Market Interface Technology Enhancements Working Group (MITE WG)

IDAM Only Session

Wednesday 5 September 2024

(2:00pm to 5:00pm)

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:

- Re-Cap of Target State Concepts
- IDAM Capabilities, Terminology and Definitions
- Re-Cap of Target State Architecture

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 to concepts, architecture, capabilities, terminology and definitions
- Leverage the materials referenced from the prior FASI working group on which this pack has been developed.
- 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	2:00pm-2:05pm	Welcome	Blaine Miner
2	2:05pm-2:10pm	Actions	Blaine Miner
3	2:10pm-2:30pm	Focus Group update	Andrew Bell
4	2:30pm: 2:50pm	Identity and Access Management Overview • Scope • Pain points and architecture principle • Capabilities Definitions • Target State Concepts	Andrew Bell Manesh Karunakaran
5	2:50pm-3:20pm	Identity management Terminology and Concept	Sivaraj Ganesan Manesh Karunakaran
6	3:20pm-3:35pm	Authentication Terminology and Concept	Sivaraj Ganesan
7	3:35pm-4:05pm	Entitlement Management • Terminology and Concept • Worked Example	Satheesh Kumar Phil Hayes
8	4:05pm-4:35pm	IDAM Conceptual Architecture IDAM Architecture worked example	Manesh Karunakaran Satheesh Kumar
9	4:55pm-4:45pm	IDAM Transition Strategy Overview	Nirmal Narayanamurthi
10	4:45pm-5:00pm	General Business and Next Steps	Blaine Miner
	Appendix	Appendix A: AEMO Competition Law Meeting Protocol, Appendix B: Upcoming focus group topics Appendix C: Workflow Examples	

2. Actions

Blaine Miner

Actions

Description	Responsible	Status	Comments
AEMO to include the link to the MITE webpage as part of the notes	AEMO	Closed	Link was provided in the August meeting notes
Confirm exact dates and lengths supporting the Sept and Oct IDX and IDAM FG sessions	AEMO	Closed	Session details have been provided in this pack.
Add a third column to the 'Proposed Future Topics' slides, to indicate which month a topic is proposed to be discussed	AEMO	Open	Slide has been added to this pack and will be presented during the session
Sept and Oct IDX and IDAM external FG nominations close Friday 16 Aug	WG Coordinators	Closed	Thank you for considering and submitting your organisation's nominations.

3. Focus Group update

Andrew Bell

Focus Group update

- AEMO called for nominations for the 4 initial Focus Groups at the last MITE WG meeting
  - IDX: Decision Tree Focus Group **and** IDX Asynchronous and Event Notification Group
  - IDAM: API Authentication & Authorisation Patterns **and** Organisation Hierarchy Use Cases

- We genuinely appreciated the time, consideration, and the quality of the nominations we received.

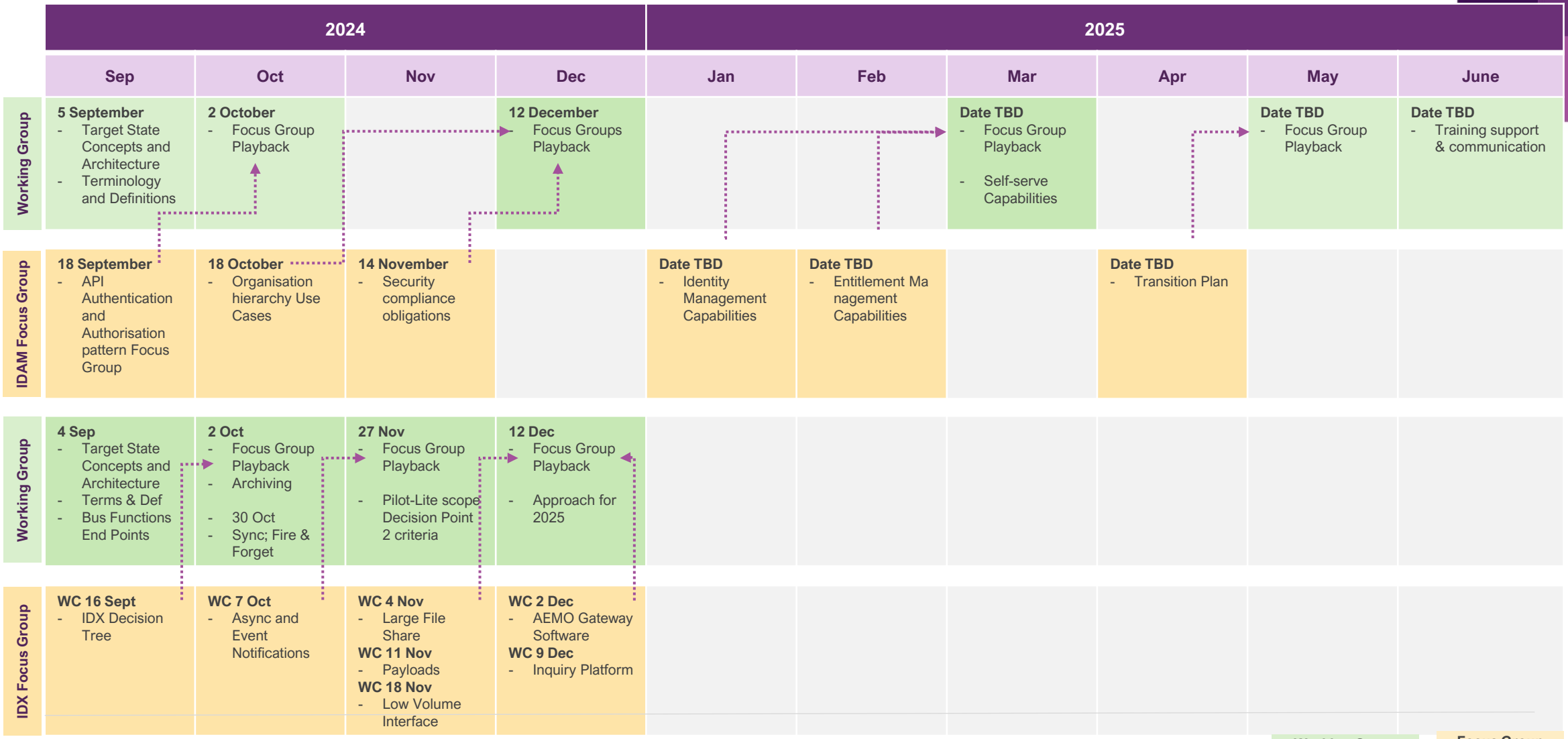
- To enable the Focus Groups to be as efficient and effective as possible, based on our previous experiences (and our preference to have face-to-face sessions), AEMO capped attendance to 12-13 representatives.

- AEMO received 30-40 nominations from almost 20 organisations for each of the four Focus Group topics, and in many cases received multiple nominations from the same organisation.

- We regretted that some of your nominations would not be able to contribute directly to the FGs, but we are committed to ensuring that every WG organisation will have the opportunity to contribute and provide feedback at the WG meetings when the FGs present their draft materials.

- In determining the proposed FG attendees, AEMO sought to balance:
  - representation across participant types and
  - ensuring the required skill mix to support each topic.

Strawman Timeline for upcoming IDAM / IDX Sessions



*These proposed dates are indicative dates

Legend *WC: Week Commencing* **Working Group Sessions** **Focus Group sessions**

4. Identity and Access Management Overview

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

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.

Establishing the foundational Capabilities

The technical capabilities of the Target state foundation are intended suitable for all energy markets: NEM, WEM and Gas involving AEMO external interactions

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

Transitioning | **New Business Services**

MITE scope does include the transition of NEM identity and entitlement services involving AEMO external interactions. Transition of WEM, gas and any other market would require a separate business case to establish and agree a transition strategy.

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

Architectural Design Principles

- AEMO will provide a **unified Identity and Access Management Platform** 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

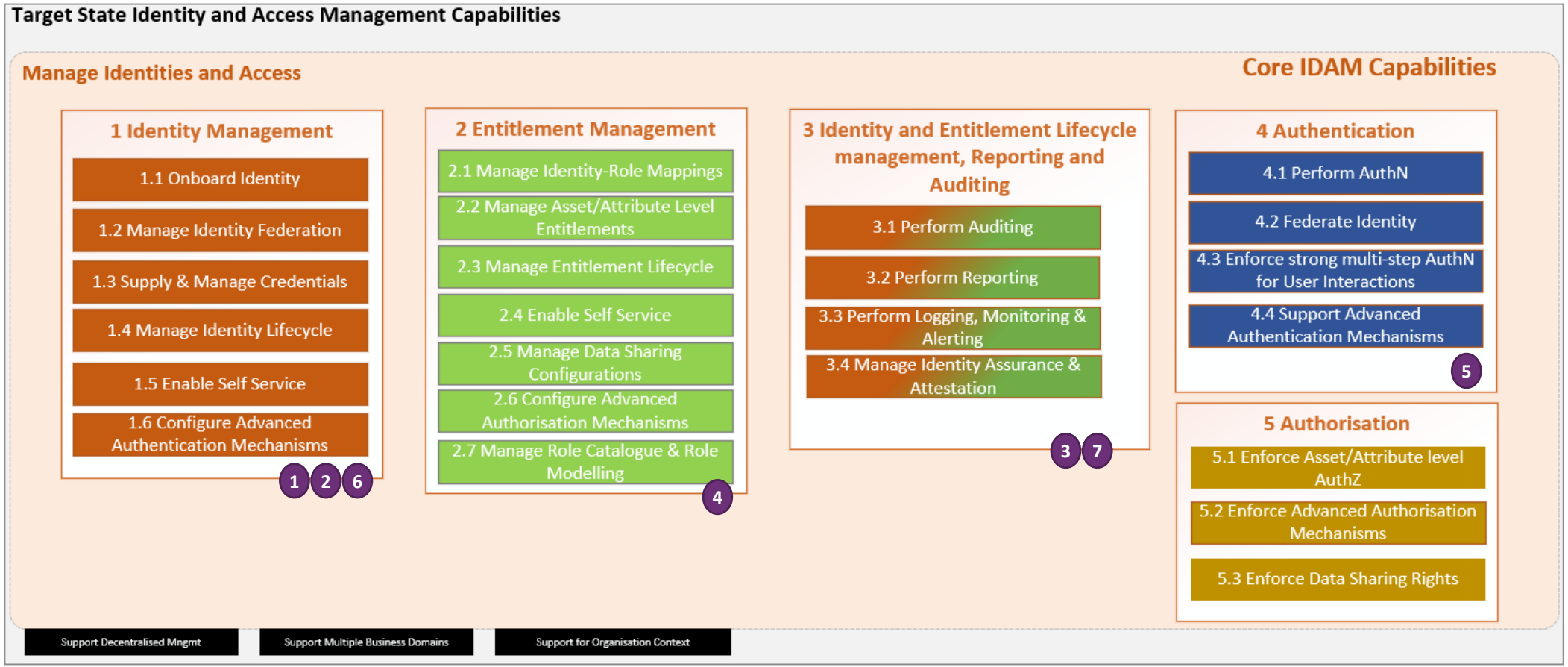
- AEMO will provide a **highly flexible access control mechanism** using **attribute-based access control**
  - Enables the stakeholders to define access control policies in a more flexible, user-friendly business language
  - Support for the definition of **more granular access control policies** based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

