Real-Time Data Procedure

Prepared by:	AEMO Market Management
Document ref:	
Version:	1.0
Effective date:	30th November 2028
Status:	Initial Draft

Approved for distribution and use by:

Approved by:	Michael Gatt
Title:	Executive General Manager - Operations
Date:	TBC

Contents

Current version release details

Version	Effective date	Summary of changes
1.0	30th November 2028	First Issue

Note: There is a full version history at the end of this document.

1. Introduction

1.1. Purpose and scope

The purpose of this Procedure is to establish the minimum operational, technical and security requirements for facilitating access to real time data (RTD) from a *small customer metering installation* to a retail customer, or their nominated Real-Time Data Authorised Recipient (RTDAR) in accordance with clause 7.16.6E of the National Electricity Rules (NER).

This Procedure specifies the manner and form in which Retailers and Metering Coordinators (MCs) must facilitate secure access to RTD between a *metering installation* and an external device.

These Procedures apply where a request for RTD access is made under NER 7.15.7 and rule 59E of the National Energy Retail Rules (NERR).

RTD provided under this Procedure:

- Is separate from metering data used for settlement.
- Does not constitute validated, substituted or estimated metering data
- Is provided for informational purposes only.

This Procedure has effect for the purposes set out in the NER. The NER and the National Electricity Law prevail over these Procedures to the extent of any inconsistency.

1.2. Definitions and interpretation

1.2.1. Glossary

Terms defined in the National Electricity Law and the NER have the same meanings in these Procedures unless otherwise specified in this clause.

Terms defined in the NER are intended to be identified in these Procedures by italicising them, but failure to italicise a defined term does not affect its meaning.

The Retail Electricity Market Procedures – Glossary and Framework:

- Is incorporated into and forms part of this Procedure; and
- Should be read in conjunction with the Procedure.

1.2.2. Interpretation

These Procedures are subject to the principles of interpretation set out in Schedule 2 of the National Electricity Law.

1.3. Related documents

All related AEMO published documents are explained within the Retail Market Procedures - Glossary and Framework.

Title	Location
Retail Electricity Market Glossary & Framework	https://www.aemo.com.au/energy-systems/electricity/national-electricity-market- nem/market-operations/retail-and-metering

2. Roles and Responsibilities

2.1. Retailer Responsibilities

a) The Retailer must:

i. receive RTD access requests from small customers or RTDARs;

ii. verify customer consent in accordance with the NERR 59E;

iii. request the MC facilitate RTD access; and

iv. notify the requesting party when RTD access has been enabled.

b) The Retailer is not responsible for technical limitations of the *metering installation*.

2.2. Metering Coordinator Responsibilities

a) The MC must:

i. facilitate RTD access at the *metering installation*;

ii. ensure RTD delivery complies with these Procedures; and

iii. ensure RTD access does not compromise the integrity or operation of the *metering installation*.

3. RTD Communications

3.1. RTD Communications Architecture

a) The MC's responsibility for RTD communications extends to the communications interface of the *metering installation*.

Communications performance beyond that interface, including within the customer's premises or through third-party communications infrastructure, is outside the responsibility of the MC, except as specified in Section 5.

b) RTD may be provided using one or more wireless communications mechanisms including:

i. direct communication between the *metering installation* and an RTD Device;

ii. communication via a gateway device; or

iii. communication via a intermediary system.

c) Where an intermediary system is used, the MC must ensure that:

i. RTD originates from the *metering installation;*

ii. The integrity and timeliness of the RTD are preserved; and

iii. The security requirements specified in these Procedures are maintained.

d) The communications architecture must not be capable of control or modification of *metering installation* functions.

3.2. Communications Protocols

a) Communications used to provide RTD at the communication and application layer must utilise open standards-based protocols to support interoperability between *metering installations* and RTD Devices.

b) Protocols used for RTD communications must:

i. Be publicly documented;

ii. Support secure authentication mechanisms;

iii. Support encrypted communications;

iv. Enable interoperable implementation by multiple vendors;

v. Implement cryptographic mechanisms consistent with contemporary industry standards for secure communications, including appropriate key lengths, algorithms and configurations.

c) Examples of protocols that may support RTD communications at the communication layer include:

- Wi-Fi
- Bluetooth

- Other open communications protocols capable of secure and interoperable data exchange.

d) Examples of protocols that may support RTD communications at the application layer include:

- Modbus
- MQTT
- HTTP-based APIs
- Other open communications protocols capable of secure and interoperable data exchange.

