Project EDGE

DER Data Hub Lessons Learnt Report

June 2023

This report has been developed with the support of:

Important notice

PURPOSE

This DER Data Hub Lessons Learnt report has been prepared for Project EDGE by the Energy Web Foundation in collaboration with AEMO and the other Project EDGE participants, AusNet Services and Mondo (collectively, the Project Participants). Energy Web Foundation is the technology vendor that provided the data exchange mechanism to facilitate the Projects EDGE and Symphony Field Trials.

This DER Data Hub Lessons Learnt report documents the lessons learnt during the Project EDGE trial which involved applying identity and data exchange within a Distributed Energy Resources (DER) Marketplace. The lessons described are provided to inform considerations of high-level models for DER integration and data exchange and are intended to be technology-agnostic. Although this report contains some details of the technology used within Project EDGE, these details have been included for information purposes only and not to endorse or further prescribe the use of the technology described. The Project Participants do not endorse or intend to prescribe any technology choices or vendors based on this report.

As with all Project EDGE reports, this content is offered in a spirit of transparency and knowledge sharing and is intended to be an input to industry deliberation about the best course of action regarding DER and how to maximise value for all consumers. As such, the intended audience for this report is expected to be electricity industry staff engaged with DER policy and operations, together with solution architects and other technical resources involved in broader industry technological uplift to support Australia's energy transition.

DISCLAIMER

The Project Participants have commissioned this DER Data Hub Lessons Learnt report by the Energy Web Foundation (EWF) for the purposes of Project EDGE. Each of the Project Participants has collaborated with EWF throughout the preparation of this DER Data Hub Lessons Learnt report to ensure the quality of the information provided but they cannot guarantee that the information, forecasts and assumptions contained it are accurate, complete or appropriate for your circumstances. This DER Data Hub Lessons Learnt report does not include all of the information that an investor, participant or potential participant in the national electricity market might require, and does not amount to a recommendation of any investment.

Anyone proposing to use the information in this DER Data Hub Lessons Learnt report (which has been prepared by EWF in collaboration with the Project Participants, and includes information and forecasts from EWF and other third parties) should independently verify its accuracy, completeness and suitability for purpose, and obtain independent and specific advice from appropriate experts.

Accordingly, to the maximum extent permitted by law, each Project Participant and its officers and employees:

- make no representation or warranty, express or implied, as to the currency, accuracy, reliability or completeness of the information in this DER Data Hub Lessons Learnt report; and
- are not liable (whether by reason of negligence or otherwise) for any statements, opinions, information or other matters contained in or derived from this, or any omissions from it, or in respect of a person's use of the information in this DER Data Hub Lessons Learnt report.

ARENA ACKNOWLEDGEMENT AND DISCLAIMER

Project EDGE received funding from ARENA as part of ARENA's Advancing Renewables Program.

The views expressed herein are not necessarily the views of the Australian Government, and the Australian Government does not accept responsibility for any information or advice contained herein.

Each Project Participant acknowledges:

- the work of the Energy Web Foundation in preparing this Data Hub Lessons Learnt report; and
- the support, co-operation and contribution of the other Project Edge participants and consultants in providing data and information used to prepare this report.

COPYRIGHT

VERSION CONTROL

Version	Release date	Changes
1	29 May 2023	
2	8 June 2023	Updated by AEMO to clarify messaging following initial stakeholder feedback

Executive summary

Project EDGE (Energy Demand and Generation Exchange) is a collaboration between AEMO, AusNet Services and Mondo, with financial support from the Australian Renewable Energy Agency (ARENA), to demonstrate a Distributed Energy Resource (DER) Marketplace that efficiently operates Distributed Energy Resources (DER) to provide both wholesale and local network services within the constraints of the distribution network.

The digital infrastructure developed to support Project EDGE's transactions and activities was an integral testing ground for a future energy market where the significant deployment and proliferation of orchestrated price-responsive DER is expected and required.

At the commencement of Project EDGE, Energy Web Foundation (the technology vendor that provided the data exchange mechanism to facilitate the Project EDGE Field Trial) committed to provide this DER Data Hub Lessons Learnt (DHLL) report, including lessons learnt through the field trial, to help inform any future development of a production grade DER data exchange solution for industry.

This report, together with other Project EDGE publications, are intended to provide a key input into AEMO's and industry's consideration of its future model for DER data exchange.

1.1 Overview and Objectives

This DHLL provides an overview of emerging DER use cases and associated data exchange problems identified by industry stakeholders, as well as how the EDGE DER Data Hub addressed them. It covers:

- challenges presented by a two-sided market with very large volumes of DER, including key identity and access management, technical integration management, as well as maintaining information integrity;
- the DER-based problem statements and use cases identified and confirmed by industry stakeholders as part of a coordinated Project stakeholder engagement effort;
- the DER Data Hub developed to support the EDGE trials, including its functional capabilities, high-level design, integration requirements, and industry roles / responsibilities;
- Lessons learnt throughout the Project relating to how a DER Data Hub could enable scalable DER data exchange;
- Recommendations for designing, developing, and deploying a DER data hub in production across the NEM noting that much of the future infrastructure could be leveraged to also serve the WEM.

For the best clarity and understanding of this subject, this report should be read in conjunction with the independent report by EY, *Project EDGE: Technology and Cybersecurity Assessment*[1], which is referenced throughout this report.

[1] AEMO, Project EDGE, Technology and Cybersecurity Assessment, June 2023

1.2 Project EDGE: The Future DER Landscape

By 2050 DER are expected to represent 40% of total installed system capacity[2] and provide a range of services benefitting individual consumers and the NEM as a whole[3]. In Western Australia the WEM is already facing significant operational issues that could be better managed with orchestrated DER. Both the WEM and NEM must adapt to facilitate broad market participation of DER, accommodating their capabilities for dynamic bi-directional trade in, and flows of, electricity.

While this DER-driven paradigm shift is acutely felt in Australia, markets around the world are grappling with the same issues[4]. Though specifics vary by region, the common theme throughout is clear - what is needed is a dramatic expansion of market access for DER via digitalisation that can coordinate DER flexibility to balance the needs of wholesale markets, local network services, and individual consumers.

Enabling widespread and beneficial DER participation in Australia means AEMO, DNSPs, aggregators, Original Equipment Manufacturers (OEMs) and customer agents must have the capability to exchange extremely high volumes of data using consistent data models, controls, and communication methods throughout the entire DER lifecycle in order to effectively perform their respective functions in the market.

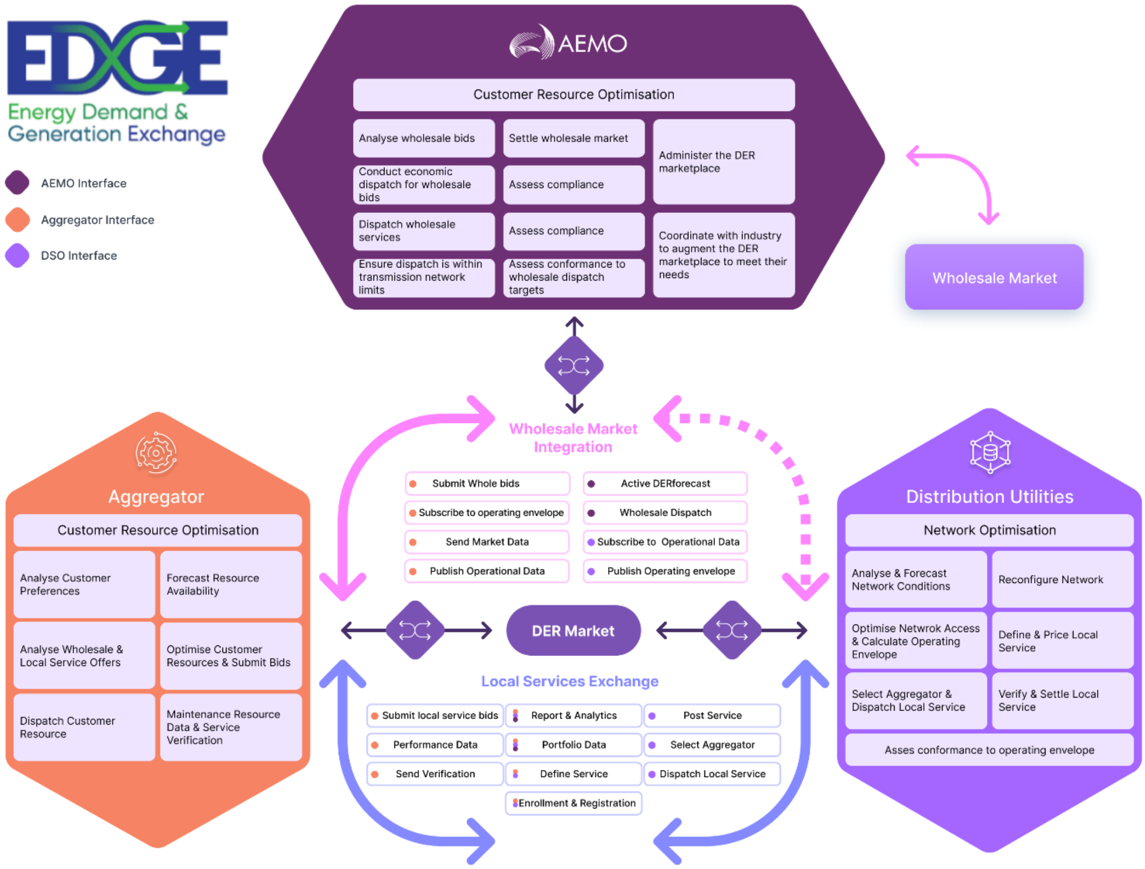
Project EDGE was established to test a DER Marketplace concept in practice which involved exploring new technologies and processes. One project element involved testing of a common digital infrastructure to reduce barriers of information technology and data silos currently inhibiting DER coordination and transactions. In Western Australia, Project Symphony was established to pilot and develop a pathway toward DER orchestration, and to demonstrate the extent to which this infrastructure can support system, market and customer outcomes.

[2] AEMO 2022 Integrated System Plan

[3] Integration of DER to provide flexibility services is a focus of the Energy Security Board's Post-2025 reforms

[4] For example: calls for improved coordination between transmission and distribution systems, as outlined by the Council of European Regulators; FERC Order 2222 in the United States; Calls for common digital infrastructure to coordinate multiple markets in the UK (Ofgem). See Section 3 for details.

Figure 1 Project EDGE Data Exchange Functions and Data Flows


EDGE
Energy Demand & Generation Exchange
AEMO Interface
Aggregator Interface
DSO Interface
AEMO
Customer Resource Optimisation
Analyse wholesale bids
Settle wholesale market
Administer the DER marketplace
Conduct economic dispatch for wholesale bids
Assess compliance
Dispatch wholesale services
Assess compliance
Coordinate with industry to augment the DER marketplace to meet their needs
Ensure dispatch is within transmission network limits
Assess conformance to wholesale dispatch targets
Wholesale Market
Wholesale Market Integration
Submit Whole bids
Active DERforecast
Subscribe to operating envelope
Wholesale Dispatch
Send Market Data
Subscribe to Operational Data
Publish Operational Data
Publish Operating envelope
DER Market
Local Services Exchange
Submit local service bids
Report & Analytics
Post Service
Performance Data
Portfolio Data
Select Aggregator
Send Verification
Define Service
Dispatch Local Service
Enrollment & Registration
Aggregator
Customer Resource Optimisation
Analyse Customer Preferences
Forecast Resource Availability
Analyse Wholesale & Local Service Offers
Optimise Customer Resources & Submit Bids
Dispatch Customer Resource
Maintenance Resource Data & Service Verification
Distribution Utilities
Network Optimisation
Analyse & Forecast Network Conditions
Reconfigure Network
Optimise Netwrok Access & Calculate Operating Envelope
Define & Price Local Service
Select Aggregator & Dispatch Local Service
Verify & Settle Local Service
Asses conformance to operating envelope

Each use case including DER being engaged with the market involves distinct stakeholders communicating specific datasets with particular formats (or schemas) at varying frequencies and volumes. Accordingly, making generalised statements about functional requirements for the industry as a whole is difficult. However, there are a few core capabilities that provide a foundation to enabling scalable DER integration and data exchange:

- Managing Identities and Permissions: inter-organisational data exchange is predicated on the ability for multiple parties to mutually authenticate each other's identity and authorise selective disclosure or communication of information between them based on their respective roles and responsibilities.
- Managing Integrations: from an operational perspective, DER data exchange relies on technical integrations between siloed, disparate systems owned and maintained by many different industry actors, such as aggregators and retailers, DNSPs, as well as AEMO.
- Maintaining Information Integrity: given the growing volume and diversity of DER data, it's imperative that all industry actors work with an accurate and consistent set of facts. The NEM and WEM will need mechanisms to ensure that data quality and integrity is maintained in the process of being exchanged among systems to enable the transition to a two-sided market with much larger volumes of DER.

While today there exist some individual digital components that address, in part, these key DER co-ordination capabilities, they are not consolidated into a cohesive ecosystem. The lack of a coherent, system-wide, digital framework that connects the many different markets for distributed flexibility is a significant barrier to realising the full value of DER, and manifests in four primary problem categories:

- DER Data Inconsistency across Industry Participants: DER standing data is replicated across multiple independent systems maintained by AEMO, DNSPs, retailers, and customer agents. Inconsistencies create significant operational challenges and inefficiencies for all stakeholders, as DER standing data represent the foundational inputs for nearly all market and Business to Business (B2B)[5] transactions.
- High Data Exchange Costs: Industry actors incur significant costs implementing and maintaining a series of bespoke, bilateral data exchange integrations with DNSPs, AEMO and other industry actors.
- Visibility of DER Between Industry Actors: DER operational data is fragmented across multiple independent IT systems, and it is costly and complicated for industry participants to selectively disclose this data with each other, inhibiting their ability to perform their respective functions in the market.
- Maintain cyber security in a decentralising power system: In the absence of widely adopted standards, the inherent variation in proprietary DER platforms and protocols currently used by industry actors makes it challenging to establish uniform, controlled, and auditable digital identities and associated data exchange systems that are guaranteed to establish trust and implement strong security and reliability capabilities. This challenge also extends to the interaction between industry participants and the DER however these interactions are not within the scope of this document.[6]

Project EDGE proceeded with a working hypothesis that a data hub model, as opposed to a point-to-point model, is the most efficient and scalable way to deliver the three core capabilities described above, and address the four problem categories associated with DER.

1.3 EDGE Data Hub Implementation for the Operational Trial

Project EDGE developed and deployed a Proof-of-Concept (PoC) DER data hub based on a common, open-access messaging infrastructure that:

- Allows multiple participants (retailers and DER aggregators) and DNSPs to send, receive, and authenticate messages based on the roles that have been issued to and associated with their self-managed identity;
- Allows participants, DNSPs, and AEMO to exchange diverse datasets, ranging from real-time telemetry to bulk file uploads, in support of multiple DER use cases;

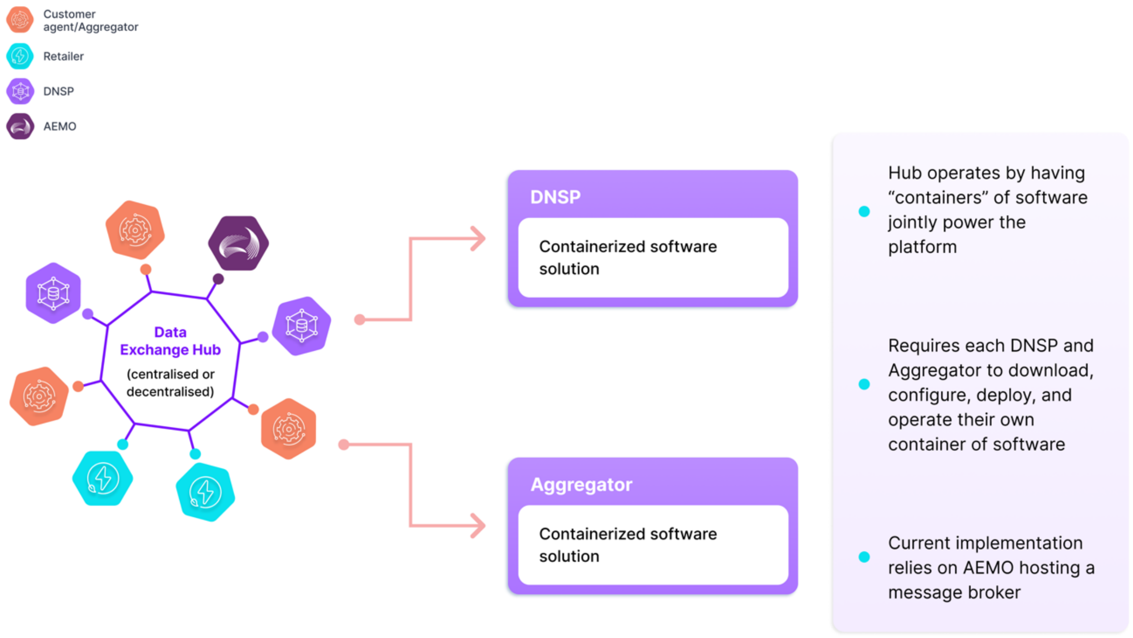
[5] In this report, the term "B2B" refers specifically to inter-organisational processes, transactions, and communications between NEM actors (i.e. AEMO, DNSPs, aggregators).

[6] For additional context on cybersecurity as it relates to DER data exchange, refer to AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023.

- Requires only a single integration mechanism with a central infrastructure in order to communicate via one:one (bilateral), one:many (broadcast), and many:many (multicast) channels.

The Data Hub implemented in EDGE is a decentralised hub operating within a centralised environment (i.e. a single node only) utilising a Container for participant integration, the conceptual architecture for which is shown in the figure below. For an outline of the data exchange options considered for EDGE, see Section 3.4 Solution Options and Challenges.