IDAM Capabilities: Definitions

IDAM for Market Interfaces refers to a technical framework and a set of processes that govern the management of digital identities and the control of access to AEMO's market systems. This IDAM platform is also a step towards compliance with the SOCI Act, ensuring that the access to critical energy infrastructure is tightly controlled and monitored.

Identity Management	Entitlement Management	Reporting and Auditing	Authentication	Authorisation
Identity Management (IdM) refers to the processes, policies, and technologies used to manage and control the digital identities of individuals, devices, or applications within an organisation or network.	Entitlement Management refers to the process of managing and controlling the assignment, monitoring, and auditing of access rights or permissions within an organisation's IT environment.	Reporting and auditing are critical processes that ensure transparency, accountability, and compliance in the management of digital identities, access rights, and entitlements across an organisation.	Authentication is the process of verifying the identity of a user, device, or system before granting access to a resource or service.	Authorisation is the process of determining and granting permission or access rights to a user, system, or entity to perform certain actions or access specific resources within a system or network.

IDAM Capabilities



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

High-Level IDAM Target State Concepts

- Organisation Admin
- Identity Federation
- New Self Service Capabilities

- Introduction of Entity and Role Catalogue
- Advanced Data Sharing

- Multi-Factor Authentication
- Context based Authentication
- Advanced Authorisation Mechanism

- Advanced reporting and auditing

Notes

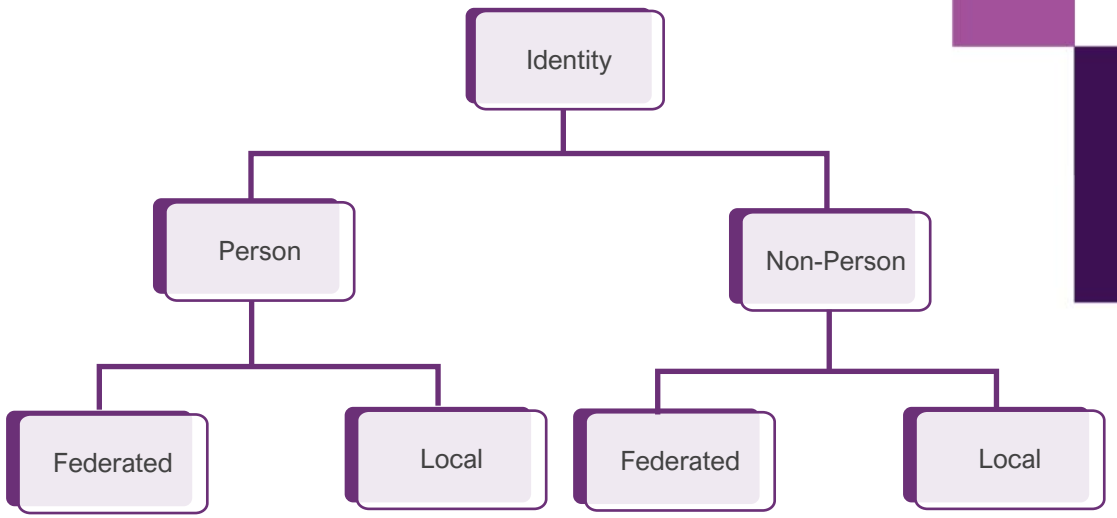
- Andrew Bell spoke to the Identity and Access Management Scope and pain points slides.
- Andrew:
  - Emphasised that IDAM initiative scope does include the transition of NEM identity and entitlement services involving AEMO external interactions. (Unlike IDX)
  - Did a re-cap of the Pain points that were captured as part of the industry consultation across NEM, WA and gas markets.
  - Noted that AEMO has created a MITE webpage which provides access to all the key information and artefacts developed during the business case phase
    AEMO | Market Interface Technology Enhancements

- Manesh Spoke to the IDAM Capabilities Definitions and provided high-level overview of the target state concepts

5. Identity Management Terminologies and Concepts

Identity Management Terminologies

- **Identity :** Identities refer to digital identities that are recognised and authenticated within a system or organisation. Identities can be categorised into two types:
  - **Person / individual Identity** – Person / individual identity refers to an identity that is associated with a human user.
  - **Non-person Identity** (e.g., service accounts, system accounts) - Non-person identities are identities that are associated with a non-human user – like a system, application, or service.



As part of the new IDAM framework AEMO would be allowing two types of Person and Non-Person identities access to AEMO systems.

- **Local Identity** – this refers to identities that are created, managed and issued to participant users and systems from AEMO's External Identity and Access Management System (similar to URM).
- **Federated Identity** – this refers to identities that are created, managed and issued to participant users and systems from their own organisation Identity and Access Management System , which are allowed to access and consume AEMO resources through federated trust

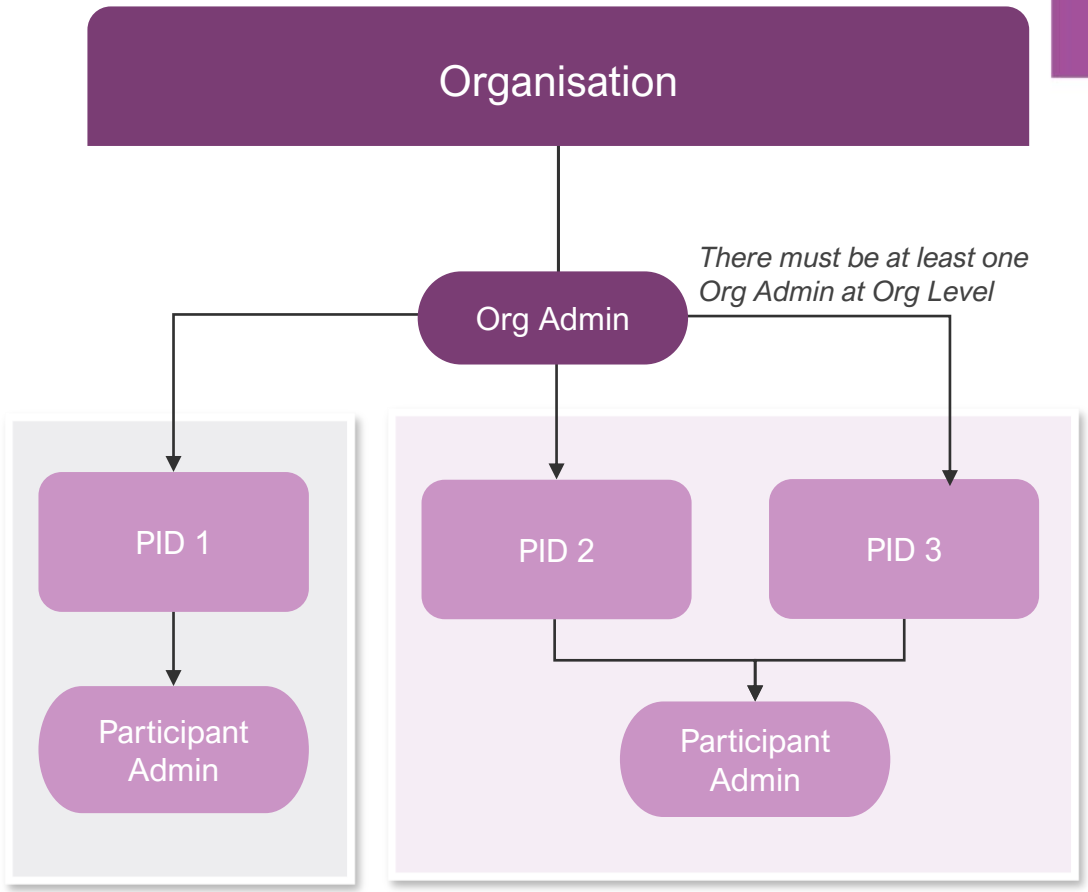
Identity Management Terminologies

- **Organisation:** An organisation comprises a collection of related entities, each assigned a unique Participant ID (PID).

- **Participant Id (PID):** Reference to a Registered participant, or energy stakeholder; A company can have more than one Participant ID registered with AEMO.

- **Organisation Administrator:** An Organisation Administrator is an admin user who is authorised to manage the access and entitlements for all person and non-person identities within that organisation to AEMO services.
  This role includes overseeing association of those identities with one or more of the Participant IDs within the Organisation.