The use of these examples does not limit the use of other protocols that meet the requirements of this clause. Protocols must not include vendor-specific propriety extensions that restrict interoperability.

e) The use of open standards does not, in itself, ensure secure communications. The MC must implement appropriate security controls, including encryption and authentication, to ensure RTD communications are protected against unauthorised access and interference.

f) Security controls must be implemented in a manner that provides defence in depth across the RTD communications environment.

g) In implementing 3.2(b)(v), MCs should have regard to recognised Australian cybersecurity guidance, including publications issued by the Australian Signals Directorate, or equivalent industry standards.

3.3. RTD Security

a) The MC must ensure:

i. RTD communications are encrypted in transit

ii. RTD communications require authenticated device connections and prevent unauthorised access

iii. that RTD is only provided following successful authentication and establishment of an encrypted connection.

iv. that cryptographic controls are periodically reviewed and updated to address emerging vulnerabilities and changes in industry best practice.

b) RTD access must not permit:

i. modification of metering data

ii. modification of meter configuration

iii. energisation or de-energisation functions

iv. any other control of the *metering installation*.

c) The MC must ensure that logical RTD communications interfaces are isolated from metrology and *metering installation* control functions through controls that are effective in preventing

interference with, or compromise of, the integrity and operation of the metering installation, in accordance with clause 2.2(a)(iii).

Such controls must be designed to remain effective in the event of a compromise of RTD communication functions, including where those functions are subject to elevated or administrative-level access.

d) RTD communications must be implemented such that data flows are limited to the provision of RTD and do not permit control of the metering installation. Where RTD access involves externally initiated communications, including request or polling mechanisms, the MC must ensure that:

   i. Inbound communications are strictly limited to authorised requests for RTD; and

   ii. Appropriate controls are implemented to prevent unauthorised access, misuse, or exploitation of the communications interface.

   The MC should, where reasonably practicable, implement RTD communications architectures that minimise exposure to externally initiated connections.

e) The MC must ensure that devices and systems used to provide RTD communications are implemented and maintained in accordance with secure design principles, including:

   i. Protection against unauthorised modification of software and firmware;

   ii. Protection of cryptographic material; and

   iii. Management of vulnerabilities in a timely manner.

f) The MC must implement controls to protect RTD communications interfaces against denial-of-service and other availability-based attacks, to the extent reasonably practicable.

g) The MC must ensure that a documented security risk assessment is undertaken prior to the deployment of RTD communications interfaces and maintained on an ongoing basis.

   The security risk assessment must:

   i. Identify and assess threats, vulnerabilities and potential impacts, which also includes the integration of the RTD components into the *metering installation*, associated with RTD communications;

   ii. Be developed using a recognised threat modelling methodology, such as the STRIDE framework or an equivalent approach; and

   iii. Inform the implementation of security controls across the RTD communications environment.

   iv. ensure any firmware, software or configuration changes that may affect RTD communications are subject to documented change control

h) The MC must implement and maintain controls that:

   a. Prevent unauthorised access to RTD communications and associated systems;

   b. Enable detection of anomalous or unauthorised access attempts;

   c. Support timely response to, and containment of, security incidents; and

   d. Support recovery from security incidents and restoration of secure operation.

i) The MC must make the security risk assessment and associated controls available to AEMO upon request.

j) RTD provided under this Procedure must not include personal information, unless required under applicable law or the NER or NERR.

4. RTD Access

4.1. Establishing RTD Access

a) Upon receiving a request from a Retailer, the MC must facilitate RTD access at the *metering installation*.

b) The MC must ensure that:

   i. only authorised RTD Devices may access RTD

   ii. RTD access is established within the timeframes specified under the NERR.

c) The MC must maintain a register of RTD connections sufficient to identify active and historical RTD access arrangements and support compliance with this Procedure and provision of RTD access information under clause 4.5, including:

   i. NMI;

   ii. device identifier;

   iii. RTDAR identifier;

   iv. connection start date; and

   v. connection termination date.

4.2. Circumstances where RTD Facilitation Timeframes May Be Extended

In addition to NERR 59E(7), the timeframe for facilitating access to RTD may be extended where one or more of the following circumstances apply.

a) Where the *metering installation* at the connection point is subject to a malfunction or fault that prevents the *metering installation* from providing RTD.

   In these circumstances:

   i. The MC must first rectify the *metering installation* malfunction in accordance with the applicable obligations in the NER and relevant AEMO Procedures; and

   ii. The timeframe for facilitating access to RTD may be extended until the malfunction has been rectified and the *metering installation* is capable of providing RTD.

b) Where the MC is unable to access the *metering installation* for the purpose of enabling RTD due to circumstances including:

i. Denial of site access by the customer or occupant;

ii. Access restrictions imposed by building management;

iii. Safety or site conditions preventing safe access to the *metering installation*.

Where access restrictions do apply, the timeframe for facilitating access may be extended until access can reasonably be obtained.

