

Identity and Access Management - May 2027

0.01 July 2026

Pre-production: 1 March 2027

Production: 2 May 2027

Rules effective: NA



Important notice

Purpose & audience

This document describes the technical changes required to participant's systems for the Identity and Access Management - May 2027 (Release). The Australian Energy Market Operator (AEMO) provides this information as a service targeting business analysts and IT staff in participant organisations. It provides guidance about the changes to their market systems under the National Gas or Electricity Rules (Rules), as at the date of publication.

How to use this document

- If you have questions about the business aspects of these changes, please see Consultations on AEMO's website.
- The references listed throughout this document are primary resources and take precedence over this document.
- Unless otherwise stated, you can find resources mentioned in this guide on AEMO's website.
- **Text in this format** is a link to related information. Some links require access to MarketNet.
- **Text in this format**, indicates a reference to a document on AEMO's website.
- **Text in this format** is an action to perform in the Markets Portal.
- This document is written in plain language for easy reading. Where there is a discrepancy between the Rules and information or a term in this document, the Rules take precedence.
- Glossary Terms are capitalised and have the meanings listed against them in the Glossary.
- Rules Terms have the meaning listed against them in the [National Gas Rules](#) or [National Electricity Rules](#) (Rules).

Privacy and legal notices

The material in this publication may be used in accordance with the [privacy and legal notices](#) on AEMO's website.

Trademark Notices

Microsoft, Windows and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the US and other countries.

© 2015 Google Inc, used with permission. Google and the Google logo are registered trademarks of Google Inc.

Distribution

Available to the public.

Document Identification

Prepared by: AEMO Digital

Last update: Wednesday, 29 July 2026 4:20 PM

Version History

0.01 Initial creation

Documents made obsolete

The release of this document changes only the version of Identity and Access Management - May 2027.

Support Hub

To contact AEMO's Support Hub use Contact Us on AEMO's website or for urgent matters phone: 1300 AEMO 00 (1300 236 600).

Contents

1	Introduction	1
1.1	Audience.....	1
1.2	Objective	1
1.3	Status	1
1.4	Solution Release dates.....	2
1.5	Projects and enhancements.....	2
1.6	Rule and procedure changes	2
1.7	Related technical specifications	2
1.8	Related documents	3
1.9	Approval to change	3
1.10	Market systems user group meetings	3
1.11	Version numbers	3
1.12	Changes in this version.....	4
2	Proposed Timeline	5
3	Participant Impact	7
4	Identity and Access Management	8
4.1	Goal	8
4.2	High-level IDAM concepts	8
4.3	Mapping terminology	9
4.4	High-level changes.....	10
5	AEMO Portal Updates.....	11
5.1	Create user.....	11
5.2	User registration.....	12
5.3	Portal login	13
5.4	Other portal updates.....	13
6	Data Sharing.....	14
7	Transition and Migration	15
7.1	Preparation.....	15
7.1.1	AEMO	15
7.1.2	Participants	15

7.2	Transition and cutover	16
7.3	Post-cutover.....	16
7.4	Pilot phase	16
7.5	Migration phase	16
8	FAQs	17
9	Implementation	18
10	Terms	19
10.1	Rules Terms	19
10.2	Glossary	20
11	References	24
12	Index	25
A1.	Version history	26

1 Introduction

1.1 Audience

AEMO provides this information as a service targeting business analysts, IT staff, and Participant Administrators.

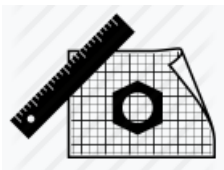
The primary audience is any external organisation accessing the AEMO services including:

- Registered Participants
- Non-registered Participants
- Non-market participants
- Potential Participants
- Service Providers

1.2 Objective

The Identity and Access Management - May 2027 (Release) describes the projects planned by AEMO from a participant perspective and includes any system related changes for participants.

1.3 Status

Version	Status
0.01	 Initial Draft for review. The design is not ready for participants' builds Presents the Identity and Access Management - May 2027 evolving design. Please send feedback to Contact Us. In the Details of your enquiry section, mention the EAS Knowledge Management team as the Resolver group.

1.4 Solution Release dates

Scheduled for implementation in:

- Pre-production: 1 March 2027
- Production: 2 May 2027

1.5 Projects and enhancements

Changes and enhancements for this Release include:

No.	Functionality	Change	Affected interface	Reference
	User Rights Management			
	System Access Management			

1.6 Rule and procedure changes

The following rules and procedures take precedence over technical specifications and guides.