- **Participant Administrator:** Participant Administrator is an admin user is authorised to manage the access and entitlements for all person and non-person identities within that Participant ID to access AEMO services.
  This role includes overseeing association of identities to Participant IDs for which the PA holds an association with



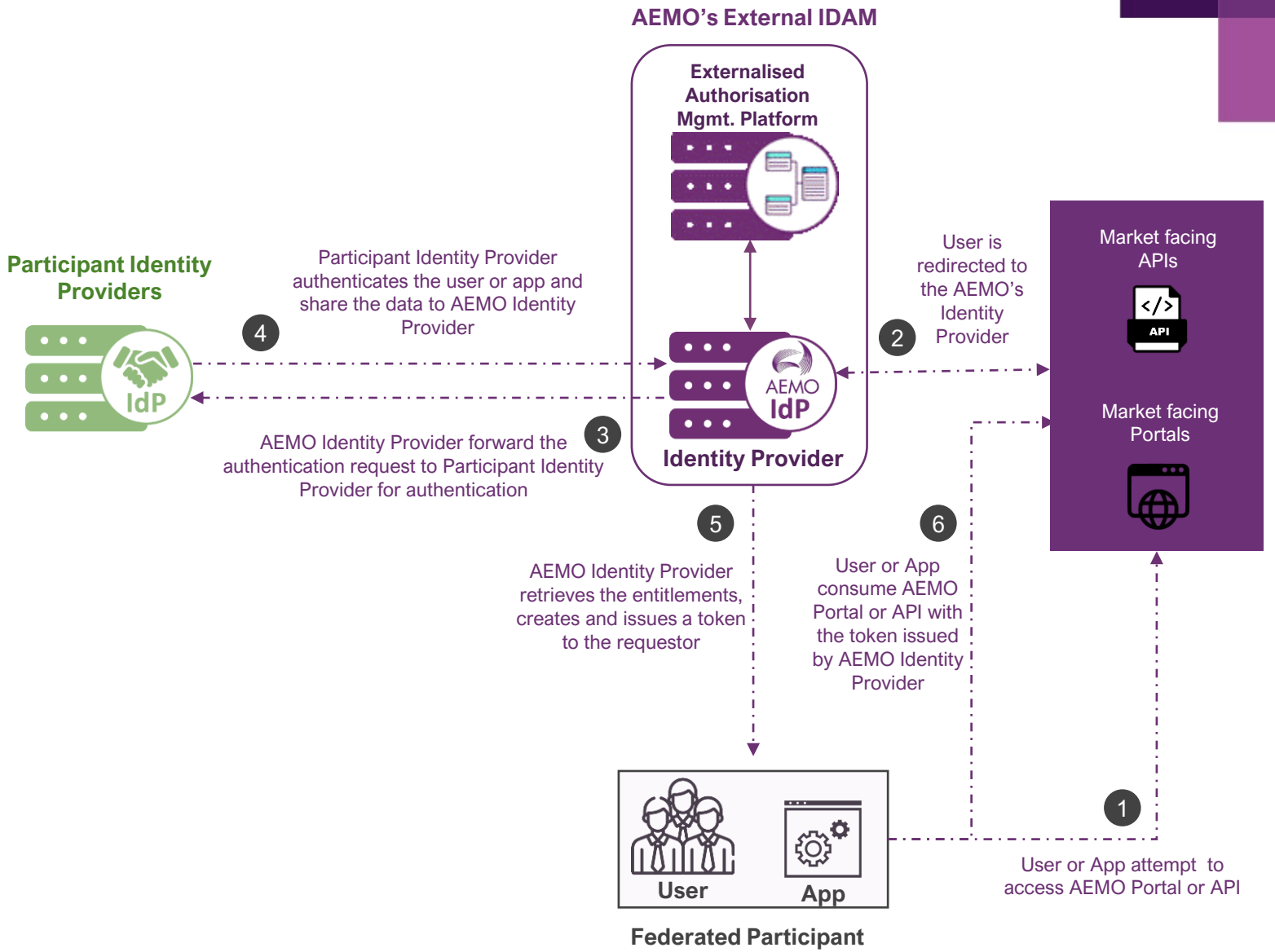
Identity Federation / BYO Identity

Identity federation allows users to access multiple systems or services by different organisations using a single, centralised set of credentials, typically provided by their organisation.

To configure identity federation with AEMO, participants would need to configure their Identity Systems to establish mutual trust with AEMO's Identity Systems and enable synchronisation of user metadata and permissions with the Market IDAM Platform. To ensure the security of market operations, AEMO may impose certain restrictions on how federation could be configured.

Once configured, participants' users will be able to access AEMO systems using their work credentials.

Additionally, the Identity Federation capabilities will introduce a feature called Right Sync, which will allow Participant Administrators to manage user permissions for accessing AEMO systems within the participant's own identity systems. These permissions will be automatically synchronised with AEMO's Identity Systems.



Notes

- Manesh Karunakaran introduced the new role: Org Admin
- Sivaraj Ganesan introduced the new concept of Identity Federation
- Siva noted a use case where a user previously had access to AEMO but moved to another team where they no longer need access to AEMO.
- Siva also mentioned that in-depth discussions regarding identity federation will be held during future focus group sessions

6. Authentication Terminologies and concept

Multi-Factor Authentication

Multi-Factor Authentication:

Multi-factor Authentication (MFA) is an authentication approach that requires the user to provide two or more verification factors to gain access to a resource such as web portal.

- By requiring multiple factors, MFA significantly reduces the likelihood that an unauthorised user can gain access to an account or system, even if one factor (like a password) is compromised.

Some of the factors used in MFA generally are:

- **Something You Know**: This typically includes passwords, PINs, or answers to security questions.
- **Something You Have**: This involves a physical device that you possess, such as a smartphone, hardware token, or security key.

MFA Enforcement

- For locally managed user accounts, AEMO's External Identity Provider will provide the MFA capability.
- For Federated accounts, the participant Identity provider will be responsible for enforcing MFA.

Example of Two-Factor authentication

High level MFA Process Flow

Participant user enters their password to the portal

If the credentials are valid, user prompted for second authentication factor

If successful, user provided access to the portal or authorised resource

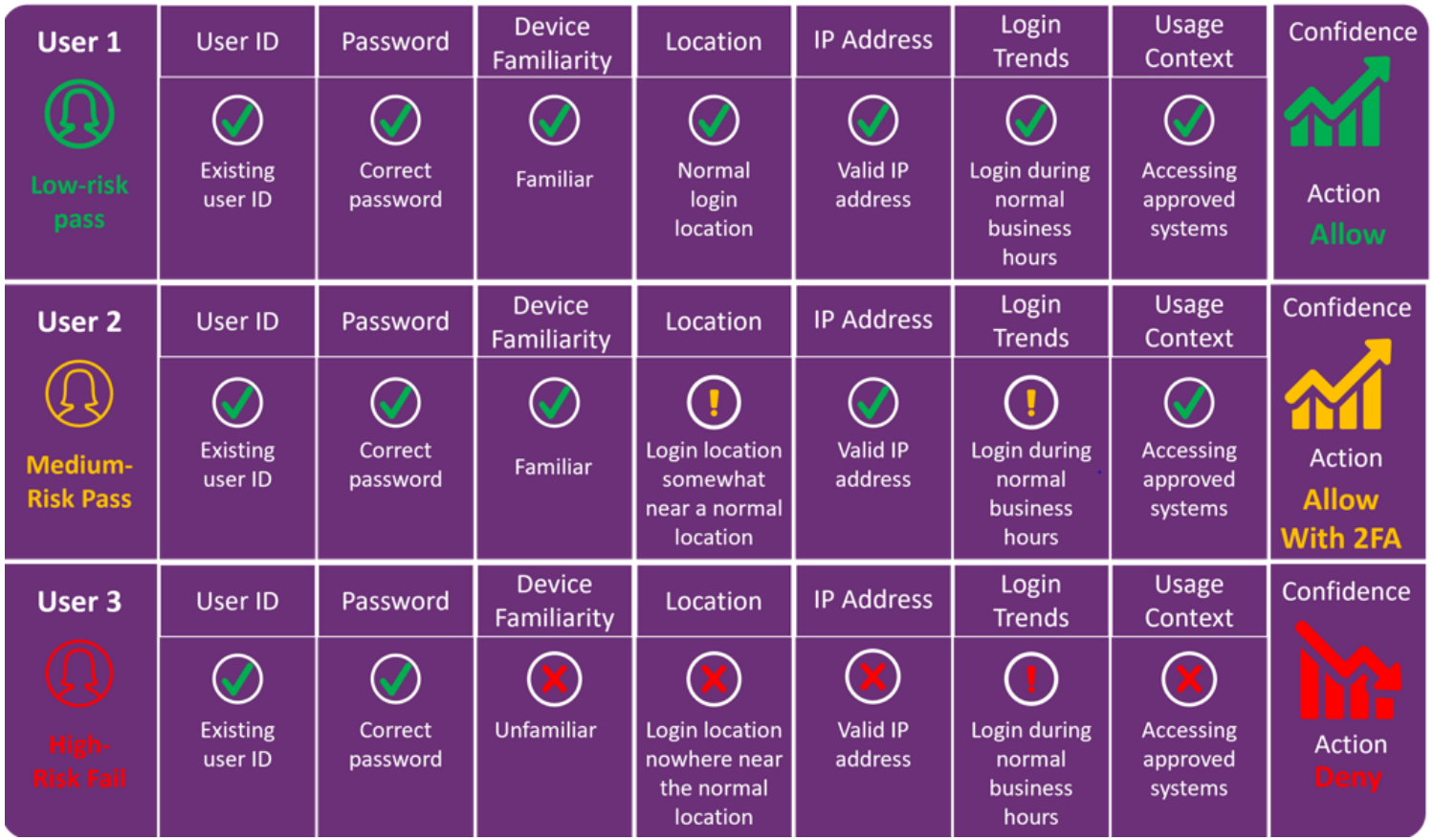
Context Based Authentication

Context Based Authentication

Risk-based or Contextual Authentication is a security mechanism that assesses the risk associated with a user's login attempt based on various contextual factors, such as the user's location, device type, and behaviour.

