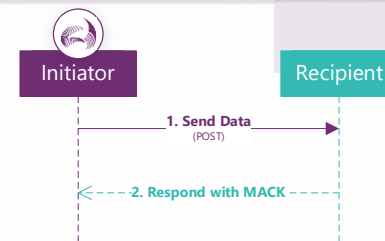
Synchronous data exchange involves real-time, sequentially ordered market workflows. Stakeholders sending a request must await the response from the corresponding stakeholder before proceeding. Responses, provided instantaneously within the same thread, include technical and business validation as well as Business data.

Initiator → Recipient
1. Send Data *(POST)*
2. Respond with Business Data
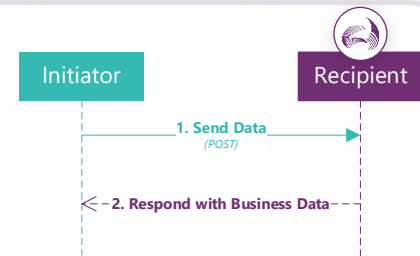
Asynchronous data exchange enables stakeholders to perform tasks independently without a specific sequence in Procedural and non-procedural business functions. While immediate technical validation may occur within the same thread, the result of business validation and the business responses itself is received separately.

Initiator → Recipient
1. Send Data *(POST)*
2. Respond with MACK

Initiator → Recipient
1. Send Data *(POST)*
2. Respond with MACK

Fire and Forget data exchange occurs in non-regulated workflows where the initiator sends a message without expecting a detailed response from the recipient. Technically, a simple acknowledgement (e.g., 200 OK) is received, but no validation details are provided.

Initiator → Recipient
1. Send Data *(POST / Publish)*
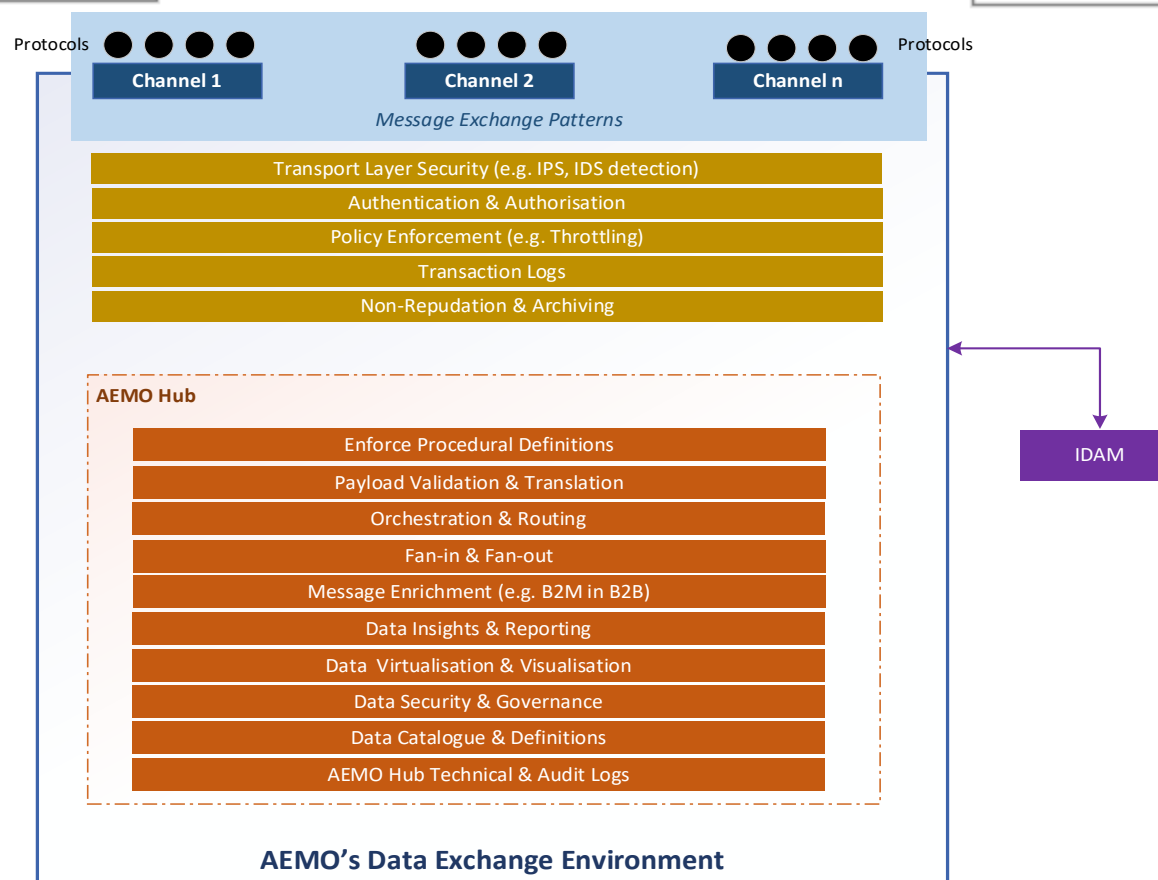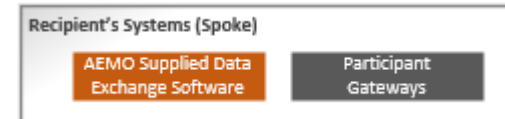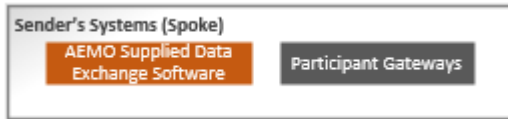1. Send Data *(POST / Publish)*
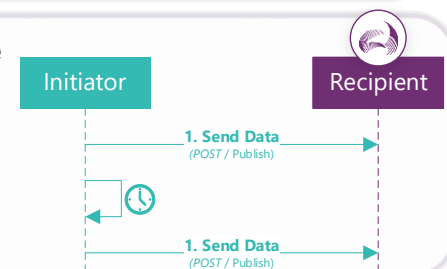
Industry Data Exchange Target State Concepts

- IDX Environment
- Decision Trees
- Outbound Data
- Business Function Transactions
- Data Payload
- AEMO Supplied Data Exchange Software
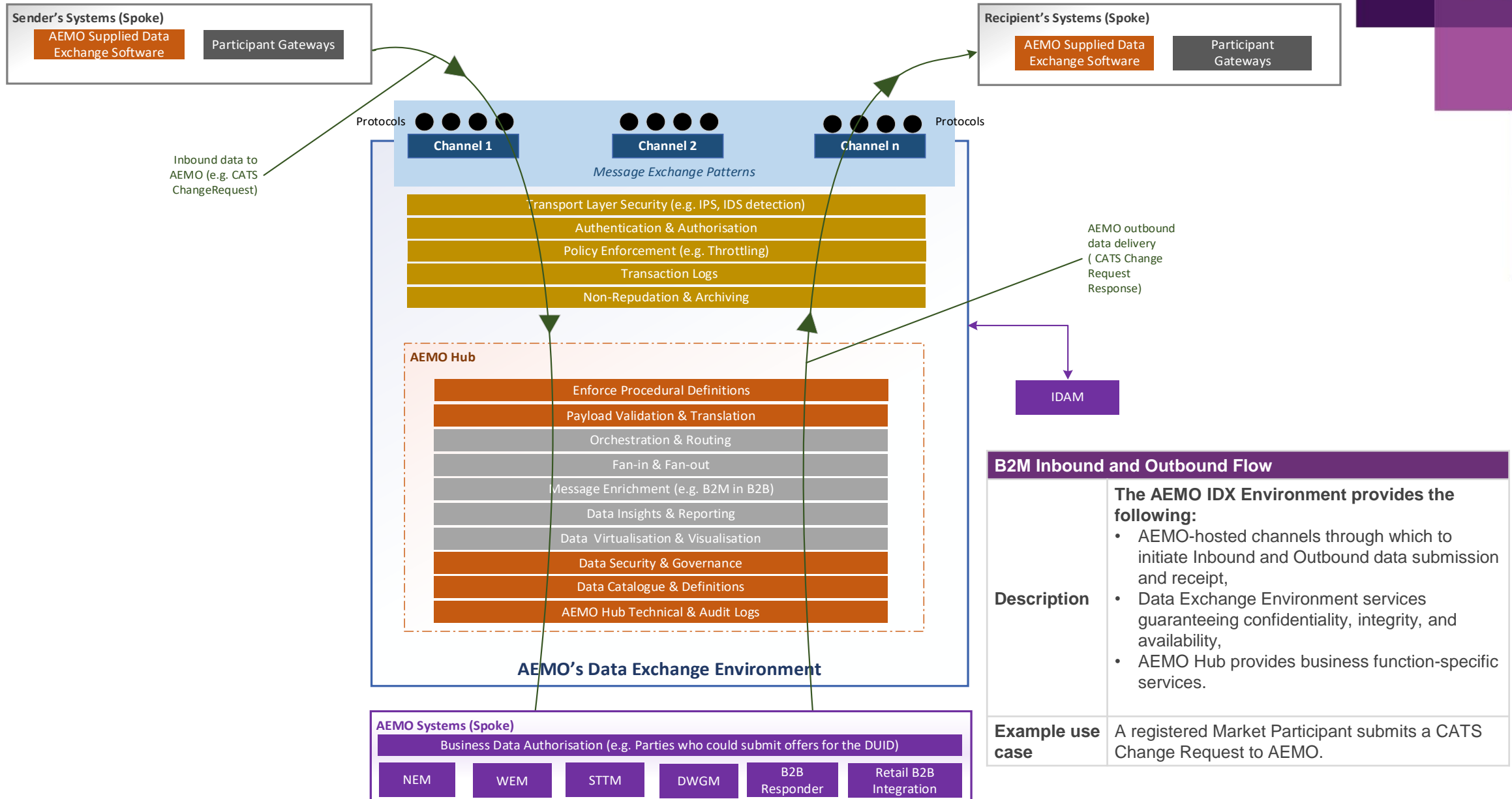
IDX Target State - AEMO IDX Environment

Pain points	Proposed Principle(s)	Target State Concept

Industry raised pain-point:
• Managing Cost-Effective Change.
• Provide centralised services to reduce industry cost and complexity.
• Lack of consistent standards across Systems / Fuels / Jurisdictions.
• Security model needs to be standardised.
AEMO's reading of Industry pain points:
• AEMO and stakeholders must allocate more resources, such as time, money, and personnel, to manage and maintain multiple IDX mechanisms.
• Inconsistent authentication and decentralised authorisation make managing IDX security and access control across various channels, protocols, and patterns challenging.
	• A **standard set of Industry agreed on channels, protocols, patterns, and capabilities** to meet the end-to-end IDX needs across all Fuels, Markets and Domains.
	• Alignment to IDX cyber security best practices.
	• Unified Low Volume Interface (LVI) to support IDX for smaller stakeholders.
		A centralised AEMO IDX Environment to support IDX between stakeholders provide the following:
		• AEMO-hosted channels through which to initiate Inbound and Outbound data submission and receipt.
		• Data Exchange Environment services guaranteeing confidentiality, integrity, and availability.
		• A hub providing business function-specific services.
		• Improve cyber resilience:
		  • Unified authorisation and authentication leveraging IDAM.
		  • Adoption of secure modern IDX protocols (e.g. OAuth).
		• Unified LVI supporting Inbox/Outbox message management, transaction logging and archiving.

IDX Target State - AEMO IDX Environment

Sender's Systems (Spoke)

| AEMO Supplied Data Exchange Software | Participant Gateways |

Recipient's Systems (Spoke)

| AEMO Supplied Data Exchange Software | Participant Gateways |

Protocols

Channel 1 **Channel 2** **Channel n**

Message Exchange Patterns

Transport Layer Security (e.g. IPS, IDS detection)

Authentication & Authorisation

Policy Enforcement (e.g. Throttling)

Transaction Logs

Non-Repudiation & Archiving

AEMO Hub

Enforce Procedural Definitions

Payload Validation & Translation

Orchestration & Routing

Fan-in & Fan-out

Message Enrichment (e.g. B2M in B2B)

Data Insights & Reporting

Data Virtualisation & Visualisation

Data Security & Governance

Data Catalogue & Definitions

AEMO Hub Technical & Audit Logs

AEMO's Data Exchange Environment

IDAM

AEMO Systems (Spoke)

Business Data Authorisation (e.g. Parties who could submit offers for the DUID)

| NEM | WEM | STTM | DWGM | B2B Responder | Retail B2B Integration |

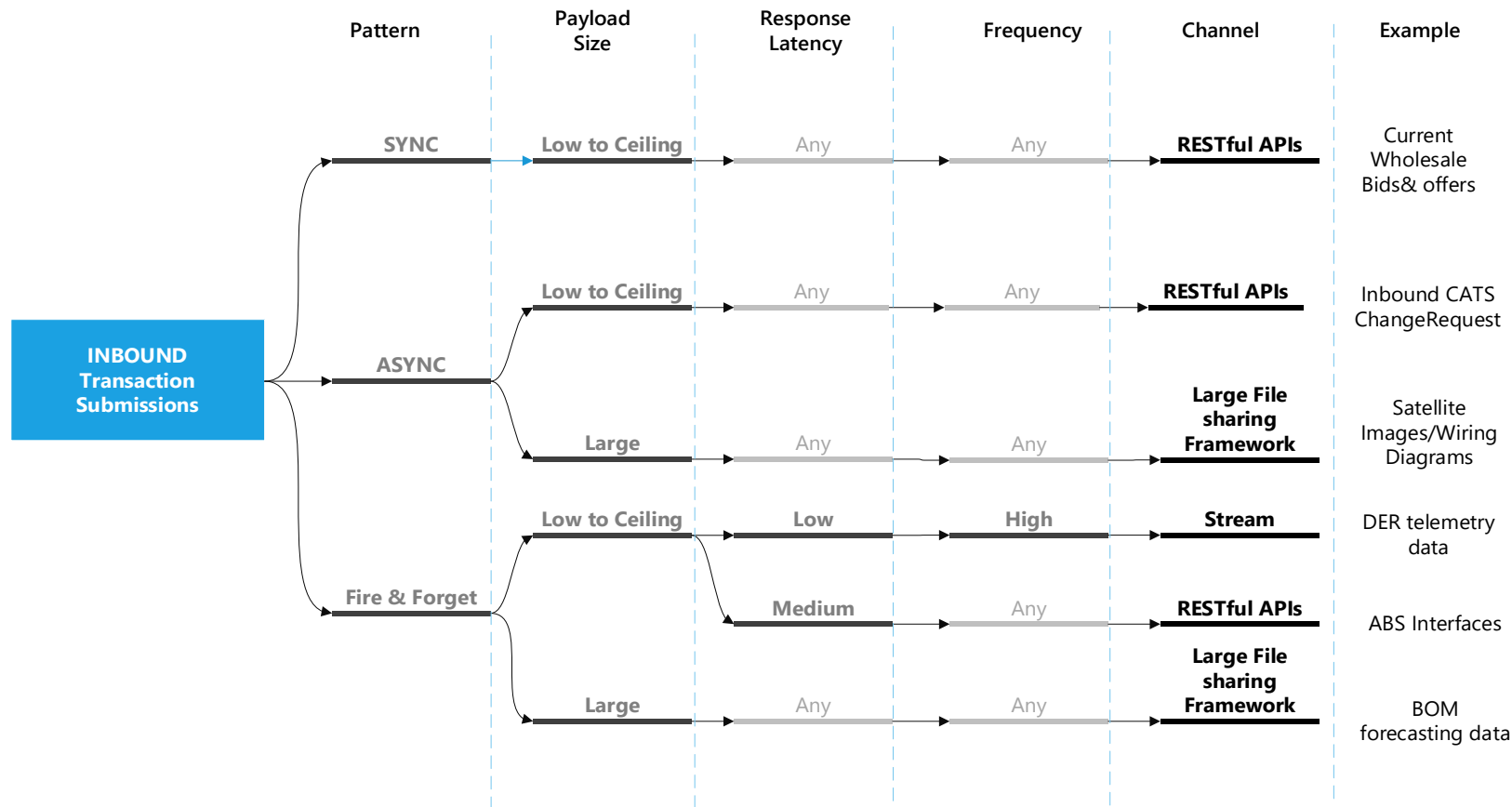| AEMO IDX Environment Elements	Description
AEMO Data Exchange Environment	AEMO provides IDX capabilities not governed by Procedures such as perimeter level security, authentication & authorisations via the supported channels and protocols.
AEMO Hub	AEMO's integration platform supports market messaging (inbound & outbound), managing regulated transaction messages.
AEMO Systems (Spoke)	AEMO systems will be considered a spoke, leading to the Hub-Spoke model for all interactions IDX supports. For example, e.g. stakeholder systems will be a spoke interacting with Hub, which acts as a Hub, and the recipient spoke being the AEMO systems. Likewise, the Hub will play the role of Hub in between the B2B stakeholders.
Senders' System (Spoke)	Sender's system initiating B2M or B2B messages to the AEMO's Data Exchange Platform.
Recipient's System (Spoke)	Recipient's system accepting B2M or B2B messages from the AEMO's Data Exchange Platform.
IDAM	AEMO's Identity and Access Management (IDAM) system