4.3. Circumstances Where RTD Cannot Be Facilitated

A *retailer* is not required to facilitate access to RTD where it is not feasible to make RTD available at the premises due to circumstances beyond the control of the MC.

In addition to NERR 59E(8), circumstances where RTD access may not be feasible include where one or more of the following circumstances apply.

a) Where the existing *metering installation* does not support the provision of RTD and:

i. The *metering installation* cannot be retrofitted to enable RTD; or

ii. The *small customer* has not requested or agreed to the replacement of the *metering installation*.

b) Where communications required to enable RTD transmission cannot reasonably be established and RTD cannot be facilitated.

Examples include:

i. Signal limitations within multi-occupancy buildings;

ii. Physical distance between the *metering installation* and the customer premises;

iii. Interference preventing reliable communication between the *metering installation* and the RTD Device.

c) Where reasonable attempts to obtain access to the *metering installation* have been unsuccessful and access is necessary to enable RTD capability, RTD cannot be facilitated.

4.4. Revocation of RTD Access

a) The MC must revoke RTD access at a *metering installation* where:

i. the customer withdraws consent, or consent expires, as notified by the Retailer;

ii. the MC is notified that the RTDAR is deregistered; or

iii. the authorisation of the device is withdrawn or where credentials of the device expire or are invalid.

4.5. Provision of RTD Access Information to the FRMP

a) The MC must, upon request from the FRMP for a *connection point*, provide details of any active RTD access arrangements associated with the metering installation at that *connection point*.

b) The information provided must include, where available:

i. The identifier of the RTD recipient;

ii. The identifier of any authorised RTD Device;

iii. The date on which RTD access was established; and

iv. Any other information reasonably required by the FRMP to understand the active RTD access arrangements.

c) The MC must provide this information within 5 *days* following receipt of the request.

d) Where a change in the FRMP occurs at a *connection point*, the MC must make reasonable endeavours to provide the New FRMP with details of active RTD access arrangements associated with that *connection point*.

5. RTD Quality

5.1. RTD Measurement Resolution and Sampling Frequency

a) RTD measurements should be capable of representing:

i. RMS voltage with a resolution of at least 0.01 volts

ii. RMS current with a resolution of at least 0.01 amperes

iii. Phase angle with a resolution of at least 0.1 degrees

b) Where the *small customer metering installation* cannot support these resolutions, the highest available measurement resolution supported by the device may be provided.

c) To maintain true RMS accuracy for Australia's power system standard nominal frequency of 50 Hz, the *small customer metering installation* must be capable of a minimum sampling frequency of 64 samples per cycle (3.2 kHz – 3200 samples per second).

d) The RTD measurements specified in clauses 5.1 (a) to (c) must be measured and structured such that they can be represented in accordance with the RTD parameters and measurement codes defined in 6.1 and 6.2.

5.2. RTD Latency and Communications Performance

(a) The MC must ensure that RTD measurements obtained from a *small customer metering installation* are capable of being transmitted to an external device with a latency of no more than 5 seconds from the time the measurement is obtained.

(b) This latency requirement applies where the external device is located within 10 metres of the *small customer metering installation* and where communications between the *small customer metering installation* and the external device are not materially impeded by structural barriers, interference, or other environmental factors.

(c) Where the RTD Device is located beyond this distance, or where communications are affected by environmental or structural constraints, the MC must provide RTD at the maximum refresh rate supported by the *small customer metering installation* and communications interface.

(d) The MC is not responsible for latency introduced by:

I. External communications networks;

II. Customer devices or customer-provided communications equipment; or

III. Physical or structural constraints within a premises.

(e) Where reliable communications cannot be established within the reference distance specified in this clause, the *small customer* or RTDAR may install additional communications equipment (such as gateways, repeaters, or other intermediary devices) to enable access to RTD.

(f) The MC is not responsible for communications performance within the customer's premises beyond the communications interface of the *small customer metering installation*.

(g) Upon request from AEMO, the MC must be able to provide evidence demonstrating that *small customer metering installations* are capable of complying with the RTD latency and communications performance requirements specified in this clause.

6. RTD Standard Format

(a) Unless otherwise agreed with the party accessing RTD, RTD must be provided in a standard structured format as described below.

6.1. RTD Parameters

(a) These parameters must be capable of being mapped to the relevant communications protocol and data structure used to provide RTD.

Field	Definition
Meter Serial Number	Meter Serial ID
RTD Measurement Code	Code to identify RTD contents. This value must correspond to a valid RTD Data Type Measurement Code listed in Section 6.2.
Voltage Value	The measurement of voltage as an instantaneous value
Current Value	The measurement of current as an instantaneous value
Phase Angle Value	The measurement of phase angle in degrees as an instantaneous value • 0 to 90 degrees indicates current lagging voltage: withdrawn from the grid. • 90 to 180 degrees indicates current leading voltage: injected to the grid. • 0 to -90 degrees indicates current leading voltage: withdrawn from the grid. • -90 to -180 degrees indicates current lagging voltage: injected to the grid.

