BIZA·IO

Response to Decision Proposal 191: Retailer to AEMO InfoSec Profile

Introduction

Decision Proposal 191 appears to be intended to make a decision as to whether data exchanged between AEMO and Retailers should adopt:

- Existing API and Information Security Profile definitions provided by the AEMO e-hub (e-hub) are to be adopted or;
- Be defined as part of the Data Standards setting process within the Energy sector

In providing feedback regarding these options Biza.io seeks to consider a number of key components notably whether the AEMO e-hub Security Profile (e-hub Profile) is:

- Fit for purpose
- Aligned to the broader Data Standards principles and guidelines
- Suitable for adoption within a competitive CDR landscape

Further Biza.io provides recommendations relative to its analysis with respect to improvements to the e-hub Profile that would be necessary before it considers it appropriate for use as a CDR backing data store.

References

The following documents were used and are referenced during preparation of this analysis:

Document Name	Date (Version)	URL
Australian Competition and Consumer Commission Certificate Policy (ACCC Certificate Policy)	11 June 2020 (1.02)	https://www.cdr.gov.au/sites/default/files/2020-12/CDR - ACCC Certificate policy.pdf
Draft Energy Standards	1 June 2021 (0.2.0 DRAFT)	https://consumerdatastandardsaustralia.github.io/standards/draft/energy-draft.html
Decision Proposal 191 (DP191)	20 June 2021 (N/A)	https://github.com/ConsumerDataStandardsAustralia/standards/issues/191
Guide to AEMO's e-Hub APIs	October 2020 (1.03 Final)	https://www.aemo.com.au/-/media/files/electricity/nem/it-systems-and-change/2020/guide-to-aemos-ehub-apis.pdf
Shared Market Protocol (SMP) Technical Guide	11 April 2018 (1.15)	https://www.aemo.com.au/-/media/Files/Electricity/NEM/Retail_and_Metering/B2B/2018/B2B-SMP-Technical-Guide.pdf
Standards | AEMO APIs	Unknown (Unknown)	https://dev.aemo.com.au/standards
AEMO e-hub	Unknown (Unknown)	https://dev.aemo.com.au/
AEMO e-hub Security Profile (e-hub Profile)	October 2020 (1.03 Final)	https://www.aemo.com.au/-/media/files/electricity/nem/it-systems-and-change/2020/guide-to-aemos-ehub-apis.pdf [Page 13]
AEMO Copyright Permissions	26 July 2021 (Unknown)	https://www.aemo.com.au/privacy-and-legal-notices/copyright-permissions
API Acceptable Use Policy	26 July 2021 (Unknown)	https://dev.aemo.com.au/terms
The OAuth 2.0 Authorization Framework (OAuth2)	October 2012 (RFC6749)	https://datatracker.ietf.org/doc/html/rfc6749

Analysis of the e-hub Profile

When attempting to analyse the linked documentation within DP191 it is apparent that the linked e-hub documentation intertwines the Information Security aspects with the API definition and Support aspects of the e-hub services.

This makes it challenging to separate commentary between DP191 and DP192 especially as the *Guide to AEMO's e-Hub APIs* makes explicit statements including:

- defining URI hierarchy (Pg 5)
- declaring support for "XML, JSON, or a custom schema" (Pg 5)
- mandating OpenAPI of unspecified version (Pg 4)
- mandating additional headers while missing those defined within the CDS (Pg 9)
- incorporating path-based endpoint versioning (Pg 6)

API Considerations

The e-hub Profile with respect to APIs:

- is a hybrid of JSON and WSDL defined XML request and responses
- are defined as OpenAPI 3 specification files, although these are erroneously referred to as Swagger files within the *Guide to AEMO's e-Hub APIs*
- mandate several AEMO specific headers notably:
  - `x-initiatingParticipantId`
  - `x-market`
  - `x-eHub-APIKey` (SMP endpoints)

In addition, the *Standards | AEMO APIs* part of the AEMO developer site appears to:

- overlap and indeed *often directly conflict* with a reasonably large portion of the Consumer Data Standards
- have variable adoption of standardisation and instead appear to be an evolution of endpoints collected over time with several different paradigms defined
- define optional participant APIs (akin to Data Recipient APIs) within the Shared Market Protocol which seem to occur via WSDL defined XML request and responses. It is unclear if these participant APIs will operate independently of potential CDR Recipient APIs
- defines a set of generic error messages which will, quite likely, be difficult to effectively translate into Data Standards error codes
- define within *Standards | AEMO APIs* that *"AEMO's API Platform enforces traffic limits. For details about the traffic limits for each individual API, see the individual API policy".*

  Biza.io went looking for the individual API traffic limits but was unable to find them for any API published on the development site and, as a consequence, it is unclear if the AEMO e-hub will provide service to participants that is sufficient for and allow them to achieve future Non Functional Requirements defined for the energy sector.

System Authentication & Authorisation Considerations

The e-hub Profile regarding authentication and authorisation define:

- use of Mutual TLS signed by an undefined Certificate Authority (presumably an AEMO controlled Private CA)

  Note*:* "Mutual TLS" is never *explicitly* stated in any accompanying documentation ` has found so this is an assumption determined on the provisioning process.

- reliance on Basic HTTP Authentication incorporating a username/password provisioned **per API endpoint** and appear to be referred interchangeably within documentation as an *API key*, *Base64 authorisation token* or *username & password*.

  Note*:* What an API Key is limited to is never *explicitly* stated within the *Guide to AEMO's e-hub APIs* however it *seems* to be outlined within the *Shared Market Protocol (SMP) Technical Guide* (Pg 10)

- credential expiration of 60 days (*Guide to AEMO's e-Hub APIs, Pg 26)* although in some cases it is specified as potentially having No Expiration (*Shared Market Protocol (SMP) Technical Guide, Page 10)*

- authorisation controls using a basic authentication pairing *per API endpoint*. It is unclear at this stage as to whether this paradigm is the intent with the currently published *Draft Energy Standards* as these standards do not currently specify any type of access control definitions for these endpoints.

Network Connectivity Considerations

The AEMO e-hub Profile defines network components including:

- that endpoints are published at both Internet accessible and via private interconnect (*"MarketNet"*)
- use of IP whitelisting as an access control mechanism
- *"defence against Denial of Service (DoS) attacks"* using variable custom ports for both HTTPS and the Shared Market Protocol administration

Cryptographic Signature Considerations

AEMO does not appear to have a published Certification Practice Statement or Certificate Policy and the e-hub Profile currently allows for a single certificate to be used by multiple participants.

Additionally, there does not appear to be consideration for the federation of cryptographic chains between the ACCC Certificate Authority and the AEMO Certificate Authority.

Intellectual Property Considerations

The *Guide to AEMO's e-Hub APIs* contains zero explicit licensing information for the documentation or the APIs. There is a footer which states "*The material in this publication* *may be used in accordance with the copyright permissions on AEMO's website".*

This appears to be a reference to the AEMO Copyright Permissions which states:

In addition to the uses permitted under copyright laws, AEMO confirms its general permission for anyone to use AEMO Material for any purpose, but only with accurate and appropriate attribution of the relevant AEMO Material and AEMO as its author.

However when joining the AEMO e-Hub website a participant must agree to the API Acceptable Use Policy which makes a number of general statements with regard to API usage, of note:

You may not use the AEMO Services without agreeing to this AAUP. Thus, you agree not to use, and not to encourage or allow any End User to use, the AEMO Services in the following prohibited ways:
[…]
3. To reverse-engineer the AEMO API;
4. To develop your application in a manner not consistent with the Developer Guide;
[…]
11. To use the AEMO API to transmit any material that infringes the intellectual property rights or other rights of third parties;

Unlike the Data Standards, which are licensed under the highly permissive and unambiguous MIT license, neither of the legal documents Biza.io found provide unambiguous permission to reproduce the APIs, for instance to provide testing sandboxes to participants.