Figure 2 Conceptual Architecture of EDGE Decentralised Data Hub Implementation with Container-based integration


Customer agent/Aggregator
Retailer
DNSP
AEMO
Data Exchange Hub
(centralised or decentralised)
DNSP
Containerized software solution
Aggregator
Containerized software solution

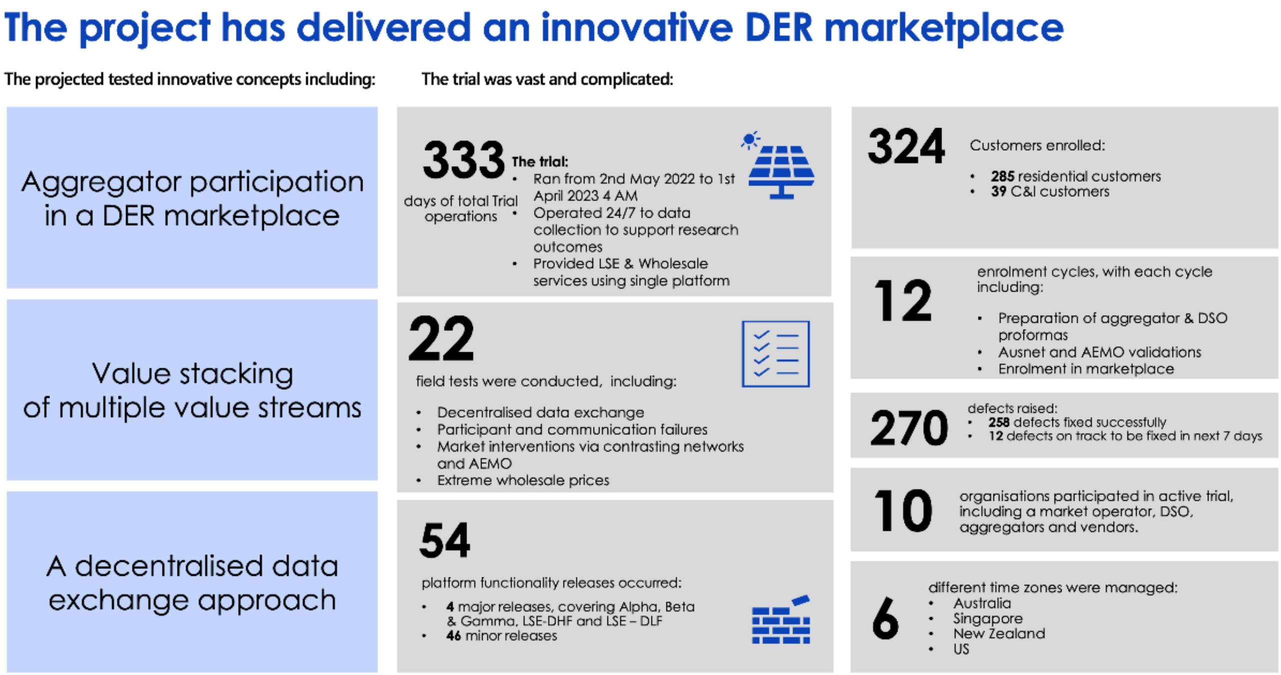
- Hub operates by having “containers” of software jointly power the platform
- Requires each DNSP and Aggregator to download, configure, deploy, and operate their own container of software
- Current implementation relies on AEMO hosting a message broker

The primary technical innovations in EDGE were related to:

- Integration: A standardised integration mechanism with a central infrastructure that enabled participants to exchange multiple data types and formats via a single integration;
- Identity and access management: Enabling participants to perform authentication and authorisation processes for multiple markets and use cases with a single portable, self-managed digital identity, and;
- Information integrity: Combining a shared messaging transport layer with identity-based message authentication and a novel distributed consensus technology to ensure consistency and security in the exchange of information between stakeholders.

To test the hypothesis that a data hub model provides a scalable and long-term approach for DER Marketplace data exchange, Project EDGE conducted field trials between May 2022 and March 2023. The EDGE data exchange platform was initially deployed in May 2022, with AEMO, AusNet, and Mondo as the initial trial participants. Further platform updates were released throughout Q3 2022, and as of September 2022 two additional aggregators were on-boarded into the field trial. The figure below highlights some key marketplace statistics about the trial.

Figure 3 Project EDGE marketplace statistics



The project has delivered an innovative DER marketplace

The projected tested innovative concepts including:

Aggregator participation in a DER marketplace

Value stacking of multiple value streams

A decentralised data exchange approach

The trial was vast and complicated:

333 days of total Trial operations

The trial:
- Ran from 2nd May 2022 to 1st April 2023 4 AM
- Operated 24/7 to data collection to support research outcomes
- Provided LSE & Wholesale services using single platform

22 field tests were conducted, including:
- Decentralised data exchange
- Participant and communication failures
- Market interventions via contrasting networks and AEMO
- Extreme wholesale prices

54 platform functionality releases occurred:
- **4** major releases, covering Alpha, Beta & Gamma, LSE-DHF and LSE – DLF
- **46** minor releases

324 Customers enrolled:
- **285** residential customers
- **39** C&I customers

12 enrolment cycles, with each cycle including:
- Preparation of aggregator & DSO proformas
- Ausnet and AEMO validations
- Enrolment in marketplace

270 defects raised:
- **258** defects fixed successfully
- **12** defects on track to be fixed in next 7 days

10 organisations participated in active trial, including a market operator, DSO, aggregators and vendors.

6 different time zones were managed:
- Australia
- Singapore
- New Zealand
- US

In addition, the data exchange platform is being utilised by Project Symphony[7], Western Australia's largest DER Orchestration Pilot, where WEM-based DER are being co-ordinated as part of a Virtual Power Plant (VPP) to unlock economic and environmental benefits for customers and the wider community.

Key elements of the field trial's operation included:

- To demonstrate DER wholesale energy market integration, AEMO established two sandboxed wholesale markets (WEM and NEM), dispatching DER via aggregators for every 5-minute market interval using a simplified dispatch engine that applied both business logic (e.g. offer validation based on market rules) as well as the aggregated DOE limits to each interval and solved for each aggregator's dispatch target based on those constraints.
- To demonstrate the local services function set alongside wholesale market transactions, AusNet used a dedicated Local Services Exchange communication channel to communicate directly with aggregators and procure local network services on a bilateral basis.

1.4 Key Learnings and Recommendations

Project EDGE established a robust evidence base – including field trial observations, feedback from project participants and industry stakeholders and independent analysis – to test the hypothesis that a data hub model is the most suitable approach for a DER-rich future compared with many point to point interactions.

The evidence suggests that introducing a production DER data hub across the entire NEM and WEM must be done thoughtfully and will require significantly more work to address important design

[7] See WA DER Program: Project Symphony

decisions and practical considerations. Beyond the technology itself, NEM stakeholders must convene to align on operational requirements, ownership and commercial structures, governance models (including roles and responsibilities), and legal frameworks[8]. Continued stakeholder engagement is required to reach consensus on a path forward.

The experiences gained during the development of the Data Hub and its use in the operational trial yielded key lessons, which are summarised below in order of relevance and timeline. These lessons relate to a data hub model for DER data exchange between industry actors and can be applied in a technology-agnostic way:

Lesson 1: There is support in industry for implementing a DER data hub concept, although further work is required to determine the optimal design

Project participants and broader industry feedback[9] indicated that, while point-to-point integrations are generally suitable at current levels of DER adoption and for first movers with an immediate problem to solve, there is support for implementing an industry-wide data hub concept in anticipation of a DER-rich future. The primary appeal of the hub concept is the ability for AEMO, DNSPs, aggregators and customer agents to exchange a wide variety of information – including real-time data, encrypted data, and bulk data – in a secure and standardised fashion via a single integration. Further, field trials and independent analysis from EY indicate that a data hub model could improve efficiency and reduce operational cost and complexity for market participants. These benefits can in turn result in benefits to consumers via more competition and innovation among participants, as well as increased value for DER from expanded access to both wholesale markets and business to business opportunities such as local network support services.

Lesson 2: A production DER data hub solution must offer the flexibility of multiple integration mechanisms while maintaining standardisation

Building a DER data hub into a market-wide solution will require the flexibility of additional integration methods that remain aligned with a common technical standard. In the current EDGE implementation, participants and DNSPs must download and run an independent application using a container-based application[10] and deploy it in a hosting environment of their choice (i.e. cloud provider or on-premise server). Using containers can improve efficiency, scalability, and performance when deploying complex applications across multiple environments, but they are relatively new in the global IT landscape, and the Australian energy market in particular. As these tools and technologies are not yet ubiquitous, there is significant variation across organisations with respect to their knowledge, proficiency, and support levels to use them. Project participants indicated that in the future it would be beneficial to develop additional integration mechanisms for a DER data hub, such as cloud-native applications, fully managed web applications, and APIs, to maximise flexibility for industry participants.

Lesson 3: Decentralisation of hub architecture and identity management systems may offer benefits compared to a centrally-administered hub, but raises questions regarding support and maintenance

[8] See Section 6.1, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[9] In addition to direct feedback from project participants, Project EDGE gathered industry feedback through multiple stakeholder forums, including retailers and aggregators in the DER Market Integration Consultative Forum (MICF), Market and Peak Bodies in the Demonstrations Insights Forum (DIF), and DNSPs in the Networks Advisory Group (NAG).

[10] A container is a unit of software that bundles code and associated dependencies into a cohesive, executable package that can be easily deployed in different environments. See https://www.docker.com/resources/what-container/ for additional context.

Both the Project Participants' and EY's analysis indicated that there are resiliency benefits to implementing a hub with a more decentralised architecture due to inherent redundancies and failover / recovery mechanisms, as well as the absence of a central point of failure with respect to digital identities. However, roles and responsibilities for providing technical support as well as ongoing maintenance and upgrades will need to be clearly defined in collaboration among industry via a robust governance mechanism.

Lesson 4: Any future DER data exchange hub must be designed with capacity to support DER coordination during Unexpected Events

As outlined in the Project EDGE Lessons Learnt #2 Report[11], aggregators of DER are able to follow AEMO intervention targets across their portfolio when directed during unexpected events, however, coordination among DNSPs and aggregators will be needed to ensure targets are achieved within dynamic network limits. This use case has been uncovered during the Project EDGE field trial and the capability to address it is not available in the current e-Hub technology given its dynamic nature and operational timeframes. A DER data hub can provide these capabilities, such as AEMO having visibility of aggregators' operational network limits through the DOEs published into the data hub. Given the nature of market operations during rare, unexpected events, the efficiency enabled by coordinating directions with DNSPs and DER aggregators via a data hub, compared to multiple point to point integrations, is significant, especially considering the anticipated large number of DER and aggregators likely to be operating in the future. However, industry will need to design any future DER data hub with appropriate failsafe mechanisms to ensure continuity in these scenarios.

Lesson 5: AEMO's Technology Strategy and IT Architecture teams should conduct a more extensive comparison of the Hub implemented in EDGE and the existing e-hub

The solution developed in Project EDGE features some enhancements relative to the current capabilities of the e-Hub, but also lacks certain capabilities that exist in the e-Hub. A detailed evaluation by AEMO's Technology Strategy and IT Architecture teams would result in a more accurate estimate of the time and effort to either develop the existing e-Hub features in a DER data hub, augment e-Hub to enable the relevant capabilities of the Data Hub, or map out a convergence between a DER data hub and the e-Hub.

Lesson 6: Decentralised Architectures align well with collective governance, which could better support innovative business models

Given the nature of the trial, Project EDGE did not explore in detail the potential ownership and governance arrangements for the solution options it considered[12]. Project participants and EY's independent analysis noted that the nature of the architecture of the progressed solutions lend themselves to alternative and more flexible governance arrangements than those in place for point-to-point[13].

As a current day example of "shared industry governance", AEMO's Information Exchange Committee[14] provides a proven mechanism that could be extended to support and evolve a shared

[11] Project EDGE | Lessons Learnt #2 Report

[12] As described in Section 3.3, Project EDGE considered four options: A) point-to-point integrations (business as usual), B) a centralised hub under the existing e-Hub model, C) a decentralised hub hosted in a centralised environment, and D) a fully decentralised hub.

[13] See discussion under heading of "Practical considerations of a decentralised data hub for DER" in AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[14] See more about the Information Exchange Committee AEMO's Information Exchange Committee

energy industry data hub solution. Determining an appropriate governance model that includes all DER-related industry actors and balances flexibility with stability will require thoughtful consideration and industry engagement.

Lesson 7: A Decentralised Hub Architecture aligns with National Electricity Objective (NEO)

EY's Technology and Cybersecurity Assessment report for Project EDGE includes a theoretical evaluation of various data exchange options which ranked a decentralised DER data exchange approach as the most suitable architecture for a secure, scalable, two-sided market, while also aligning closely to the assessment's success criteria and the NEO. The report noted that while current volumes of DER data exchange is relatively small, there is less distinction between centralised and decentralised options, but there may come a tipping point where the advantages of decentralised approaches may outweigh the costs and complexities of transitioning towards decentralised technologies. However, introducing a production DER data hub across the entire NEM must be done thoughtfully, and will require more focused work to address important design decisions and practical considerations. For example, building in the flexibility to decentralise the initial DER data exchange approach so that the associated benefits can be captured should this option become feasible. Beyond the technology itself, NEM stakeholders must convene to align on operational requirements, ownership and commercial structures, governance models (including roles and responsibilities), and legal framework[15]. The AEMO Engineering Framework[16] should also be consulted in the design phase. Continued stakeholder engagement is required to reach consensus on a path forward that will result in a data hub that can scale and adapt to evolving industry requirements over time.

Recognising the need for further stakeholder engagement as well as considerations of the lessons above, the Project yielded recommendations for a future DER data hub:

Recommendation 1: Assess Opportunities to Leverage EDGE & Symphony Technology Investments

Several of the software components that were developed in EDGE and underpin the successfully trialled hub solution – including the Self Sovereign Identity (SSI) technologies, the Distributed Ledger Technology-based data registry, Decentralised Data Hub client gateway, and Decentralised Logic Execution – demonstrated capabilities that can meet some of the functional requirements for emerging DER use cases for which there is no incumbent technical solution. These components are available under an open-source licence, meaning that AEMO or any other actor is free to utilise and modify the source code without paying licence fees. AEMO should incorporate these components in its long-term technology strategic evaluation and identify areas where they may add value going forward.

Recommendation 2: For a Production-Grade DER data hub Deployment, it should be a requirement to develop Various Integration Mechanisms to promote Standardisation while maintaining flexibility for Industry

[15] See Section 6.1, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[16] AEMO Engineering Framework documents (various) available at: https://aemo.com.au/en/initiatives/major-programs/engineering-framework

For a production-grade deployment of a DER data hub, integration must be further streamlined via automation and support multiple additional options so participants can manage the integration without key specialised IT skills or resources. For future iterations of a data hub, AEMO should specify various integration methods be developed such as offering integration applications in enterprise cloud marketplaces, standalone web and/or desktop applications, and APIs.

Recommendation 3: Prioritise Development of Functional Capabilities to Support DER Use Case with No Incumbent Solution

EY's report outlines a conceptual roadmap[17] for a phased implementation of a DER data hub that eases participants' migration pathway by initially deploying the hub in support of an emerging DER use case for which there is no incumbent solution with a select number of participants. A benefit of this approach is that functional and technical capabilities can be developed in a similarly phased approach in order to reduce overall complexity, achieve technical proof points incrementally, and meet market needs as they emerge. When scoping a future production-grade DER data hub, AEMO in consultation with industry, should prioritise functional requirements related to one or more emerging DER use cases that lack existing "off the shelf" solutions.

Recommendation 4: Integrate Technology Evaluations and Demonstrations with Governance, Legal, and Commercial Workstreams

EY's report[18] outlines a number of important governance, legal, and commercial questions that must be addressed through continued industry stakeholder engagement. DER data hub design should ideally be driven by the desired outcome(s) nominated by industry and policy makers. AEMO, DNSPs, industry participants, and regulatory stakeholders should establish strong and continuous feedback loops between commercial and policy discussions / decisions and technology evaluations. As the technology landscape continues to evolve rapidly, it is critical to evaluate how the unique attributes capabilities of different technologies – especially with respect to decentralised architectures – can align with the desired outcomes of those stakeholder and policy decisions (and vice versa).

Recommendation 5: Consider Further Decentralisation of the Hub Architecture and Hosting, including Shared Ownership

Enabling a decentralised architecture and hosting offers additional benefits with respect to resilience and scalability [19]. The EY assessment concluded that a decentralised hub architecture couple provide data exchange efficiency benefits over a centralised hub for large volumes but this tipping point is unknown. Similarly, a decentralised ownership and governance model featuring co-investment and joint ownership by multiple entities may offer benefits with respect to interoperability and innovation. As AEMO works with industry stakeholders to further refine requirements for a production data hub solution under the NEM Reform Implementation Roadmap[20], it should consider design principles and technologies that support decentralisation in both domains while also aligning with AEMO

[17] Ibid

[18] See Section 6.1, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[19] AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[20] DER Data Hub and Registry Services initiative brief available at: https://aemo.com.au/initiatives/major-programs/nem-reform-implementation-roadmap

Engineering Framework[21] requirements. Governance mechanisms and associated fee structures for decentralised service provision would need to be agreed and finalised through continued industry stakeholder engagement to support effective decentralisation of a data hub.

Recommendation 6: Consider Options to Expand Scope Beyond DER Use Cases

Over the long term as DER become increasingly prevalent and play a larger role in wholesale market operations as well as distribution network operations, there are many potential benefits for harmonising DER data and workflows with non-DER operations such as transmission and distribution system planning, renewable generation transmission connection, and electric transport planning and operations[22] [23]. The concept of a market's "Digital Spine" - a common digital layer for transactions and interoperability for *all actors and processes* in an energy system - is being developed in other energy markets[24]. When designing a DER data hub it is advised to design as many components to be extendable (e.g. support non-DER market processes), as scalable as possible (e.g., support both business to business as well as business to consumer workflows), and able to be used for functionality beyond the original requirement.

[21] Ibid. p. 25

[22] Race for 2030 National Charge Link, 2022 available at: https://issuu.com/racefor2030/docs/national_charge_link

[23] Portuguese industry data hub for EV data (MOBI.E), 2021, available at: https://www.mobie.pt/documents/42032/143944/MOBIE_OCPI_Phase2_v1_3_Public.pdf/e304dc46-e2f4-a984-88fd-0c95bd7b8613?t=1628096661952

[24]Most notably the UK; see Digital Spine Feasibility Study

Contents

Tables

Figures

Glossary

Term	Definition
Aggregator	The aggregator's primary role in Project EDGE is customer resource optimisation. This includes analysing wholesale and local service offers within its DER portfolio. The aggregator as the customer representative has the most interactive role, participating in both wholesale and local services in the DER Marketplace. To enable its functions, the aggregator will need to sign up customers and manage a portfolio of customer DER, and develop incentives and business models for optimising the value stack for all parties (customers, aggregator, and DSO).
Application Programming Interface (API)	A mechanism for multiple independent programs or systems to interact and communicate with each other (e.g. perform read/write functions within an application). APIs can enable programs to automatically perform functions that human users perform via user interfaces (e.g. desktop or mobile application).
Container (Containerised Application)	A container is a unit of software that bundles code and associated dependencies into a cohesive, executable package that can be easily deployed in different environments
Client Gateway	An application that represents a standardised integration mechanism for all participants. Published as a “containerised” application for participants to run within a hosting environment of their choosing. Each participant client gateway is an independent application. The deployment of the client gateway results in a connection with the common messaging transport layer hosted within AEMO’s environment, establishing a standard single integration method that enables each participant to communicate with AEMO or any other organisation.
Data Hub	The solution that was implemented for Projects EDGE & Symphony. For the avoidance of doubt, the term used in lower case “data hub” refers to the concept generally and not the specific technology implementation for the Projects.

Term	Definition
Decentralised Identifier (DID)	Decentralised Identifiers (DIDs) are a new type of globally unique identifier. They are designed to enable individuals and organizations to generate their own identifiers using systems they trust. These new identifiers enable entities to prove control over them by authenticating using cryptographic proofs such as digital signatures. Since the generation and assertion of DIDs is entity-controlled, each entity can have as many DIDs as necessary to maintain their desired separation of identities, personas, and interactions. The use of these identifiers can be scoped appropriately to different contexts. They support interactions with other people, institutions, or systems that require entities to identify themselves, or things they control, while providing control over how much personal or private data should be revealed, all without depending on a central authority to guarantee the continued existence of the identifier.
Decentralised Logic Execution (DLE)	Distributed computing technology developed for EDGE that can establish multiparty consensus about the state of certain datasets, or the results of certain business processes while preserving the privacy of underlying input data. DLE is where a distributed network of independent worker nodes - a cluster of computing resources operated by separate hosting providers - ingest data from external sources, execute custom workflows based on predefined business logic, and vote on results in order to establish consensus without revealing or modifying the underlying data. DLE borrows concepts from public distributed ledger solutions, namely distributed consensus protocols which use cryptographic techniques to establish provably correct and timely results.