15

IDX Target State - AEMO IDX Environment

IDX Target State - IDX Decision Trees

Pain Points	Proposed Principle(s)	Target State Concept
Industry raised pain-point: • Cost and complexity. • Lack of alternative data exchange mechanisms *AEMO's reading of Industry pain points:* • AEMO offers multiple patterns for the same regulated transactions, each with different infrastructure requirements. This creates unnecessary complexity. • Management multiple patterns, most of which have had **zero** uptake (B2BMessagingSync, B2BMessagingPull, B2MMessagingPull), has high ongoing operational and implementation costs for AEMO and, in turn, industry.	• For each use case, **a single channel and protocol** is to be offered.	• The IDX platform will offer multiple channels and protocols. However, for each specific use case, **an industry-agreed-upon decision tree** for data exchange will lead to the selection of a single channel and protocol.

IDX Target State - IDX Decision Trees

- Interacting and exchanging data with AEMO and Industry happens in various ways depending on the use case.
- Decision trees offer a visual and structured approach to decision-making, which in the context of IDX, can provide certainty to the Industry regarding the channels employed for IDX use cases based on agreed parameters and their nodes.
- Each branch of the decision tree is a node, where a decision is made based on a parameter's value, determining the decision tree's path and outcome.
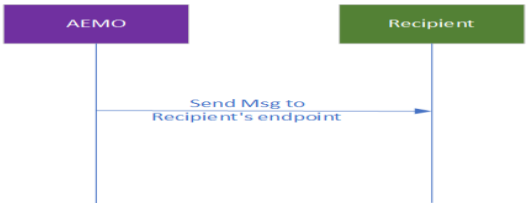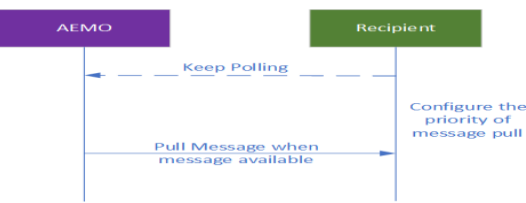
Pattern	Payload Size	Response Latency	Frequency	Channel	Example
SYNC	Low to Ceiling	Any	Any	**RESTful APIs**	Current Wholesale Bids& offers
ASYNC	Low to Ceiling	Any	Any	**RESTful APIs**	Inbound CATS ChangeRequest
	Large	Any	Any	**Large File sharing Framework**	Satellite Images/Wiring Diagrams
Fire & Forget	Low to Ceiling	Low	High	**Stream**	DER telemetry data
	Medium	Any		**RESTful APIs**	ABS Interfaces
	Large	Any	Any	**Large File sharing Framework**	BOM forecasting data

INBOUND Transaction Submissions

Decision node	Definition	Decision node values
Payload Size	The amount of data, variable by channel and Market being transmitted excluding any additional overhead or protocol information.	Low to Ceiling / High
Response Latency	The time delay from when a request is sent to when a response is received.	Low: Very quick milliseconds / Medium: 2 sec / High: 60 – 120 sec
Frequency (Interface volumes)	The rate at which data requests and responses are transmitted over an interface in a given amount of time.	Low / Medium / High

*Outbound and Inquiry services decision trees are in Appendix B.

IDX Target State – Outbound Data

Pain points	Proposed Principle(s)	Target State Concept
Industry raised pain-point: • Cost and complexity. *AEMO's reading of Industry pain points:* • Requires stakeholders to create and manage API gateways, networking setups and troubleshooting efforts at their cost. • Current patterns depend on the recipient system's uptime; availability issues result in suboptimal FIFO delivery to clear queued messages. • Participants currently have no option to configure message delivery orders. • Requirement to implement additional cyber security controls to allow external connectivity by AEMO.	• Minimise ongoing IT change for stakeholders in the data delivery processes while reducing their costs and efforts associated with the transition to IDX. • Empower stakeholders with the ability to prioritise the order of data delivery, providing maximum control over the data reception process. • Provide near real-time visibility of critical market transactions.	• AEMO-hosted Outbound Pull using Event-Driven Integration shall be the foundation of outbound data delivery. • By hosting Outbound Pull endpoints within the AEMO IDX environment, the infrastructure requirements for stakeholders are minimised, reducing their costs and maintenance efforts. • Event Notifications enable stakeholders to subscribe to messages for real-time reception, eliminating the need to poll the AEMO-hosted Outbound data endpoint. This approach supports real-time messaging, with a particular emphasis on asynchronous responses.

IDX Target State – Outbound Data

Capability	Outbound Push (current)	Outbound Pull (current)	Outbound Pull with Event Notification
Definition	AEMO delivers outbound message to Recipient's endpoint.	Recipient pulls outbound message from AEMO (polling for new messages)	AEMO sends event notification when an outbound message is available. Upon receipt of event, Recipient pulls the message from AEMO.
Diagrammatic representation			
Speed of Data Delivery	●	◔	◔
Prioritise Order of Data Delivery	○	●	●
Operational Overheads	◕	◕	◕
Cost to Industry	◑	◕	◕
Reduce Barrier to Entry	◕	◕	◕
Increased cyber security controls	◔	◑	◕

IDX Target State – Business Function Transactions

Pain Point	Principle	Target State Concept
• Disparate payload formats across fuels, markets and domains that don't accommodate the flexibility for change (e.g., JSON for wholesale, aseXML retail, AEMO CSV vs other embedded CSV formats).	• Modern payload standards shall be implemented for new services or services unregulated by Procedures.	• Unified modern payload standards for all fuels, markets, and domains for Transactional and Bulk Data messages.
• As Procedural changes to a transaction cascade change to the entire schema, stakeholders must undertake non-functional updates to maintain compliance with the supported schema. • For Retail Schema, versioning to the header increases implementation time and cost to the extent that AEMO extends support for the previous version (n-1).	• Stakeholders not impacted by a Procedural change should not be required to perform updates to their market integration solutions.	• IDX versioning to be managed at the business function level.
• Difficult and costly to perform schema upgrades (e.g., parkbox to manage schema upgrades).	• Uninterrupted business services across the market and Procedural change.	• Enabled on-demand transformations of outbound content.
• For Inquiry services, stakeholders must undertake non-functional updates despite the query parameters or results attributes remaining unchanged (e.g., applications undertaking NMID be updated with schema change).	• Processes consuming inquiry services that have no dependencies on new data introduced via Procedural change should not need to be updated.	• Inquiry services can utilise standard data exchange protocols such as GraphQL to shield consumers from changes in the underlying data source

IDX Target State – Business Function Transactions

- For new services or services unregulated by Procedures (e.g., Bids and Offers):
  - The IDX unified modern payload standards shall be applied.
  - Instead of a single master schema incorporating multiple transaction message types, **schemas can be maintained at a business function level** (e.g., a schema per business function).
  - The schema hierarchy and versioning will be at the business function (e.g., transaction group) level.
- Only directly impacted stakeholders need to update their schema for Procedural changes with schema impact.
- If a business function is unaffected by a procedural change, its schema version remains unchanged. Similarly, stakeholders with unaffected functions remain on version n.

- The example on the right illustrates the current state pain point: a stakeholder on the braking change **n-2** must perform an unnecessary upgrade.
- In the target state, these braking changes cease to exist.

	Power of Choice aseXML_r36	Mandatory?	Life Support Notifications aseXML_r38	Mandatory?	Planned Interruption Notification (PIN) aseXML_r41	Mandatory?	Shared Fuse One-Way Notification aseXML_r43
	B2B Schema Changes – Current State						
RB	aseXML_r36	P	aseXML_r38	P	aseXML_r41	P	aseXML_r43
DNSP	aseXML_r36	P	aseXML_r38	P	aseXML_r41	P	aseXML_r43
MP	aseXML_r36			n-2	aseXML_r41		n-2
MDP	aseXML_r36			n-2	aseXML_r41		n-2
MC	aseXML_r36			n-2	aseXML_r41		n-2
ENM	aseXML_r36	P	aseXML_r38			n-2	aseXML_r43

To remain Procedurally compliant, Participants with impacted business functions must move to the latest schema

Participants with business functions unimpacted by Procedural change can delay changing their schema version, staying on n-1 until their verison becomes an unsupported n-2

- For **RESTful API endpoints**, AEMO proposes a move from a single endpoint for all functions to business function-specific endpoints.
- The objective is to provide a more structured and targeted approach to data exchange that also allows AEMO to support at the business function level:
  - Policy enforcement (e.g., throttling) for improved API security and stability.
  - unified API naming standards at the business function level to isolate deployments and simplify maintenance.
  - Avoid the need to introspect the business function during message ingestion for faster processing and improved efficiency.

IDX Target State – Data Payload

Adopting business-function-specific schemas and endpoints for Retail markets offers an opportunity to unify IDX schema across all markets and domains, making them more modern and effective.

Characteristics	Option 1 Transition Retail B2B and B2M to Unified IDX Schema	Option 2 Retain aseXML schema for Retail B2B and B2M
Market	Retail B2B and B2M	Retail B2B and B2M

Definition	• Adopt business-function-specific schemas and endpoints.
	• Transitioning Retail B2B and B2M to modular schemas aligned with modern payload standards.
	• Implementing unified IDX schemas across all AEMO fuels, markets, and domains.
		• Adopt business-function-specific schemas and endpoints.
		• Retail B2B and B2M transactions would continue using:
		  • aseXML, preserving industry-specific data structures.
		  • Various CSV formats embedded in aseXML for bulk data.
		• All other markets and domains transition to a unified IDX schema aligned with modern payload standards.

Transactional Message Format	JSON	aseXML
Bulk Data Format	AEMO CSV	MDFF and other miscellaneous CSV formats.
Inquiry Services	Use a modern open-source query language such as GraphQL serviced using JSON format.	Retain aseXML query format (e.g. NMID).
Deviations from Principles of IDX		• A unified set of Industry agreed on channels, protocols, patterns, payloads and capabilities to meet the end-to-end IDX needs across all Fuels, Markets and Domains. • Modern payload standards shall be implemented for all new services or services unregulated by Procedures.
Extensibility	Changes to be built on a widely adopted standard with extensive tools, libraries, and community.	Changes continue to be built indefinitely on aseXML, a niche payload standard,.

Industry Feedback Required

- **AEMO believes that a move to JSON has clear technical advantages, but we don't have knowledge of the specific impact on stakeholders' systems.**
- **It's important for us to understand how each option would affect your systems. AEMO asks stakeholders to evaluate the impact of each outcome and provide feedback.**
- **Through this feedback, AEMO can incorporate industry insight into creating the business case for IDX.**
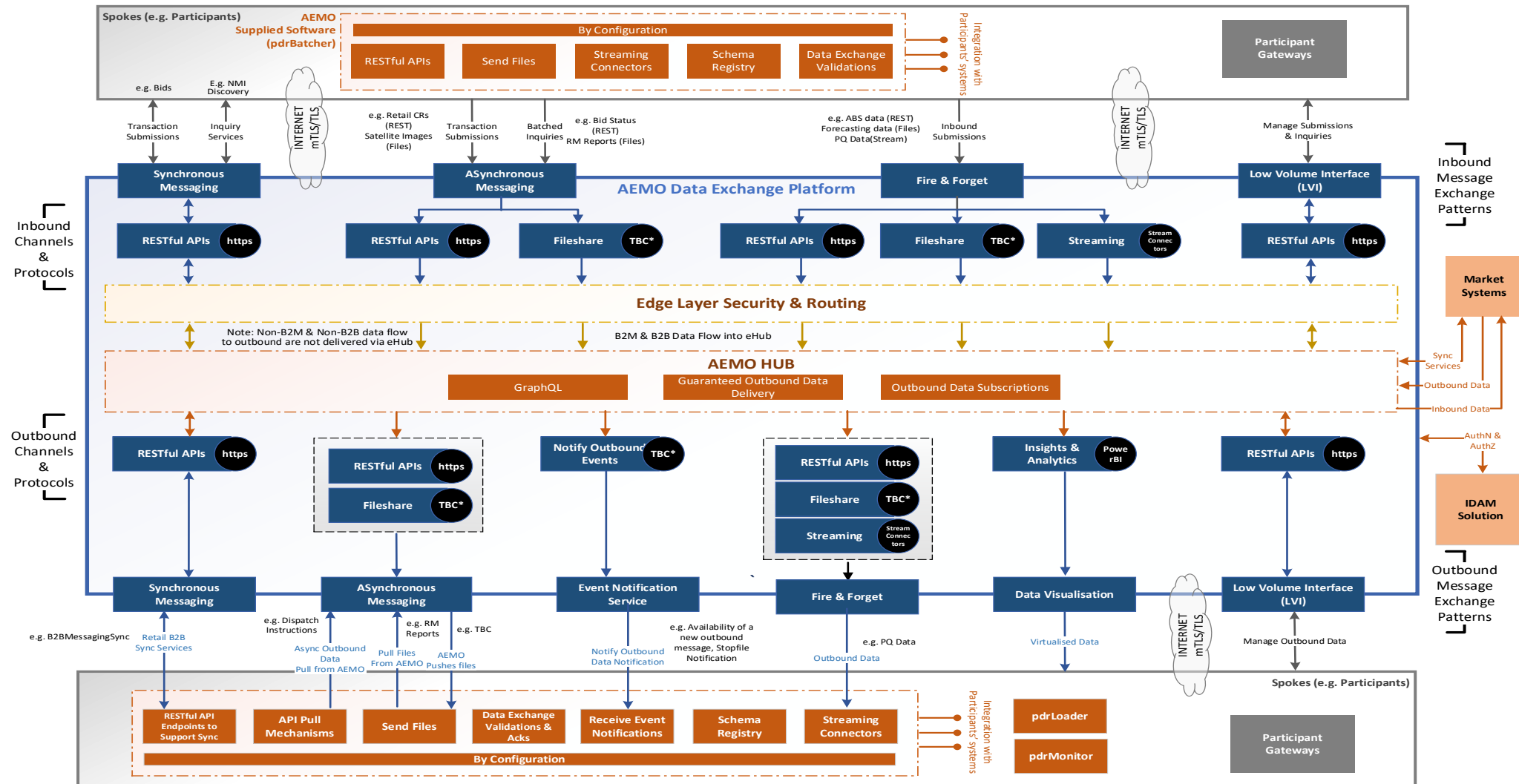
IDX Target State - AEMO Supplied Data Exchange Software