Title	Project	Version/status	Effective
Enhancing access for registered participant representatives (Electricity) AEMC	IDAM	Final	May 2027
Procedure For Accessing AEMO Systems (PFAAS)	IDAM	In progress	

1.7 Related technical specifications

Title	Description
NA	

1.8 Related documents

Once published, these resources take precedence over this technical specification

These guides and resources are updated according to this technical specification and published for the pre-production Release Date.

Title	Description	Status
AEMO Portals Help	Includes the following updates: - Adds new IDAM topic - Updates the URM topic as required - Updates some details in the About portal topic pertaining to the new authentication and authorisation methods.	Not started

1.9 Approval to change

No approval or agreement to change required from participant change controllers. Agreement was sought in the [Market Interface Technology Enhancements Working Group](#).

1.10 Market systems user group meetings

The Market Systems User Group (MSUG) is an industry user group established to discuss NEM wholesale and retail IT systems releases. Its purpose is to facilitate the continuing improvement of AEMO's IT systems by seeking feedback and collaboration from participants.

MSUG meetings are open to all interested parties, with invitations sent to all included on the distribution list. If you have a technical question for a project and want to attend the MSUG ask your company's support team to include your email address in their **AEMO Help Desk Bulletin (CRM)** distribution list.

1.11 Version numbers

AEMO releases new versions of this document as the technical requirements are streamlined.

Incremental version numbers such as 1.01, 2.01 and so on mean there is a minor change to the technical specification.

Major version numbers such as 1.00, 2.00 means there are substantial changes to the technical specification. Participants must carefully review these changes, detailed on page 4.



1.12 Changes in this version

No changes, this is the initial version.

2 Proposed Timeline

The dates for the Market System User Group Meetings (MSUG) are tentative. We will provide an invitation one week prior to the meeting.

Milestone	Date	Description
Approval required	NA	Final date for participant approval of this Release
Revised Technical Specification	September 2026	AEMO releases new versions of this document as the technical requirements are streamlined. During the project this document is the source of truth From the production release, the technical specification becomes final and the Related documents become the source of truth Technical Specification Portal
Related Documents publication	1 March 2027	Release of guides and resources mentioned in Related on page 3
Next MSUG meeting	26 August 2026 (TBC)	Market Systems User Group Meeting (MSUG) to review the technical specification and ask AEMO technical SMEs questions This date is tentative. The Knowledge Management Team provides the invitation prior to the meeting
Pre-production refresh	NA	Refresh of the pre-production system with data refreshed from the production system. An outage of up to five days can occur to the pre-production environment during this period. Participant access is not restricted, however, AEMO do not guarantee the pre-production data content or system availability. During the refresh, access to other AEMO systems such as AWEFS, EMMS, OPDMS, and STTM may be intermittently affected
Pre-production implementation	1 March 2027	AEMO implements components of the Release to pre-production for participant testing AEMO has full access to the system during this period Participant access is not restricted; however, the data content or system availability is not guaranteed

Proposed Timeline

Milestone	Date	Description
Pre-production available	1 March 2027 (TBC)	Testing period begins for participants
Market trial	1 March 2027 - 23 April 2027 (TBC)	AEMO coordinated testing with all participants (the Pre-Production environment will remain available for Participant testing after the technical cutover)
Production implementation	2 May 2027	AEMO implements the release to production Transition existing users, roles, etc from legacy systems to the new IDAM platform. Participants commence using the new IDAM platform
Production systems available	2 May 2027 (TBC)	Production systems available to participants Existing and limited new functionality
Commence industry migration	5 July 2027 (TBC)	Participant migration period commences All new functionality available
Default migration	3 months before end of migration period (TBC)	Participant organisations who have not commenced the migration are automatically set to commence progressive migration.



3 Participant Impact

To comply with this Release, participants must review and complete the following activities:

- Identify service accounts in both pre-production and (especially) production environments.
- Confirm organisation hierarchy to manage participant ID mapping to a single system-access organisation.
- Identify an organisation administrator.
- Provide a list of email domain to whitelist.

In addition to these activities, for the production environment, participants must also clean-up any inactive users.



4 Identity and Access Management

4.1 Goal

The NEM External Identity and Access Management (IDAM) project introduces a unified identity and access management framework to streamline authentication and access for participants, enhances cybersecurity and ensures AEMO's compliance with regulatory mandates.