6.2. RTD Measurement Code

(a) RTD Measurement Codes to be used in reference to the table in Section 6.1. are as follows:

RTD Measurement Code	Meaning
C1	Current for the first element
C2	Current for the second element
C3	Current for the third element
V1	Voltage for the first element
V2	Voltage for the second element
V3	Voltage for the third element
A1	Phase angle for the first element
A2	Phase angle for the second element
A3	Phase angle for the third element

7. RTD Management Obligations

7.1. RTD Management by RTDAR

(a) RTDARs must:

i. obtain customer consent to access RTD in accordance with the NERR;

ii. only use RTD for the purposes authorised by the customer;

iii. cease accessing RTD and ensure that any record of RTD is deleted within 2 *days* upon notification that authority to access RTD has ceased or been withdrawn; and

iv. treat RTD as confidential information.

7.2. Compliance Monitoring

(a) AEMO may monitor compliance with these Procedures through measures including:

i. information requests

ii. audits

iii. investigation of suspected non-compliance.

(b) MCs and RTDARs must retain records necessary to demonstrate compliance with these Procedures.

(c) Should AEMO notify an MC or RTDAR of a suspected non-compliance, the MC or RTDAR must respond within two business days confirming compliance status and providing supporting information as requested by AEMO in the notice.

(d) The MC or RTDAR must inform AEMO immediately upon identification of a non-compliance, including where the non-compliance is identified as a result of the MC's or RTDAR's audit.

7.3. Security and System Information

(a) The MC must maintain documentation relating to the RTD communications environment sufficient to support security risk management and incident response.

(b) This documentation should include, where applicable:

i. High-level architecture descriptions of RTD communications implementations;

ii. Information on software and firmware components relevant to RTD communications;

iii. Nominated security contact details for incident management; and

iv. Any other information reasonably required to assess and respond to security risks associated with RTD communications

(c) The MC must make this information available to AEMO upon request.

7.4. Record Keeping

(a) MCs must maintain records relating to RTD access, including:

i. RTD access requests;

ii. device registrations;

iii. RTD access activation and termination; and

iv. security incidents related to RTD communications.

(b) Records must be retained for a period of 7 years.

8. RTDAR Accreditation Management

8.1. Audits undertaken by AEMO

(a) The RTDAR must undertake all services in a manner that is auditable by AEMO and must provide all reasonable assistance to AEMO in discharging its obligations under the NER in relation to RTDARs.

(b) AEMO will undertake periodic certification reviews to a negative assurance level of any relevant database maintained by the RTDAR to assess the RTDARs compliance with the NER, applicable procedures under the NER and this Procedure and for the maintenance of its accreditation as a RTDAR.

(c) All scheduled reviews will be through a centralised review process established by AEMO and will be undertaken at the RTDARs cost.

8.2. RTDAR to Assist

(a) Where a review is conducted under this Procedure, the RTDAR must, at its cost, provide all reasonable assistance including making databases, equipment and premises available for inspection, making personnel available for questioning, and providing copies of any data or information as requested.

8.3. Timing of Audits

(a) Scheduled reviews of the RTDARs performance will be annually or biennially at AEMO's discretion.

8.4. Notice of Audit

AEMO must provide the RTDAR a minimum of:

(a) 30 *business days'* notification prior to a scheduled review; and

(b) 15 *business days'* notification for the provision of any specific data requests as part of the audit.

8.5. Other Audits

(a) Audits may be undertaken at any time by AEMO in accordance with the NER.

(b) Each RTDAR must assist AEMO with reasonable requests for the provision of information about RTD that are the subject of a market audit.

8.6. Review of Accreditation

AEMO may review a RTDARs accreditation and subsequently require the RTDARs to apply for re-accreditation in accordance with the Qualification Procedure if:

(a) A RTDAR has been suspended from providing real-time data services and seeks to have the suspension lifted;

(b) There are changes to the NER and NERR or procedures under the NER that require significant functional system, process or procedural changes to be made by RTDARs;

8.7. Disputes

For the purposes of dispute resolution in accordance with clause 8.2 of the NER, the RTDAR is considered to be a *Registered Participant*. If a dispute arises between a RTDAR and AEMO, a *Registered Participant*, an MDP, an MP, an ENM, an NMISP and RTDAR in relation to the provision of services or this Procedure, the process detailed in clause 8.2 of the NER shall apply.

Version release history

Version	Effective Date	Summary of Changes
1.0	30th November 2028	First Issue