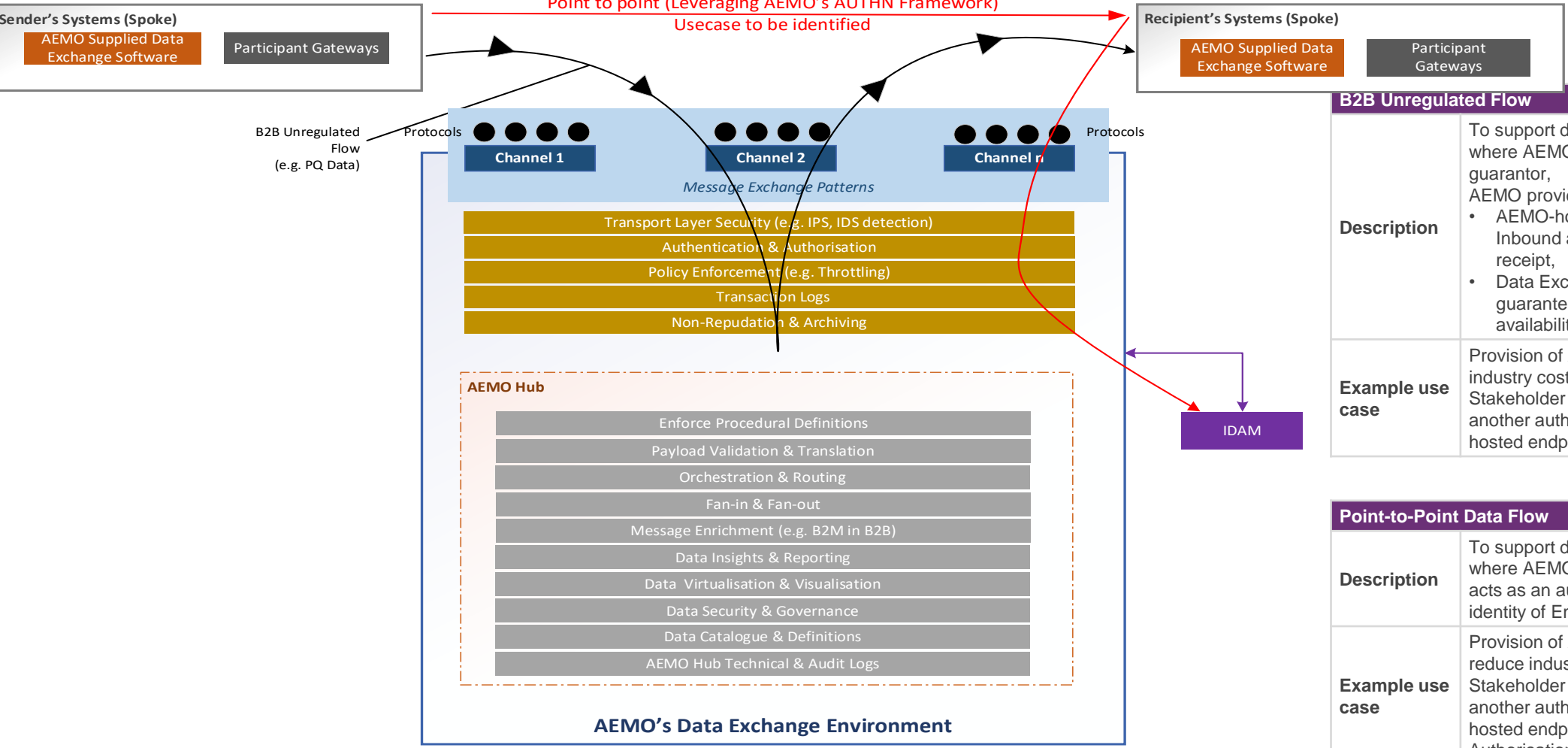| Pain Point	Principle	Target State Concept
• Disparate AEMO-supplied data exchange software with unique features across markets, e.g. participantBatcher supporting NEMRetail interactions and pdrBatcher and pdrLoader suite supporting NEMWholesale interactions. • AEMO data exchange software is not continuously enhanced by introducing new channels, protocols and patterns, e.g. participantBatcher is not enhanced to support data exchange via API channel. • Industry feedback indicated broad support from stakeholders that AEMO-supplied data exchange software should be further extended and enhanced to deliver value and assist with Industry cost takeout.	• Unified AEMO-supplied data exchange software must support the proposed IDX data exchange channels, protocols and patterns across markets.	• Unified data exchange software must provide a mechanism to support multiple inbound & outbound data exchange patterns, channels and protocols; adhering to the agreed decision tree outcomes. • Unified data exchange software must be highly configurable to meet the specific requirements of organisations utilising it, e.g. Participants must have the ability to configure the priority of outbound messages to be processed. (e.g., high-priority service orders are processed over other transaction groups). • Ability to deploy the data exchange software on-prem or major cloud providers.

Industry Data Exchange Conceptual Target State & Potential Flows

IDX Target State - Conceptual Diagram

- Target state concepts are summarised in the following conceptual diagram.
- This target state conceptual overview is the basis for IDX transition planning and the business case.

IDX Target State – Potential Future Flows

Point to point (Leveraging AEMO's AUTHN Framework)
Usecase to be identified

Sender's Systems (Spoke)
| AEMO Supplied Data Exchange Software | Participant Gateways |

Recipient's Systems (Spoke)
| AEMO Supplied Data Exchange Software | Participant Gateways |

B2B Unregulated Flow (e.g. PQ Data)

Protocols

Channel 1   Channel 2   Channel n

Protocols

Message Exchange Patterns

Transport Layer Security (e.g. IPS, IDS detection)
Authentication & Authorisation
Policy Enforcement (e.g. Throttling)
Transaction Logs
Non-Repudiation & Archiving

AEMO Hub

Enforce Procedural Definitions
Payload Validation & Translation
Orchestration & Routing
Fan-in & Fan-out
Message Enrichment (e.g. B2M in B2B)
Data Insights & Reporting
Data Virtualisation & Visualisation
Data Security & Governance
Data Catalogue & Definitions
AEMO Hub Technical & Audit Logs

IDAM

AEMO's Data Exchange Environment

B2B Unregulated Flow

Description	To support data exchange between stakeholders where AEMO only plays a role as a data delivery guarantor, AEMO provides the following: • AEMO-hosted channels through which to initiate Inbound and Outbound data submission and receipt, • Data Exchange Environment services guaranteeing confidentiality, integrity, and availability,
Example use case	Provision of AEMO gateway solutions to reduce industry costs, e.g. an authorised Energy Stakeholder exchanges Power Quality data with another authorised stakeholder through AEMO-hosted endpoints.

Point-to-Point Data Flow

Description	To support data exchange between stakeholders where AEMO plays an Identity Provider role, AEMO acts as an authorisation service to guarantee the identity of Energy Stakeholders.
Example use case	Provision of AEMO's authorisation solutions to reduce industry costs, e.g. An authorised Energy Stakeholder exchanges Point-Point data with another authorised Energy Stakeholder using self-hosted endpoints but leveraging AEMO's Authorisation Framework.

Industry Feedback Required

- AEMO believes that these flows may fulfil future use cases.
- AEMO has no immediate plans to implement these end-to-end flows, but our target state design includes them as potential extensions to the system's functionality.
- We would like to know if the industry sees any value in these flows.

IDX - Next Steps

- AEMO's intention currently is to agree in principle a position on the target state collaboratively with industry and incorporate into the transition strategy and business case for Industry Data Exchange
- A consensus position is sought with industry. Where there are diverging views, these will be acknowledged.

- AEMO is seeking feedback on the following questions:
    1. Are there any material gaps or concerns in the Target State requiring further consideration?
    2. With these definitions can you identify further benefits or impacts for industry of the proposed Target States?
    3. Do you have additional feedback to share on the consultation process in general?
    4. And specific to IDX:
        - Slide 23: Industry's view on Options 1 and 2 of the IDX data payload?
        - Slide 27: Benefits of supporting potential future data flows for B2B Non-Regulated and Point-to-point data?

- Feedback is due by 26 May to NEMReform@aemo.com.au.

Lunch break
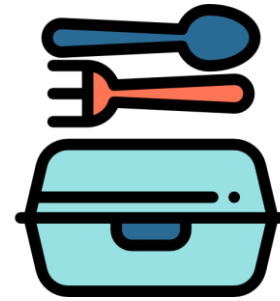
Identity & Access Management workshop
begins 1.30pm

AEMO

3. Proposed Target State

Identity & Access Management

Identity & Access Management foundation

- Scope
- Pain points
- Objectives
- Design principles

Identity and Access Management Scope

Identity and Access Management: A unified mechanism to authenticate and authorise external identity when accessing AEMO services, consolidating and improving overall cyber security controls.

Problem Statement:

AEMO's Identity and Access Management (IDAM) services are disparate, requiring users to retain multiple sets of credentials in order to access AEMO business services. The legacy IDAM services do not implement best practices in cyber security controls (e.g., multifactor authentication) and are insufficient to meet new industry obligations introduced under the SOCI Act.

IDAM Current State Context Diagram:
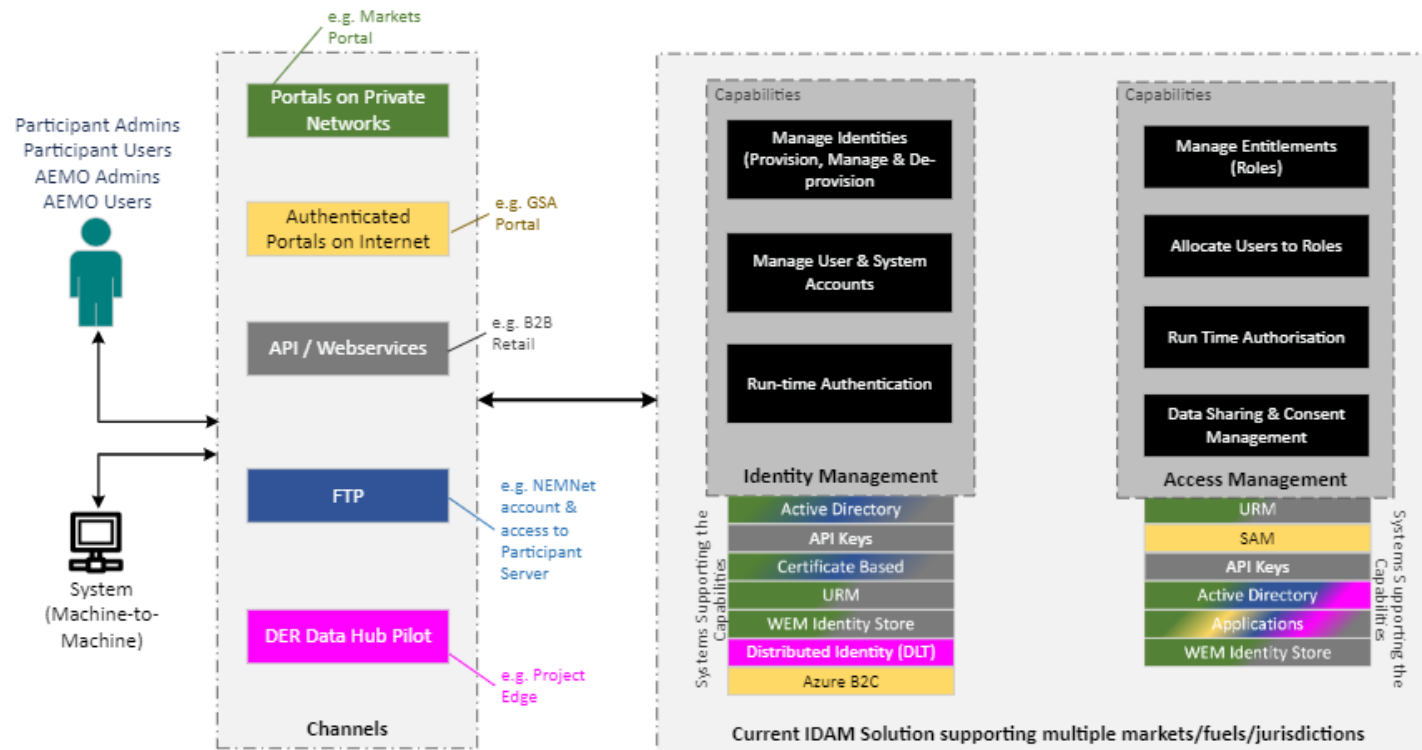
Note: Channels & IDAM Stores illustrated in this slide are indicative only and not the finite list

Following areas will be explored during the IDAM feasibility phase.

In Scope	Out of Scope
✓ NEM, WEM and Gas involving AEMO external interactions	✗ Network layer security
✓ External Identities including: - Registered Participants - Non-registered Participants - Potential Participants - Service Providers	✗ Control systems communications / interactions
	✗ Direct device communications /interactions
✓ External System Accounts Interactions via all supported channels (current & future)	

IDAM Pain points (unranked)

Below is a summary of the key pain points from Business and Technical focus group discussions, classified into themes according to the challenges they pose to the legacy IDAM services.

User accounts

Participant Administrator (PA) experience

- Perform **repetitive tasks** e.g., creation of roles, unable to inherit the roles from an existing set
- Lack of ability **to identify inactive, unused, and suspicious accounts**
- Inability to set **expiration dates for user access** to automatically revoke access upon expiration
- Lack of **reporting capabilities** to conduct **periodic assessments**
- Inability to **automate user offboarding**, resulting in increased risk of unauthorised access and security risks
- Need to extend PA concept to other markets.
- Lack of **role catalogue** with pre-defined roles.

User experience

- **Multiple credentials** required to access different AEMO systems
- **Lack of integration between the Participant's organisation and AEMO's identity store (Federation)**
- Inadequate **self-service capabilities** e.g. Password reset, consent management, etc
- Inadequate training material, support, and documentation to support the complex user management landscape
- Lack of **designation of account to a specific AEMO environment** such as pre-production or production

Governance and Compliance

- Lack of the visibility of the **audit trail to monitor significant identity and access management services**
- Need for **Multi-Factor Authentication (MFA)** to enhance security by requiring multiple forms of authentication, such as tokens, SMS verification, fingerprint or facial recognition (Windows Hello), and authenticator apps.