Term	Definition
Distributed Energy Resource (DER)	Distributed energy resources (DER) refer to often smaller generation units that are located on the consumer's side of the meter. Examples of Distributed Energy Resources that can be installed include: • roof top solar photovoltaic units • wind generating units • battery storage • batteries in electric vehicles used to export power back to the grid • combined heat and power units, or tri-generation units that also utilise waste heat to provide cooling • biomass generators, which are fuelled with waste gas or industrial and agricultural by-products. • open and closed cycle gas turbines • reciprocating engines (diesel, oil) • hydro and mini-hydro schemes • fuel cells. Many of these technologies are not exclusively found "behind the meter" but also connected directly to the distribution network. Within the Australian regulatory and policy making context, DER is often referred to as Consumer Energy Resources (CER), acknowledging these resources are investments made by energy consumers.
Distributed Ledger Technology (DLT)	A combination of infrastructure (e.g. computing resources) and consensus protocols that support concurrent replication, synchronisation, and validation of data across a distributed network of independent nodes. DLT is used to establish a persistent and tamper proof record of events, transactions, and/or data among multiple parties.

Term	Definition
Distribution Network System Provider (DNSP) / Distribution System Operator (DSO)	The DNSP's primary function is network optimisation. In Project EDGE, the DNSP supports aggregator participation in the wholesale market by determining and providing the distribution network limits (via site-level Dynamic Operating Envelopes) within which bids can be constructed. In the Local Services Exchange, the DNSP interacts with aggregators to procure local services via the DER Marketplace. These local services use DER to enable improved reliability and quality of network supply to customers via the alleviation of operational constraints. Traditionally, the DNSP has referred to the organisation whose responsibility and role is to own, maintain and operate physical distribution assets. The term DSO recognises the more dynamic nature of a future role to manage a more dynamic distribution network with the increased penetration of DER. Within this report, the terms have been used interchangeably.
Dynamic Operating Envelope (DOE)	In Project EDGE, Dynamic Operating Envelopes (DOEs) are calculated and published by the DNSP and represent safe operating limits for customer imports and exports for a given time and location. DOEs are provided to Aggregators to apply distribution network limits to customer DER service participant and AEMO for operational visibility.
e-hub	The B2B e-Hub is an electronic information exchange platform that is currently provided, operated and maintained by AEMO to facilitate retail market Business to Business Communications.
Hash	A cryptographic function that translates any arbitrary data into a uniform sized output; used for encryption and validation purposes.
Local Services Exchange (LSE)	Applications that enable DNSPs to procure (via bilateral arrangements, or potentially in the future, trading / flexibility market mechanisms) network support services (e.g. voltage management, peak shaving) from DER aggregators.

Term	Definition
Market and System Operator (MSO)	The Market and System Operator's primary function is market optimisation and keeping the power system secure and reliable. In Project EDGE this is AEMO and includes enrolling aggregators, subscribing to operational data, and running wholesale dispatch with instructions sent to aggregators to fulfill using their fleet of DER. The MSO will also collaborate with DNSPs more as distribution connected resources (DER) have a greater impact on local and whole of system operations over time. The MSO's interaction with the LSE is the role of facilitating the data exchange for the trade of services, reporting and analytics. It is not directly involved in the bilateral trade or execution of local services between the DSO and aggregator.
Problem Statements	Challenges that NEM participants face related to emerging DER use cases.
Platform as a Service (PaaS)	A cloud-computing model in which hardware and software resources are "virtualised" and delivered via the internet. PaaS enables users to provision, maintain, and configure computing resources and platforms via the cloud, rather than physically running their own servers.
Sandbox	A testing environment for new and untested software or code so it can be run securely. Such software, or systems, are isolated so they can access only certain resources, programs, and data within an environment and not impact the operation of other software and systems.
Self-Sovereign Identity (SSI)	Self-Sovereign Identity is a growing digital identity paradigm that promotes an individual's control over their identity and their data. This is in contrast to the current paradigm where most official identifiers (driver's license, birth certificate, usernames, etc.) are given to users and maintained by a central authority, and where user data can be shared without their knowledge or consent (especially in the event of a cybersecurity breach) and where roles, access, and permissions can be centrally revoked without user knowledge.

Term	Definition
Standing Data	Business Rules and Reference data that is specific to a participant's or device's profile (e.g. meta-data like Inverter settings), and can be attached to digital identities for the participant and device.
Use Cases	Specific operational functions and business processes that enable DER participation in wholesale markets and/or local services.
Value Stack	Where an energy resource offers a variety of services which allows them to receive multiple streams of revenue or other compensation. These multiple compensation streams are known as value stacking, as the resource provides benefits to customers, utilities / grid and the market. For example, when DER are aggregated and controlled together they can offset traditional generation resources. They also can reduce and shift electrical load on-site to lower monthly customer utility bills and avoid peak demand charges. They further have the potential to provide services to the grid, such as improved local congestion management and participation in wholesale ancillary and energy markets to help regulate power, particularly useful for balancing utility-scale wind and solar generation.
Verifiable Credential (VC)	A Verifiable Credential is a secure and machine-verifiable digital credential which respects a standard data model. The use of digital signatures makes verifiable credentials more tamper-evident and more trustworthy than many conventional role-based digital identifiers and certificates.
Zero-Export Limit (ZEL)	Instructions communicated by retailers to customer agents capable of communicating with and/or controlling customer DER devices (i.e. inverters) in order to curtail export and manage their exposure to negative market prices. This use case could also go beyond zero exports and turn on controlled load to, for example, be paid by the market for charging customer batteries.

2 Introduction

This section provides an overview of Project EDGE ("Project" in this report), its key objectives, the structure and purposes of this report, as well as common assumptions and definitions for terminology used throughout the report, and an overview of the approach undertaken to assess various data exchange models considered by the Project.

2.1 Project EDGE Overview & Objectives

Project EDGE (Energy Demand and Generation Exchange) is a collaboration between AEMO, AusNet Services and Mondo, with financial support from the Australian Renewable Energy Agency (ARENA), to demonstrate a Consumer / Distributed Energy Resource (DER) Marketplace that efficiently coordinates DER to provide both wholesale and local network services within the constraints of the distribution network.

The Project demonstrates how consumer participation in a DER marketplace could be facilitated by a data exchange solution that enables communication and coordination among AEMO, DNSPs, and aggregators.

The Project seeks to demonstrate four key functions:

- Scalable Data Exchange: how to exchange data between all organisational actors in an efficient and scalable way.
- Wholesale integration of DER: how to dispatch DER fleets as a type of scheduled resource for wholesale markets, whilst considering distribution network limits in the dispatch process.
- Local Network Services: how to facilitate visible and scalable trade of local network services with DNSPs that enable DER operators to efficiently stack value streams - bundling grid applications and services, improving DER economics.
- Customer Value Proposition: Developing DER customer incentives and offerings that promote active market participation.

Project EDGE considers scalable industry-wide DER data exchange as a critical future requirement to design for now (in line with the NEO), especially as it is not specifically contemplated in any detail in the ESB DER Implementation roadmap[25]. The digital infrastructure deployed to enable the DER data exchange and support Project EDGE's field trial transactions and activities was an integral testing ground ("sandbox") for a future energy market where the significant deployment and proliferation of orchestrated price-responsive DER is expected.

At the commencement of Project EDGE, Energy Web Foundation (the technology vendor that provided the data exchange mechanism to facilitate the Projects EDGE and Symphony Field Trials) committed to provide this DER Data Hub Lessons Learnt (DHLL) report, including lessons learnt through the field trial, to help inform any future development of a production grade DER data exchange solution for industry.

[25] Roadmap as published in the ESB Post-2025 Market Design Final Advice to Energy Ministers

The lessons described in this report, alongside other Project EDGE publications, are intended to provide a key input into AEMO and industry's consideration of its future model for DER data exchange.

2.2 Purpose of This Report

The purpose of this report is to outline the DER data exchange solution developed for the EDGE trial, articulate lessons learned, and provide options and recommendations for implementing a production DER data exchange solution, including identifying relevant practical considerations, barriers, risks and mitigations required to achieve the anticipated benefits described in the report's sections. This report draws on the experiences of the operational trial itself, as well as research activities including participant interviews, industry stakeholder engagement and an independent Technology and Cybersecurity assessment conducted by EY[26]. This report enables stakeholders to:

- Understand the data exchange challenges presented by a two-sided market with the anticipated huge volumes of DER, and their implications for market participants and consumers;
- Understand how Project EDGE is testing the working hypothesis that an industry data hub offers benefits relative to the current ad-hoc point-to-point data exchange approaches;
- Gain insight into the functional capabilities, high-level design, and industry roles and responsibilities a DER data hub based on experience with the solution developed in Project EDGE;
- Understand the assessment framework utilised by the Projects, as well as how the lessons learned via operational trials inform its conclusions and recommendations;
- Identify the approximate costs, governance arrangements, operational timelines, and barriers to implementation associated with developing a DER data hub to support one or more emerging DER use cases across the NEM and WEM.

2.3 Structure of This Report

This report provides a high-level summary of the emerging data exchange requirements for the NEM given the current and forecast penetration of DER across the market due to Australia's decarbonisation efforts. It then outlines Project EDGE's data exchange efficiency hypothesis and describes how the project team undertook an assessment of this hypothesis through developing, using, and evaluating a DER data hub to facilitate the trial's DER marketplace.

This report also highlights the project's stakeholder engagement activities and their identification and confirmation of problem statements and associated use cases relating to DER data exchange. A description of Project EDGE's operations and its deployment of a data hub model for data exchange is then provided, together with key findings and lessons learned during the Project.

[26] Project EDGE Technology and Cybersecurity Assessment, EY, June 2023. This EY report provides an overview and evaluation of four options considered by Project EDGE for the delivery of DER identity and data exchange between energy market participants.

Finally, a proposed implementation pathway for a production version of a DER data hub is provided as part of detailed recommendations.

2.4 Additional Evaluation of DER Data Exchange Approaches

While this report focuses exclusively on lessons learned from the Data Hub that was designed and deployed in support of the EDGE operational trials, Project EDGE also conducted extensive analysis of three alternative data exchange approaches.

The findings of this analysis are detailed in a separate report prepared by EY, who was engaged to independently develop a comprehensive evaluation framework and conduct a robust process involving many industry stakeholders to assess the relative strengths and weaknesses of four DER data exchange models (discussed in detail in Section 3.4 Solution Options and Challenges). The output of this work includes four key deliverables[27]:

- Theoretical Evaluation of Data Exchange Options
- Data Exchange Resilience and Compensatory Controls
- Cyber Security Threat and Risk Assessment Report
- Lessons Learnt[28]

Additionally, Deloitte Access Economics was commissioned to conduct an independent Cost-Benefit Analysis (CBA). The Project team collected feedback from industry on the CBA, giving stakeholders the opportunity to test and challenge the robustness of the CBA's process, methodology and underlying assumptions[29]. It also facilitated capturing additional information and views on methodology inputs, including costs and benefits.

[27] Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

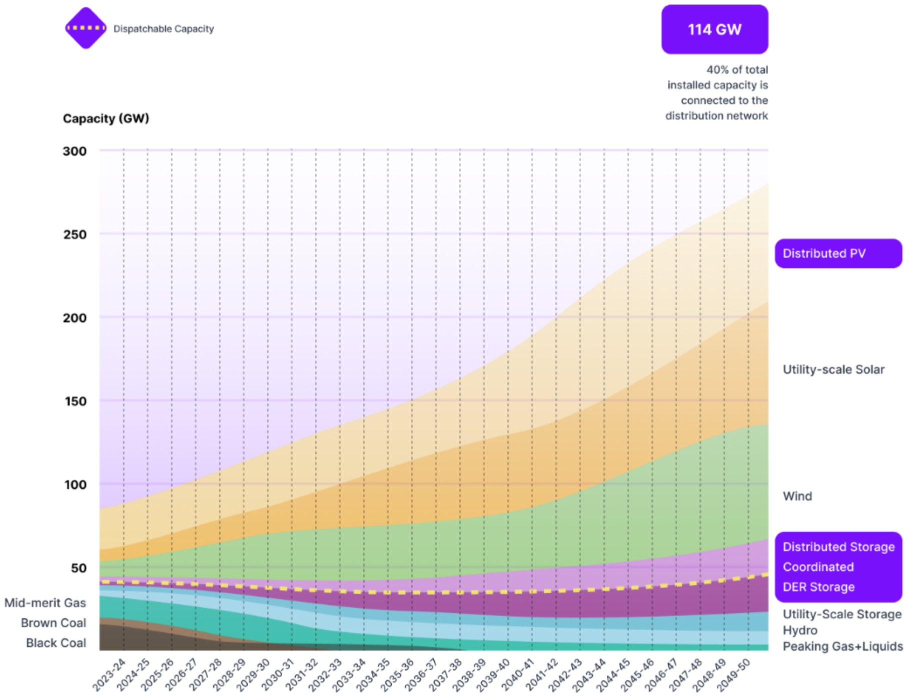
[28] Project EDGE, Lesson Learnt Report #2, November 2022

[29] Project Edge CBA Methodology

3 Emerging DER Data Exchange Requirements

By 2050 DER are expected to represent 40% of total installed system capacity[30] and provide a range of services benefitting individual consumers and the NEM as a whole[31]. In Western Australia the WEM is already facing significant operational issues that could be better managed with orchestrated DER. For Australians to fully realise the financial and environmental benefits of their DER investments, energy systems and trading frameworks must adapt to facilitate broad market participation of DER, accommodating their capabilities for dynamic bi-directional trade in, and flows of, electricity.

Figure 4 Installed Capacity by Resource Type: 2023-2050. AEMO 2022 ISP Step Change Scenario



While this DER-driven paradigm shift is acutely felt in the NEM, markets around the world are grappling with the same issues. In Europe, policymakers are addressing the challenge via a TSO-

[30] Under the Optimal Development Path of AEMO's 2022 Integrated System Plan, 200 GW of new clean energy capacity will be built across Australia by 2050, including 69 GW of capacity resulting from consumer adoption of technologies like rooftop solar, battery storage, and related controls. The result is a total of 114 GW of DER capacity. More information is available at 2022 Integrated System Plan

[31] Integration of DER to provide flexibility services is a focus of the Energy Security Board's Post-2025 reforms

DSO coordination framework[32]. In the US, regulatory reforms such as FERC 2222[33] are at the forefront. And in the UK, market access and coordination issues have resulted in official calls for a "flex-centric system" that can facilitate distributed flexibility that might not otherwise emerge organically[34].

Though specifics vary by region, the common theme globally is clear - what is needed is a dramatic expansion of market access for DER via digitalisation that can coordinate DER flexibility to balance the needs of wholesale markets, local services, and individual consumers.

Enabling widespread and beneficial DER participation means AEMO, DNSPs, aggregators, and customer agents must have the capability to exchange extremely high volumes of data using consistent data models, controls, and communication methods throughout the entire DER lifecycle in order to effectively perform their respective functions in the market.

As highlighted in a recent report[35] by Great Britain's energy regulator, Ofgem, while some individual digital components that address key DER co-ordination needs exist today, market failures preclude them from being consolidated into a cohesive ecosystem. The lack of a coherent, system-wide, digital framework that connects the many different markets for distributed flexibility is a significant barrier to realising the full value of DER. Overcoming this barrier can be accomplished via "a common digital energy infrastructure able to unlock flexibility in multiple markets by facilitating information provision, market access and coordination, and effective trust and governance structures" - a *digital spine*.

Project EDGE was established to test a DER Marketplace concept in practice which involved exploring new technologies and processes. One project element involved testing of a common digital infrastructure to reduce barriers of information technology and data silos currently inhibiting DER coordination and transactions. In Western Australia, Project Symphony was established to pilot and develop a pathway toward DER orchestration, and to demonstrate the extent to which this infrastructure can support system, market and customer outcomes.

3.1 Industry DER Data Exchange Requirements

Each use case including DER being engaged with the market involves distinct stakeholders communicating specific datasets with particular formats (or schemas) at varying frequencies and volumes. Accordingly, making generalised statements about functional requirements for the industry as a whole is difficult. However, there are a few core capabilities that provide a foundation to enabling scalable DER integration and data exchange:

- Managing Identities and Permissions: inter-organisational data exchange is predicated on the ability for multiple parties to mutually authenticate each other's identity and authorise selective disclosure or communication of information between them based on their respective roles and responsibilities. Achieving secure and scalable data exchange to enable emerging DER use cases requires consistent authentication and authorisation frameworks,

[32] In Europe, the transition from reliance on a small number of centralised fossil fuel generators to a larger number of variable renewable and distributed resources highlights the need for improved coordination between transmission and distribution systems, as outlined by the Council of European Regulators

[33] FERC Order 2222 is a U.S. federal policy designed to remove barriers to DER participation in wholesale capacity, energy, and ancillary services markets; a key tenet of the Order is "coordination among the regional grid operator, the DER aggregator, the distribution utility and the relevant retail regulatory authority"

[34] Ofgem Call for Input: The Future of Distributed Flexibility, June 2023

[35] Ibid

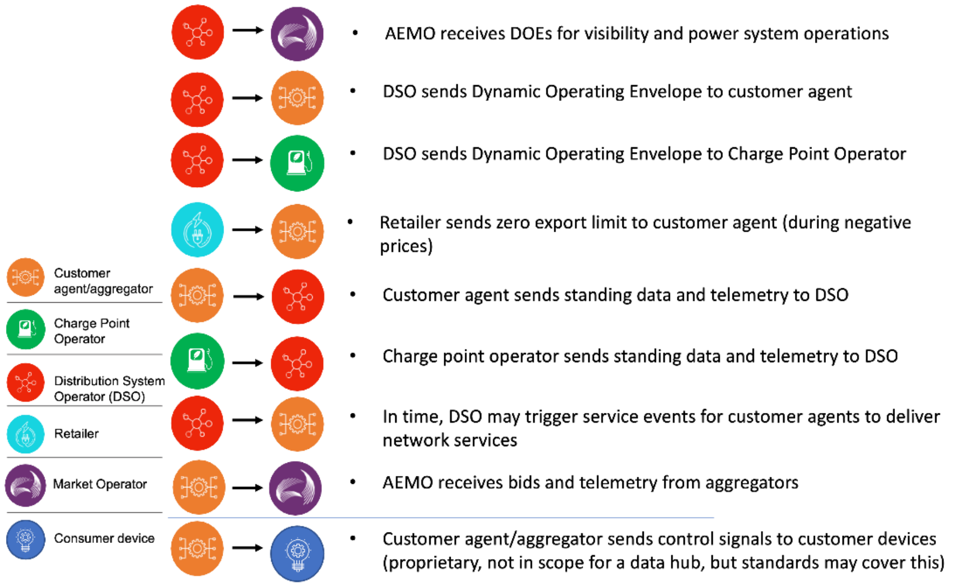
collectively referred to as Identity and Access Management ("IDAM"). A national digital IDAM approach can improve interoperability and streamline the establishment of trusted relationships between devices, systems, and organisations[36] - the NEM needs a digital "passport" solution for DER to be fully engaged in market transactions and services.