The project implements core capabilities such as identity and entitlement management, authentication, authorisation, lifecycle management, and reporting.

The project introduces new features like identity federation, self-service capabilities, multi-factor authentication, advanced data sharing, and role-based access to improve security, efficiency, and user experience.

For new terms and definitions, see [Market Interface Technology Enhancements Working Group - IDAM Only Session](#).

4.2 High-level IDAM concepts

At a high-level, IDAM includes the following concepts:

- Identity management – Refers to the complete management of human and non-human identities interacting with AEMO services. This includes authentication, authorisation, access management, Identity Governance and Administration (IGA), Lifecycle Management (JML), SSO and Federation. It includes the following:
 - Non-federated identity refers to identities created, managed and issued to the participant users and systems from AEMO's Identity and Access management system.
 - Federated identity refers to identities created, managed, and issued to participant users and systems from their own organisations Identity and Access Management systems. These systems are allowed to access and consume AEMO resources through a federated trust.
- Entitlement management – Introduces improved tools to define and manage user roles.
- Data sharing – Creates a more flexible data sharing model aligning with the new Rule.
- Runtime authentication and authorisation – Introduces multi-factor authentication (MFA).

These concepts are further broken down into the following processes AEMO, and the participants follow to manage identity and access to the AEMO systems:

- Create or register identity – Create and onboard new users to into AEMO's IDAM platform.

- Create and assign roles – Document roles and assign attributes to a registered identity
- Authenticate – Enforce and validate user identities
- Authorise – Determine user has right entitlements to access systems
- Manage consent – Inform user the data collected and provide them an opportunity to refuse
- Self-service – Manage user information, password updates. Sync details with other systems.
- Segregation of duties – is a security control that splits up the privileges into different roles and assigns them to different uses.
- Deprovision – Revoke permissions and unauthorise user identities to enterprise systems.
- Governance and compliance – Define guidelines, rules and policies.
- Logging and monitoring – Capture anomalies and events for unwarranted behaviour from identities.
- Identity lifecycle management – Manage the identities on an ongoing basis and ensure to only retain relevant identity data per the use case.

4.3 Mapping terminology

In the new IDAM platform, the terms used are:

URM terminology	SAM terminology	IDAM terminology
Entity	Right	Resource
Right	Role	Role
NA	Group	Group
User	Member	Business user (human)
Participant Administrator (PA)	Participant Administrator	Participant Administrator
NA	NA	Organisation Administrator (OA)
User	NA	Service account (non-human)

4.4 High-level changes

Function	Description	Reference
AEMO portals	- Introduces the new Identity and Access Management Platform in the portal for organisation and participant administrators - Updates to the users to verify email, set up a new password that meets AEMO security policies, and set up MFA methods according to their organisation policies. The IDAM platform eventually replaces the User Rights Management (URM) capabilities.	AEMO Portal
Data sharing	IDAM provides organisations with data sharing agreements configurations to manage the level of access to the AEMO market services available to the organisation's participants. The user identities are mapped to the organisation based on the email domains.	Data Sharing

5 AEMO Portal Updates

The IDAM project introduces the following changes to the AEMO portals, namely the Markets and the Application portals.

The design is in progress for this change and AEMO provides more details as these are finalised.

5.1 Create user

An authorised administrator can create and onboard the following user types of non-federated users to the IDAM platform:

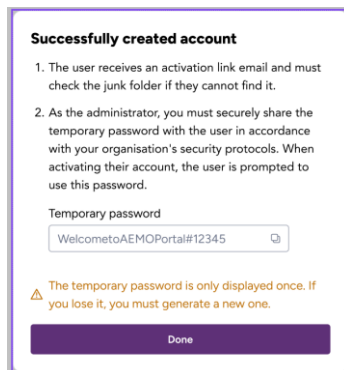
- Organisation administrator
- Participant administrator
- User – Can be human or non-human identity
 - Human identity refers to an identity associated with a business user.
 - Non-human identity refers to accounts associated with system applications or services.

The screenshots used are examples only and the final web screen may be different.

The screenshot shows a web browser window with the URL 'https://www.marketsportalidamexample.com'. The page title is 'AEMO Portal name'. The main heading is 'Create a user'. The form includes the following fields and options:

- Organisation: A dropdown menu with 'XYZ Industries' selected.
- First name: A text input field.
- Last name: A text input field.
- Email: A text input field.
- A note: 'This becomes the username.'
- User type: Three radio buttons with 'Organisation administrator' selected.
- Start date: A date picker showing '01/06/2025'.
- End date (optional): A date picker.
- Buttons: 'Cancel' and 'Create user'.

