Data Standards Body

Technical Working Group

Decision 191 – Retailer to AEMO InfoSec Profile

Contact: James Bligh

Publish Date: 13th September 2021

Decision Approved By Chairman: 21st September 2021

Context

A peer-to-peer model has been adopted for the energy sector under the Consumer Data Right (CDR) regime. Under this model Accredited Data Recipients (ADRs) will interact with electricity retailers to seek authorisation for data sharing and to initiate data sharing requests.

As AEMO is also a designated data holder for the energy sector but will not have direct interaction with ADRs, the retailers will need to contact AEMO to obtain requested data for which AEMO is the designated data holder.

This means that there is a need for a specific information security profile to prescribe the mechanism for an electricity retailer to authenticate with, and initiate, data requests with AEMO.

Consultation on the approach for this information security profile has been conducted with a focus on the following scope:

- The content of the information security profile for retailers to interact with AEMO
- The level of detail of the information security profile
- The ongoing maintenance and management of the information security profile over time

The options presented in this consultation were as follows:

- **Options for Retailer to AEMO Information Security Profile**
    - **Option 1 – AEMO e-Hub Security Profile**
      Delegate to the existing e-Hub security profile already maintained by AEMO. Ongoing maintenance and management will be managed by AEMO
    - **Option 2 – CDR Specific Security Profile**
      Create a standalone, specific, security profile that will be maintained by the DSB on an ongoing basis
- **Options for Level of Specificity in Consumer Data Standards**
    - **Option A – Delegated Documentation**
      Delegate the documentation of the information security profile to AEMO
    - **Option B – Light Documentation**
      The security profile would be documented in the CDR standards but only at a high level with key principles being called out
    - **Option C – Prescriptive Documentation**
      The standards will be expanded to include detailed documentation of the new information security profile to a level consistent with the current profile

Decision To Be Made

Define the information security profile to be used for retailers to initiate data requests with AEMO.

Feedback Provided

The original proposal and the associated feedback can be found at:
https://github.com/ConsumerDataStandardsAustralia/standards/issues/191

This proposal recommended the adoption of Option 1 (AEMO e-Hub Security Profile) and Option A (Delegated Documentation).

Feedback indicated the following:

- Strong support for the recommendation from the energy retailer community
- Feedback on specific items regarding the AEMO information security profile as it currently stands
- Feedback from the banking community that FAPI should be adopted for the interaction between AEMO and retailers
- It was flagged that, if delegation to AEMO occurred and there were issues, there may be a future need for any delegation to be revisited

In addition, the recommendation was strongly supported by AEMO. This feedback was provided during the formulation phase of the proposal and was recorded in the proposal itself. This feedback was not provided in the consultation thread.

Decision For Approval

As a result of the feedback received the following is decided:

Use of AEMO e-Hub Security Profile

In its function as market operator of the National Energy Market, AEMO already maintains a registration process for industry participants and shares data with participants using real time, RESTful APIs. This is done via the platform known as the e-Hub.

These processes currently include support processes for registration, maintenance of certificates, and the management of change. Documentation includes a developer portal, API documentation and a security profile. More information can be found at:
https://www.aemo.com.au/-/media/files/electricity/nem/it-systems-and-change/2020/guide-to-aemos-ehub-apis.pdf

The CDR standards will require the use of the e-Hub platform and associated mechanisms for the requesting of data from AEMO by retailers as a normative standard.

Ongoing Management of e-Hub Security Profile

The existing mechanisms that are already in place to manage and evolve the e-Hub Security Profile will continue to be used with AEMO accountable for the management of that process.

The DSB will direct any requests for clarification or change regarding the e-Hub Security Profile to AEMO.

As is done for all normative standards the DSB will document the adoption of the normative standard, including a specific version. The DSB will seek approval of the Chair to update the standards to adopt new versions of the e-Hub Security Profile when notified of change by AEMO.

Future Changes to Normative Standard Adoption

The adoption of any normative standard is a positive statement in the CDR standards and, like any aspect of the standards, open to change in the future.

If there are ongoing concerns with the e-Hub Security Profile raised by the CDR community this decision may be revisited in the future, in the same way that the use of any normative standard is open to review. Any such event would take into account all of the considerations of such a change including the implementation considerations for existing participants.