- Managing Integrations: from an operational perspective, DER data exchange relies on technical integrations between siloed, disparate systems owned and maintained by DER agents, such as Original Equipment Manufacturers (OEMs), aggregators and retailers, and DNSPs, as well as AEMO. Today such integrations are piecemeal and bilateral, with the diversity of technologies and integration methods between stakeholders meaning consumers and industry face higher costs, unnecessary complexity, and technical challenges that directly diminish the value of DER participation in flexibility markets.[37] Continuing on this trajectory is undesirable, as the number of discrete integrations will need to grow exponentially. As EY have assessed, a more efficient approach is to enable NEM participants to exchange a variety of data types and formats via a single integration with a common digital infrastructure[38].
- Maintaining Information Integrity: given the growing volume and diversity of DER data, it's imperative that all market organisations work with an accurate and consistent set of facts. Stakeholders and actors will need mechanisms to ensure that data quality and integrity is maintained in the process of being exchanged among systems to enable the transition to a two-sided market with much larger volumes of DER.

The capabilities mentioned above will need to be enhanced across Australia's electricity markets to facilitate many discrete DER use cases involving significantly more stakeholders and exponentially larger volumes of data compared to today's energy market landscape. Examples of emerging and future DER use cases[39] are shown in the figure below.

[36] ESB Interoperability Policy for Consultation, Section 4.4, October 2022
[37] Ofgem Call for Input: The Future of Distributed Flexibility, June 2023, Section 1.4
[38] Project EDGE Technology and Cybersecurity Assessment, EY, June 2023.
[39] For a comprehensive description of emerging DER use cases and problem statements, see Project EDGE Technology and Cybersecurity Assessment, EY, June 2023, Appendix A.

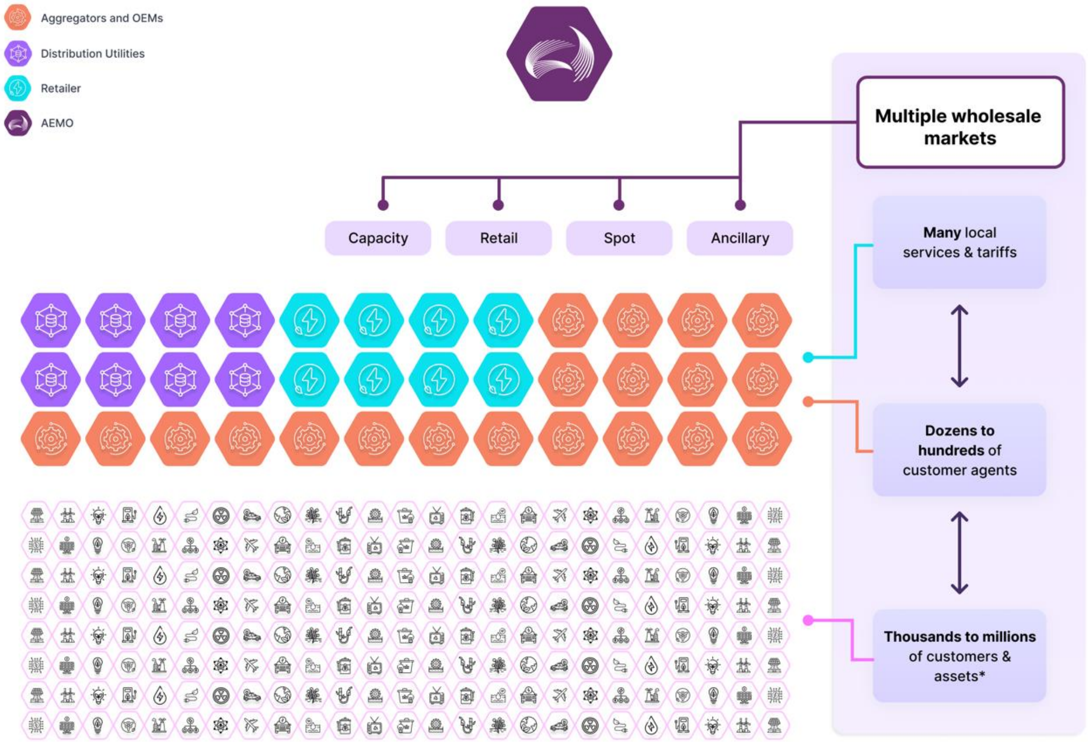
Figure 5 Indicative Energy Market DER Data Exchange Use Cases



- AEMO receives DOEs for visibility and power system operations
- DSO sends Dynamic Operating Envelope to customer agent
- DSO sends Dynamic Operating Envelope to Charge Point Operator
- Retailer sends zero export limit to customer agent (during negative prices)
- Customer agent sends standing data and telemetry to DSO
- Charge point operator sends standing data and telemetry to DSO
- In time, DSO may trigger service events for customer agents to deliver network services
- AEMO receives bids and telemetry from aggregators
- Customer agent/aggregator sends control signals to customer devices (proprietary, not in scope for a data hub, but standards may cover this)

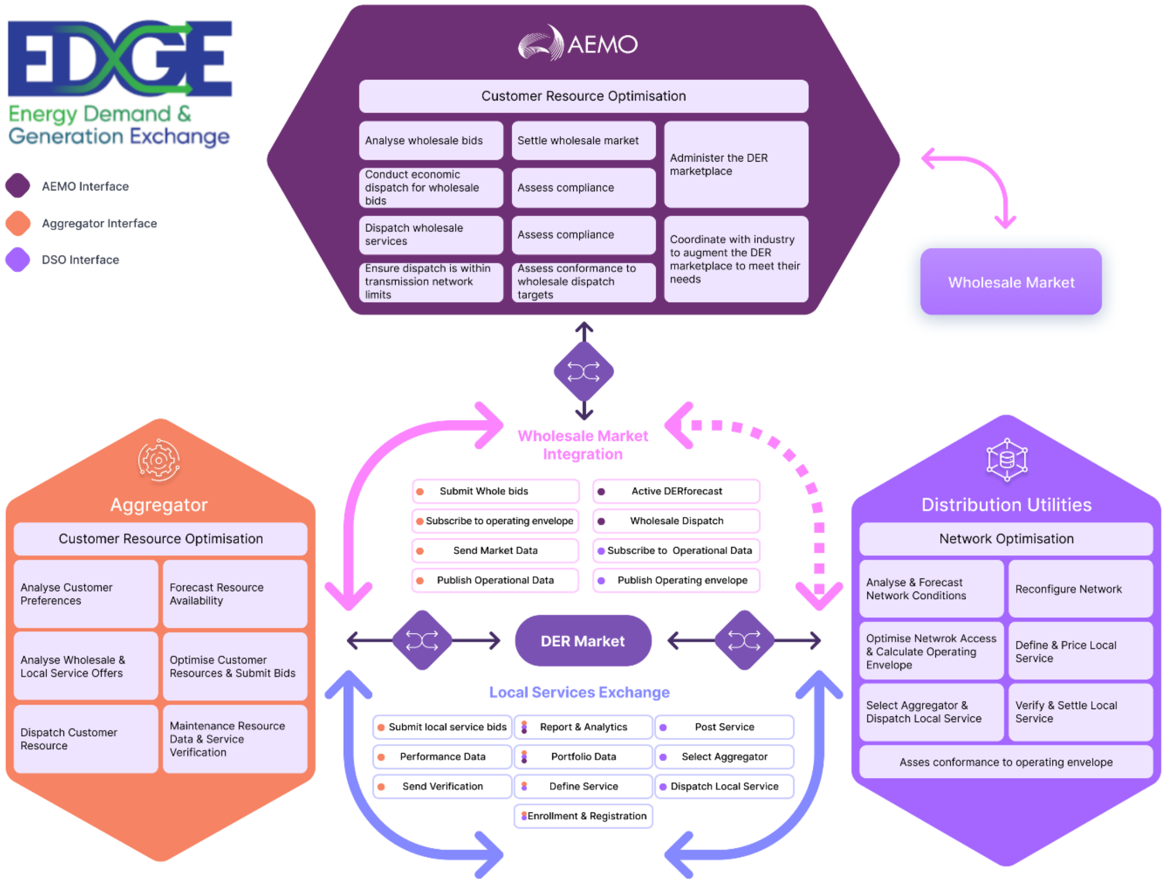
The figure below provides a graphical overview of the data exchange challenges confronting the future market; with DER uptake the number of participants and DER customers will grow. This growth will make the market's data exchange challenges exponentially more difficult than today.

Figure 6 The Future Market's Data Exchange Challenge


Aggregators and OEMs
Distribution Utilities
Retailer
AEMO
Multiple wholesale markets
Capacity
Retail
Spot
Ancillary
Many local services & tariffs
Dozens to hundreds of customer agents
Thousands to millions of customers & assets*

The figure below indicates the business functions and data flows that a DER Data Exchange mechanism must enable to support the DER Marketplace concept.

Figure 7 Project EDGE Data Exchange Functions and Data Flows


EDGE
Energy Demand & Generation Exchange
AEMO Interface
Aggregator Interface
DSO Interface
AEMO
Customer Resource Optimisation
Analyse wholesale bids
Settle wholesale market
Administer the DER marketplace
Conduct economic dispatch for wholesale bids
Assess compliance
Dispatch wholesale services
Assess compliance
Coordinate with industry to augment the DER marketplace to meet their needs
Ensure dispatch is within transmission network limits
Assess conformance to wholesale dispatch targets
Wholesale Market
Wholesale Market Integration
Submit Whole bids
Active DERforecast
Subscribe to operating envelope
Wholesale Dispatch
Send Market Data
Subscribe to Operational Data
Publish Operational Data
Publish Operating envelope
DER Market
Local Services Exchange
Submit local service bids
Report & Analytics
Post Service
Performance Data
Portfolio Data
Select Aggregator
Send Verification
Define Service
Dispatch Local Service
Enrollment & Registration
Aggregator
Customer Resource Optimisation
Analyse Customer Preferences
Forecast Resource Availability
Analyse Wholesale & Local Service Offers
Optimise Customer Resources & Submit Bids
Dispatch Customer Resource
Maintenance Resource Data & Service Verification
Distribution Utilities
Network Optimisation
Analyse & Forecast Network Conditions
Reconfigure Network
Optimise Netwrok Access & Calculate Operating Envelope
Define & Price Local Service
Select Aggregator & Dispatch Local Service
Verify & Settle Local Service
Asses conformance to operating envelope

3.2 DER Data Exchange Problem Statements

Project EDGE consulted with DNSPs, aggregators, OEMs and retailers via multiple stakeholder engagement forums to identify and define problem statements that industry is currently, or may soon, face in the transition to a more distributed two-sided market[40]. Further, Use Cases associated with these problem statements, and how the Project EDGE Data Hub environment addresses them (compared to alternative approaches), were also shared with industry and have been detailed in Section 5.

Those problem statements identified as high priority by industry are summarised into four generalised problem categories below. A detailed outline of all problem statements developed and considered by the project is outlined in EY's report[41].

- DER Data Inconsistency across Industry Participants: today, DER standing data - the metadata of DER devices such as equipment type, model, and capability - is replicated across multiple independent systems maintained by AEMO, DNSPs, retailers, and customer

[40] DER problem statements were socialised and endorsed by various Project EDGE industry stakeholder forums, including the DER Market Integration Consultative Forum (MICF), the Demonstrations Insights Forum (DIF), and the Networks Advisory Group (NAG).

[41] AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

agents. Data reconciliation processes are limited, and discrepancies inevitably arise over time. These inconsistencies create significant operational challenges and inefficiencies for all stakeholders, as DER standing data represent the foundational inputs for nearly all market and Business to Business (B2B) transactions.

- High Data Exchange Costs: currently, market participants incur significant costs implementing and maintaining a series of bespoke, bilateral data exchange integrations with DNSPs and AEMO. These costs present barriers to entry for new participants and burdens for existing ones, which can restrict competition in the retail market. Ultimately high data exchange costs diminish the value proposition of DER for consumers by making it uneconomical for market participants to enrol DER in markets and/or offer competitive, innovative plans.
- Visibility of DER Between Industry Actors: DER operational data is fragmented across multiple independent IT systems, and it is costly and complicated for industry participants to selectively disclose this data with each other, inhibiting their ability to perform their respective functions in the market.
- Maintain cyber security in a decentralising power system: In the absence of widely adopted standards, the inherent variation in proprietary DER platforms and protocols currently used by industry actors makes it challenging to establish uniform, controlled, and auditable digital identities and associated data exchange systems that are guaranteed to establish trust and implement strong security and reliability capabilities. This challenge also extends to the interaction between industry participants and the DER however these interactions are not within the scope of this document.[42]

3.3 Hypotheses Tested in EDGE

Project EDGE proceeded with a working hypothesis[43] that a data hub model[44] provides a more efficient and scalable way to facilitate data exchange (at the GW scale) for the various use cases outlined as well as broader business to electricity market and business to consumer use cases, more so than the current point-to-point (P2P) approach.

While a data hub approach has been the working hypothesis to achieve market efficiency, there are two factors that warrant challenging conventional assumptions about how a data hub could be implemented. First, DER participate in wholesale markets impacting transmission systems (under the purview of AEMO), while also having the capability to concurrently provide local services within distribution network systems (under the purview of DNSPs). Accordingly a DER data hub necessarily impacts both domains. Second, recent advances in enterprise software architectures, particularly distributed computing technologies, present an opportunity to design a hub that can be jointly operated by multiple parties.

Accordingly, Project EDGE tested an additional data exchange hypothesis that a hub based on decentralised digital infrastructure (i.e. hosted and operated by multiple independent entities

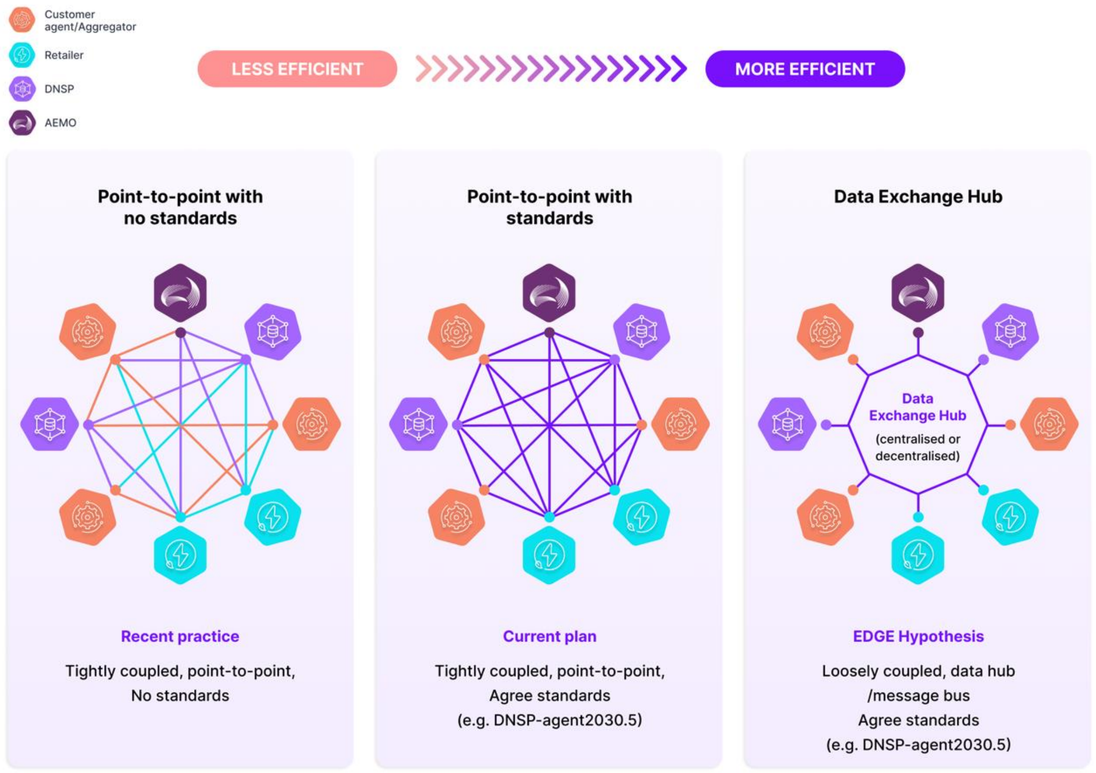
[42] For additional context on cybersecurity as it relates to DER data exchange, refer to AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023.

[43] For a comprehensive list of the hypotheses and research objectives of Project EDGE, reference the EDGE Research Plan

[44] Within the NEM, the concept of data hubs is generally well understood, with the establishment and operation of AEMO's e-Hub, a B2B communication platform supporting Electricity Retail Transactions. The e-Hub includes the Shared Market Protocol (SMP) platform (providing an API gateway and portal to support B2B and value add web services) and the MSATS B2B Handlers (providing B2B FTP support). See the e-hub fact sheet.

rather than a single administrator), with digital identities and associated governance arrangements, enables opportunities for broader benefits to the efficient operation of, and participation in, electricity markets, while addressing cybersecurity risks and consumer data privacy.

Figure 8 Project EDGE Data Exchange Efficiency Hypothesis


Customer agent/Aggregator
Retailer
DNSP
AEMO
LESS EFFICIENT
MORE EFFICIENT
Point-to-point with no standards
Point-to-point with standards
Data Exchange Hub
Data Exchange Hub
(centralised or decentralised)
Recent practice
Tightly coupled, point-to-point,
No standards
Current plan
Tightly coupled, point-to-point,
Agree standards
(e.g. DNSP-agent2030.5)
EDGE Hypothesis
Loosely coupled, data hub /message bus
Agree standards
(e.g. DNSP-agent2030.5)

3.4 Solution Options and Challenges

Project EDGE considered four solution architectures to enable DER data exchange and integration. These are summarised in below - full descriptions and evaluations are available in the EY report[45].