The authentication system uses this information to determine the appropriate level of authentication required for the user.

For example, if the system detects a login attempt from an unusual location or device, it may require additional forms of authentication, such as a security token or biometric data. Conversely, if the system detects a login attempt from a trusted location or device, it may only require a password.



This is image has been developed for illustration purposes only, further details will be discussed during future focus group sessions.

Notes

- Sivaraj Ganesan introduced two new Target state concepts, Multi-factor Authentication and Context Based Authentication
- Siva noted that context-based authentication is advanced capability and will be enforced via policy and guidelines.
- Siva noted that further details around these topics will be discussed during upcoming focus group sessions

7. Entitlement Management Terminologies and Concepts

Entitlement Management Terminologies

Entity: Entities are the individual components or building blocks that represent individual pieces of functionality within applications (for example, Ability to perform actions on FCAS Bids). Entities can be of type “batch” (using the Batch Handlers) or “interactive” (using AEMO’s web portal).

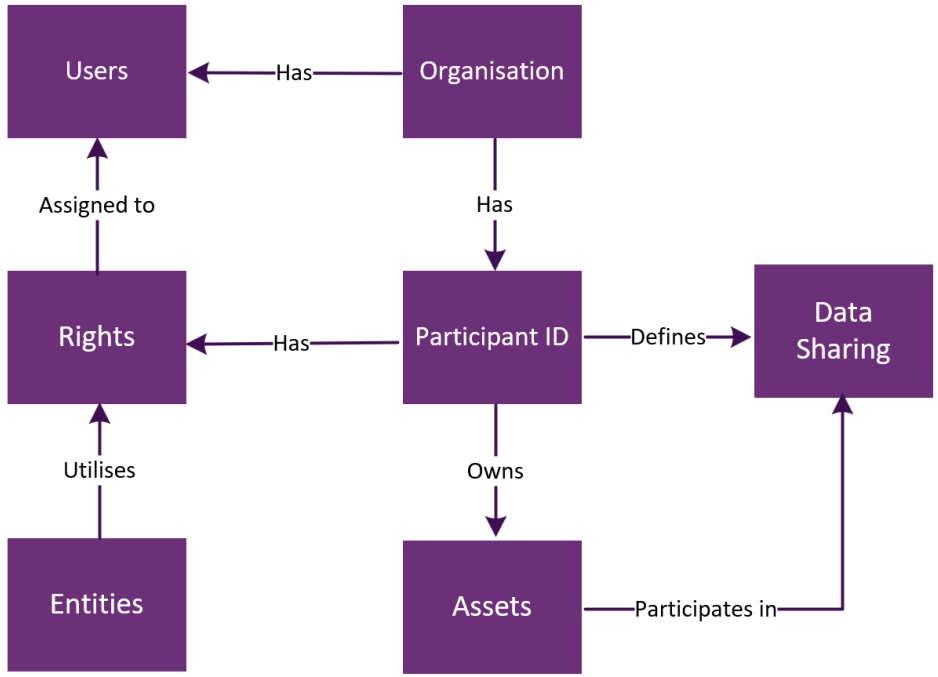
Entity Catalogue: The Entity Catalogue is a searchable catalogue of Application Functions / Entities. It allows Participant Administrators to efficiently locate Application Functions (Entities) for managing user access along with the associated technical components, such as API endpoints and user interface screens, that are mapped to those Entities..

Rights: A Right is a collection of permissions / entitlements on an Entity or group of Entities. In the real world it translates to a right definition that a Participant administrator has created to be granted to one or more users.

Rights Catalogue: A Rights Catalogue is a curated list of typical role definition templates created by AEMO, for various participant types. Participant Administrators will be able to reuse these right definitions or use them as the basis of a custom rights / role definition, instead of creating new role definitions from scratch.

Data Sharing: 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.

Assets: Represent a collection of physical assets for which energy flows and are of a category which are eligible for Data sharing e.g. grid scale generation unit



*This is image has been developed to provide high level overview and further details will be discussed during future **focus group sessions**.*

Entitlements Management Worked Example

Entity Catalogue

The Entity Catalogue is a searchable catalogue of Application Functions / Entities. It allows Participant Administrators to efficiently locate Application Functions (Entities) for managing user access along with the associated technical components, such as API endpoints and user interface screens, that are mapped to those Entities.

Entities are the individual components or building blocks that represent individual pieces of functionality within applications.

A given functionality may be invoked from

- User Interface Layer, or
- System to System Interfaces e.g. via APIs

Related Industry Pain point

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

Action	Action Description	API Method
C	Create	POST
R	Read	GET
U	Update	PUT
D	Delete	DELETE
G	Grant	NA
L	Delegate	NA

What is the Admin Flag?	
Y	An entity that defines if the user has an admin right If a user is tagged as 'Org Admin' or 'Participant Admin', then the associated rights MUST have only entities with the admin flag turned on. This will ensure an account doesn't have a mix of business entities & admin entities; separation of duties
N	Entities that are non-admin business discrete services

Entity #	Business Function	Market	Entity Name	Entity Description	Eff Date	Last Eff Date	Actions Allowed	Admin?	Data Classification	API Endpoint	UI Screen/Menu Name
ENT.001	Bids/Offers	NEM	Manage Energy-FCAS Bids	Submit bids to participant in trading	1/01/2000	31/12/9999	CRUGL	N	5	.../bidsoffers/nem/energyfcas/bids	Energy & FCAS 5min Bids -> Edit
ENT.002			Energy-FCAS Bids list	Provides a list of bids for the input	1/01/2000	31/12/9999	RGL	N	4	.../bidsoffers/nem/energyfcas/bids/list	Energy & FCAS 5min Bids -> List
ENT.003			Energy-FCAS Bids Reports - Public	Access to outbound public bid reports	1/01/2021	31/12/9999	RGL	N	1	.../bidsoffers/nem/energyfcas/bids/reports/public	N/A
ENT.004			Energy-FCAS Bids Reports - Private	Access to outbound private bid reports	1/01/2021	31/12/9999	RGL	N	4	.../bidsoffers/nem/energyfcas/bids/reports/private	N/A
ENT.005	Bids/Offers	WEM	Manage Energy-FCAS Bids	Submit bids to participant in trading	1/01/2020	31/12/9999	CRUG	N	5	.../bidsoffers/wem/energyfcas/bids	WEM Bids & Offers
ENT.006			Energy-FCAS Bids list	Submit bids to participant in trading	1/01/2020	1/01/2024	RG	N	4	N/A	N/A
ENT.007	Discoveries	NEM	NMI Discovery	Type 1, 2 & 3 NMI Discovery	1/01/2000	31/12/9999	RG	N	3	.../Retail/NEM/NMIDiscovery	NMI Discovery
ENT.008	Market Change Req	NEM	Change Requests	Manage Change Request Lifecycle	1/06/2024	31/12/9999	CRG	N	4	.../Retail/NEM/changeRequests	Create Transactions
ENT.009					2/01/2024	31/05/2024	CRG	N	4	N/A	N/A
ENT.010					1/01/2000	1/01/2024	CRG	N	4	N/A	N/A
ENT.011	Administrative	NEM	Admin	Defines if the user has Admin rights	1/01/2000	31/12/9999	RG	Y	5	N/A	N/A
ENT.012		NEM	Entities	Ability to manage entities	1/01/2000	31/12/9999	CRU	Y	3	N/A	User Administration -> Entities
ENT.013		NEM	Rights	Ability to manage Rights	1/01/2000	31/12/9999	CRUG	Y	4	N/A	User Administration -> Create Rights

This is image has been developed for illustration purposes only

Data Classification	
1	Public data
2	Internal
3	Restricted
4	Private
5	Critical

Rights Catalogue

Rights Catalogue is a curated list of typical role definition templates created by AEMO, for various Participant Types. Participant Administrators will be able to copy these role definitions and customise them, instead of creating new role definitions from scratch.

In the Rights Catalogues for each Participant Type, AEMO will publish various Rights template that meet the typical access management requirements of various Participants categories (e.g. Retailers, Distributors, Generators etc.)

Please note that the, role catalogue will be specific to a particular market and will not have a mix of permissions belonging to multiple markets

Related Industry Pain point

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

	Role Name	Role Description	Eff Date	Last Eff Date	Associated Entity	Ref Entity	CRUDGL Operations
ROL.001	NEM Retailer Business Centre	Business Centre Agent Capabilities	1/01/2000	31/12/9999	NMI Discovery	ENT.007	R
ROL.002	NEM Participant FRC Functions	Manage Market Change Request Process	1/01/2000	31/12/9999	NMI Discovery	ENT.007	R
			1/01/2000	31/12/9999	Change Requests	ENT.008	CR
ROL.003	NEM Bidding Functions	Ability for Generators / Traders to bid in wholsale market	1/01/2000	31/12/9999	Manage Energy-FCAS Bids	ENT.001	CRU
			1/01/2000	31/12/9999	Energy-FCAS Bids list	ENT.002	R
			1/01/2000	31/12/9999	Energy-FCAS Bids Reports - Private	ENT.004	R
ROL.004	Organisation Admin	Create Organisation Admin	1/01/2000	31/12/9999	Admin	ENT.011	RG
			1/01/2000	31/12/9999	Entities	ENT.012	R
			1/01/2000	31/12/9999	Rights	ENT.013	CRUG

This is image has been developed for illustration purposes only

Create a right from a rights catalogue

Organisation Admin or a Participant Admin can create the role by copying the template from the Right Catalogue

SCENARIO

Organisation Admin belonging to 'Emerald Energy Holding' is creating the Rights for their organisation.

