Data Standards Body

Technical Working Group

Decision Proposal 191 – Retailer to AEMO InfoSec Profile

Contact: James Bligh

Publish Date: 1st July 2021

Feedback Conclusion Date: 23rd July 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.

The scope of this consultation will cover the following:

- 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

This decision proposal has been developed to balance the following principles adopted for the development of standards for the CDR:

- **Outcome Principle 1: APIs are secure**
  An appropriate level of security must be enforced to protect consumers and participating entities. The profile described in this decision proposal must meet this objective.

- **Outcome Principle 5: Standards are consistent across sectors**
  While the interaction between retailers and AEMO is sector specific, the concept of a secondary data holder may occur in subsequent sectors as a pattern. The model adopted for the energy sector must therefore be developed considering the precedent being set for future sectors and the potential that more sector specific profiles may be required.

- **Technical Principle 3: APIs are simple**
  Simplicity of implementation and maintenance should be a guiding factor in the development of this profile. This will reduce risk, reduce cost and simplify governance.

Decision To Be Made

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

Identified Options

This section identifies the key options to be considered for feedback. The options fall into two categories. The first category of options describes options for the proposed content of the information security profile, the second category describes options for the level of specificity to be included in the data standards.

Options for Retailer to AEMO Information Security Profile

Option 1 – 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

Under this option, the CDR standards would require the use of the e-Hub platform and associated mechanisms for the requesting of data from AEMO by retailers. This would effectively delegate the ongoing management of this security profile to the existing AEMO mechanisms.

It is expected that this option would reduce the implementation and ongoing maintenance costs for retailers and AEMO by leveraging existing mechanisms that must already be maintained.

Option 2 – CDR Specific Security Profile

The DSB would define and consult on a CDR specific security profile to be implemented by both retailers and AEMO. This profile may leverage, but would not align to, the existing mechanisms in place in the e-Hub. Ongoing change of the profile would be managed exclusively using CDR processes.

If this option was adopted, then further consultations would be required and existing patterns already in use in the CDR standards would be leveraged as much as possible.

Options for Level of Specificity in Consumer Data Standards

Option A – Delegated Documentation

This option is only applicable if Option 1 for the first category is selected. If the decision is made to adopt the AEMO e-Hub Security Profile then the CDR standards would refer to this standard as a

normative standard and delegate maintenance and clarification of implementation questions to AEMO.

As with other normative standards underpinning the CDR standards there may be some specific aspects of the e-Hub Security Profile that must be constrained to meet CDR specific functionality or rules. These specific cases would be documented by exception.

Option B – Light Documentation

In this option the security profile would be documented in the CDR standards but only at a high level.

If Option 1 is adopted, then this would mean that the e-Hub Security Profile would be described at a high level with reference to AEMO documentation as required. Any changes made to the e-Hub Security Profile by AEMO would need to be synchronised with the CDR standards.

If Option 2 is adopted, then the security profile would be documented at a high level with specificity provided by normative standards.

Option C – Prescriptive Documentation

In this option the security profile would be documented in full within the CDR standards.

If Option 1 is adopted, then this would mean that the e-Hub Security Profile would be described in full and any changes made would need to be managed in tandem by AEMO and the CDR regime.

If Option 2 is adopted, then the security profile would be documented at a level similar to that already defined for the ADR to data holder security profile.

Current Recommendation

The recommendation of the DSB, based on current understanding, is to adopt:

- Option 1 – AEMO e-Hub Security Profile, and
- Option A – Delegated Documentation

This recommendation is open to change in response to feedback.

These recommendations have been made considering the following factors:

- Leveraging an existing mechanism, with all associated processes, that a group of industry participants are already familiar with will reduce cost both in the initial phases but also on an ongoing basis.
- Documenting an existing security profile again in a different location will create ongoing maintenance costs to ensure the documentation is synchronised. It will also create confusion as to the appropriate entity to engage with to request change.
- The model of reuse of existing industry norms where there is no compelling reason for CDR specific treatment is an approach that can be used for future sectors.

Implementation Considerations

The options included in this consultation have implementation considerations due to the associated build costs for the participating parties. Feedback is specifically requested regarding the expected implementation and maintenance impacts of the options presented.