[45] see Section 3, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

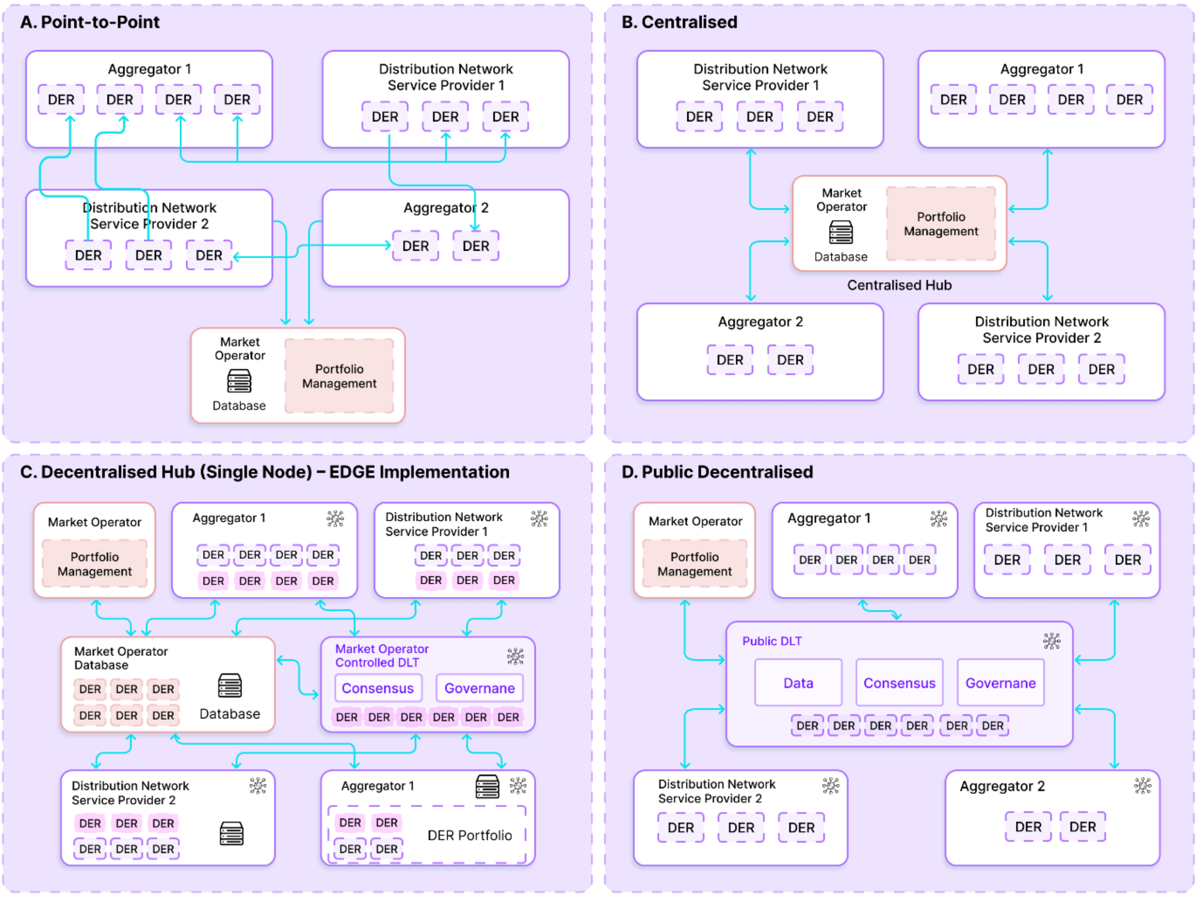
Table 1 Data Exchange and Integration Solution Options considered by Project EDGE

Option	Summary
A. Point to Point Integrations	This approach is an extension of current practices for emerging DER use cases under which no mandate for use of a data hub exists, unlike the retail market e-Hub46. In this approach, each party maintains its own independent platform(s) and related IT infrastructure. Data exchange between parties is accomplished via a series of bilateral integrations performed manually or automatically.
B. Centralised Hub under the existing e-Hub model	This approach is an extension of the e-hub model currently used for the NEM retail market. In this scenario, e-hub would be augmented to accommodate additional use cases beyond its existing scope for retail transactions, to include a wider range of DER operational workflows involving aggregators and DNSPs. Some enhancement required relates to some of these use cases, such as DOEs, ZELs and local network support services, requiring intraday data exchange.
C. Decentralised hub within a centralised environment (Single node)	This is the approach that was trialled in Project EDGE. In the EDGE Data Hub, each participant downloads and hosts a decentralised container to facilitate data exchange with other participants, but the transport layer and automated message broker is still contained within a centralised private cloud environment. The public "containerised" application is published for participants to run within their hosting environment, establishing a standardised integration method across the DER market.
D: Decentralised Data Hub (DDHub)	This is the approach, conceptually, that was envisaged by Project EDGE's proponents. This approach incorporates elements from all three of the preceding models. Like approaches B & C, the Decentralised Hub standardises data exchange processes through common data models, shared security patterns, and single integrations. However, the Decentralised Hub is operated by a network of independent nodes hosted by AEMO, DNSPs, market participants and/or non-energy service providers under a governance model that represents the whole industry rather than being administered by a single broker (i.e. AEMO).

High level architectures representing these solution options are shown below.

[46] See AEMC Rules Chapter 7.17.1 via https://energy-rules.aemc.gov.au/ner/390/116919

Figure 9 High level architecture options for DER Data Exchange



Source: EY

The EDGE team gave serious consideration to all four options during the project design phase, identifying key benefits and challenges for each approach[47]. Upon review of the initial theoretical evaluation, the Project team identified Option C: Decentralised Hub (Single Node) as the best fit to achieve the design principles and objectives of Project EDGE. Following additional consultation with Project EDGE participants, Option C was ultimately implemented as the Proof-of-Concept solution for the operational field trials.

[47] Detailed analysis and evaluations for these options is available in Section 3, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023.

4 DER Integration and Data Exchange Solution

As outlined in EY's independent report, certain design principles were identified for data exchange for the EDGE Project. In addition to these principles, for Project EDGE & Symphony, Energy Web sought to establish various objectives underpinning its development of a data exchange solution that enabled a wide variety of DER communications amongst stakeholders through a single integration mechanism. These objectives include:

- Reduce complexity and cost for industry by reducing the number of integrations required by participants to exchange data associated with multiple use cases;
- Standardise rule-based logic for data exchange;
- Simplify reporting, reconciliation, and incident management;
- Make it easier to coordinate and perform maintenance / system updates over time;
- Be protocol agnostic – the data exchange solution architecture should not be predicated on a specific communication protocol and vice versa; any communication protocol or standard can be utilised without rigid hardware requirements;
- Improve system resiliency by eliminating single points of failure and implementing highly available infrastructure with built-in failover and recovery mechanisms;
- Enable participants to configure their own bespoke communication channels to support data exchange with many others (broadcasts), or directly with a single participant (unicast);
- Empower all participants to self-manage their own identity and credentials, and to have direct control over their data (instead of relying on a separate administrator);
- Reduce error and disputes by enforcing rules, roles, and responsibilities defined via collaborative, shared industry governance in code; and
- Foster innovation and build market value by enabling participants to build custom applications on top of shared infrastructure, with new use cases being established and supported.

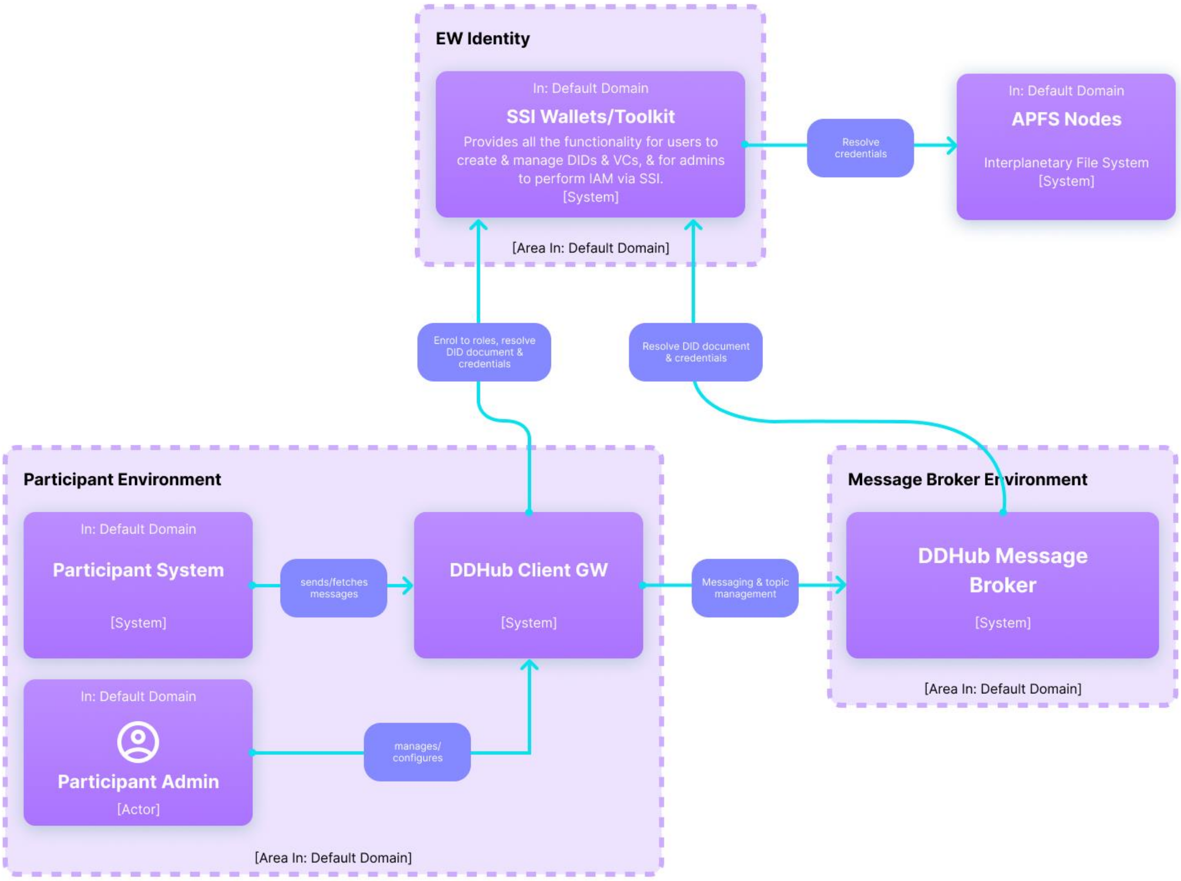
An overview of the Option C: Decentralised Hub (Single Node) solution, and a description of how it meets the design principles and objectives of Project EDGE, is provided in the following subsections. For a more detailed description of the Option C architecture and functional capabilities, see Appendix A1.

4.1 Solution Overview of Option C: Decentralised Hub in Centralised Environment (Single Node)

As shown in the figure below, Projects EDGE & Symphony ('The Projects') implemented a secure, open-access messaging infrastructure that:

- Allows participants and DNSPs to send, receive, and authenticate messages based on the roles that have been issued to and associated with their self-managed identity;
- Allows participants, DNSPs, and AEMO to exchange diverse datasets, ranging from real-time telemetry to bulk file uploads, in support of multiple DER use cases;
- Requires only a single integration mechanism with a central infrastructure in order to communicate via one:one (bilateral), one:many (broadcast), and many:many (multicast) channels.

Figure 10 Projects EDGE & Symphony Messaging and Integration Solution architecture



EW Identity
In: Default Domain
SSI Wallets/Toolkit
Provides all the functionality for users to create & manage DIDs & VCs, & for admins to perform IAM via SSI.
[System]
[Area In: Default Domain]
Resolve credentials
In: Default Domain
APFS Nodes
Interplanetary File System
[System]
Enrol to roles, resolve DID document & credentials
Resolve DID document & credentials
Participant Environment
In: Default Domain
Participant System
[System]
sends/fetches messages
DDHub Client GW
[System]
In: Default Domain
Participant Admin
[Actor]
manages/ configures
[Area In: Default Domain]
Messaging & topic management
Message Broker Environment
DDHub Message Broker
[System]
[Area In: Default Domain]

Note: in EDGE architecture diagrams, the hub infrastructure is often referred to as DDHub, a reference to the concept of a decentralised data hub

Legend:

- Participant Environment: Hosting environment (e.g. public cloud instance, or on-premise server) where DNSPs and aggregators deploy and operate the DDHub Client Gateway Application.
- Participant System: Participant applications (e.g. DER management system, market operation systems) that send and receive messages on relevant channels (within the shared message broker) via the Client Gateway.
- Decentralised Data Hub ("DDHub") Client Gateway: The interface presenting UI, and API for interacting with the Message Broker to send and receive messages
- DDHub Message Broker: The component that routes messages between Client gateways (using API to control NATS messaging).
- SSI Toolkit: Libraries and components that implement identity and access management functionalities as described in Appendix A2
- IPFS: Distributed file storage system used to store and manage identity and role definitions (as described in Appendix A2).

Conceptually, this approach mimics the functionality of a shared personal computer in which multiple independent users have the ability to run multiple applications on top of a common operating system and hardware.

In the Projects, the shared message broker is analogous to a computer - it is foundational infrastructure upon which DNSPs and market participants gain the ability to establish their own "profiles", exchange messages, and run their own applications. The DDHub Message broker is the central component hosted by AEMO that routes and translates messages between participants. Messages are structured and organised in distinct channels corresponding to specific DER use cases, and formatted in topics which define data formats and schemas.

AEMO, DNSPs, and market participants gained the ability to exchange data with each other by integrating with the Message Broker via the DDHub Client Gateway, an independent application that participants downloaded and ran in an environment of their choosing. During installation, participants specify connection details to the DDHub Message Broker, and these configurations provided a standardised integration method for all participants. An integration service option where participants did not host their own container but accessed (via API) a separately hosted DDHub Client Gateway was offered, however, all participants chose to host the gateway application directly.

In order to access certain channels and gain permissions to send and/or receive specific message types, participants acquired roles that reflected their role within the market, using credentials attached to their self-determined identity. Credentials were granted by AEMO and determined the participant's ability to send messages to other participants using channels (what messages are sent and received) and topics (data schemas that define the payload of a message). Recipients in turn had the capability to restrict who they received messages from, could send to, as well as authenticate messages to ensure they are valid.

The following sections summarise the EDGE & Symphony Data Hub approach as well as an overview of how the approach meets the required capabilities relating to Managing Integrations, Identity & Permissions, and Information Integrity.

4.2 Managing Integrations

Key Benefit - Lowering Integration Costs: A standardised integration mechanism with a central infrastructure enables participants to exchange multiple data types and formats via a single integration, and thus can reduce industry costs and complexity

The EDGE & Symphony solution enables all industry participants to exchange data with each other via a common messaging transport layer, which is accessed via a client gateway application. In this architecture, aggregators gained the ability to engage with multiple markets - wholesale and local services - via a single integration rather than integrating separately with AEMO as well as DNSPs. It should be noted that the same data exchange solution was utilised across both projects, EDGE in the NEM and Symphony in the WEM[48] demonstrating that it could support participants in the east and west coast markets.

The client gateway application represents a standardised integration mechanism for all participants, this was published as a "containerised"[49] application for participants to run within a hosting environment of their choosing. Offering the gateway application via a container gave participants a great deal of flexibility in terms of hosting, as one of the primary benefits of containers is portability and interoperability across different environments (e.g. public cloud, on-premise database, etc.). Containers also helped streamline application deployment and scaling by packaging all components and dependencies into a cohesive bundle.

Once integrated, participants were assigned permissions based on their role within the industry. These permissions governed the ability to send messages to other participants via the common Message Broker through channels and topics; recipients in turn had the capability to authenticate messages to ensure they are valid.

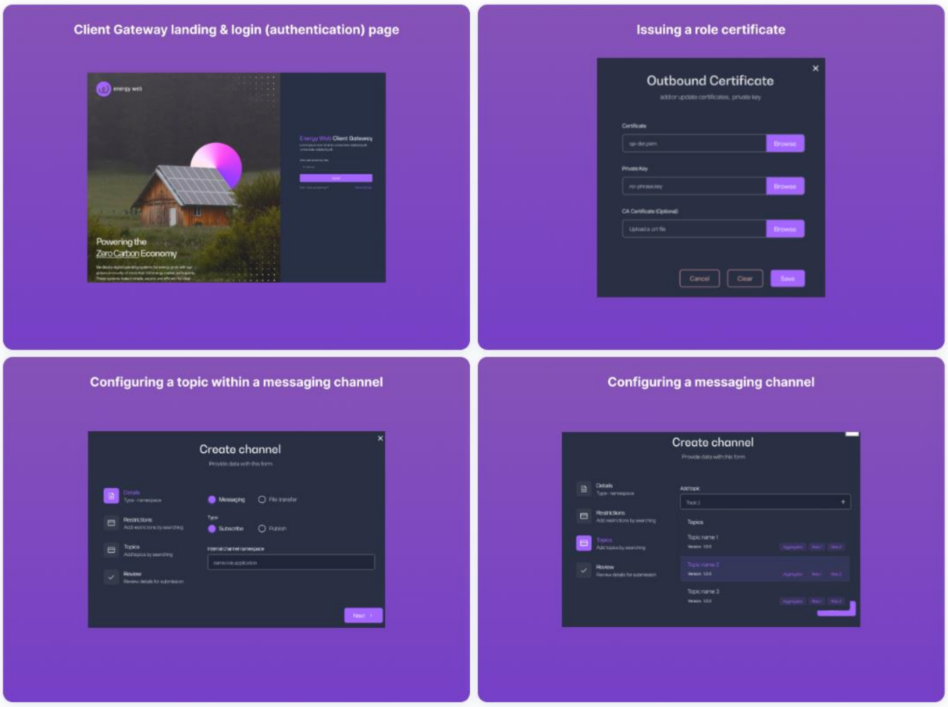
A Hub Administration application, which is provided as part of the Client Gateway Container, enabled participants to manage topics and schemas, as well as manage enrolments to application-specific roles within the Data Hub. Sample screens from this administration application are shown in the figures below. Starting from the upper left and moving clockwise, the screens demonstrate:

- The Client Gateway landing page and login (authentication) page (see 4.3)
- Issuing a role certificate (see 4.3)
- Configuring a topic within a messaging channel (see A1.1)
- Configuring a messaging channel (see A1.1)

[48] See WA DER Program: Project Symphony

[49] A container is a unit of software that bundles code and associated dependencies into a cohesive, executable package that can be easily deployed in different environments. See https://www.docker.com/resources/what-container/ for additional context.

Figure 11 Screens from the Hub Administration application


Client Gateway landing & login (authentication) page
energy web
Energy Web Client Gateway
Powering the
Zero Carbon Economy
Issuing a role certificate
Outbound Certificate
add or update certificates, private key
Certificate
Browse
Private Key
Browse
CA Certificate (Optional)
Upload a crt file
Browse
Cancel
Clear
Save
Configuring a topic within a messaging channel
Create channel
Provide data with this form
Details
Type - namespace
Restrictions
Add restrictions by searching
Topics
Add topics by searching
Review
Review details for submission
Messaging
File transfer
Type
Subscribe
Publish
Internal channel namespace
Next
Configuring a messaging channel
Create channel
Provide data with this form
Details
Type - namespace
Restrictions
Add restrictions by searching
Topics
Add topics by searching
Review
Review details for submission
Add topic
Topics
Topic name 1
Topic name 2
Topic name 3

4.3 Managing Identity and Permissions

Key Benefit - Streamlining Identity and Access Management: the Data Hub enabled participants to perform authentication and authorisation processes for multiple markets and use cases with a single portable, self-managed digital identity

Identity and Access Management (IDAM) in EDGE & Symphony serves three primary functions:

- Authorising participant client gateways to interact with the common messaging transport layer;
- Authorising participants to access and read / write information within dedicated topics (i.e. individual communication channels dedicated to specific use cases / processes) via the Client Gateway based on their role;
- Authenticating messages to ensure that both sender and recipient are known and trusted.

As implemented through The Projects, IDAM functionalities are enabled using Self-Sovereign Identity (SSI)[50] technologies based on World Wide Web Consortium (W3C) standards, namely Decentralised Identifiers (DIDs)[51] and Verifiable Credentials (VCs)[52]. This approach to IDAM is analogous to the way a person uses a physical passport and visas to travel. Like a passport, a DID is a persistent and universally recognised identifier that can be presented to authenticate identity in different settings. VCs function similarly to visas, in that they are separately issued credentials that grant the DID holder specific permissions in specific contexts, and can be revoked under certain conditions. Appendix A2 explains these SSI concepts in more detail.