Organisation Admin is creating a Right from the Role Catalogue; assigning that Right to few PIDs of the Organisation:

- Organisation Admin Creates a Right by copying a Role from the Role Catalogue
- Organisation Admin then makes further changes after copying the data from the Right Catalogue
- Organisation Admin associates the Right to few of the PIDs of their Organisation i.e. only to EMERVIC1 & EMERVIC2

Related Industry Pain point

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

Use Case Steps

STEP 1:

Organisation Admin creates a new Right; RT.006

STEP 2:

Organisation Admin copies the template ROLE.003 from the Role Catalogue

STEP 3:

Organisation Admin is making changes to the RT.006 after copying the ROL.003 into RT.006

- *Removes Entity 'Energy-FCAS Bids Reports - Private' that was inherited from the Role Catalogue (ROL.003)*
- *Adds new entity to the RT.005 that was not in the ROL.003*
- *Amendments made by the Organisation Admin are shown in **red***

STEP 4:

Organisation Admin associates the Right RT.006 to the ParticipantIDs EMERVIC1 & EMERVIC2

If a user is assigned to this right; the user will be able to manage above market functions for the following ParticipantIDs ONLY — **EMERVIC1 EMERVIC2**

The user will NOT be able to manage above market functions for other ParticipantIDs (see below) in his/her Organisation — **EMERGEN EMERWEM1**

Data

Right ID	Right Name	Ref Role Catalogue	Right Status	Eff Date	Last Eff Date
RT.006	EMERALD Custom Role 2	ROL.003	A	4/01/2024	31/12/9999

Associated Entity	Ref Entity	CRUDGL Operations	Assigned to OrganisationID / ParticipantID	Name
Manage Energy-FCAS Bids	ENT.001	CRU		
Energy-FCAS Bids list	ENT.002	R		
Energy-FCAS Bids Reports - Private	ENT.004	R		

Right ID	Right Name	Ref Role Catalogue	Right Status	Eff Date	Last Eff Date
RT.006	EMERALD Custom Role 2	ROL.003	A	4/01/2024	31/12/9999

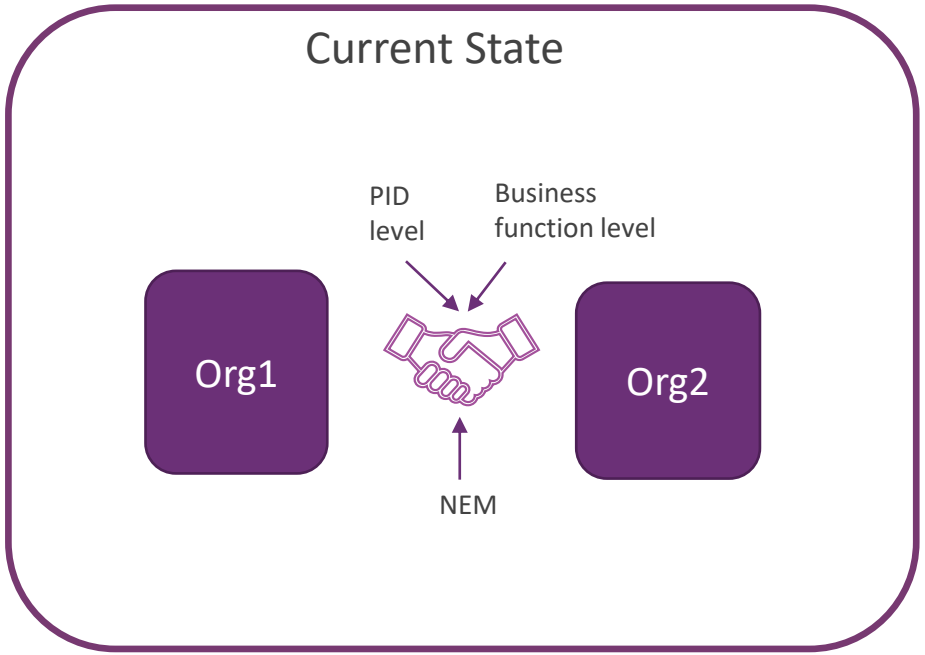
Associated Entity	Ref Entity	CRUDGL Operations	Assigned to OrganisationID / ParticipantID	Name
Manage Energy-FCAS Bids	ENT.001	CRU		
Energy-FCAS Bids list	ENT.002	R		
~~Energy-FCAS Bids Reports - Private~~	~~ENT.004~~	~~R~~		
Energy-FCAS Bids Reports - Public	ENT.003	R		

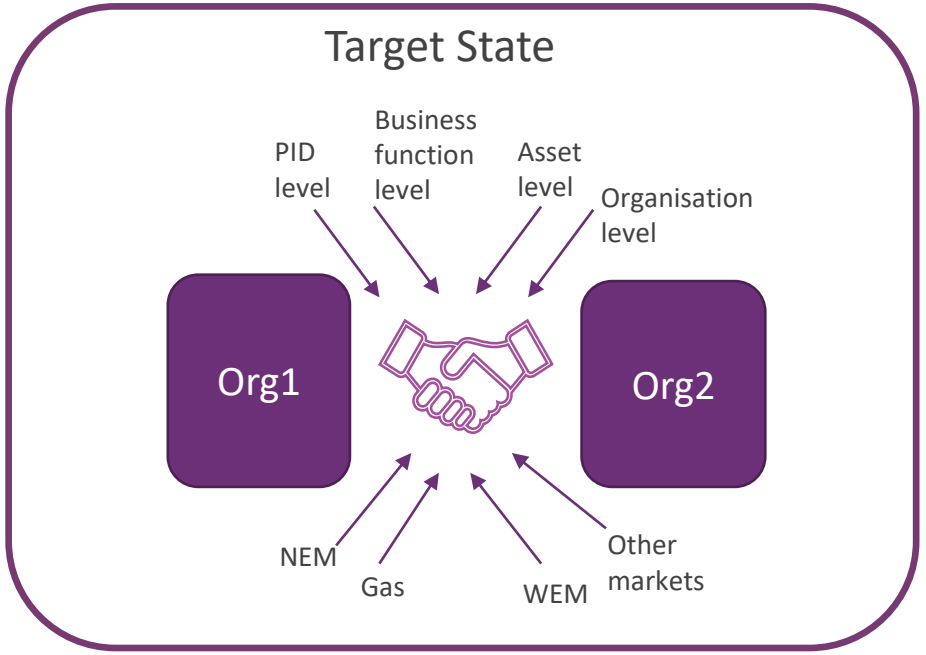
Right ID	Right Name	Ref Role Catalogue	Right Status	Eff Date	Last Eff Date
RT.006	EMERALD Custom Role 2	ROL.003	A	4/01/2024	31/12/9999

Associated Entity	Ref Entity	CRUDGL Operations	Assigned to OrganisationID / ParticipantID	Name
Manage Energy-FCAS Bids	ENT.001	CRU	EMERVIC1 & EMERVIC2	Emerald Energy Retail (C&I) & Emerald Energy Retail (Mass Market)
Energy-FCAS Bids list	ENT.002	R		
Energy-FCAS Bids Reports - Public	ENT.003	R		

Data Sharing

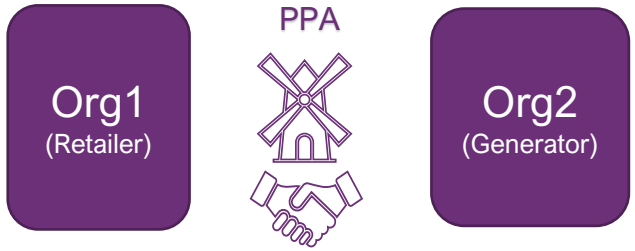
An access agreement that allows actions and data confidential to one participant to be made available to another participant based on an agreement between those parties and registering this agreement with AEMO.



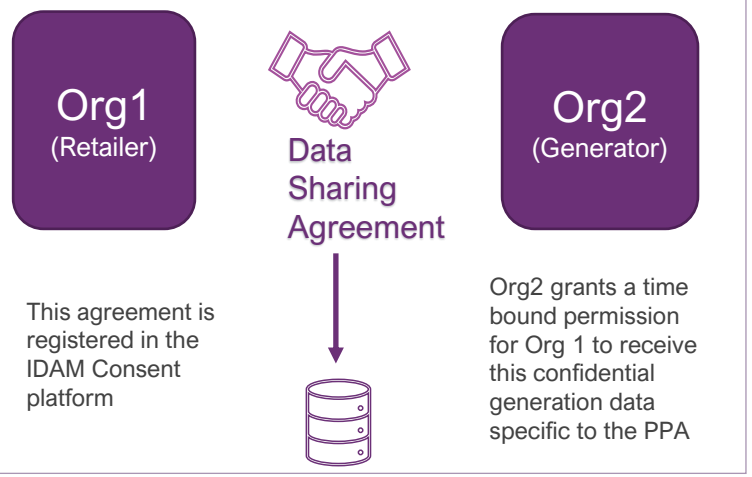


Data Access Permission Examples

Scenario 1



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



This agreement is registered in the IDAM Consent platform

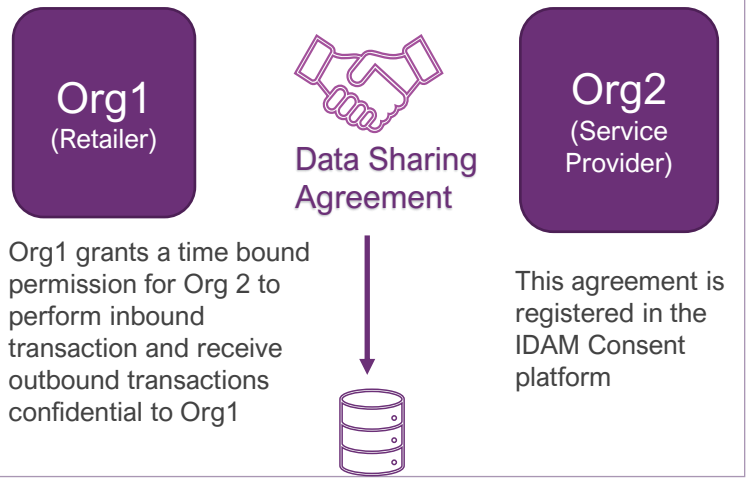
Org2 grants a time bound permission for Org 1 to receive this confidential generation data specific to the PPA