System accounts

Management of Service Accounts

- **Multiple user credentials** are required to access AEMO systems
- **Multiple access controls** to access AEMO systems
- **Multiple AuthN patterns** e.g., API keys, Basic Auth and OAuth
- Inadequate capabilities for **managing password changes** e.g., the use of shared credentials across multiple applications necessitating concurrent change
- Lack of **designation of account to a specific AEMO environment** such as pre-production or production

Future

Future Needs and capabilities

- **Context based authentication** - Dynamic risk assessment is embedded into the access decision by calculating risk using user behaviour and context analytics to protect against stolen credentials.
- Explore **data sharing capabilities** in markets beyond NEM

IDAM Objectives
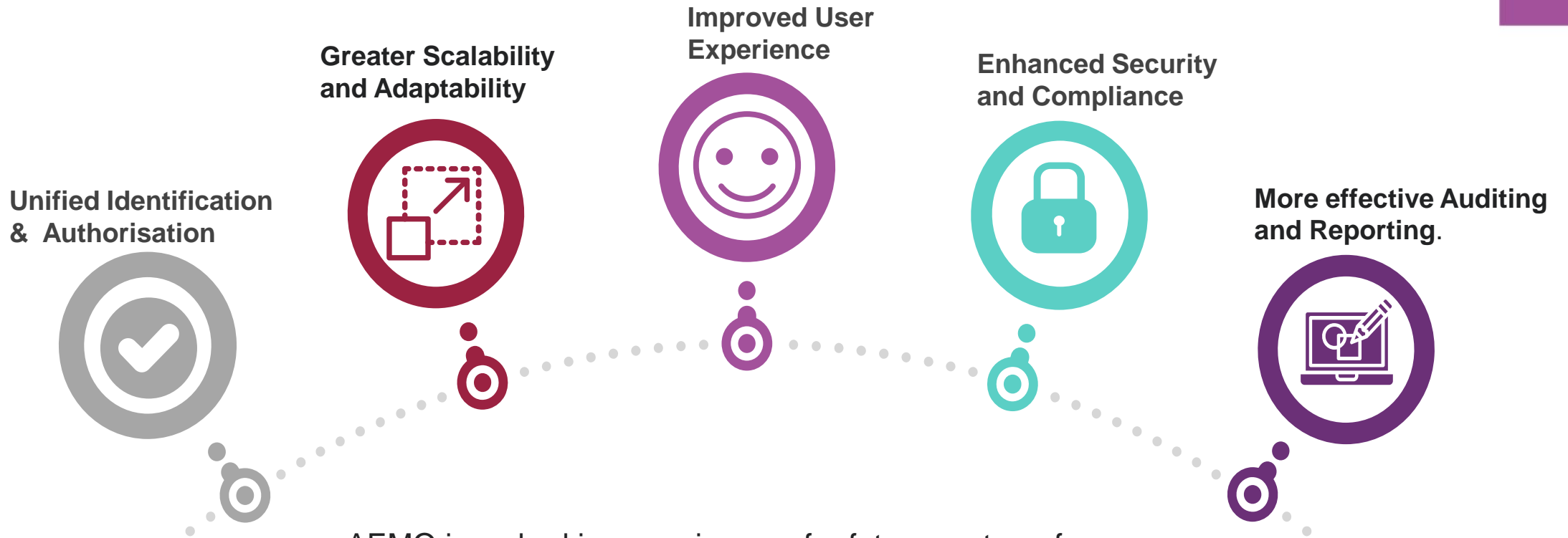
Unified Identification & Authorisation

Greater Scalability and Adaptability

Improved User Experience

Enhanced Security and Compliance

More effective Auditing and Reporting.

AEMO is embarking on a journey for future sector reforms, which will entail the introduction of a unified identity and access management framework
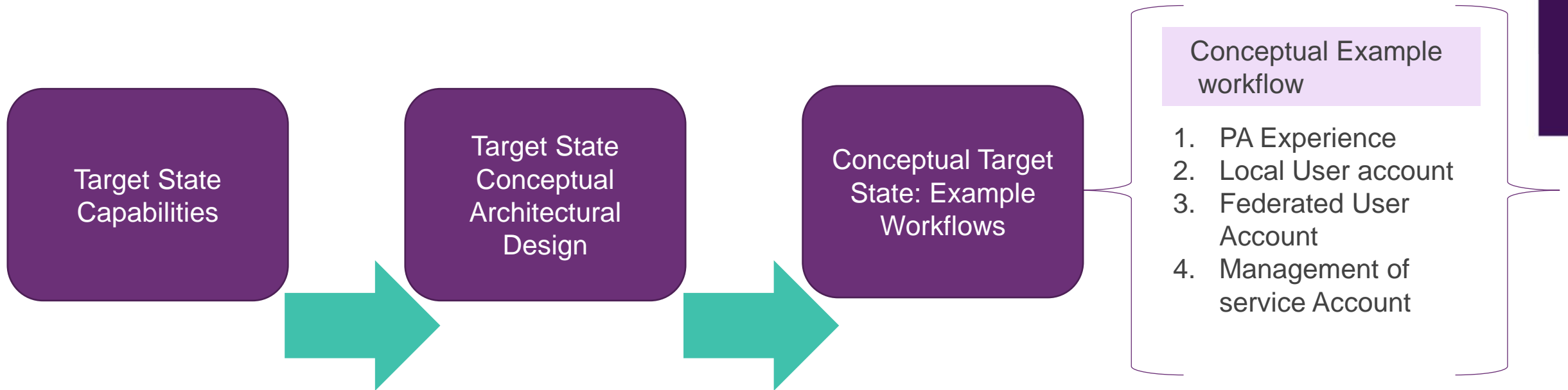
Conceptual Architectural Design Principles

- AEMO will provide a **unified Identity and Access Management Platform** (Identity Fabric*) for its stakeholders:
  - Support for industry standard **modern authentication and authorisation protocols**
  - **Single source of truth** for person and non-person identities
  - **Centralised i**dentity and access management

- AEMO will support the use of **single unique credential** to access all AEMO hosted applications and services.
  - Enables the stakeholders to leverage their **Enterprise Identity to access AEMO hosted applications and services.**
  - Provides a **strong authentication** mechanism using **two distinct authentication factors**, one of which will be through an approved cryptographic technique, providing a high degree of confidence that the claimant has complete control over those authentication factors.
  - Protection against cyber threats like stolen credentials using dynamic risk-based authentication employing user behaviour and context analytics

- AEMO will provide a **highly flexible access control mechanism** using **attribute-based access control**
  - Enables the stakeholders to define access control policies in a more flexible, user-friendly business language
  - Support for the definition of **more granular access control policies** based on various attributes of the user, groups, resource types, actions etc.,
  - Support for more advanced and evolving business use cases

* Identity Fabric is not a single technology, tool, or cloud service, but a paradigm for architecting IAM within enterprises.

Identity & Access Management Conceptual Target State

- Approach
- Capability View
- Conceptual Architectural Design

Approach: Conceptual Target State

```
┌─────────────────┐      ┌─────────────────┐      ┌─────────────────┐
│                 │      │  Target State   │      │ Conceptual      │
│  Target State   │  ▶   │  Conceptual     │  ▶   │ Target State:   │
│  Capabilities   │      │  Architectural  │      │ Example         │
│                 │      │  Design         │      │ Workflows       │
└─────────────────┘      └─────────────────┘      └─────────────────┘
```

Conceptual Example workflow

1. PA Experience
2. Local User account
3. Federated User Account
4. Management of service Account

IDAM Target State Capability View
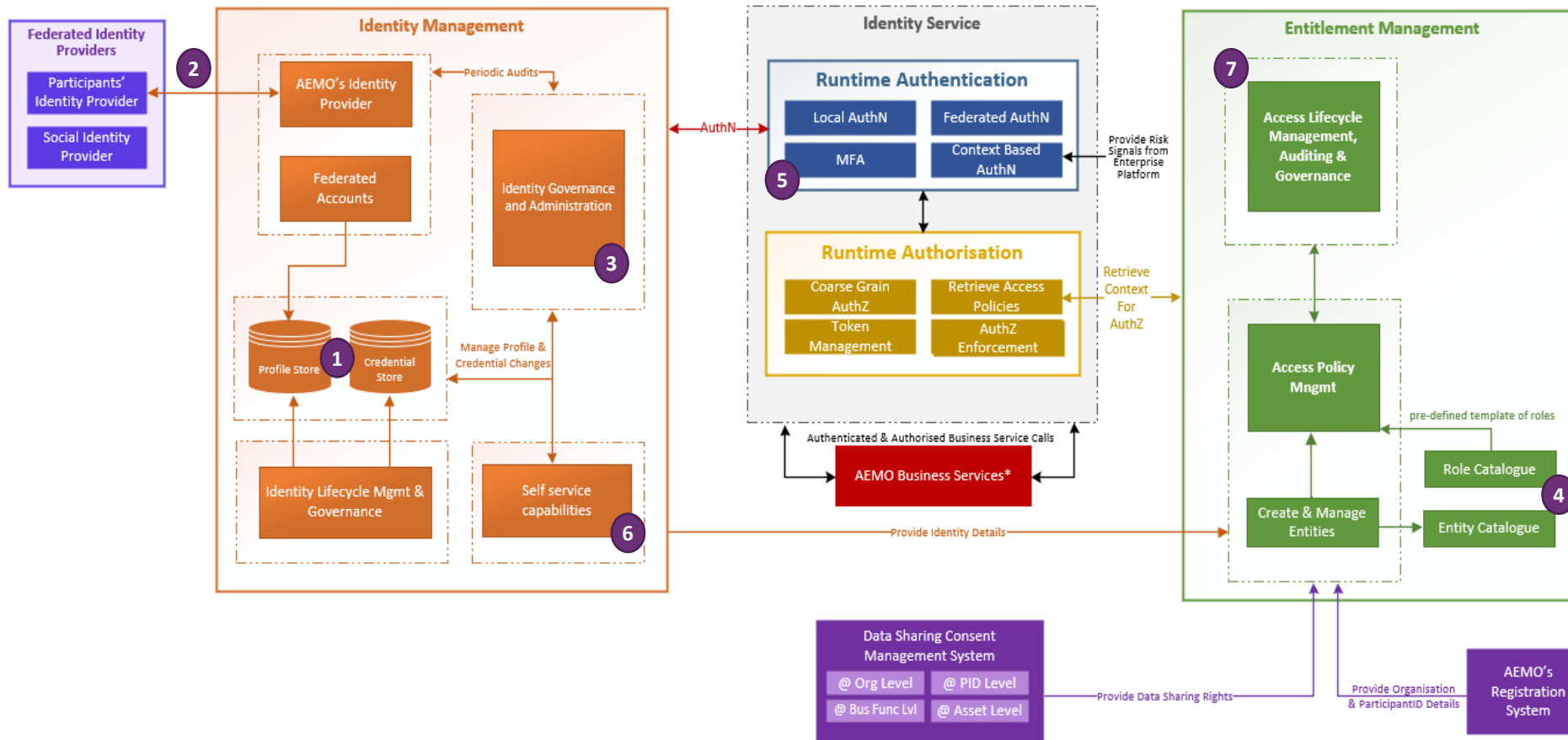
Industry Key Pain Points