An IDAM registry using Distributed Ledger Technology (DLT) was implemented, that defined a hierarchy of standardised roles for aggregators and DNSPs. For The Projects implementation, role hierarchy was defined with AEMO being the parent organisation, under which there were four applications to which roles are assigned. This means that AEMO is currently the primary issuing authority for all roles for all participants. However, the functionality exists for DNSPs to create their own separate organisations, applications, and roles in the future in line with an efficient national and sovereign approach to identity and certificate management.[53]

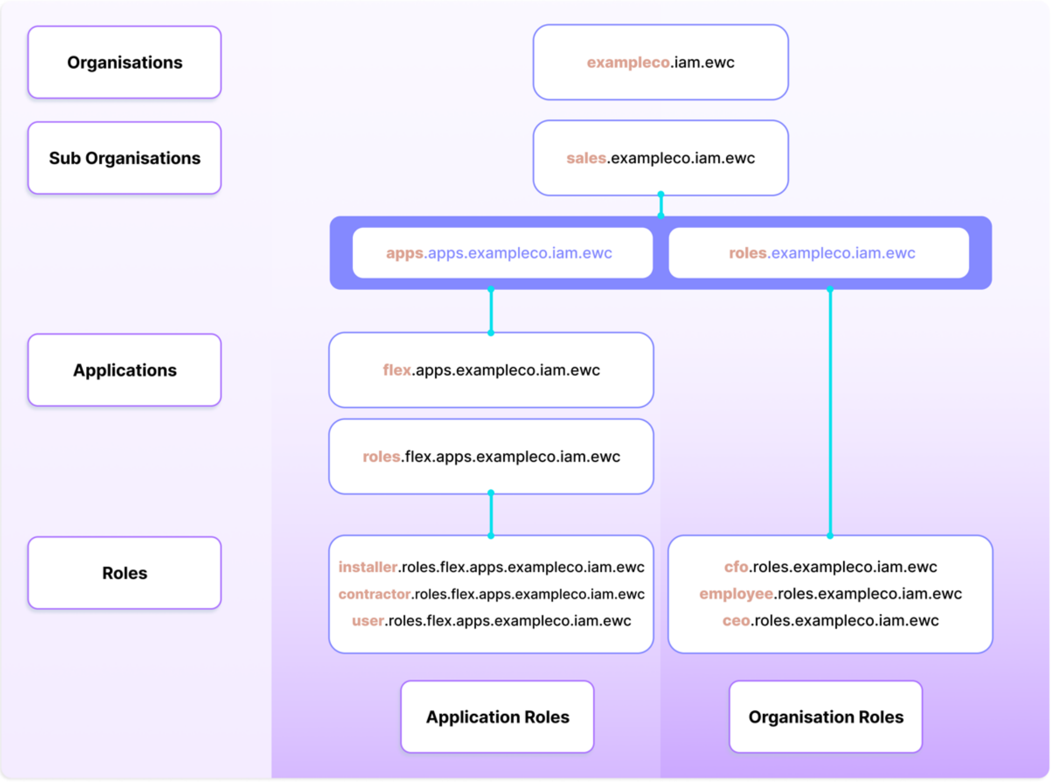
[50] 'Self-Sovereign Identity' is a growing paradigm that promotes an individual's control over their identity and their data. This is in contrast to the current paradigm where most official identifiers (driver's license, birth certificate, usernames, etc.) are given to users and maintained by a central authority, and where user data can be shared without their knowledge or consent (especially in the event of a cybersecurity breach) and where roles, access, and permissions can be centrally revoked without user knowledge. Further

[51] A DID is an identifier that can be generated and controlled by individuals or organizations without an external authority. Technical specifications are available at https://www.w3.org/TR/did-core/

[52]A Verifiable Credential is a secure and machine-verifiable digital credential which respects a standard data model. Technical specifications are available at https://www.w3.org/TR/vc-data-model/

[53] ESB Interoperability Policy Directions Paper, Section 4.4

Figure 12 Example of Organisational Role Hierarchy


Organisations
exampleco.iam.ewc
Sub Organisations
sales.exampleco.iam.ewc
apps.apps.exampleco.iam.ewc
roles.exampleco.iam.ewc
Applications
flex.apps.exampleco.iam.ewc
roles.flex.apps.exampleco.iam.ewc
Roles
installer.roles.flex.apps.exampleco.iam.ewc
contractor.roles.flex.apps.exampleco.iam.ewc
user.roles.flex.apps.exampleco.iam.ewc
cfo.roles.exampleco.iam.ewc
employee.roles.exampleco.iam.ewc
ceo.roles.exampleco.iam.ewc
Application Roles
Organisation Roles

To access and perform functions within the hub, participants acquired two separate roles. The first step was issuing a credential that strictly governs access to the common messaging transport layer - this allows for authorisation and authentication of participants. The second step was issuing user roles (e.g. the role of "Aggregator") granting access to specific channels (what messages are sent and received on, dedicated to specific use cases like Wholesale Market, Local Services Exchange) and topics (data schemas for specific message payloads). Based on their role(s), participants were assigned permissions to perform different functions, including the ability to send messages to other participants through channels and topics. Recipients in turn had the capability to authenticate messages using the public key of the sender to ensure their validity before processing the message.

4.4 Maintaining Information Integrity via Shared Messaging, Mutual Authentication, and Distributed Consensus

Key Benefit - Ensuring Information Integrity: Combining a shared messaging transport layer with identity-based message authentication and a novel distributed consensus technology ensures consistency and security in the exchange of information between stakeholders

Messaging for The Projects was accomplished via a secure, open-access Message Broker that was hosted in a dedicated Azure cloud environment by AEMO, as shown below. Once participants are integrated with the Message Broker, they acquired one or more roles to access one or more channels, and topics within channels, to exchange data with relevant counterparties.

In the current EDGE & Symphony implementation, there are three Channels ("Topics") corresponding to three different use cases evaluated in the trial:

- "EDGE": dedicated to facilitating messaging between participants and AEMO (i.e. offers and dispatch instructions) as well as between DNSPs and AEMO (Dynamic Operating Envelopes, which inform DER dispatch).
- "Local Services Exchange": dedicated to facilitating messaging between participants and DNSPs to enable DER to provide local network services either bilaterally or via a market mechanism.
- "Internal": used primarily for testing purposes.

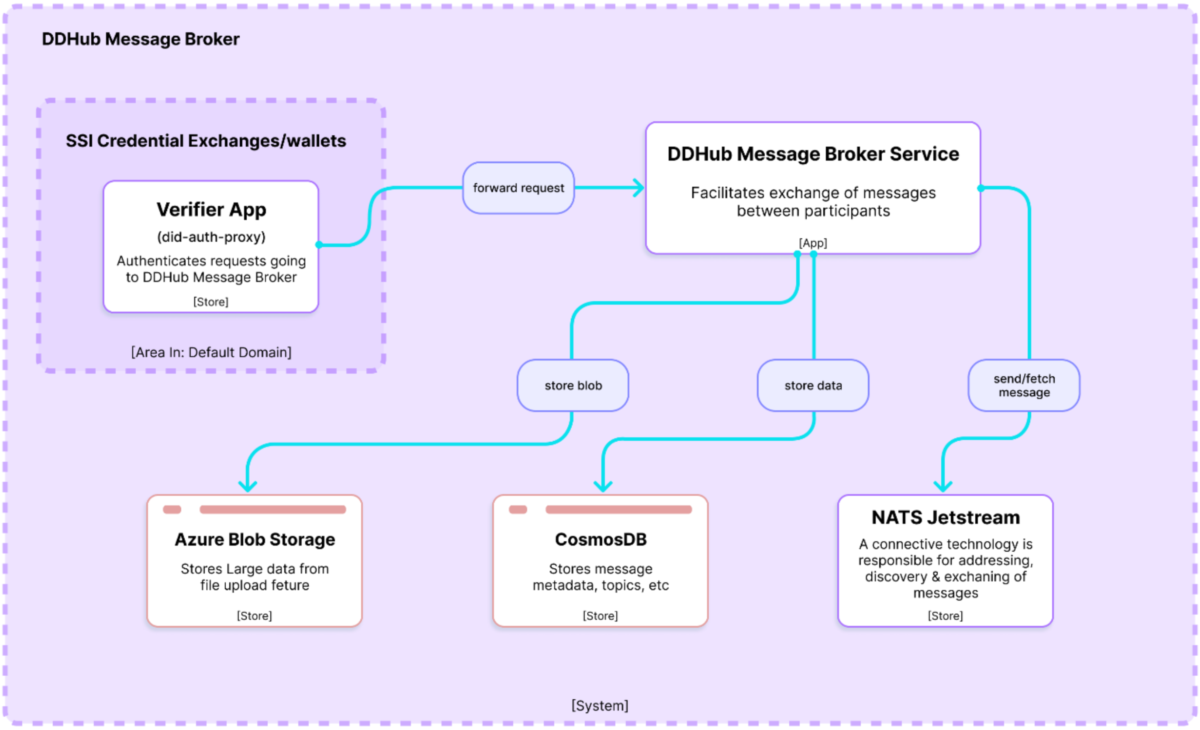
Topics are data schemas that define the payload of a message within a channel. They are grouped under owners that are used as an authorisation unit for visibility. For example, the application under the AEMO organisation owns a number of topics including *boffer* which is a type of market transaction.

Establishing a unified role-based access control mechanism to dedicated communication channels that featured standardised data schemas provided a foundation for ensuring information integrity. However, The Projects also implemented two additional features that further augmented this capability.

First, all messages broadcast within channels were cryptographically signed by the public key of the sender, which enabled recipients to authenticate the origin. This is a well-established approach for communicating information securely between two parties, and was implemented for bilateral data exchange processes where both sender and recipient are known to each other and agree to disclose underlying data within the message.

However, some emerging DER use cases such as Dynamic Operating Envelopes require the transmission of information among three or more parties in a way that does not necessarily reveal all data to all parties. EDGE experimented with a novel approach called Decentralised Logic Execution (DLE). DLE is where a distributed network of independent worker nodes - a cluster of computing resources operated by separate hosting providers - ingest data from external sources, execute custom workflows based on predefined business logic, and vote on results in order to establish consensus without revealing or modifying the underlying data. DLE borrows concepts from public distributed ledger solutions, namely distributed consensus protocols which use cryptographic techniques to establish provably correct and timely results. In EDGE, DLE was implemented to demonstrate the capability for DNSPs to broadcast Dynamic Operating Envelopes to relevant aggregators while maintaining full confidentiality of sensitive commercial information - that is, without knowing the specific aggregator responsible for each NMI, the DNSP was able, using DLE functionality, to have routed to each aggregator only those NMIs for which they were responsible.[54]

Figure 13 Message Broker Architecture


DDHub Message Broker
SSI Credential Exchanges/wallets
Verifier App
(did-auth-proxy)
Authenticates requests going to DDHub Message Broker
[Store]
[Area In: Default Domain]
forward request
DDHub Message Broker Service
Facilitates exchange of messages between participants
[App]
store blob
store data
send/fetch message
Azure Blob Storage
Stores Large data from file upload feture
[Store]
CosmosDB
Stores message metadata, topics, etc
[Store]
NATS Jetstream
A connective technology is responsible for addressing, discovery & exchanging of messages
[Store]
[System]

[54] As currently implemented, all messages and message requests ingress into AEMO's environment, however, this was a design choice to expedite the completion of the trial. Moreover, in the EDGE trial AEMO maintained a participant registry, including their DID, roles, and associated NMIs (with respect to aggregators), and utilises this registry to ensure DOEs are routed to the correct aggregator (aka, "partitioning"). In a future state, and as outlined in Section 6, AEMO and/or multiple other third parties could be delegated the responsibility of hosting the Message Broker and/or worker nodes. See Section 7 and Appendix C for further details.

5 Addressing Industry DER Data Exchange Problem Statements & Emerging DER Use Cases

From its inception, Project EDGE established a series of stakeholder forums to engage market participants about its research, operations, and to test hypotheses about current and envisaged DER-based problems and use cases. These forums engaged Retailers, DNSPs, and aggregators / VPP operators.

Through engagement with stakeholders, the Project's proponents developed and socialised a suite of problem statements relating to current and anticipated DER coordination concerns. The full suite of statements is outlined in the EY report[55].

Related to these problem statements are a number of key DER use cases identified on the ESB reform roadmap[56] and regarded as important by industry stakeholders. This section outlines how the Data Hub solution resolves the challenges inherent in the problem statement categories, as well as supports the specific emerging DER use cases highlighted by industry during the stakeholder engagement process. A data hub approach can be applied to resolving the challenges and enabling the DER data exchange use cases discussed below regardless of the technology choices that underpin that particular data hub.

5.1 High Data Exchange Costs

Today market participants incur costs associated with implementing and maintaining a series of bespoke, bilateral data exchange integrations with DNSPs and AEMO. These costs can act as barriers to entry for new participants, and burdens for existing ones. Where such costs manifest directly as excessive administrative overhead for market participants, they can contribute to higher market prices due to diminished DER participation, and ultimately result in foregone revenue opportunities for customers.

During the stakeholder engagement process, market participants highlighted the cost and compliance burdens of maintaining multiple mechanisms to serve customers across multiple DNSP territories. There was consensus among stakeholders[57] that having a single-entry point to

[55] see Appendix A, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[56] See https://esb-post2025-market-design.aemc.gov.au/

[57] DER problem statements were socialised and validated in various Project EDGE stakeholder forums, including the DER Market Integration Consultative Forum (MICF), the Demonstrations Insights Forum (DIF), and the Networks Advisory Group (NAG).

selectively disclose DER portfolio information with all relevant counterparties in a standardised way would reduce the cost to serve customers and lead to more opportunities for profitable customer participation in more markets and services.

A common DER data hub solution can help mitigate these costs by delivering participants with a uniform tool to integrate with and exchange data with other industry stakeholders. The table below summarises three specific challenges that drive high data exchange costs today and how the EDGE solution can alleviate them.

Table 2 Challenges and Potential Solutions for High Data Exchange Costs

Industry Challenge	EDGE Hub Approach Benefits
Administration of non-standard contractual processes to execute data sharing agreements between aggregators, retailers, DNSPs, and AEMO.	Addressing this challenge systemically would require both industry collaboration to define standardised data-sharing agreements that apply to different actors within the NEM based on their roles, as well as a technology solution to implement and enforce those standards. The robust IDAM mechanism implemented in EDGE offers an example of how agreements could be initiated and executed using a universal authorisation and authentication mechanism for all parties, which could reduce friction and costs.
Duplication of administrative identity verification procedures to deliver "similar but distinct" network services	EDGE demonstrated the potential of a market-wide IDAM mechanism that streamlines market enrolment (and related data exchange processes) by eliminating the need for multiple manual identity verification across markets.
The need to procure and maintain multiple technologies to manage integrations	A standardised integration mechanism, made available in multiple formats, consolidates technology investments and reduces technical burden on market participants. Also, the establishment of common data schemas and consistent security and communication patterns on a shared digital infrastructure expands market access for DER agents without requiring incremental technical integrations.

5.1.1 Dynamic Operating Envelopes (DOE) Use Case

The problem of High Data Exchange Costs for participants includes the distribution of Dynamic Operating Envelopes by DNSPs to Aggregators. This is a key use case confirmed and agreed by stakeholders through consultation as the most pressing emerging DER requirement.

Table 3 Representative DOE Use Case

Actor	I have a problem that	Therefore, I want to	So that I can
Aggregator	I need to integrate into multiple, separate, and bespoke data exchange systems with each DNSP to know which Dynamic Operating Envelopes to apply in operating my portfolio in addition to integrating with AEMO to provide wholesale market services. This adds to my compliance burden and cost to serve customers	Be able to access all DOEs that relate to my portfolio across different DNSP jurisdictions in the NEM via one integration point	minimise my operational costs and cost to serve customers

How the Operating Envelopes Use Case is enabled within the Point to Point approach, as compared to the Data Hub approach, has been shown in the following diagrams.

Figure 14 Dynamic Operating Envelopes Use Case in Point to Point architecture

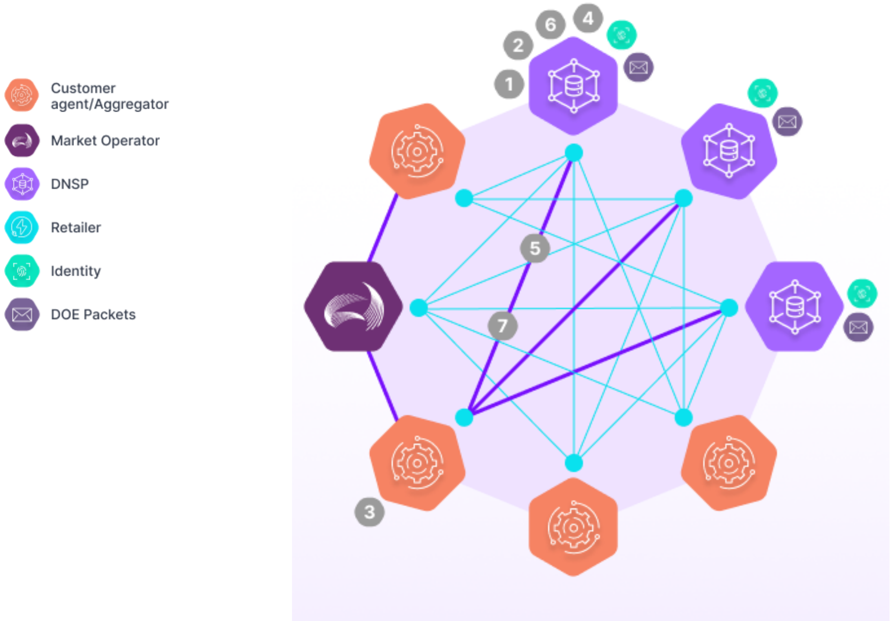
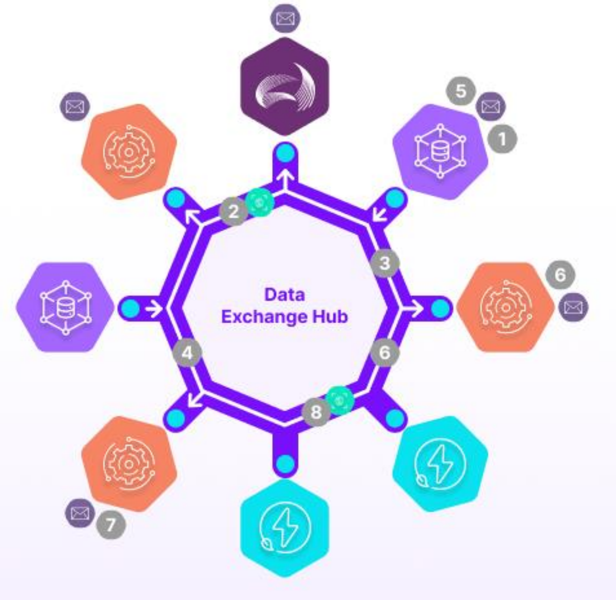


Figure 15 Dynamic Operating Envelopes Use Case in Data Hub architecture



Note: In the Point-to-Point architecture, all lines represent Point-to-Point integrations. Purple-coloured lines highlight an example of 1x agent/aggregator integration for the use case shown, however, this integration would need to be replicated for each agent/aggregator:DNSP pair

These steps outline the *Point to Point* process for the Dynamic Operating Envelopes use case shown above:

1. DNSP notified of a site with an aggregator (aka customer agent) that DOEs must be delivered to
2. The Aggregator then undertakes an organisation identity and portfolio registration process with each party
    a. *Note: The Identity verification process may not be standardised across parties. Several identities can exist for one aggregator, and be managed by different parties. The verification process may be in addition to the existing identity held with AEMO for Market Participation*
3. Single integration established between Aggregator and DNSP.
    a. *Note: For the Aggregator, integration is required per DNSP connection and this may not be standardised*
4. DNSPs map NMIs to portfolios and send a packet of DOEs per aggregator.
    a. *Note: DNSPs have a constant re-mapping process and must send multiple DOE packets*
5. Aggregator receives and operates within DOEs
6. The Aggregator updates their portfolio information as sites and DER change with each party.
    a. *Note: The Aggregator makes DER portfolio updates with each counterparty. This process may not be standardised*
7. DNSP re-maps NMIs to portfolio updates and send a packet of DOEs per aggregator.