Org 1 can grant IDAM accounts to receive Org2 confidential data

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

Scenario 2

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 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 grant IDAM accounts to submit and receive Org1 confidential data

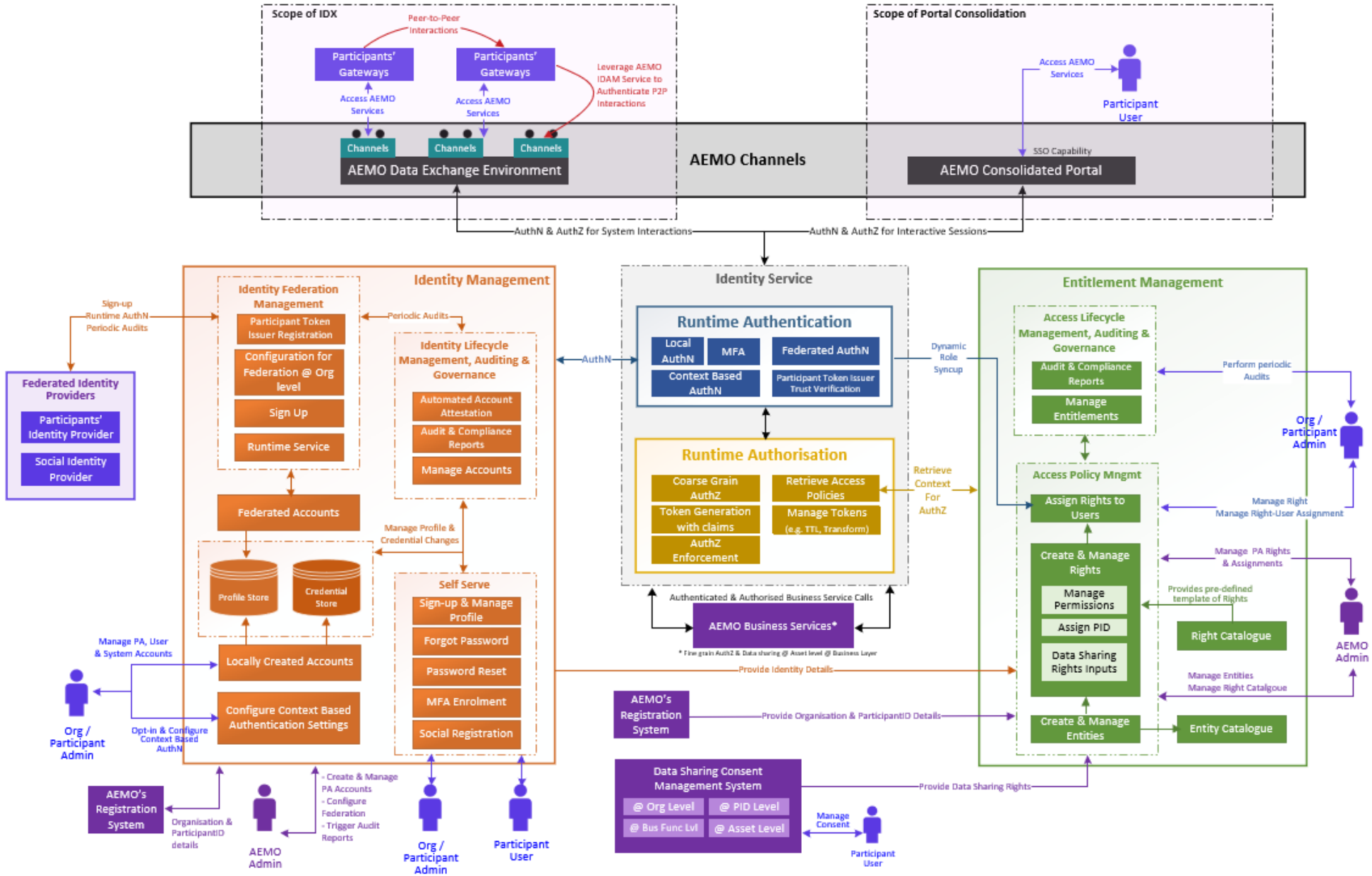
Org 2 can interact with the Retail Market on Org 1's behalf

Notes

- Satheesh Kumar introduced terminologies related to Entitlement Management.
- Phil Hayes elaborated on some of the target state concepts, such as Entity Catalogue and Rights Catalogue.
- Phil also gave a recap of the Data Sharing concept and provided an example. Phil mentioned that further discovery work will be conducted with the industry on this topic as part of the future focus group sessions.

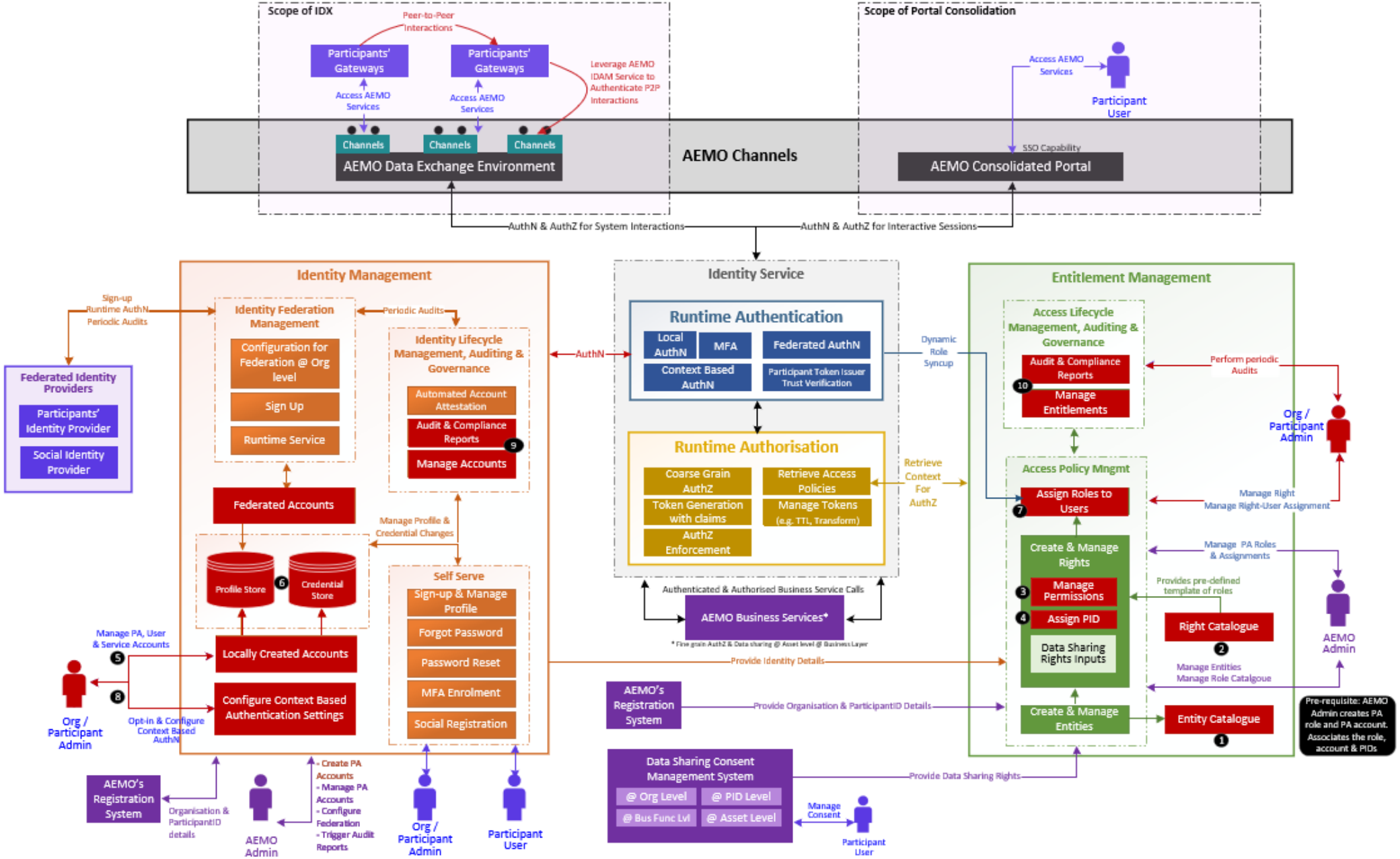
8. Identity and Access Management Architecture