1. **Multiple credentials** required to access different AEMO systems

2. Lack of integration between Participant's Organisation and AEMO Identity store **(Federation)**

3. Inability to **automate user offboarding**, resulting in unauthorised access and security risks

4. Lack of **pre-defined entity catalogue and role catalogue**

5. Need for **Multi-factor authentication** to enhance security

6. Inadequate **self-service capabilities** Password reset

7. Lack of **reporting capabilities** for PAs to conduct periodic assessments

IDAM Target State Conceptual Architectural Design

Example Workflows

Participant Admin (PA) Workflow

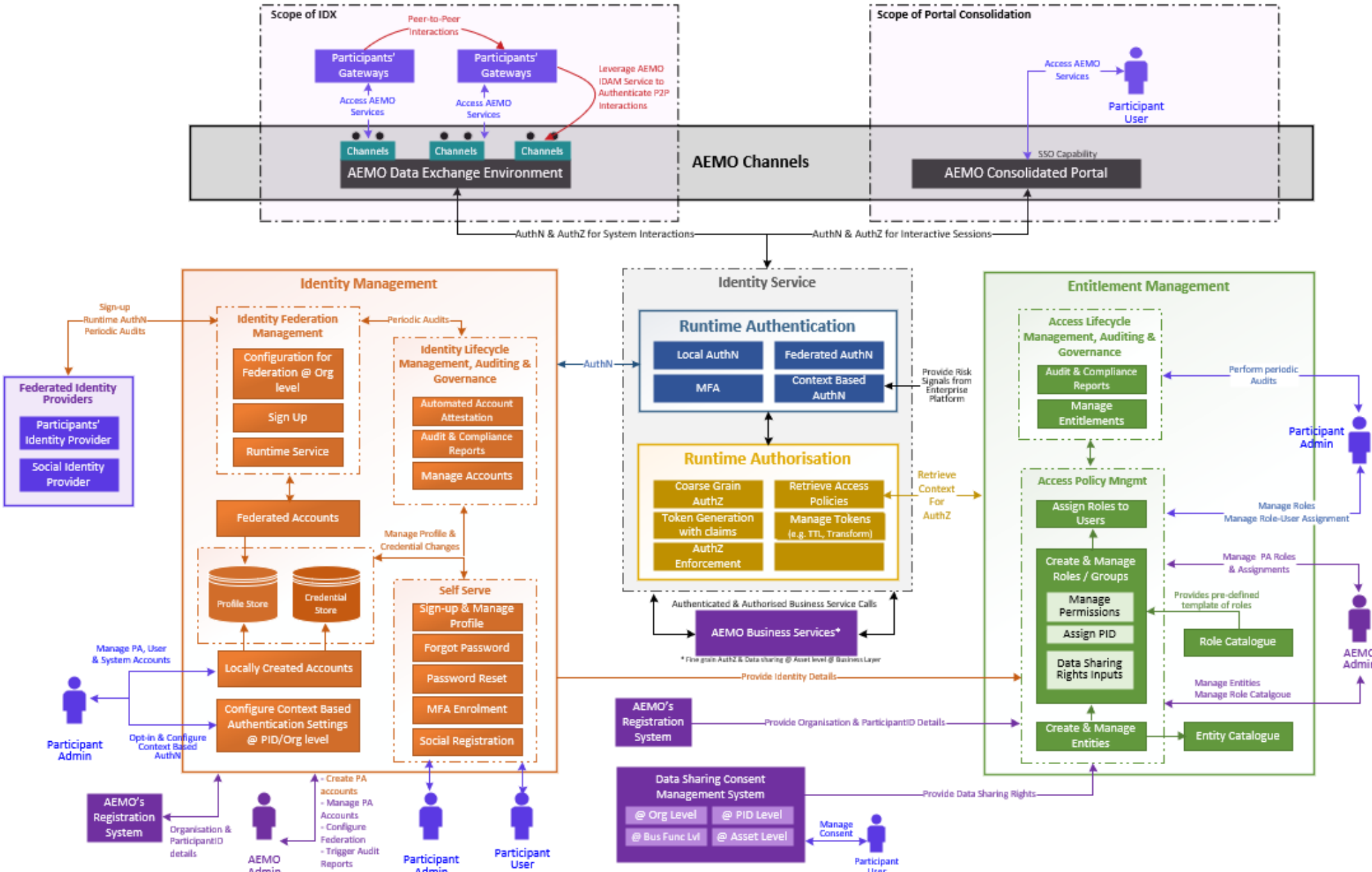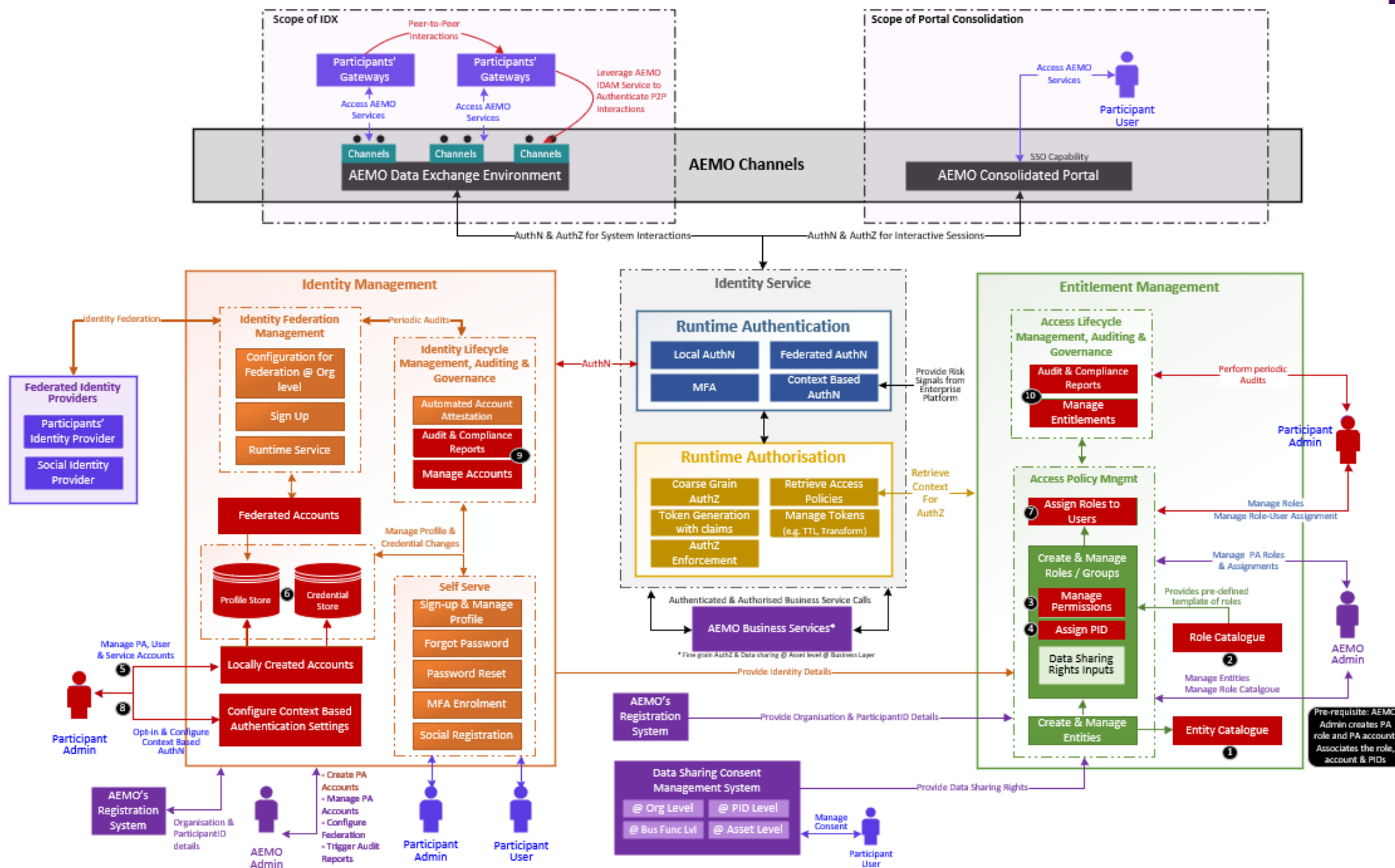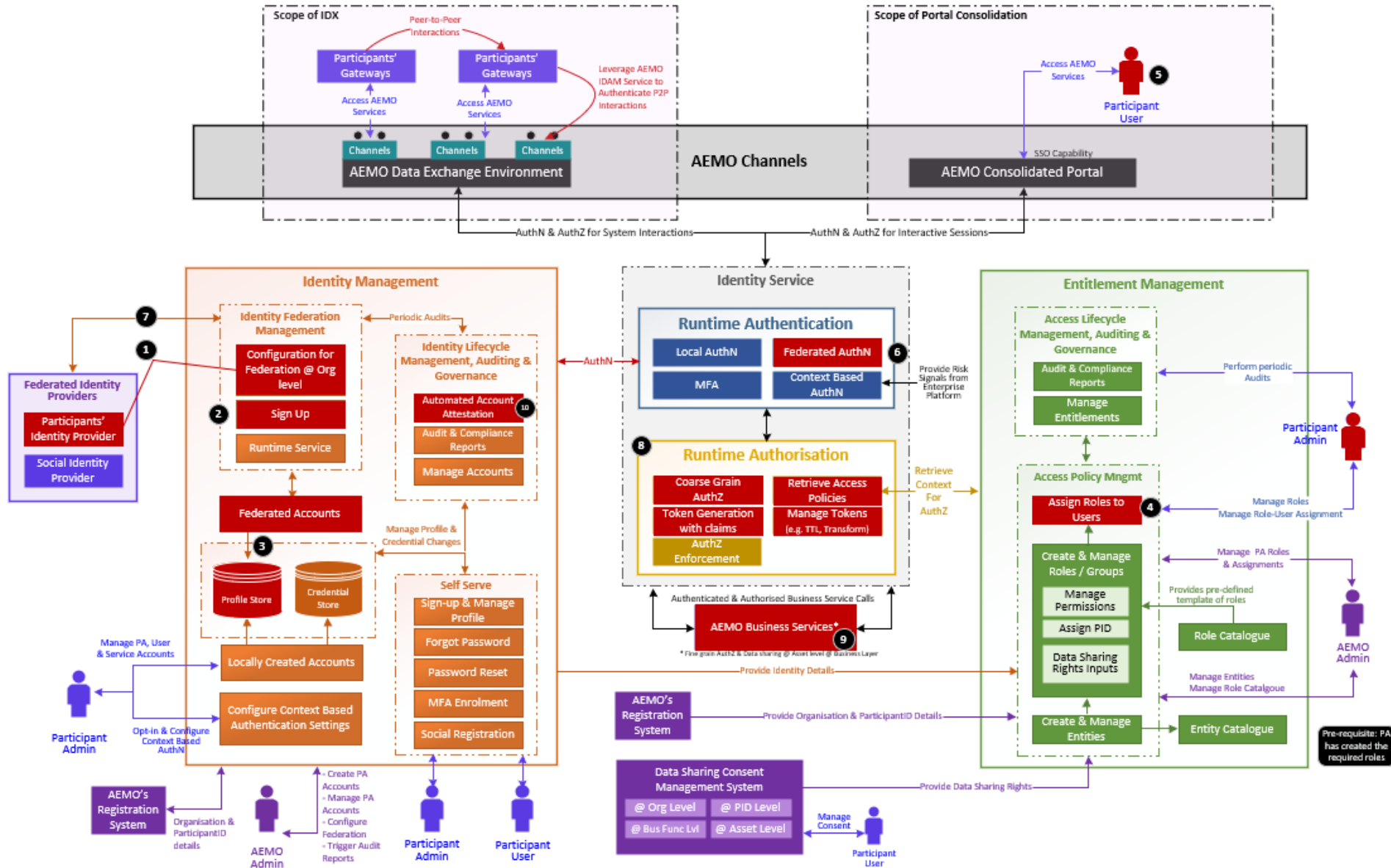| Step	Description
Pre-requisite	AEMO admin creates the PA role and associates the PA role with the PA Admin account. AEMO provides the initial credentials for the PA. The AEMO administrator also provides access to the pre-defined role catalogue as well as the entity catalogue. PA accounts can be locally created or federated based on organisation preference. Account setup will be done by the AEMO System Admin.
1	The PA can access the entity catalogue to establish the role. (***An Entity catalogue is a suite of atomic business functions that can be assembled into one or more roles.***)
2	The PA can consume the pre-defined roles available in the AEMO role catalogue or create a custom role based on the roles available in the role catalogue.
3	The PA then can associate the entities with the roles they consume/define and mark the permissions.
4	The PA can thereafter associate one or more Participant IDs (PIDs) to the role they have created.
5	The PA can create additional PAs, users or service accounts.
6	Person accounts can be locally created or federated based on an organisation's preference.
7	The PA can then assign roles to the users.
8	The PAs can also configure Context-Based Authentication for locally managed accounts.
9	The PAs can get audit reports and perform housekeeping activities like account reconciliation.
10	Capability to get Audit reports to review the access levels and action access levels.

Example2: Management of Federated User Account

Management of Federated User Account

Step	Description
Pre-requisite	The PA has already created all the required roles.
1	System will establish a Federation trust relationship between the AEMO identity provider (IdP) and the participant identity provider.
2	The users can sign up using their enterprise identity.
3	User profiles are then created for these users in the profile store.
4	The PA can assign the role to the user accounts available in the profile store.
5	The users can then access the portal services through their browsers.
6	The identity service identifies the incoming identity as a federated identity and automatically redirects the authentication request to the Participant IdP for authentication.
7	The participant identity provider authenticates the user using their enterprise credential and, if successful, shares the identity assertion to AEMO IdP, which passes it on to the authorisation platform.
8	Coarse grain authorisation is applied based on the user attributes and the user us presented with the screen relevant to their profile.
9	Access privileges related to the user are retrieved and fine grain access is enforced through an appropriate access token which the participant user uses to access the authorised entities.
10	The PAs are provided with the capabilities to manage the deprovisioning of user accounts when they leave the organisation.

Confidential Actions and Data Access Permission to other entities

An access agreement that allows actions and data confidential to one participant to be made available to another participant based on an agreement between those parties and registering this agreement with AEMO.
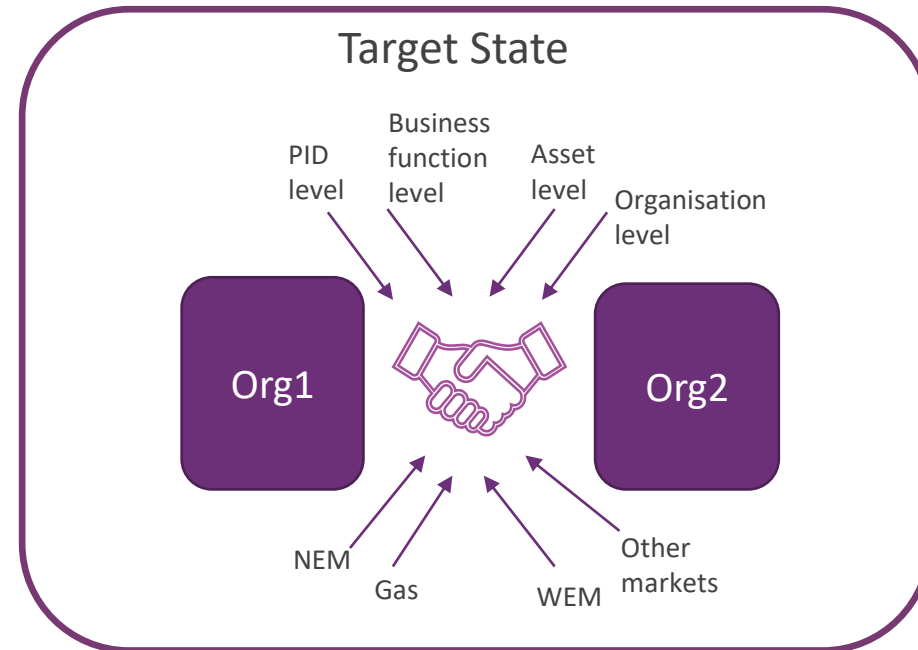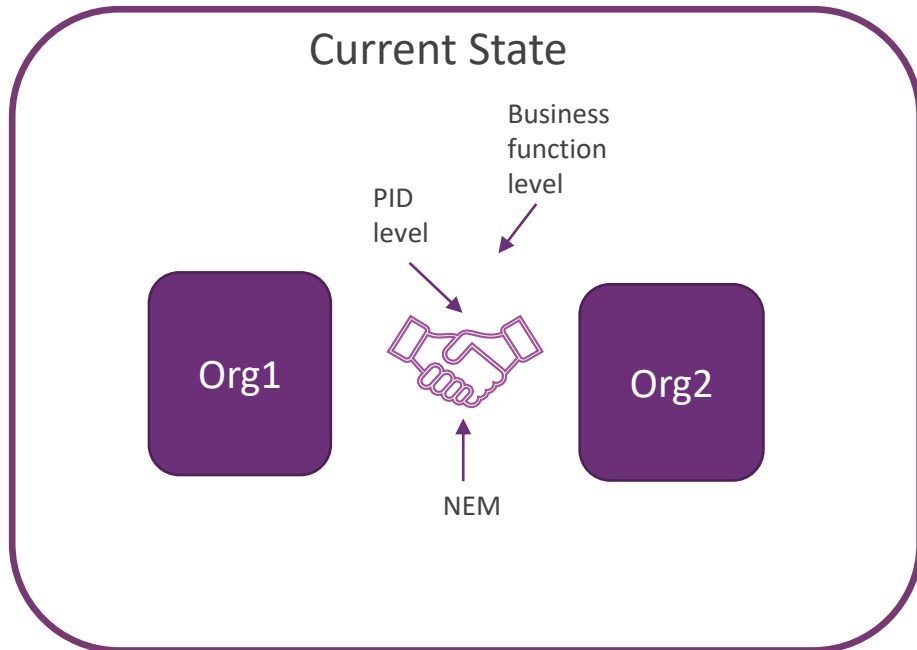
An Organisation is a collection of entities each having their own Participant ID (PID). The PIDs may or may not have the same ABN as the parent organisation .

Data Access Permission Examples

Top row

Org1 (Retailer) — PPA — **Org2 (Generator)**

Org1 requires visibility of the generation volumes of the asset against which the PPA agreement is written to manage their trading exposure

→

Org1 (Retailer) — Data Sharing Agreement — **Org2 (Service Provider)**

This agreement is registered in the IDAM Consent platform

Org2 grants a time bound permission for Org 1 to receive this confidential generation data

→

Org 1 can permission IDAM accounts to receive Org2 confidential data

Org 1

Org 1 should receive its own confidential data + permissioned data of Org 2 in a single channel

Bottom row

Org1 (Retailer) — Contract — **Org2 (Service Provider)**

Org1 enters into a commercial agreement with Org2 to provide a range of services interacting with a Retail Market on the behalf of Org1

→

Org1 (Retailer) — Data Sharing Agreement — **Org2 (Generator)**

Org1 grants a time bound permission for Org 2 to perform inbound transaction and receive outbound transactions confidential to Org1

This agreement is registered in the IDAM Consent platform

→

Org 2 can permission IDAM accounts to submit and receive Org1 confidential data

Org2

Org 2 can interact with the Retail Market on Org 1's behalf

IDAM - Next Steps

- AEMO's intention currently is to agree in principle a position on the target state collaboratively with industry and incorporate into the transition strategy and business case for Identity and Access Management.
- A consensus position is sought with industry. Where there are diverging views, these will be acknowledged.

- AEMO is seeking feedback on the following questions:
  1. Are there any material gaps or concerns in the Target State requiring further consideration?
  2. With these definitions can you identify further benefits or impacts for industry of the proposed Target States?
  3. Do you have additional feedback to share on the consultation process in general?
  4. And specific to IDX:
     - Slide 23: Industry's view on Options 1 and 2 of the IDX data payload?
     - Slide 27: Benefits of supporting potential future data flows for B2B Non-Regulated and Point-to-point data?
- Feedback is due by 26 May to NEMReform@aemo.com.au.

We're on a break

Portal Consolidation workshop begins 3.45pm

4. Proposed Target State

Portal Consolidation

Portal Consolidation - foundation

- Scope
- Objectives
- Pain points
- Design principles

Scope

Portal Consolidation: The aim of the Portal Consolidation project is to enable a unified stakeholder experience that hosts web applications. The portals framework is an enabling platform that supports energy market participants and other partners to consume AEMO browser services in a secure manner.