These steps outline the *Data Hub* process for the Dynamic Operating Envelopes use case shown above:

1. DNSP notified of a site with an aggregator (aka customer agent) that DOEs must be delivered to
2. The Aggregator then undertakes an organisation identity and portfolio registration process with each party.
    a. *Note: The established identity is managed by one party (e.g. AEMO) and then utilised by other parties. This reduces duplicating processes and thereby enhancing marketplace trust.*
3. Integration established between DNSP and DER Data Hub.
    a. *Note: Any existing Hub integration may be leveraged throughout all use cases.*
4. Integration established between the Aggregator, DER Data Hub and DNSP.
5. DNSPs add new NMIs to batch of DOEs and send one packet of DOEs to the hub
6. The Hub broker takes the single DOE packet based on portfolio information and sends the correct DOEs to their site Aggregator. DOEs could be simultaneously delivered to AEMO for operational visibility.
7. Aggregator receives and operates within DOEs
8. Aggregator updates their portfolio information as sites and DER changes with AEMO.
    a. *Note: The Hub maintains participants and portfolio mapping to facilitate B2B interactions.*
9. This process repeats with any updates to an Aggregator's Portfolio. Callout: DNSPs can always send one DOE packet without maintaining and managing frequent aggregator portfolio updates.

Feedback received highlighted that the benefit of a data hub for DNSPs is the availability of a single, standard interface, and that without the hub, a utility server integration requires connectivity to multiple customer agent touchpoints (i.e. vendor cloud, gateway device, direct to device), potentially repeated for all agents. A data hub removes complexity for DNSPs by matching communications to the right point (agent, device, etc) which ideally leads to DOE routing managed to the 'last mile' more seamlessly across DNSPs.

5.1.2 Retailer (ZEL) Use Case

A further Use Case related to the problem of High Data Exchange Costs confirmed by stakeholders during EDGE's round of consultations relates to a Retailer's need to issue a "Zero Export Limit" to customer agents during times of negative pool pricing. It is noted that in the case of extreme negative prices, a retailer may want generation to be turned off and load turned up, the data exchange for this request could be fulfilled with this pattern.

Table 4 Representative Retailer ZEL Use Case

Actor	I have a problem that	Therefore, I want to	So that I can
Retailer	I need to integrate into multiple, separate, and bespoke data exchange systems with Aggregators and customer agents to request 'zero exports' at my retail sites during negative spot market prices to avoid paying for these (up to $1,000/MWh). This is in addition to integrating with AEMO to provide wholesale market services. This adds to my cost of managing risk and cost to serve customers	Be able to broadcast my zero exports need to a single market interface	Access many potential zero export limit providers including new ones that emerge through a single integration point, lowering my cost of managing spot price risk and serving customers.

How the Retailer (ZEL) Use Case is enabled within the Point to Point approach, as compared to the Data Hub approach, has been shown in the following diagrams.

Figure 16 Retailer (ZEL) Use Case in Point to Point architecture

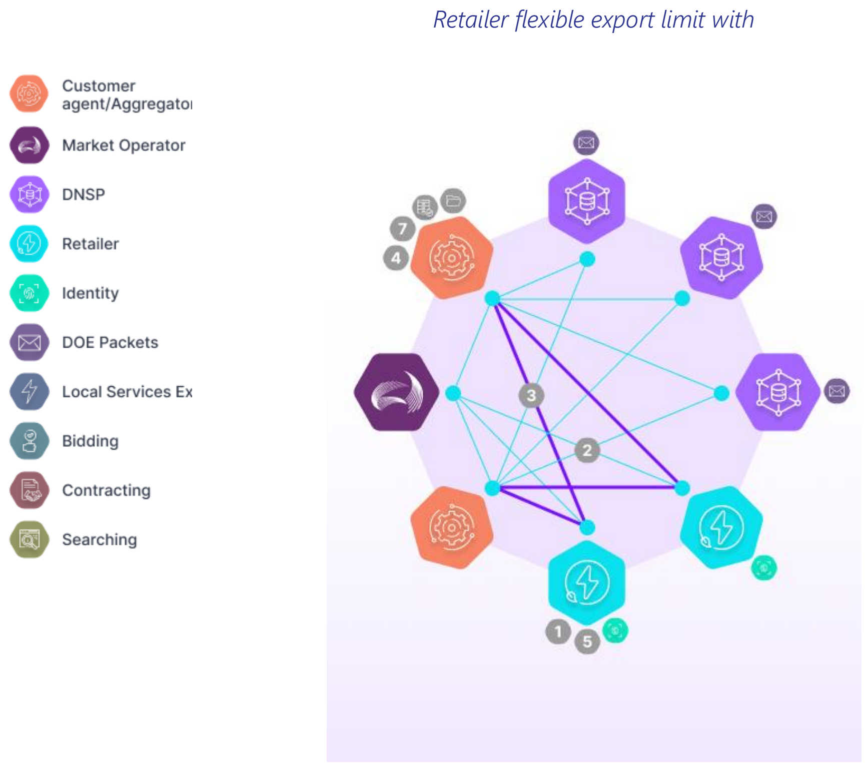
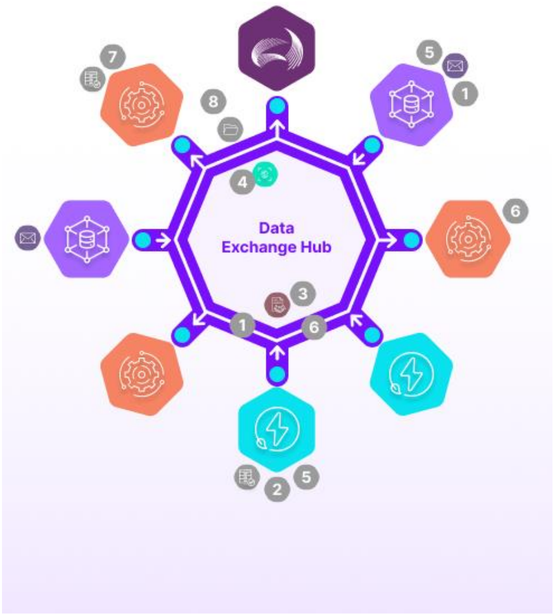


Figure 17 Retailer (ZEL) Use Case in Data Hub architecture



Note: In the Point-to-Point architecture, all lines represent Point-to-Point integrations. Purple-coloured lines highlight an example of 1x agent/aggregator integration for the use case shown, however, this integration would need to be replicated for each agent/aggregator:DNSP pair

These steps outline the *Point to Point* process for the Retailer (ZEL) use case shown above:

1. Customer Agent / Aggregator or OEM is approached by a retailer to curtail solar generation (ZEL) at some of their sites during negative spot prices.
2. Single integration established between aggregator and Retailer
    a. *Note: The Identity verification process may not be standardised across actors. Several identities can exist for one aggregator, and be managed by different parties. The verification process may be in addition to the existing identity held with AEMO for Market Participation*
3. Retailers map NMIs to portfolios and send a ZEL request per Aggregator.
4. Aggregator receives and executes ZEL.
5. Retailer re-maps NMIs to portfolio updates ready to send new ZEL request per Aggregator.
    a. *Note: Retailers have a constant remapping process and must send multiple ZEL requests per event.*
6. The retailers repeats this process with any updates to the Aggregator's Portfolio.
    a. *Note: Aggregator makes DER portfolio updates with each counterparty, this process may not be standardised.*
7. Service verification obtained through smart meter data or file transfer.

These steps outline the *Data Hub* process for the Retailer (ZEL) use case shown above:

1. Integration established between Retailer and DER Data Hub.
    a. Note: *Any existing Hub integration can be leveraged in this use case including the existing retailer identity managed by AEMO.*
2. Retailer establishes ZEL channel(s) to signal ZEL needs.
3. Retailer uses broadcast messenger function to notify registered aggregators on the hub and facilitate connection.
    a. *Note: The established identity is managed by one party (e.g. AEMO) and then utilised by other parties. This reduces duplicating processes and thereby enhancing marketplace trust.*
4. Aggregator existing integration to the hub used to apply to subscribe to retailer ZEL channel(s).
    a. *Note: Configuration of channels is easier than integrating with other organisations.*
5. Retailer approves access to their ZEL channel based on aggregator credentials.
    a. *Note: The Retailer controls how the ZELs are distributed. The mapping of NMIs by a Retailer may exist in the Retailer's system or this could be leveraged by portfolio Management system linked to the Hub in the future. The Hub maintains participants and portfolio mapping to facilitate B2B interactions.*
6. Retailer sends ZEL request to channel.
7. Aggregator receives request and actions ZEL at their sites.
8. Service verification obtained through smart meter data or file upload via data hub.

5.1.3 Local Services Exchange (including Identity) Use Case

An additional use case related to the problem of High Data Exchange Costs for participants, confirmed and agreed by stakeholders as part of the Project's extensive consultations, is the Local Services Exchange, an example of which is outlined below.

Table 5 Representative Local Services Exchange Problem Statement

Actor	I have a problem that	Therefore, I want to	So that I can
Aggregator	I need to integrate into multiple, separate, and bespoke data exchange systems with DNSPs to deliver 'similar but different' local network services across the NEM in addition to integrating with AEMO to provide wholesale market services. This complexity means it's difficult, and potentially not scalable or economic, for me to deliver these services using my portfolio or participate in new B2B services as the arise.	Be able to access a market interface to discover and bid on local network support opportunities and wholesale market services across the NEM via one integration point	Maximise service revenue opportunities for my customers, minimise market operational costs, and so make local services economic for my portfolio

The LSE Use Case incorporates a further Use Case which underpins DER market transactions, that relating to Identity, as described below.

Table 6 Representative Identity Problem Statement

Actor	I have a problem that	Therefore, I want to	So that I can
DSO and Aggregator	I need to participate in multiple, separate and bespoke organisation identity verification processes with DNSPs to deliver 'similar but different' local network services across the NEM as well as AEMO to provide wholesale market services and any other entity for additional B2B services. This adds to my compliance burden and cost to serve customers	have a single process to verify my organisation identity that can be used across all energy market actors	minimise my administration overhead and barriers to accessing non-market revenue opportunities to recruit more customers by sharing greater financial value with them.

How the Local Services Exchange Use Case (including Identity) Use Case is enabled within the Point to Point approach, as compared to the Data Hub approach, has been shown in the following diagrams.

Figure 18 LSE (including Identity) Use Case in Point to Point architecture

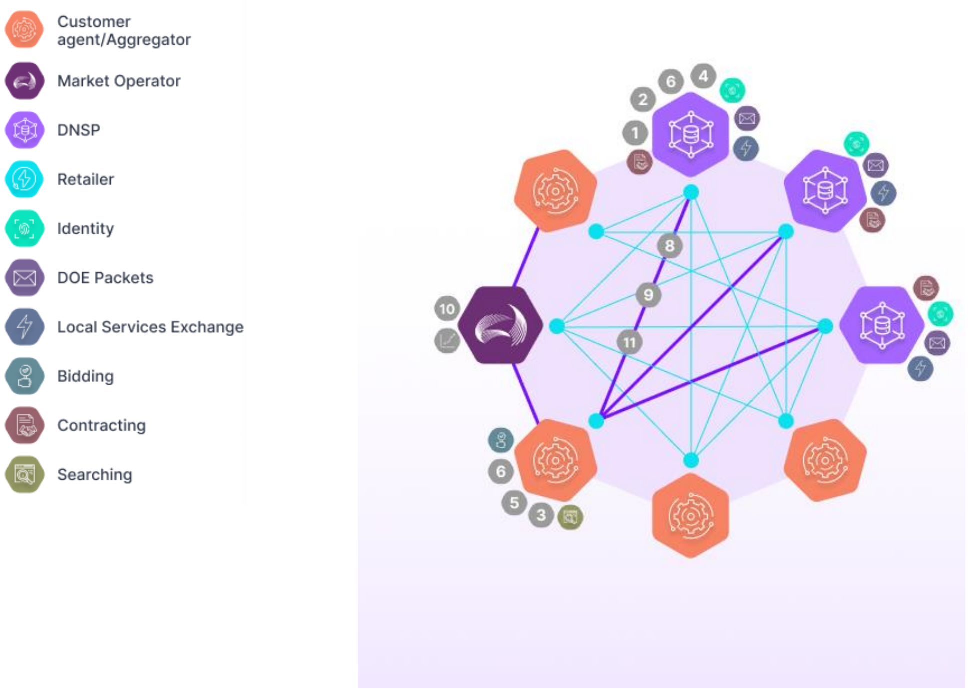
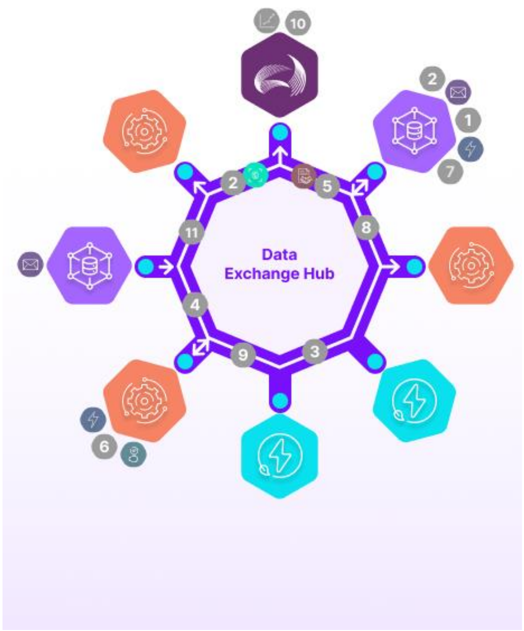


Figure 19 LSE (including Identity) Use Case in Data Hub architecture



Note: In the Point-to-Point architecture, all lines represent Point-to-Point integrations. Purple-coloured lines highlight an example of 1x agent/aggregator integration for the use case shown, however, this integration would need to be replicated for each agent/aggregator:DNSP pair

These steps outline the *Point to Point* process for the LSE (including Identity) use case shown above:

1. Each DNSP establishes an LSE interface.
2. DNSPs post service needs.
    a. *Note: Service definitions may not be standardised across the DNSPs for Aggregators.*
3. Aggregators search each DNSP website or exchange to discover local network service opportunities.
    a. *Note: Service discovery is Aggregator driven.*
4. Aggregator negotiates and contracts with each DNSP they want to service.
    a. *Note: For Aggregators, the contracts across each DNSPs may not be standardised.*
5. Integration established between aggregator and DNSP. The Aggregator undertakes an organisation identity and portfolio registration process with each DNSP.
    a. *Note: the Identity verification process may not be standardised across actors. If several identities exist for one aggregator, it can be managed by different parties*
6. Aggregators bid on services for which they are qualified
7. *DNSP awards contract (not shown)*
8. DNSP issues service activation notice
9. Aggregator receives activation notice and prepares portfolio
10. Aggregator updates market offer to AEMO that includes capacity committed to all DNSPs through separate integration.
    a. *Note: When provided to AEMO, it through the existing separate integration for market services assuming the material portfolio size.*
11. Service verification obtained through smart meter data or other method if required.
    a. *Note: The Service verification data requirements may not be standardised for similar services across the DNSPs.*
12. This process repeats with any updates to the Aggregators Portfolio.
    a. *Note: Aggregator makes DER portfolio updates with each counterparty, this process may not be standardised.*

These steps outline the *Data Hub* process for the LSE use case (including Identity) shown above:

1. Each DNSP establishes a Local Services Exchange interface.
2. Using existing hub integration, DNSP establishes LSE channel(s) to signal service needs.
    a. *Note: Any existing Hub integration can be leveraged in this use case including existing identities managed by AEMO. This example assumes DNSPs and Aggregators are already integrated to the Hub for the DOE use case.*
3. DNSP uses broadcast messenger function to notify registered Aggregators/Agents on the hub of the channel, service opportunities, contract terms and how to connect.
    a. *Note: Service discovery can be promoted by the DNSP.*
4. Aggregator existing integration to the hub used to apply to subscribe to DNSP LSE channel(s).
5. DNSP approves access to their LSE channel based on aggregator credentials. Aggregators bid on services they are qualified for.
6. DNSP awards contract.
7. DNSP issue service activation notice.
8. Aggregator receives activation notice and prepares portfolio.
9. Aggregator updates market offer to AEMO that includes capacity committed to all DNSPs through existing hub integration.
10. Service verification obtained through smart meter data or other method if required.
11. This process repeats with any updates to the Aggregators Portfolio.
    a. *Note: The Hub maintains participants and portfolio mapping to facilitate B2B interactions.*

5.1.4 Backwards Compatibility Use Case

A further Use Case related to the problem of High Data Exchange Costs confirmed by stakeholders during EDGE's round of consultations relates to a Backwards Compatibility, the ability to support different schemas being used within the hub for messaging at the same time:

Table 7 Representative Backwards Compatibility Use Case

Actor	I have a problem that	Therefore, I want to	So that I can
Data Hub Administrator	Market systems cannot be improved quickly if all registered hub users are not able to adopt schema updates at the same time	Have backwards compatibility in the Data Hub which means I am able to support multiple different schemas for the same transaction at the same time	support multiple (backward compatible) versions of messages from different participants for a period to give them time to upgrade

The Backwards Compatibility Use Case is enabled within the Data Hub approach via its support of 2 (or more) different schemas at the same time (e.g. v1 and v2 messages can be supported for a period of time).

In the current deployment, message topics can have multiple schemas supported. Senders of messages are required to send all versions of message topic schemas to recipients in order for recipients to consume the message in the schema version they currently support. This enables participants to migrate to the latest schema version at different times without impacting market system upgrade schedules. Over time, all participants move to the latest schema version enabling former versions to be retired.

5.1.5 Visibility of DER

As is the case with High Data Exchange Costs, all stakeholders face challenges stemming from limited access to, and inconsistent quality of, DER operational data.

For many emerging DER use cases, a primary challenge is not necessarily a lack of data but rather limited capabilities for different stakeholders to access it in an efficient and timely manner. For example, AEMO currently lacks visibility into distribution network conditions and the amount of flexible DER capacity committed to off-market services, making it difficult to properly execute operational planning and market dispatch. Aggregators lack visibility into the location and operating profiles of all types of DER, making it difficult to recruit new customers into VPP offerings that benefit both the system and customers themselves. DNSPs have limited ability to discover and contract with DER aggregators for network support, thus leaving significant potential value on the table. And all of these problems are exacerbated when it comes to electric vehicles (EV), as highlighted by the ESB's recent EVSE Standing Data paper[58].

[58] Energy Security Board, Electric Vehicle Supply Equipment (EVSE) Standing Data Consultation Paper, December 2022

The Data Hub solution sought to overcome these challenges by extending the concepts introduced for DER standing data to operational data as well. As described in Section 4.1.2 and 4.1.3, combining a robust role-based access control to govern the ability to read/write data with strong authentication mechanisms can reduce friction in exchanging a wide variety of data types and formats.

As an indicative example, the architecture could be applied to create a dynamic DER register - including EV standing data - that would enable different entities involved in the DER lifecycle to create, read, and/or update DER records (or potentially, specific fields within records) based on their role within the market and the relationship to the DER (or associated customer). Any given entity could publish certain data to the shared registry once, and authorised subscribers can access the data based on their role.