IDAM Target State Conceptual Architectural Design



Example Workflows

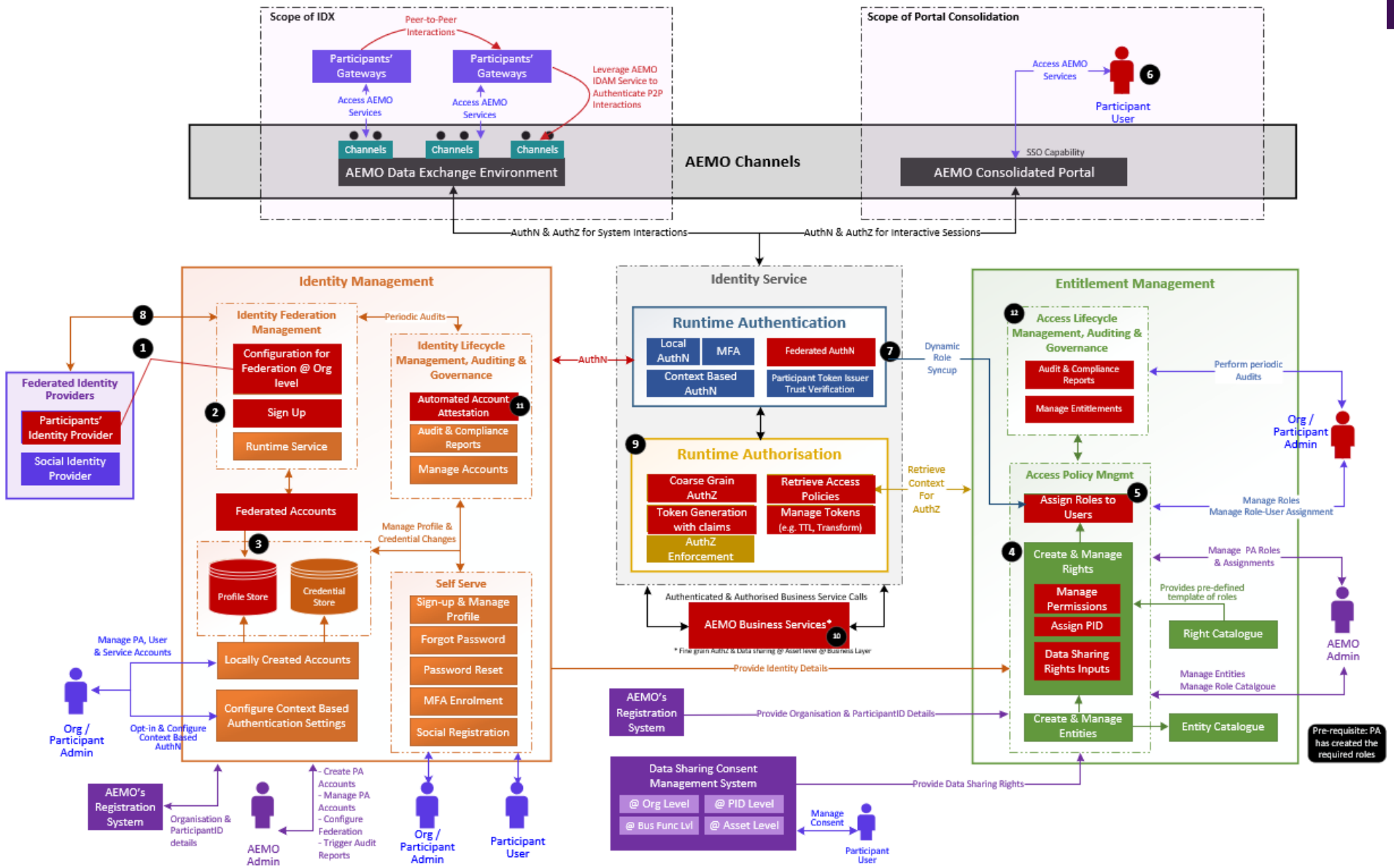
Example1: Participant Admin (PA) Workflow



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 right. *(An Entity catalogue is a suite of atomic business functions that can be assembled into one or more AEMO defined roles).* *More details: Refer slide 26*
2	The PA can consume the pre-defined right available in the AEMO right catalogue or create a custom right based on the right available in the right catalogue.
3	The PA then can associate the entities with the right they consume/define and mark the permissions.
4	The PA can thereafter associate one or more Participant IDs (PIDs) to the right 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 right 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

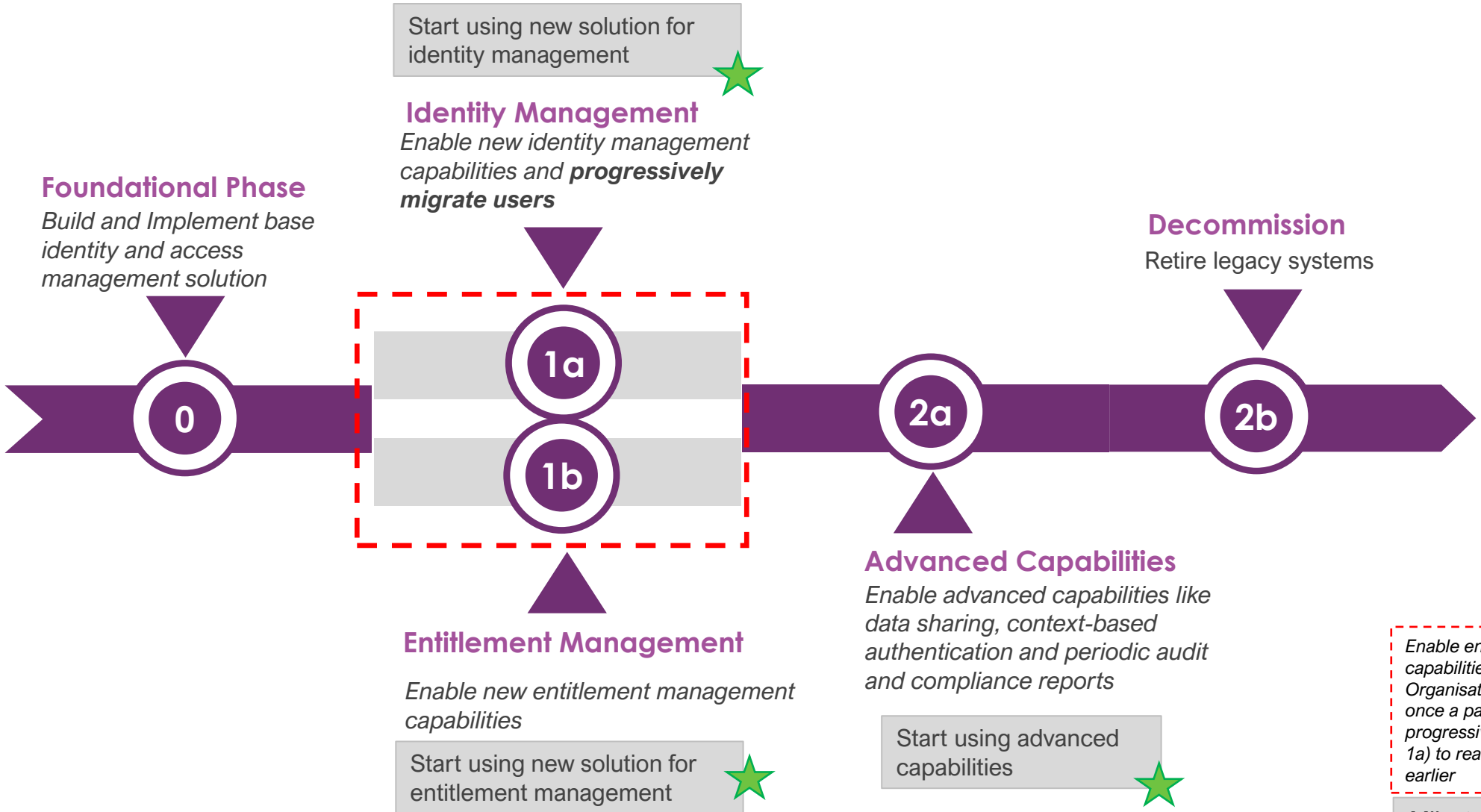
Step	Description
Pre-requisite	The PA has already created all the required roles.
1	System will establish a Federation trust relationship between the AEMO identity provider (IdP) and the participant identity provider.
2	The users can sign up using their enterprise identity.
3	User profiles are then created for these users in the profile store.
4	The PA creates and Manges rights
5	The PA can assign the right to the user accounts available in the profile store.
6	The users can then access the portal services through their browsers.
7	The identity service identifies the incoming identity as a federated identity and automatically redirects the authentication request to the Participant IdP for authentication.
8	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.
9	Coarse grain authorisation is applied based on the user attributes and the user us presented with the screen relevant to their profile.
10	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.
11 and 12	The PAs are provided with the capabilities to manage the deprovisioning of user accounts when they leave the organisation.

Notes

- Manesh Karunakaran did a re-cap of the IDAM Target State Conceptual Architectural Design.
- Satheesh Kumar did a re-cap of the two use cases:
  - Participant Admin workflow
  - Management of Federated User Account.
- Satheesh noted that Roles and Rights in this pack are synonym.
- Satheesh noted that new capability is added to the target state called Dynamic Role Sync-up on the basis of the industry feedback during FASI consultation

9. Transition Strategy

IDAM Transition Strategy



What is Progressive Migration

Through the business case, Progressive Migration Transition Strategy was proposed for person identities to ensure a seamless progression to the IDAM Target State.

What is Progressive Migration?

Progressive migration is a migration approach in which the **person identity** migration happens upon user login (first time post cut-over). Migrating the account / registration of the account in the target state IDAM solution involves a series of pre-defined activities such as email id verification, enrolment to MFA

Benefits of Progressive Migration

Account de-duplication and automatic account linking
This approach eliminates the migration of inactive and duplicate accounts from the legacy IDAM platform to the new platform and reduces any additional administrative overheads associated with linking multiple accounts belonging to the same user.

Reduced Risk
The coexistence of legacy and new systems for a set period gives AEMO adequate time to monitor the successful execution of the step-by-step migration process and allows the migrations to occur gradually. Additionally, it provides an easy rollback to the old IDAM system if any unexpected issues are encountered during the migration phase.

Bulk Upload Capability: Even though AEMO proposes progressive Migration, it is intended to also support bulk upload capability allowing organisations to bulk upload person identities into the new system solution. Participants will be responsible to eliminate inactive and duplicate person accounts manually.

Please note that this slide provides a recap of the high-level definition of the progressive migration. According to the forward plan, multiple Focus Group sessions will be held to discuss the transition plan in collaboration with industry stakeholders.

Notes

- Nirmal Narayanamurthi provided re-cap of the transition Strategy and provided high-level overview of the progressive migration.
- Nirmal noted multiple focus group sessions will be conducted to deep-dive this topic with the industry as per the forward plan.