Problem Statement

AEMO browser services are exposed over a disparate range of end points and require multiple sets of credentials to consume these services. This results in a suboptimal user experience for energy stakeholders. The requirement to access browser services via private networks creates technical barriers to consuming these services.

Following AEMO browser services will be explored during the Portal Services feasibility phase.

In Scope	Out of Scope
✓ External Authenticated Portals (accessed by Market Participants and other External Users). ✓ AEMO users using Internal Portal for control room and market services.	✕ Public Un-authenticated Portals (e.g. aemo.com.au) ✕ Portals in the Corporate Services ✕ SharePoint Apps pertaining to Corporate Services

Portals Current State Context Diagram
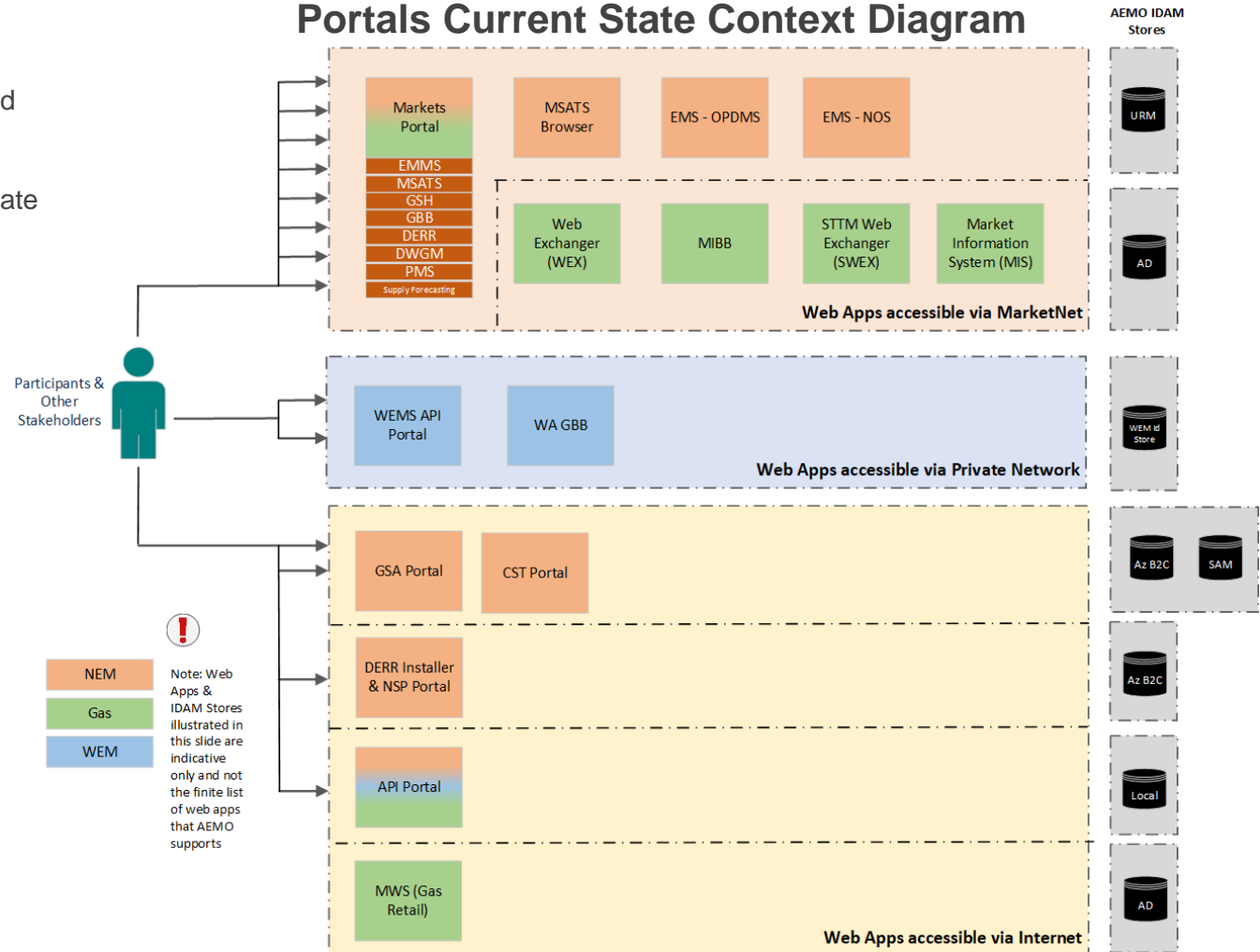
Portal Consolidation Objectives

Provide integration with the enterprise identity management and user authentication solution

Implement framework and roadmap for transition and implementation

Enable a unified portal experience

Enhance self-service capabilities
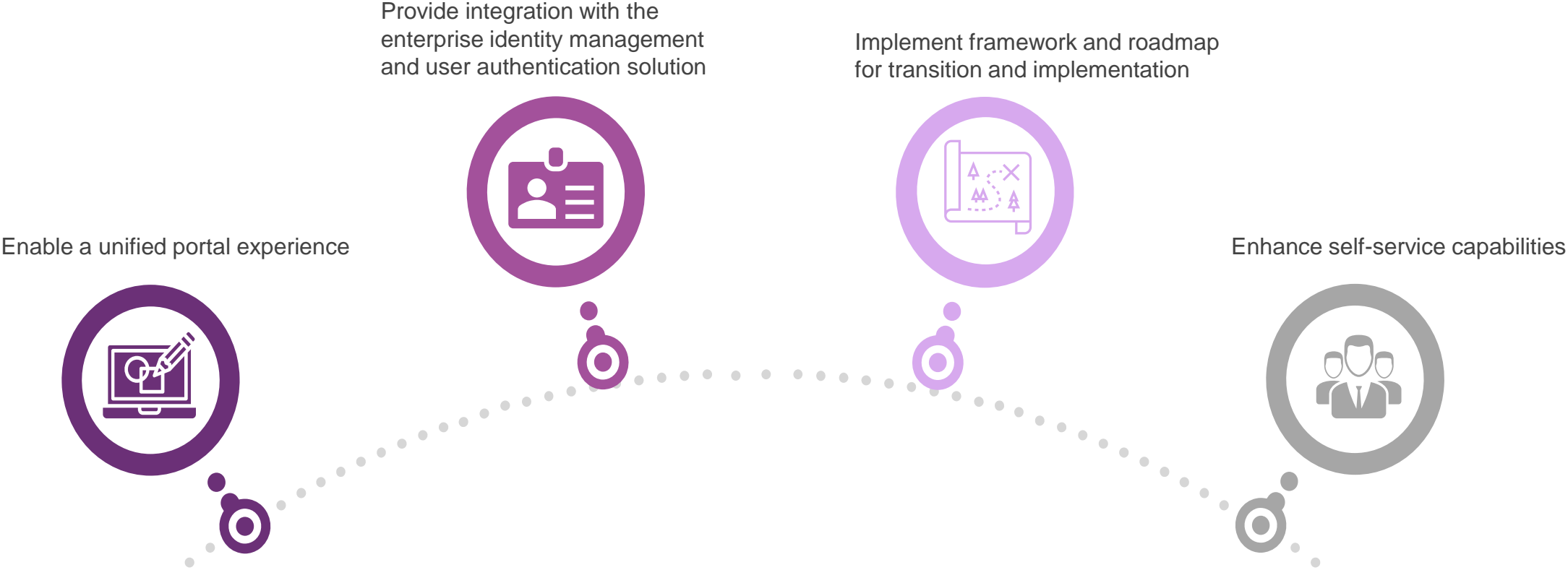
Context: Industry Pain Points Summary

Industry Pain Points Workshop session:

User Experience

- **Disparate portals:** AEMO's browser services are exposed over a disparate range of portals that require uses to switch between multiple URLs and maintain multiple credentials. The user experience for portals is also inconsistent across different markets and domains.

- **Cross browser compatibility**: Browser standards should be supported for endpoints and different devices e.g., Chrome, Safari, IE, Edge, mobile devices

Training, Support and Documentation

- Inadequate resources for **training, support, and documentation** was highlighted. Participants struggle with unclear and scattered documentation, inadequate support from AEMO, and a lack of comprehensive knowledge of the portals.

Cost & Complexity

- Maintenance of the disparate portals appears to be costly (e.g., costs associated with training users and support costs).

Future Needs and Capabilities

- **Personalisation features:** Currently there are inadequate personalisation features available on the portal (e.g., participants cannot create shortcuts to access web applications per their requirements)

Design Principles

AEMO will provide a **single Portal Platform experience** for its stakeholders:

- **Single User Login** for all hosted web applications with IDAM support
- **Accessible** through MarketNet, Internet or VPN dependent on application

AEMO Portal will be **designed with configuration and personalisation**

- **Customising** Menu's and Displays
- **Personalisation** of user profile with saved preferences

AEMO Portal / future web applications will be:

- Designed according to **AEMO's Experience and Design Practice (CX / UX / UI)**
- Using **AEMO's Development Frameworks and Design Guides**
- **Common User experience** across all markets – NEM, WEM and Gas

AEMO Portal will enhance the **User Experience**

- **Self Service** including password reset and tickets
- **Advanced Searching** for data / meta-data objects
- **Support** through Online Help, Guides and access to training material

Portal Consolidation Conceptual Target State

- Target State Proposal
- Solution Capability

Target State Proposal
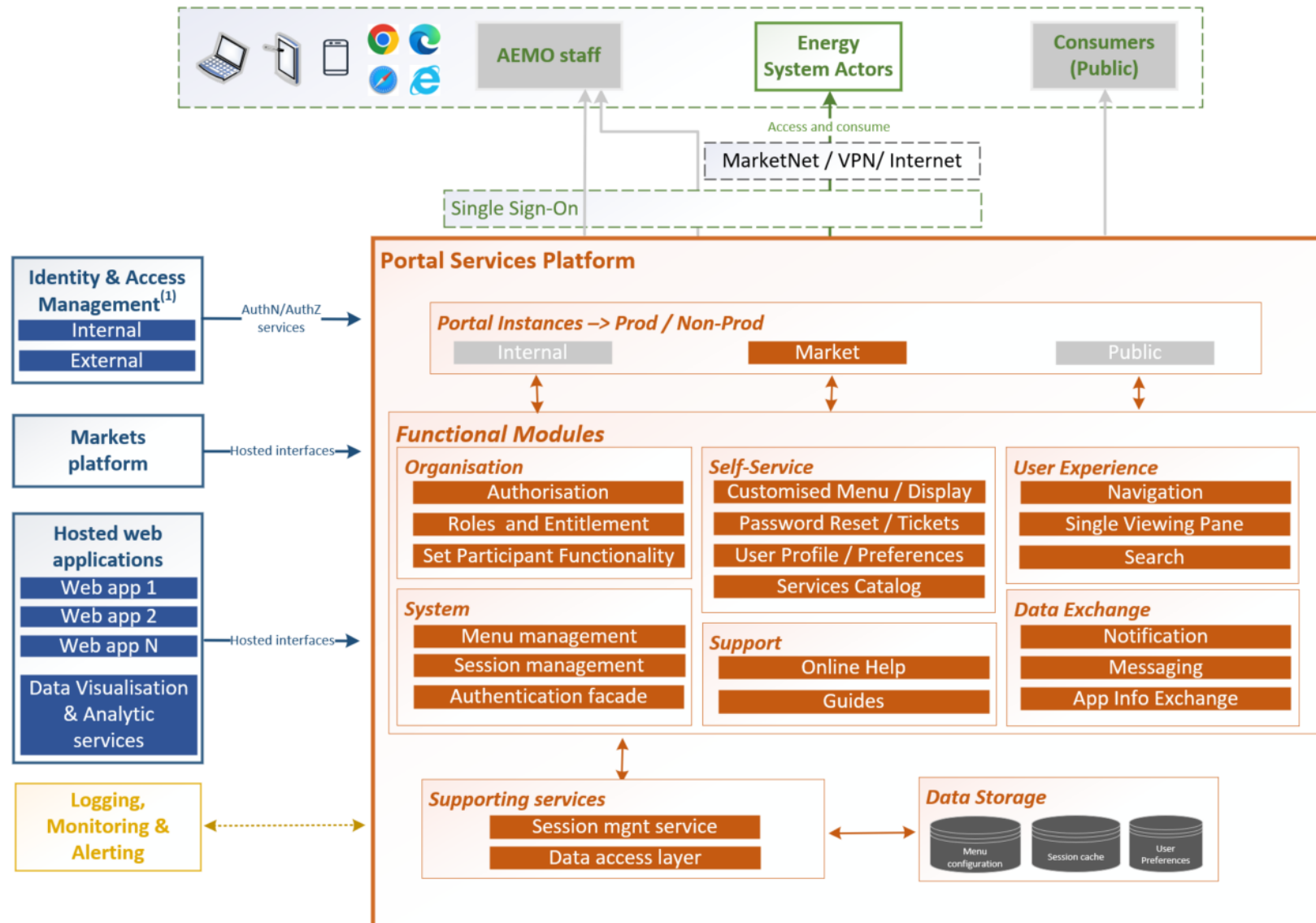
Solution Capability View
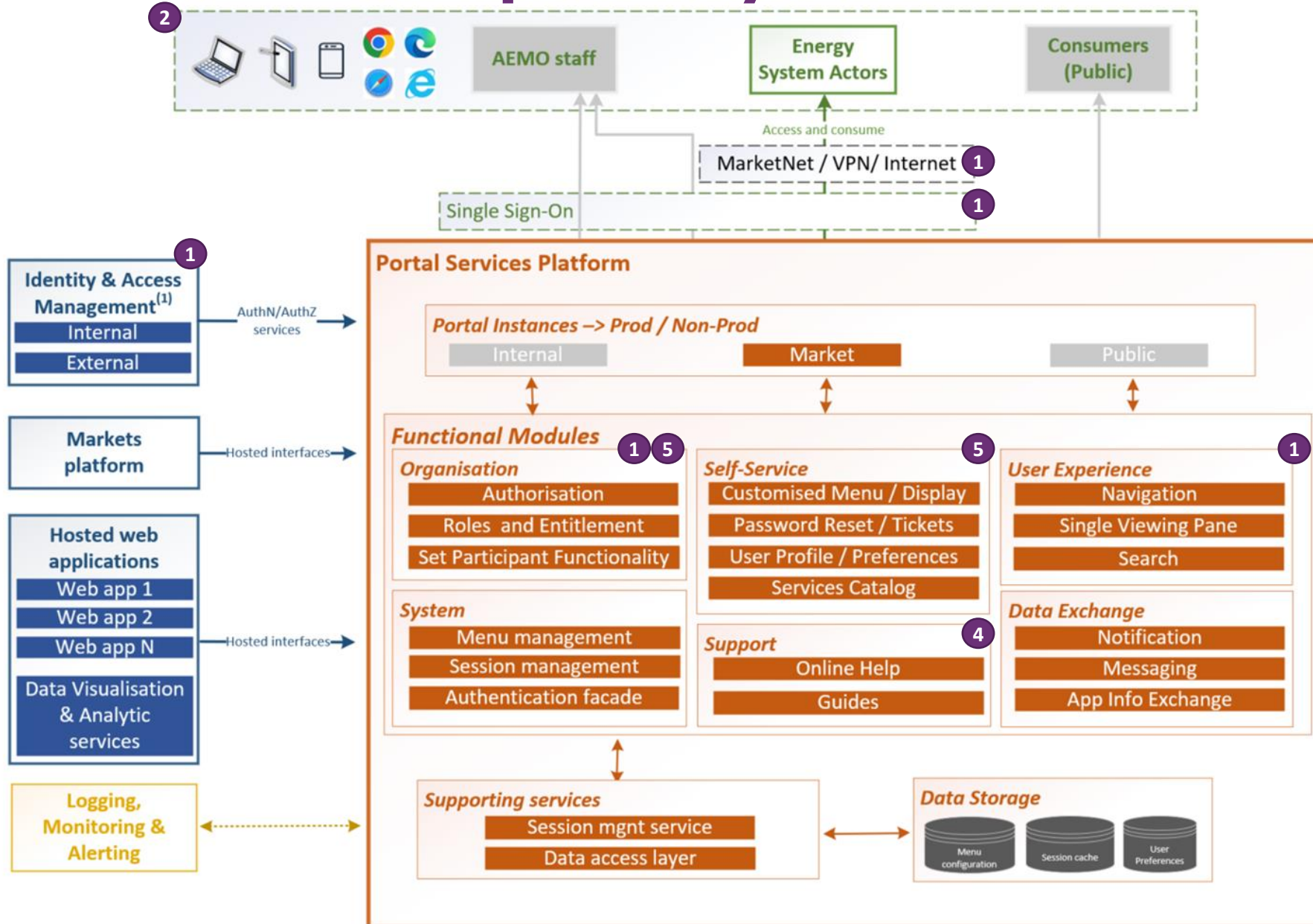
This **proposed capability view** indicates the areas the industry pain points will be addressed

KEY INDUSTRY PAIN POINTS

① **Disparate portals:** Browser services exposed over a disparate range of portals

② **Cross browser compatibility**: Endpoints and different devices support for browsers

③ **Cost Contributor:** Maintenance of the disparate portals

④ **Training, support, and documentation:** Inadequate resources

⑤ **Personalisation features:** inadequate features available on portal

PC - Next Steps

- AEMO's intention currently is to agree in principle a position on the target state collaboratively with industry and incorporate into the transition strategy and business case for IDX, IDAM and PC.
- A consensus position is sought with industry. Where there are diverging views, these will be acknowledged.