When an administrator creates a new user, the identity status is set to **Pending** and the system creates a temporary password with the following message:



Successfully created account

1. The user receives an activation link email and must check the junk folder if they cannot find it.
2. As the administrator, you must securely share the temporary password with the user in accordance with your organisation's security protocols. When activating their account, the user is prompted to use this password.

Temporary password

WelcometoAEMOPortal#12345

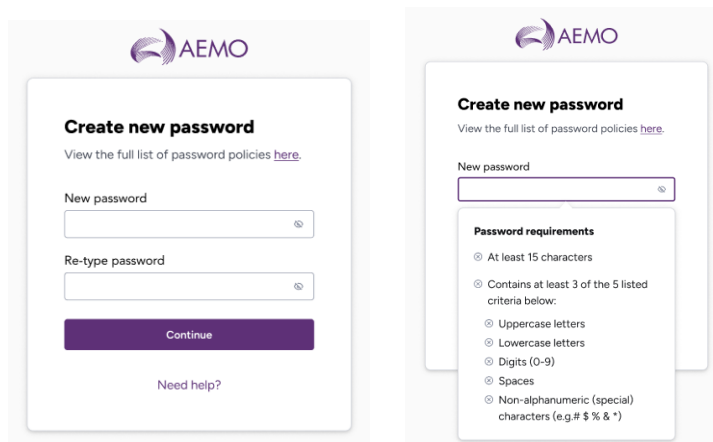
⚠ The temporary password is only displayed once. If you lose it, you must generate a new one.

Done

5.2 User registration

Following the create user process, an activation link is generated and emailed to the user.

As a part of the registration, the user must accept the terms and conditions, set up a secure password based on AEMO's password standards.



The first screenshot shows the 'Create new password' screen with the AEMO logo at the top. It includes a link to 'View the full list of password policies here.', input fields for 'New password' and 'Re-type password', a 'Continue' button, and a 'Need help?' link.

The second screenshot shows the 'Create new password' screen with the AEMO logo at the top. It includes a link to 'View the full list of password policies here.', a 'New password' input field, and a 'Password requirements' section with the following criteria:

- ⊗ At least 15 characters
- ⊗ Contains at least 3 of the 5 listed criteria below:
- ⊗ Uppercase letters
- ⊗ Lowercase letters
- ⊗ Digits (0-9)
- ⊗ Spaces
- ⊗ Non-alphanumeric (special) characters (e.g. # \$ % & *)

The user must then set up at least one MFA method. Once the user completes this successfully, the user identity status updates to **Active**.

AEMO accepts the following MFA methods – passkey, push notification, authenticator app, SMS OTP, email OTP.

AEMO recommends the user set up multiple MFA methods to ensure continued connection to AEMO systems.

5.3 Portal login

On completing user registration, the user must login using the username and password. Accept terms and conditions and authenticate with the MFA method registered using the registration process to log in to the portal.

The authentication is dynamic and routed based on the identity type. For non-federated users, login using the username, password and MFA. Federated users are redirected to the participant organisation's identity provider. For legacy users, AEMO provides temporary support to continue username, password authentication during the transition.

5.4 Other portal updates

There are some new changes such as the ability to search on the menu items, favourite menu items, and display the environment for pre-production. See [Portal Consolidation UI changes](#).



6 Data Sharing

AEMO allows participants share access to AEMO's services to another organisation who can then act on their behalf, for example, a service provider. In this example, an organisation can enable the service provider to transparently access AEMO systems and establish and manage their own users and roles to act on the original participant's behalf.

The design is in progress for this change and AEMO provides more details as these are finalised.



7 Transition and Migration

Transition - The process allows AEMO to transition the existing user base from the current URM solution to the new authentication and authorisation services and manage user lifecycle with the new IDAM solution, occurring on 2 May 2027.

Industry Migration - The activities involved in organisations moving their users from legacy user to target state users post the completion of transition, starting with pilots in production. Organisations choose the method by which their organisation migrate their users and the timing within the migration window.

The following sections describe the high-level process.

7.1 Preparation

During the preparation phase, AEMO and participants must complete the following steps.