10. General Business and Next Steps

NEMReform@aemo.com.au

General Business and Next Steps

MITE Working Group Forward Plan

Purpose		Timing
Review Recommendations from the Focus Groups	**IDAM** • Review Recommendations from IDAM API Authentication and Authorisation focus groups if available	**2 October**
Message Exchange Pattern	**IDAM** • None required	**30 October**

Focus Group Forward Plan

Purpose		Timing
Deep Dive Focus Group	**IDAM** API Authentication and Authorisation pattern Focus Group	**18 September**
Deep Dive Focus Group	**IDAM** Organisation Hierarchy Use cases Focus Group	**18 October**

If you have any feedback to share on the topics presented today, please send us through to NEMReform@aemo.com.au.

AEMO | Market Interface Technology Enhancements

Notes

- Blaine Miner noted that appendix contains some slides regarding the upcoming focus group sessions and two more use case related to the IDAM target state workflows.
- No new actions have been captured as a part of this MITWG session.

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

Appendix B

Upcoming Focus Group Topics

IDAM Focus Group: API Authentication and Authorisation Patterns

The objective of this focus group meeting is to assess the proposed API Authentication and Authorisation flows for Industry Data exchange, exploring both practical and technical aspects to ensure robust security and ease of use.

- Authentication and authorisation, in simple terms, involve verifying a user's or service account's identity and then determining their access permissions, respectively.
- The IDAM Focus Group will discuss the integration of OAuth Client Credentials Flow within IDX systems to bolster security and also deliberate on strategies for maintaining the integrity and security of client credentials.

Audience Skill Set for Focus Group Discussion

- Technical Leads / Gateway / Support teams
- Cyber Security Teams / Security Architecture Teams
- Integration Architecture Teams (Market Interface Specific)

Topics for discussion

- Overview of Service Accounts Authentication and Authorisation using OAuth 2 Client Credentials Flow
- Proposed Authentication and Authorisation Flows

This working group discussion will be relevant to all stakeholders who participate in exchanging data between AEMO and energy stakeholders

IDAM Focus Group: 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.

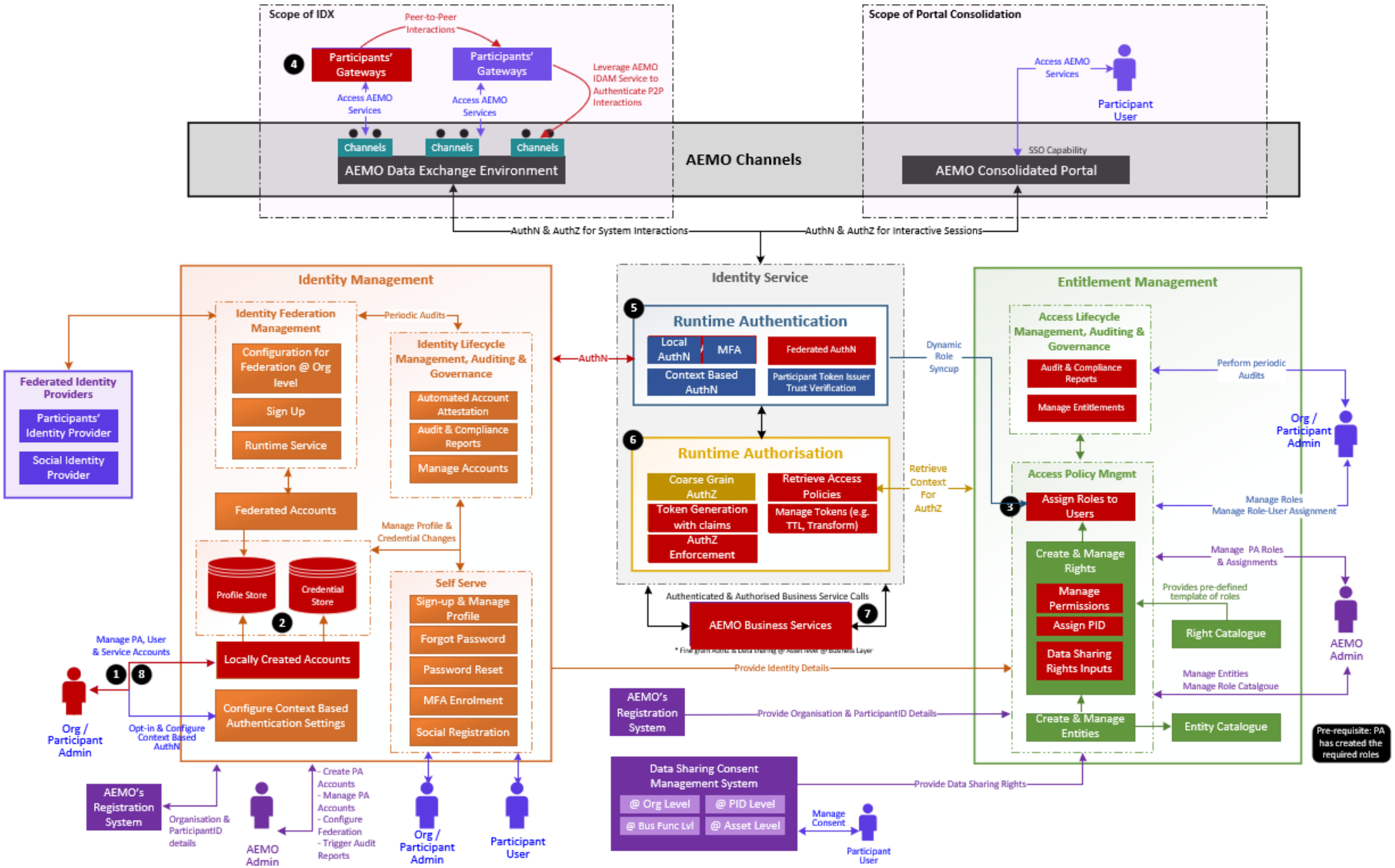
Note: This focus group discussion will be relevant to the organisations with multiple participants Ids and all stakeholders who leverage data sharing capabilities.

Appendix C

Workflow Examples

- Management of Service Accounts
- Management of Local User Accounts

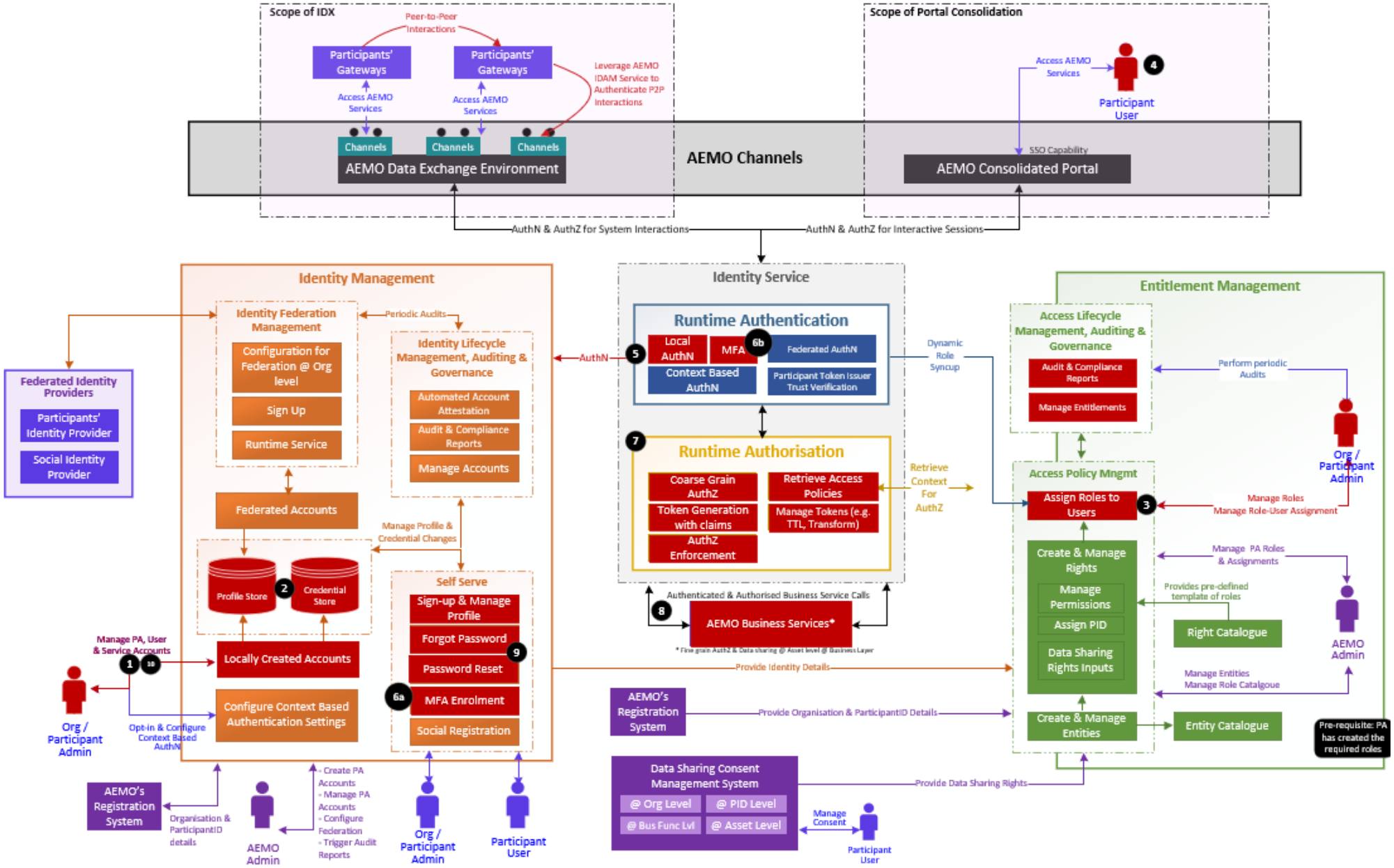
Example4: Management of Service Accounts



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.

Example3: Management of Local User Account



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 right 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.