- AEMO is seeking feedback on the following questions:
    1. Are there any material gaps or concerns in the Target State requiring further consideration?
    2. With these definitions can you identify further benefits or impacts for industry of the proposed Target States?
    3. Do you have additional feedback to share on the consultation process in general?

- Feedback is due by 26 May to NEMReform@aemo.com.au.

5. Summary & close

Next steps

	March	April	May	June	July
Milestones	⭐ Intro Session	⭐ Discovery Workshop	⭐ Target State Discussions	⭐ Transition Strategy	⭐ Conclusion & business case ⭐ Publication of business case
IDAM	Discovery		Consultation		
Portal Consolidation	Discovery		Consultation		
IDX	Discovery completed 2021		Consultation		

Legend: ⭐ Milestone
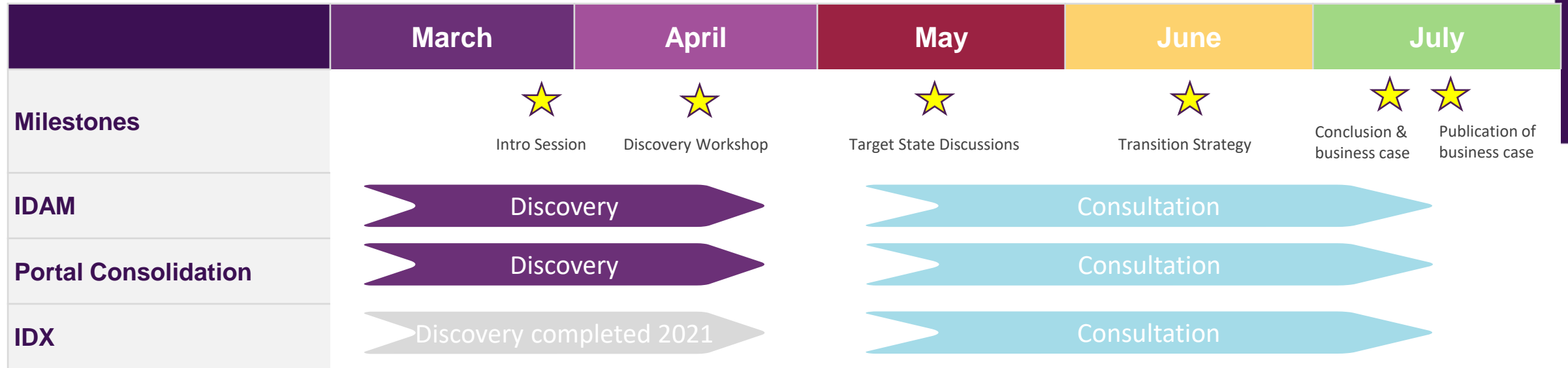
Recap - Ask of the Focus Group

- AEMO's intention currently is to agree in principle a position on the target state collaboratively with industry and incorporate into the transition strategy and business case for IDX, IDAM and PC.

- A consensus position is sought with industry. Where there are diverging views, these will be acknowledged.

> **AEMO welcomes any feedback from Focus Group members on this approach**

Request of the Focus Group

- Focus Group members to consider proposed target states for IDX, IDAM and PC and discuss with their internal colleagues.
- Focus Group members to provide additional feedback to AEMO, in response to the following questions:
    1. Are there any material gaps or concerns in the Target State requiring further consideration?
    2. With these definitions can you identify further benefits or impacts for industry of the proposed Target States?
    3. Do you have additional feedback to share on the consultation process in general?
    4. Initiative specific questions:
        1. For IDX initiative; what is your view of the IDX data payload options (slide 23)?
        2. For IDX initiative; do you see value in the potential flows (slide 27)?

Proposed actions

Activity	Responsibility	Timing
Focus Group members to further reflect on Target States set out in this pack, engage within their organisations as required, and provide any feedback as outlined in the ask of the Focus Group. Send to NEMReform@aemo.com.au	Focus Group members	26 May
AEMO to consider feedback and update Target State ahead of June Transition Strategy workshops.	AEMO	12 June
Focus Group members to consider what the transition may look like, given the target state concepts discussed, ahead of June Transition Strategy workshops.	Focus Group members	19 and 26 June

See you next at:
- Target state discussion for Business Focus Group on 22 May
- Transition Strategy discussions in June:
    - Technical Focus Group: 19 June 2023
    - Business Focus Group: 26 June 2023

Please reach out

NEMReform@aemo.com.au

AEMO | NEM Reform Foundational and Strategic Initiatives Focus Group

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.

Please visit: https://aemo.com.au/en/consultations/industry-forums-and-working-groups

Appendix B

Indicative workshop schedule

SESSION 2:

Dates	Purpose	Audience	Session Outline	Time [AEST] / Length
SESSION 2: Discovery Workshops – IDAM and Portal Consolidation				
17 April 2023	**Introduction: IDAM and PC**	**Technical and Business Focus Groups**	• Introduction and Objectives – IDAM and PC • Recap on IDX Discovery (pain points) • AEMO view of IDAM/PC pain points from internal workshop • Workshop outline	1:00 – 1:30pm (30 mins)
	Technical Discovery Workshops: IDAM	**Technical Focus Group** – IDAM	• Mural board walk through • Industry pain points workshop • Industry benefits workshop	1:30 – 3:00pm (1.5 hrs.)
	Business Discovery Workshops: IDAM	**Business Focus Group** - IDAM	• Mural board walk through • Industry pain points workshop • Industry benefits workshop	1:30 – 3:00pm (1.5 hrs.)
	COFFEE BREAK 3:00 – 3:15PM			
	Technical Discovery Workshops: PC	**Technical Focus Group** – PC	• Mural board walk through • Industry pain points workshop • Industry benefits workshop	3:15 – 4:15pm (1 hr.)
	Business Discovery Workshops: PC	**Business Focus Group** - PC	• Mural board walk through • Industry pain points workshop • Industry benefits workshop	3:15 – 4:15pm (1 hr.)
	Workshop Close	**Technical and Business Focus Groups**	• Summary • Next steps	4:15 – 4:30pm (15 mins)

SESSION 3A:

Dates	Purpose	Audience	Session Outline	Time [AEST] / Length
SESSION 3A: Target State Proposal for Technical Focus Groups				
15 May 2023	Introduction	Technical Focus Groups – IDX, IDAM, PC	• Introduction • Workshop outline	10:00 - 10:15am (15 mins)
	Target State Proposal for IDX	Technical Focus Group - IDX	• Concept walkthrough • Recap on Discovery workshop outcomes • Proposed Target State models • Feedback	10:15am – 12:15pm (2 hrs.)
	LUNCH 12:15 – 1:30PM			
	Target State Proposal for IDAM	Technical Focus Group – IDAM	• Concept walkthrough • Recap on Discovery workshop outcomes • Proposed Target State models • Feedback	1:30 – 3:00pm (1.5 hrs.)
	AFTERNOON TEA 3:00 – 3:15PM			
	Target State Proposal for PC	Technical Focus Group - PC	• Concept walkthrough • Recap on Discovery workshop outcomes • Proposed Target State models • Feedback	3:15 – 4:15pm (1 hr.)
	Session Close	Technical Focus Groups – IDX, IDAM, PC	• Summary • Next steps	4:15 – 4:30pm (15 mins)

SESSION 3B:

Dates	Purpose	Audience	Session Outline	Time [AEST] / Length
SESSION 3B: Target State Discussion for Business Focus Groups				
22 May 2023	Introduction	Business Focus Groups – IDX, IDAM, PC	• Introduction • Workshop outline	1:00 – 1:15pm (15 mins)
	Target State Discussion for IDX	Business Focus Group - IDX	• Concept walkthrough • Recap on Discovery workshop outcomes • Sample use cases – B2B, B2M, non-NEM • Feedback	1:15 – 2:30pm (1.25 hrs.)
	COFFEE BREAK 2:30 – 2:45PM			
	Target State Discussion for IDAM	Business Focus Group – IDAM	• Concept walkthrough • Recap on Discovery workshop outcomes • Sample use cases – B2B, B2M, non-NEM • Feedback	2:45 – 3:45pm (1 hr.)
	Target State Discussion for PC	Business Focus Group – PC	• Concept walkthrough • Recap on Discovery workshop outcomes • Sample use cases – B2B, B2M, non-NEM • Feedback	3:45 – 4:45pm (1 hr.)
	Session Close	Business Focus Groups – IDX, IDAM, PC	• Summary • Next steps	4:45 – 5:00pm (15 mins)

SESSION 4A:

SESSION 4A: Transition Strategy for Technical Focus Groups

Dates	Purpose	Audience	Session Outline	Time [AEST] / Length
19 June 2023	Introduction	Technical Focus Groups – IDX, IDAM, PC	• Introduction and objectives • Workshop outline	10:00 – 10:15am (15 mins)
	Transition Strategy, Impacts & Benefits – IDX and IDAM	Technical Focus Group – IDX Technical Focus Group – IDAM	**IDX:** • Enabling progressive transition • N -1 discussion • Sunset timeframe discussion • Propose principles for utilization **IDAM:** • Aligned with IDX & PC take up • Sunset timeframes Impacts & Benefits of IDX and IDAM initiatives – Technical view	10:15am – 12:30pm (2.25 hrs.)
	LUNCH 12:30 – 1:30PM			
	Transition Strategy, Impacts & Benefits - PC	Technical Focus Group – PC	**PC:** • Align to initiatives • Sunset timeframes Impacts & Benefits of PC initiative – Technical view	1:30 – 2:45pm (1.25 hrs..)
	Session Close	Technical Focus Groups – IDX, IDAM, PC	• Summary • Next steps	2:45 – 3:00pm (15 mins)

SESSION 4B:

Dates	Purpose	Audience	Session Outline	Time [AEST] / Length
SESSION 4B: Transition Roadmap for Business Focus Groups				
26 June 2023	Introduction	Business Focus Groups – IDX, IDAM, PC	• Introduction and objectives • Walkthrough of the principles for NEM2025 • Overview of the IDX, IDAM and PC Transition Roadmap	1:00 – 1:30 (30 mins)
	Transition Roadmap, Impacts & Benefits – IDX and IDAM	Business Focus Group – IDX Business Focus Group – IDAM	• Present Roadmap for IDX and IDAM aligned to NEM2025 • Present Impacts and Benefits – Business view	1:30 – 3:30pm (2 hrs.)
	COFFEE BREAK 3:30 – 3:45PM			
	Transition Roadmap, Impacts & Benefits – PC	Business Focus Group – PC	• Present Roadmap for PC aligned to NEM2025 • Present Impacts and Benefits – Business view	3:45 – 4:45pm (1 hr.)
	Session Close	Business Focus Groups – IDX, IDAM, PC	• Summary • Next steps	4:45 – 5:00pm (15 mins)

SESSION 5:

Dates	Purpose	Audience	Session Outline	Time [AEST] / Length
SESSION 5: Conclusions and Business Case				
10 July 2023	Conclusions & Business Case	Business Focus Groups – IDX, IDAM and PC	• Introduction and re-cap of Sessions 3 and 4 • Present key options – Incremental upgrade vs Early Transition • Recommendations and considerations • Session close	1:00 – 3:00 pm (2 hrs.)

Appendix C

IDX Proposed Principles - Summary

Inbound (Inquiry) Decision trees

Outbound Decision Trees

IDX Target State - AEMO IDX Environment

Sender's Systems (Spoke)
- AEMO Supplied Data Exchange Software
- Participant Gateways

Recipient's Systems (Spoke)
- AEMO Supplied Data Exchange Software
- Participant Gateways

Protocols ● ● ● ●   ● ● ● ●   ● ● ● ● Protocols

| Channel 1 | Channel 2 | Channel n |

Message Exchange Patterns

- Transport Layer Security (eg: IPS ,IDS detection)
- Authentication & Authorisation
- Policy Enforcement (e.g. Throttling)
- Transaction Logs
- Non-Repudiation & Archiving

AEMO Hub
- Enforce Procedural Definitions
- Payload Validation & Translation
- Orchestration & Routing
- Fan-in & Fan-out
- Message Enrichment (e.g. B2M in B2B)
- Data Insights & Reporting
- Data Virtualisation & Visualisation
- Data Security & Governance
- Data Catalogue & Definitions
- eHub Technical & Audit Logs

IDAM

AEMO's Data Exchange Environment

AEMO Systems (Spoke)
- Business Data Authorisation (e.g. Parties who could submit offers for the DUID)

| NEM | WEM | STTM | DWGM | B2B Responder | Retail B2B Integration |

IDX Environment Capabilities	
Term	**Definition**
Transport Layer Security	Security in transit measures shall be taken to protect data during transmission over the IDX Environment.
Authentication & Authorisation	Only authenticated and authorised users shall access the endpoint in the IDX Environment.
Policy Enforcement	To prevent overuse and abuse of the IDX Environment, which can lead to degraded performance, increased costs, and security risks, throttling policies shall be enforced to limit the number of data requests that can be made over a given period.
Transaction Logs	Exchange Technical Transaction Logs shall provide complete visibility of data transferred over the data exchange environment by enabling stakeholders to view an audit trail of data delivery.
Non-Repudiation & Archiving	Data exchanged between Initiators and Recipients through an IDX Environment shall be archived for future reference and accompanied by non-repudiation methods to provide evidence that either party cannot deny.
Enforce Procedural Definitions	AEMO shall be able to enforce compliance with Procedural definitions of the Market data required for business processes defined in Rules or Procedures.
Payload Validation & Translation	AEMO shall be able to validate supplied data and formats, sending back the appropriate response.
Orchestration & Routing	AEMO shall provide data orchestration services to coordinate, standardise and manage data flow across different systems, applications, and Market services.
Fan-in & Fan-out	AEMO shall support fan-in and fan-out data exchange, collecting data from multiple stakeholders/systems and bringing it together into a single destination or distributing data from a single source to multiple stakeholders/systems.
Message Enrichment	AEMO shall utilise its role as a host of Energy standing data to offer message enrichment, providing additional information, context, or Market value during data exchange.
Data Insights & Reporting	AEMO shall offer various reporting services to access reporting data through the Request/Response, Large Data, or Inquiry Services message patterns.
Data Virtualisation & Visualisation	Stakeholders shall be able to access the data they are entitled to, deriving valuable information and knowledge from that data through analysis, interpretation, and visualisation.
Data Security & Governance	AEMO shall provide mechanisms that support stakeholders' compliance with their Market obligation to protect sensitive and confidential data.
Data Catalogue & Definitions	A data catalogue shall be employed to provide a centralised and organised view of energy data to promote a shared understanding of Industry data assets and reduce the risk of misinterpretation.
Hub Technical & Audit Logs	The IDX Environment shall provide technical and audit logging to provide insights into data exchange processes.