7.1.1 AEMO

AEMO must:

- Communicate the schedule and activities to the organisations.
- Identify the active user accounts. Active accounts are accounts with password changed within the last 180 days.
- Provide a view of entitlement constraints indicating when whether a participant type should have access to certain resources.

7.1.2 Participants

Participants must:

- Identify the service accounts.
- Confirm organisation hierarchy and the initial organisation administrator.
- Provide email domains to whitelist.



7.2 Transition and cutover

During the transition and cutover phase, the following activities are completed:

- Transition identity and entitlement from the legacy URM platform to the new IDAM platform.
- Apply entitlement constraints to roles as they transition.
- Map users and service accounts to the appropriate new human and non-human identity types.
- Reconfigure portals to authenticate and authorise using the new IDAM platform.

7.3 Post-cutover

If the organisation failed to complete the steps during the Preparation, there are some post-cutover steps.

This refers to a stabilisation period:

- Participants must recreate any missing service accounts.
- Participants must recreate any missing user accounts.

AEMO does not anticipate any impacts to participants during this phase.

7.4 Pilot phase

Details TBC

7.5 Migration phase

Details TBC



8 FAQs

Updated with queries from the MSUG.



9 Implementation

See Transition and Migration for implementation details.

10 Terms

10.1 Rules Terms

You can find the following terms defined in the [National Electricity Rules \(NER\)](#).

Term
AEMO
AEMO Markets Portal
AEMO Website
Market Participants
NEM
Registered Participant

10.2 Glossary

You can find a full list of AEMO glossary terms in [Industry Terminology](#) on AEMO's website.

Abbreviation/Term	Explanation
Access Control Model	An access control model is a framework used to manage and control access to resources, systems, and data. Access control models provide a set of rules and procedures that determine who is allowed to access a particular resource or system and what level of access they are granted. These models help organizations ensure that their systems and data are protected against unauthorized access, and they can help to enforce security policies and regulatory compliance.
Access Pattern	An access pattern refers to the overall approach or strategy used to manage access control within a system or application. It can include specific technologies or protocols used to implement access control, such as authentication mechanisms, authorisation mechanisms, encryption, and network security protocols etc.
AEST	Australian Eastern Standard Time
AEMO Administrator	AEMO Administrator, is a AEMO employed privileged user who has the authority to manage the identity and access control system for AEMO and its Energy Stakeholders.
Authentication	Authentication refers to the process of verifying the identity of a user, device, or other entity that is attempting to access a system or resource.
Authorisation	Authorisation is the process of determining what actions a user or entity is allowed to perform once they have been authenticated.
Authorisation Store	An authorisation store is a component of any Identity and Access Management system that stores and manages the permissions or access rights assigned to users or groups of users within an organization. It typically contains a collection of access control policies and rules that determine which resources or services a user or group of users can access, and what actions they are authorized to perform.
Correlation ID	Correlation ID is a unique identifier that is used to track a specific transaction or request as it passes through multiple systems and components. It is typically used in distributed systems, where a single transaction may require the involvement of multiple systems and services. The Correlation ID enables efficient troubleshooting and issue resolution, as it allows developers and administrators to easily trace a request as it moves through multiple systems and components.
Deprovision	The process of removing an identity from the IDAM platform.

Abbreviation/Term	Explanation
Energy Stakeholder	An active identity (person or non-person), who/which accesses AEMO's system and resources for certain requirements. From the IDAM point of view, Energy stakeholders can be categorised into - - Registered Participants (including Admins and users) - Non-registered Participants - Potential Participants - Service Providers - Internal users accessing Market applications - External System Accounts
EMMS	Electricity Market Management System; software, hardware, network and related processes to implement the wholesale energy market
Entitlement Catalog	An entitlement catalog typically includes a list of all the AEMO defined Roles and what privilege/privileges can be assigned to those individual Role.
Entity	Entities are the individual components or building blocks that represent individual pieces of functionality. For instance, the business service to submit a bid to the wholesale NEM Market shall be defined as an Entity called "Bids".
Federated Identity	Identities created, managed, and issued to participant users and systems from their own organisation Identity and Access Management System. These identities are allowed to access and consume AEMO resources through a federated trust.
Federated Single Sign-On	Federated Single Sign-On (FSSO) is an extension of Single Sign-On (SSO) that enables users to access multiple web applications or services across different organizations using a single set of login credentials, based on the established Federated trust.
Federated Trust	Federated trust is a concept in which organizations establish a trust relationship between their respective identity and access management systems to enable secure access to resources across different organizations.
Group	A group is a collection of one or many roles with permissions. AEMO System Administrator or Participant Administrator can optionally assign specific Groups to the users to simplify the management of users and roles.
Identity	Identities refer to entities that are recognized and authenticated within a system or organization. Identities can be categorised into two types - 1. Human identity - Human identity refers to an identity associated with a human user. 2. Non-human identity (e.g., service accounts, system accounts) - non-person identities are not associated with a human user, but rather with a system, application, or service. Non-human identities are used to authenticate and authorize access to resources by machines, applications, or other automated processes.
Identity Provider	An identity provider (IdP) is a service or a component of any organisation's Identity and Access Management platform that authenticates and asserts the identities for the purpose of enabling secure access to systems and resources.
Local Identity	Identities created, managed, and issued to participant users and systems from AEMO's External Identity and Access Management System (similar to URM).