Summary of issues for AEMO e-hub Profile Adoption

The following issues have been identified with respect to the adoption of the AEMO e-hub security profile:

- Authentication is conducted on a per API and HTTP Basic authenticated key mechanism. This is not only a weak authentication mechanism but also represents the potential for a significant maintenance burden if the keys are per API
- The APIs delivered by the *AEMO e-hub* appear to be quite proprietary in nature incorporating custom authentication mechanisms, custom headers, custom port allocations. This does not appear to be aligned to the:
  - *Outcome Principal 5: Standards are consistent across sectors* or;
  - *Technical Principal 3: APIs are simple.*
- There is no Certificate Policy or Practice Statement which may lead to a violation for a Holder onboarding infrastructure within a dual role between CDR Data Holder APIs and AEMO relayed APIs
- Sharing of certificates among *multiple* participants is permitted. This could be a violation of the *ACCC Certificate Policy*. For multiple data holder brands this could increase the chances of a loss of data containment.
- The trust chain between Data Recipient and Data Holder's is completely separated from the trust chain between a Data Holder and AEMO. This represents not only a key store management challenge but also means that designated data will flow over channels for which the ACCC Certificate Authority has no purview
- Whitelisting of source IPs may present a challenge for cloud based SaaS providers of Data Holder solutions

Recommendations

We believe it is important to align the security characteristics of participating systems to the level expected between Holders and Recipients and therefore put forward the following suggestions for improvement:

- Utilise a trust chain incorporating the ACCC Certificate Authority. This can be done via a tertiary level intermediary or a new intermediary within the same ACCC Root Certificate authority
- Formally adopt the existing or develop an equivalent certificate policy that is aligned with the currently mandated *ACCC Certificate Policy*
- Adopt a token based authentication method for e-hub Profile API access which utilises Data Standards & Register Standards aligned OAuth2 JWT client assertions (ie. `private_key_jwt`) coupled with OAuth2 scopes. This will allow alignment to existing key management practices already present in CDR solutions.
- Remove Source IP whitelisting as it is a potential limiter to cloud based deployments and is a questionable information security control
- Uplift existing documentation to incorporate unambiguous technical detail so that implementers are able to interpret more effectively.
- Update the intellectual property guidelines of the *e-hub Profile* to be clear and unambiguous to facilitate active market participation of CDR solution providers without restriction or risk of AEMO or AEMO Contracted parties to restrict development of CDR solutions such as Development Sandboxes, As-a-Service products etc.

Broadly speaking Biza.io is in favour of utilising existing infrastructure to lower implementation costs however we question whether the current e-hub Profile security posture is appropriate for the use within the CDR.

Biza.io understands there are existing integrations already in play but notes that a Data Holder’s achievement of CDR APIs would require them to adopt many of the recommendations above which would, at least somewhat, ameliorate the perceived additional complexity of cascading these components through to AEMO controlled endpoints.

About Biza.io

Biza.io are the market leaders in Data Holder solutions to the Consumer Data Right and are the only *pure-play* CDR vendor in Australia. Founded by the former Engineering Lead of the Data Standards Body (DSB), Biza.io has been involved in the Data Standards setting process since the very beginning and its personnel remain the largest non-government contributors to the consultations. In addition to its participation within the CDR, Biza.io is also a contributing member of the Financial-grade API (FAPI) Working Group, contributors to the FAPI 1.0 information security profile and co-authors of the Grant Management for OAuth 2.0 specification.

About Our Customers

As of July 2021, Biza.io is directly responsible for delivering, or heavily involved in the verification of, **one in three** of all active Data Holders. Beyond just a contractual engagement Biza.io considers all of its customers partners in the journey toward open data. Our customers choose us to not only achieve compliance but to compete then command the consumer data ecosystem.