IDX Proposed Principles - Summary

Core Principle	Proposed Principle
1. AEMO to simplify IDX offerings to the stakeholders	Uninterrupted business services across the market and Procedural change.
	Process consuming inquiry services that have no dependencies on new data introduced via Procedural change should not need to be updated.
	Uninterrupted business services across the market and Procedural change.
	Process consuming inquiry services that have no dependencies on new data introduced via Procedural change should not need to be updated.
2. AEMO shall ensure stakeholders can optimise message processing.	Minimise ongoing IT change for stakeholders in the data delivery processes while reducing costs and efforts associated with the transition to IDX.
	Empower stakeholders with the ability to prioritise the order of data delivery, providing maximum control over the data reception process.
	Provide near real-time visibility of critical market transactions.
3. AEMO IDX offerings to accommodate Procedural change while minimising impacts to Roles not mandated to change.	Stakeholders not impacted by a Procedural change should not be required to perform updates to their market integration solutions.
	Uninterrupted business services across the market and Procedural change.
	Process consuming inquiry services that have no dependencies on new data introduced via Procedural change should not need to be updated.
4. AEMO shall provide optional software to reduce the cost of IDX.	Unified AEMO-supplied data exchange software must support the proposed IDX data exchange channels, protocols and patterns across markets
5. Security.	Alignment to IDX cyber best practices.

Decision Tree – Inquiry Services

	Pattern	Payload Size	Latency	Frequency	Channel	Example
INBOUND Inquiry Services	SYNC	Low to Ceiling	Medium	Any	RESTful APIs (Payload: JSON with graphQL)	NMI Discovery
	ASYNC	Low to Ceiling	Medium	Any	RESTful APIs (Payload: JSON with graphQL)	MSATS RM Reports

Decision Tree – Outbound

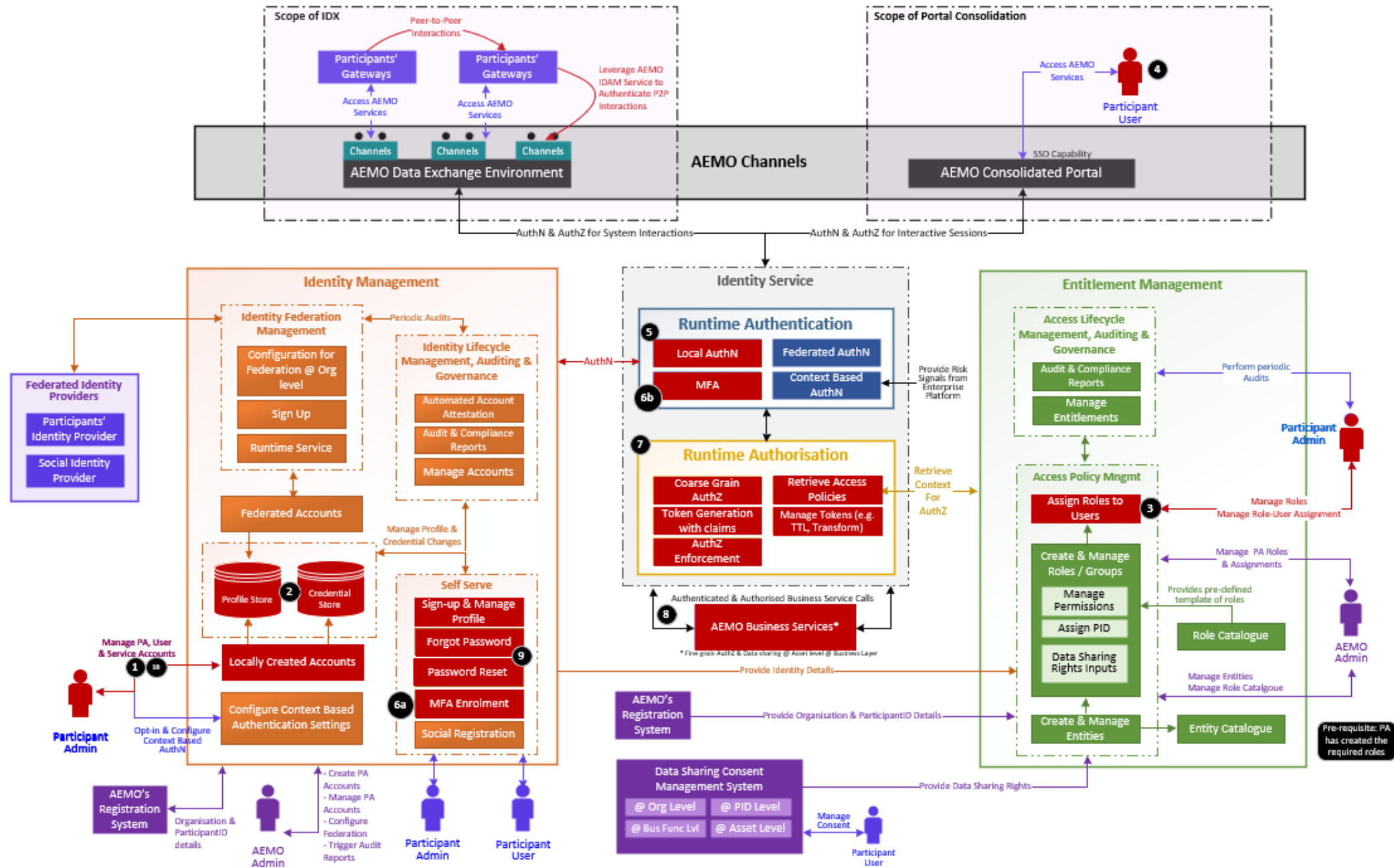| Pattern	Payload Size	Response Latency	Frequency	Channel	Example
SYNC	Low to Ceiling	Any	Any	**RESTful APIs**	Current Wholesale Bids & offers
ASYNC PULL with Event Notification Service	Low to Ceiling	Medium	Any	**RESTful APIs**	Dispatch Instructions
	Large	Any	Any	**Large File sharing Framework**	TBC
Fire & Forget	Low to Ceiling	Low	High	**Stream**	TBC
	Medium	Any		**RESTful APIs**	PQ Data
	Large	Any	Any	**Large File sharing Framework**	TBC

OUTBOUND Transaction Submissions

Appendix D

IDAM Example Workflows for the Conceptual Target Solution

IDAM Key Definitions

Management of Local User Account

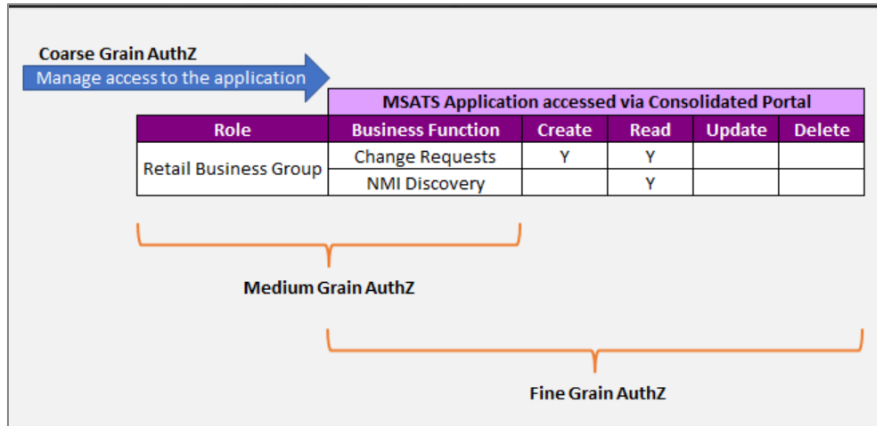| Step	Description
Pre-requisite	The PA has already created all the roles that are required.
1	The PA can create users individually or leverage the bulk provisioning feature of the identity administration layer.
2	Person accounts can be locally created. It will populate the credential and profile stores.
3	The PA can assig the role to the user accounts available in the credential store.
4	The users can then access the portal services through their browsers.
5	The identity service identifies the incoming identity as a locally managed identity and forwards it to the local credential store for authentication.
6a	The users have to enrol for the MFA when logging in for the first time.
6b	The users will be prompted for the MFA during subsequent logins.
7	Coarse-grained authorisation is applied based on the user attributes and presented with the screen relevant to their profile.
8	Access privileges related to the user are retrieved and fine-grained access is enforced through appropriate access token which the participant user uses to access the authorised entities.
9	The users will have self-serve capabilities.
10	The PAs are provided with the capabilities to manage the deprovisioning of user accounts when they leave the organisation.
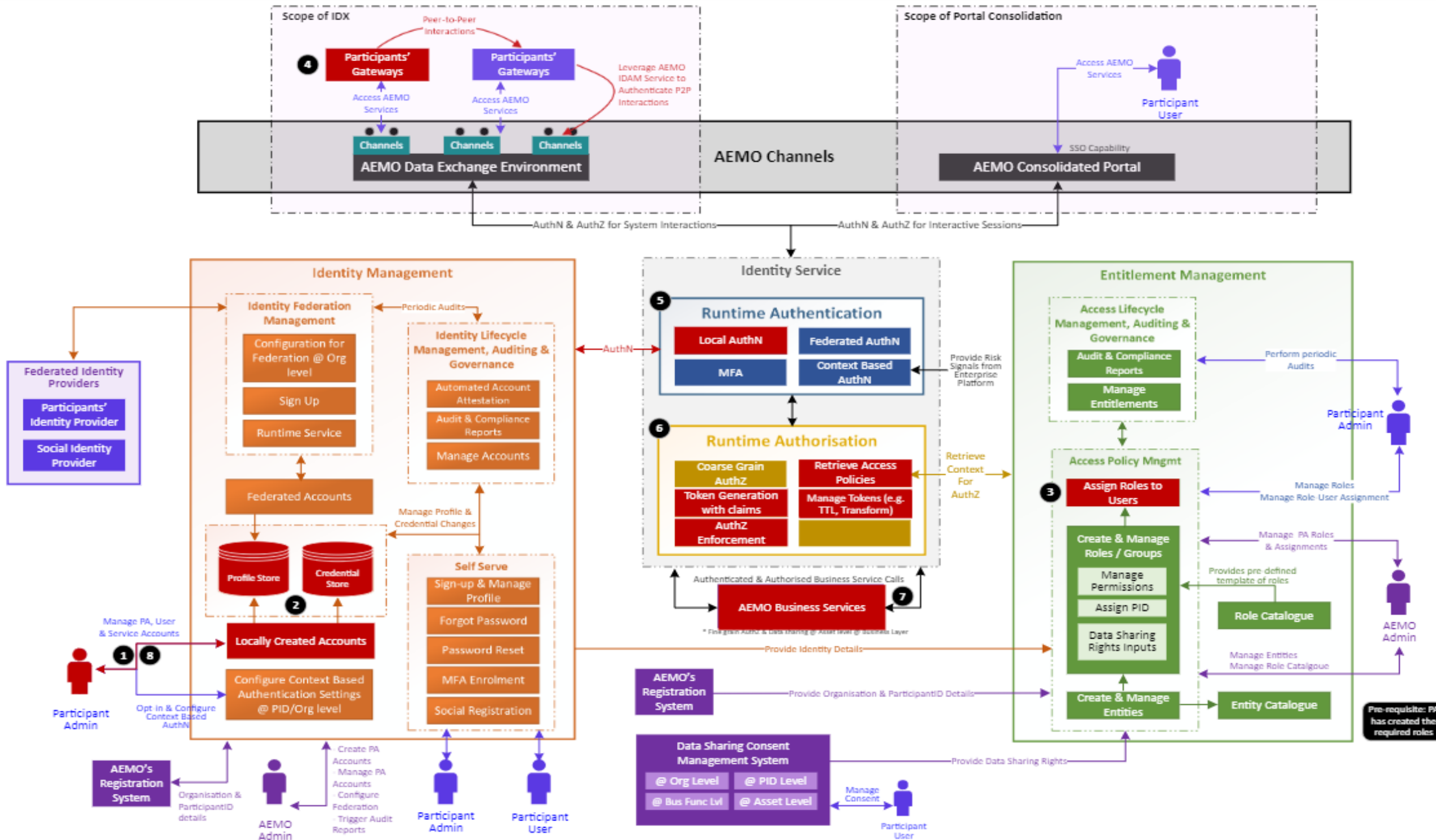
Management of Service Account

Step	Description
Pre-requisite	The PA has already created all the roles that are required.
1	The PA can create the service account.
2	Service Accounts can only be locally created. It will populate the credential store.
3	The PA then assigns the role to the service accounts available in the credential store.
4	The PA can configure their API gateway.
5	The Identity service identifies the incoming identity as a non-person entity or service account and forwards it to the local credential store for authentication.
6	The identity service identifies the incoming identity as a non-person entity or service account and, after validation, forwards it to the authorisation layer for token issuance.
7	Access privileges related to the service account are retrieved and fine-grained access is enforced through an appropriate access token, which the participant uses to access the authorised entities.
8	The PAs are provided with the capabilities to manage the deprovisioning of the service account.

IDAM Key Definitions

Subject	Definitions
Coarse grained authorisation	Coarse grained authorisation is enforced to an end user gaining access to an application e.g. the ability to limit access to a specific application (e.g. 'MSATS application') in the consolidated portal
Medium grained authorisation	Medium-grained authorisation is enforced through Role or Group membership to constrain what an end-user can attempt to perform without taking into consideration the actions the user may be granted on the resource(s) e.g. Role 'Retail Business Group' having access to 'Change Request' processes
Fine grained authorisation	Fine-grained authorisation constrains what actions an end-user can perform based on the role and resource level entitlements. E.g user assigned to role 'Retail Business Group' can retrieve the submitted change requests and submit new change requests
Entity Catalogue	An entity catalogue is a suite of atomic business functions that can be assembled into one or more roles.
Context-Based Authentication	Context based authentication is a method of applying a set of configured policies that will step up (e.g. MFA) or grant or deny access to the resources by determining the risk level of the user login/session. e.g. Prompting a user for MFA if the access request is originating from an IP address different to historical network traffic
Federated Identity	Federated identity refers to the process of allowing users to use the same digital identity across multiple domains and organizations. In simpler terms, it allows users to authenticate themselves with one organization and then use that same authentication to access services and applications from other organizations without having to create a new account or login credentials.
Multi-Factor Authentication (MFA)	Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
Participant Admin (PA)	Participant Administrator. Super-users who manage and perform system administration tasks for their own organisation's participant users.