Abbreviation/Term	Explanation
MFA	Multi-Factor authentication
MSATS	Market Settlement and Transfer Solution for retail electricity
NER	National Electricity Rules
Parent/Holding Company	A Parent Company, also known as a Holding company, is a type of business organization that owns one or more other companies (subsidiaries), usually with a controlling interest.
Participant Administrator	Participant Administrator, is a privileged user, who is employed by the respective Registered Participant organisation and has the authority to manage the AEMO-provisioned identity and access control system, for their own organisations users wanting to get access to AEMO's system and resources.
Privileges/Entitlements	Privileges/Entitlements refer to the permissions that are granted to a Role to access certain resources or perform specific actions within a system or application. These actions can include viewing, creating, modifying, or deleting data, running applications, executing a batch, and more.
Release	Identity and Access Management - May 2027
Release Dates	Pre-production: 1 March 2027 Production: 2 May 2027
Risk-based or Contextual 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.
Role	Role is a collection of specific Entities with their associated access privileges. For instance, an admin user creates a Role called "Settlement Management" that requires access to the "Bids", "Settlements", and "Change Request" Entity. Also, to complete the Role configuration, SA or PA assigns 'Create', 'Read' and 'Update' permissions to each of the Entities.
SAM	System Access Management. SAM is used by Participant Administrators to set up Participant Member access to AEMO's Application Portal. It does not require access to AEMO's private data network, MarketNet. For details, see System Access Management (SAM) .
Security Breach	Refers to an incident whereby AEMO system or data is accessed by an unauthorised individual or software system.
SoD	Segregation of Duties

Abbreviation/Term	Explanation
Single Sign-On	Single Sign-On (SSO) is an authentication mechanism that enables users to access multiple web applications or services with a single set of login credentials.
Software Development Lifecycle	Software development lifecycle (SDLC) is a process that outlines the stages involved in designing, developing, testing, and maintaining software. It typically includes several phases such as planning, requirements gathering, design, development, testing, deployment, and maintenance.
SPOC	The abbreviation SPOC is a business term used with the meaning "Single Point of Contact" to refer to a single person or team within a company who are designated as the point of contact for all communications or communications related to a specific area in the business.
System	System refers to all the Web-based and File-based User Interfaces, Backend Services, APIs, Databases.
TBC	To be confirmed
Token	In the context of Identity and Access Management, a Token is a small piece of data that is issued by an authentication system to prove the identity of a user or service. Tokens are used to grant access to resources and services without the user having to provide their credentials (such as a username and password) for each request.
User	A user is a person who uses the system, either through UI (interactive) or by Batch processing (batch). To use the system each user must be associated with a participant ID and a Role. The Role assigned to the user determines the menu options and interfaces the user can access, and what actions (privileges) the user can complete.
URM	User Rights Management. AEMO's guide to user rights management in AEMO's Market Systems. For details, see User Rights Management

11 References

Guide to AEMO's e-Hub APIs: Provides details about using AEMO's e-Hub as an interface to communicate information with AEMO. It assists Wholesale electricity and gas participants developing their own APIs.

Guide to Information Systems: Provides guidance for *Registered Participants* and interested parties about AEMO's participant electricity market systems.

Guide to User Rights Management: Assists participant administrators (PAs) to use the user rights management functions in the MSATS Web Portal.

Market Interface Technology Enhancements (IDAM Only Session)

12 Index

C

continuing improvement of AEMO's IT systems, 3

I

industry user group, 3

M

Market Systems User Group, 3
MSUG, 3

A1. Version history

No version history, this is the initial draft release.