An additional example of how operational visibility use cases could be delivered is demonstrated by the streamlined distribution of Dynamic Operating Envelopes from DNSPs to aggregators and AEMO:

- A shared DER registry caches a subset of the standing data (NMI/Aggregator mapping) and breaks DOE's from DNSP.
- Thus the DNSP can simply publish a DOE once to the registry, which partitions the DOE to send to the appropriate Aggregator without needing to be routed by AEMO.
- This same logic of "publish once, broadcast to all subscribers" applies to other operational data - e.g. location, current state, etc.

It's also important to note that the data exchange hub can be leveraged for any necessary market operator and DNSP / DSO visibility of planned aggregate DER behaviour arising from participant B2B services.

5.1.6 Market Operations Use Case

A Use Case related to the problem of Visibility of DER confirmed by stakeholders during EDGE's round of consultations relates to Market Operations.

Table 8 Representative Market Operations Use Case

Actor	I have a problem that	Therefore, I want to	So that I can
Market and System Operator	where I need to provide market directions to aggregations of DER, I do not know the distribution network limits within which they can draw or inject power	have visibility of each Aggregator's assigned DOEs	account for distribution network limits in forming market directions for the aggregator DUID as well as other resources

How the Market Operations Use Case is enabled within the Point to Point approach, as compared to the Data Hub approach, has been shown in the following diagrams. Note this use case focusses on DOEs that are delivered to aggregators but visibility of DOEs delivered to passive DER is also possible.

Figure 20 Market Operations Use Case in Point to Point architecture

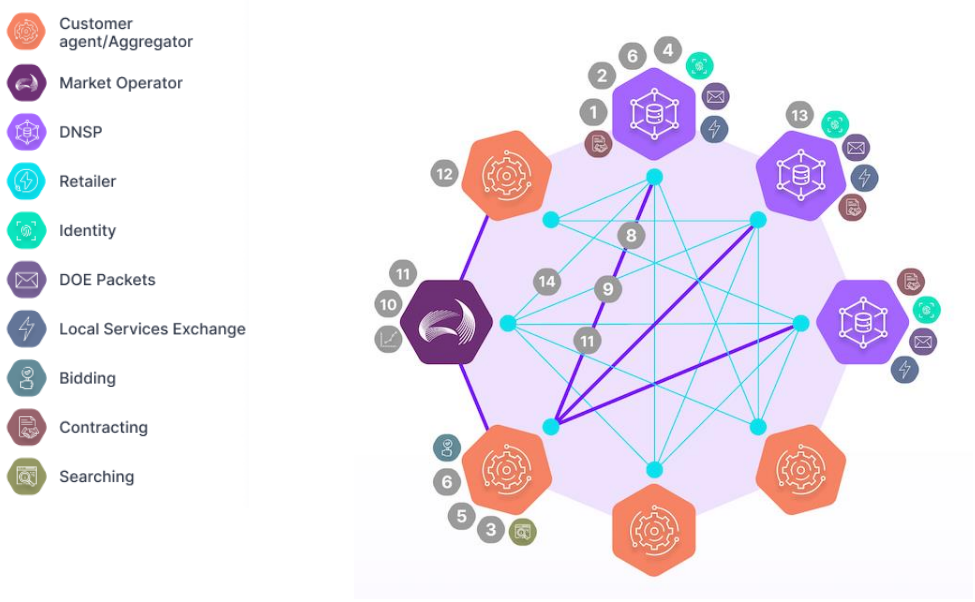
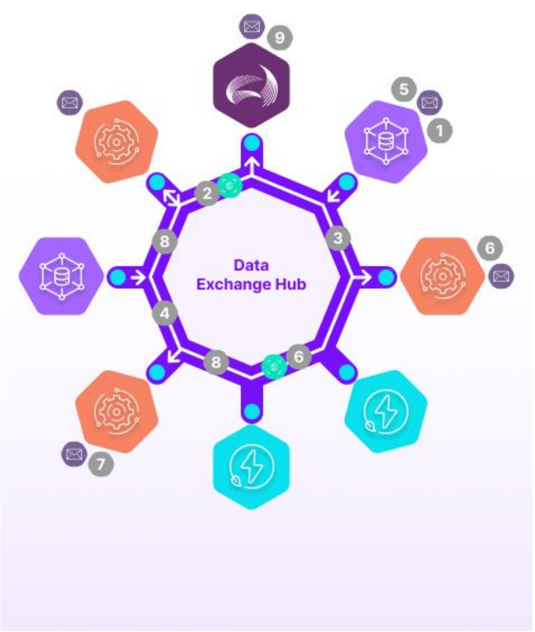


Figure 21 Market Operations Use Case in Data Hub architecture



Note: In the Point-to-Point architecture, all lines represent Point-to-Point integrations. Purple-coloured lines highlight an example of 1x agent/aggregator integration for the use case shown, however, this integration would need to be replicated for each agent/aggregator:DNSP pair

These steps outline the *Point to Point* process for the Market Operations use case shown above:

1. DNSP notified of a site with an aggregator (aka customer agent) that DOEs must be delivered to
2. The Aggregator then undertakes an organisation identity and portfolio registration process with each party
    a. *Note: The Identity verification process may not be standardised across parties. Several identities can exist for one aggregator, and be managed by different parties. The verification process may be in addition to the existing identity held with AEMO for Market Participation*
3. Single integration established between Aggregator and DNSP. An additional integration is established between DNSP and AEMO..
    a. *Note: For the Aggregator, integration is required per DNSP connection and this may not be standardised*
4. DNSPs map NMIs to portfolios and send a packet of DOEs per aggregator.
    a. *Note: DNSPs have a constant re-mapping process and must send multiple DOE packets*
5. DNSP sends AEMO the update to its NMI / Aggregator / DER Portfolio registry
6. DNSP sends AEMO Operating Envelopes DOEs per NMI per Aggregator
7. DNSP sends each aggregator a packet of DOEs relevant to their portfolio
8. AEMO updates its NMI / Aggregator / DER Portfolio registry
    a. *Note: Several identities can exist for one aggregator, and AEMO will need to verify the identity of the aggregator data provided by the DNSP against its own identity records*
9. Aggregator receives DOEs
10. Aggregator submits wholesale market bids to AEMO in accordance with DOE parameters
11. AEMO validates wholesale market bid meets network constraint information (aggregate DOE parameters)
12. The Aggregator updates their portfolio information as

These steps outline the *Data Hub* process for the Market Operations use case shown above:

1. DNSP notified that a site needs a DOE
2. The Aggregator undertakes organisation identity and portfolio registration process with each party.
    a. *Note: The established identity is managed by one party (e.g. AEMO) and then utilised by other parties. This reduces duplicating processes and thereby enhancing marketplace trust.*
3. Integration established between DNSP and DER Data Hub.
    a. *Note: Any existing Hub integration may be leveraged throughout all use cases.*
4. Integration established between the Aggregator and DER Data Hub.
5. DNSPs add new NMIs to batch of DOEs and send one packet of DOEs to the hub
6. The Hub broker takes the single DOE packet based on portfolio information and sends the correct DOEs to their site Aggregator.
7. AEMO also receives a copy of the DOEs within which to ensure market directions to aggregators are achievable
8. Aggregator receives DOEs
9. Aggregator submits wholesale market bids to AEMO in accordance with DOE parameters
10. *(not shown)* AEMO validates wholesale market bid meets network constraint information (DOE parameters)
11. *(not shown)* Aggregator updates portfolio information as sites & DER changes with AEMO.
    a. *Note: The Hub maintains participants and portfolio mapping to facilitate B2B interactions.*
12. *(not shown)* This process repeats with any updates to an Aggregator's Portfolio.

sites and DER change with each party.

   a. *Note: The Aggregator makes DER portfolio updates with each counterparty. This process may not be standardised*

13. DNSP re-maps NMIs to portfolio updates and send a packet of DOEs per aggregator.

14. DNSP sends AEMO the update to its NMI / Aggregator / DER Portfolio registry

15. AEMO updates its NMI / Aggregator / DER Portfolio registry

   a. *Note: Several identities can exist for one aggregator, and AEMO will need to verify the identity of the aggregator data provided by the DNSP against its own identity records*

a. Note: DNSPs can always send one DOE packet without maintaining and managing frequent aggregator portfolio updates.

Further Market Operations use cases were highlighted by the project although not directly mapped or subject to broad stakeholder consultation. These use cases are shown below.

Table 9 Other representative Market Operations Use Cases

Actor	I have a problem that	Therefore, I want to	So that I can
Market and System Operator	where I need to provide market directions to aggregations of DER, I do not know the capacity of that portfolio to draw or inject power on an operational timescale (on the day)	have visibility of each Aggregator's forecast generation and load from DER and close to real time updates on stored battery energy	account for DER portfolio capacity in forming market directions for the aggregator DUID as well as other resources
Market and System Operator	I do not have visibility of flexible capacity committed to off-market services such as those between aggregators and DSOs to incorporate into my operational planning and market solve (e.g. observe DNSP procured 300MW of peak demand support under a TNI on a given day)	receive both forecast as well as actual data of capacity committed to off-market services	take this into account to better balance supply and demand to run an efficient market, plan contingency reserves, RERT and other interventions

5.1.7 Ensuring Consistency in DER Standing Data across Industry Participants

Today DER standing data is replicated across multiple independent systems, and although processes exist to transfer data among these systems based on certain events, they are only loosely coupled and discrepancies inevitably arise over time. DER standing data represent the foundational inputs for nearly all other market transactions, so inconsistencies can create significant operational challenges and inefficiencies across AEMO, DNSPs, and DER agents.

The NEM's DER Register (DERR), maintained by AEMO, is a database populated with records provided by DNSPs who collect DER standing data in their own separate databases during the initial installation and commissioning process. This approach is sufficient for capturing "as installed" data but fails to reflect changing conditions over time. When DER settings, configurations, or capabilities change - for example, firmware updates, network protection setting configuration changes, augmentation of rooftop PV capacity, charge/discharge rates - there are no mechanisms in place to reflect those changes in the DER Register (DERR). As a result, the DERR does not show "as-is" settings, making it difficult for DNSPs to ensure compliance with mandated standards (e.g. AS4777) and accurately calculate Dynamic Operating Envelopes (based on DER capabilities), as well as complicating AEMO's operational planning and aggregator's VPP registration information (and thus their portfolio optimisation activities).

These discrepancies could also increase the frequency and impact of errors and disputes among AEMO and DNSPs. Based on expected DER growth and increasing participation in wholesale and local services, this could create operational challenges in coordinating DER activities. Were the DERR used to store EV Standing Data, as recently proposed by the ESB[59], enabling EV coordination would be heavily restricted by the DERR's lack of dynamic updates (as some submissions to the ESB have pointed out[60]).

Given that DER standing data represents the foundational inputs for market transactions, it is imperative that the principle of enabling data consistency across market participants and systems be applied to all use cases, including those we may not currently reference in this report or may even be aware of within today's policy landscape.

Project EDGE demonstrated how a multi-pronged technology strategy, combining streamlined IDAM with standardised and auditable data exchange channels, can ensure consistency in DER standing data across the industry.

Streamlining access management involved using the technologies associated with self-sovereign identities is outlined in Section 4.3.

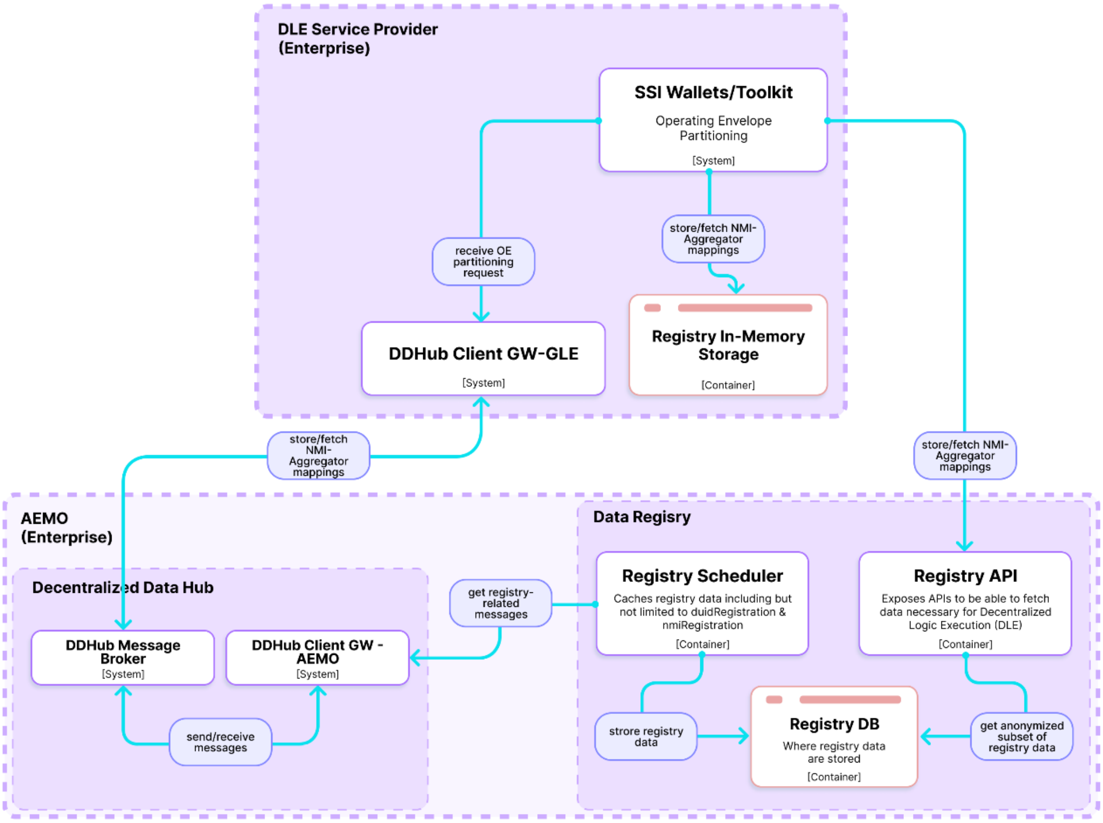
To enhance auditability, the Project utilised verifiable data registries "anchored" on a distributed ledger. Distributed Ledger Technology (DLT) involves many independent network nodes independently validating the state of data and events through a distributed consensus protocol. That is, multiple, independent computers (servers) which host DLT nodes assess how data is added or changed for a registry (e.g. which DID made the change, was it valid, etc) to determine whether the data amendment is valid or not. If validated, a "block" is created in the ledger to confirm the new state of the data registry. This approach enables maximum security and protection around registries, or "single sources of truth", as any hack or malicious penetration of the data registry would require the simultaneous hack of a majority of nodes hosting the DLT.

[59] Energy Security Board, Electric Vehicle Supply Equipment (EVSE) Standing Data Consultation Paper, December 2022
[60] See the Clean Energy Council's submission

Moreover, the "digital fingerprints" provide a persistent and immutable audit trail of all events (who last created, read, or updated the record or field)[61]. It is important to note that the Data Hub applied DLT functionality to identities, and not to standing or operational data.

The EDGE trial implemented a mechanism to ensure consistency in DER standing data. The DER standing data registry was stored in a database, then anonymised and verified using hashing techniques. As shown in the figure below, DER standing data is organised in a common structure and stored in a common environment with a pairwise, pseudonymous DID (a false / fictitious identifier which relates to the identity of the organisation (or user) which owns the data). The Pairwise ID can be regularly rotated for security purposes, thereby removing the potential to reverse engineer the identity of an organisation's pairwise ID. This approach effectively creates a unique and persistent record for each DER asset that serves as a common source of truth for all participants. Only the standing data curator (e.g. AEMO, or another regulated third party) and the identity owner (e.g. organisation, user) can associate the primary and pairwise DIDs for audit purposes.

Figure 22 Architecture to support DER standing data consistency


DLE Service Provider (Enterprise)
SSI Wallets/Toolkit
Operating Envelope Partitioning
[System]
receive OE partitioning request
store/fetch NMI-Aggregator mappings
DDHub Client GW-GLE
[System]
Registry In-Memory Storage
[Container]
store/fetch NMI-Aggregator mappings
store/fetch NMI-Aggregator mappings
AEMO (Enterprise)
Decentralized Data Hub
DDHub Message Broker
[System]
DDHub Client GW - AEMO
[System]
send/receive messages
get registry-related messages
Data Regisry
Registry Scheduler
Caches registry data including but not limited to duidRegistration & nmiRegistration
[Container]
Registry API
Exposes APIs to be able to fetch data necessary for Decentralized Logic Execution (DLE)
[Container]
strore registry data
Registry DB
Where registry data are stored
[Container]
get anonymized subset of registry data

[61] Though not implemented in EDGE, in a future production solution this concept could be implemented at a more granular level to further enhance standing data consistency. For example, to maintain accuracy of records over time advanced role-based access controls could be established at not only the record but also at the individual field level. Field access control configuration would be stored by the DLT to mitigate the risk of corruption and ensure consistency across entities. Instead of AEMO and DNSPs maintaining separate records, each of which are governed by different security and access policies, both organisations can be granted limited access to specific fields relevant for their needs.

To maximise scalability, availability, and cost, actual standing data is stored in a decentralised storage using existing database systems (RDS or NoSQL DB). In this context, the storage is "decentralised" in the sense that AEMO and DNSPs can host independent nodes that maintain consistency via standing data by referencing "hashes" derived from DLT consensus and access configurations stored separately by the DLT.

5.1.8 Standing Data Use Case

The problem of inconsistent (and ultimately inaccurate) DER-related data across participants relates to one of the key Use cases highlighted by stakeholders through consultation, that relating to Standing Data.

While this use case was not field tested during the Project, it was unanimously highlighted across industry stakeholders as a high value and priority problem for which to determine a solution. Example Standing Data problems are shown below.

Throughout EDGE's consultations, the problem of standing data inconsistency was identified by stakeholders as needing a solution soon, with the scale of the problem only growing with the deployment of additional DER. Similar stakeholder sentiment is now arising in Western Australia.

Table 10 Representative Standing Data Problem Statements

Actor	I have a problem that	Therefore, I want to	So that I can
Use Case: Standing Data - Inverter settings			
Aggregator	Cannot update market on inverter settings If required, as the customer's DER representative, I cannot update Market system and network operators with updated inverter settings of DER devices in my VPP portfolio following a firmware upgrade.	I want to write and update inverter settings of a DER device following a firmware upgrade	fulfil my obligation to reflect accurate settings about DER device functionalities in the DER Register which is used by the market, service and standards compliance authorities and participants as an up-to-date and enduring single source of truth
Market and System Operator	Unknown DER standard non-compliance I cannot confirm whether inverters connecting to the network and integrating with the grid are compliant with the specified service requirements and standards. This inhibits the MSO's ability to plan for power system disturbances, increasing costs to the power system relating to need for greater operating reserve.	view inverter standard compliance and performance threshold settings of registered DER in aggregate at a region level and initiate changes (within appropriate permissions)	reliably identify whether inverter settings are compliant with standards and service requirements (e.g. droop settings for FCAS and fault ride-through settings)

Actor	I have a problem that	Therefore, I want to	So that I can
Use Case: Standing Data - Inverter settings			
DSO	Inaccurate DER Configurations the DER Register does not necessarily reflect the "as-is" configured state of the connected DER, as settings can be changed after the installation, and this can have a consequential impact on network DER hosting capacity assessments and dynamic operating envelope calculations	view inverter settings of registered DER (within appropriate permissions)	adapt network DER connection assessments and DOE calculations to accurately reflect the existing installed DER status
DSO	Unknown DER standard non-compliance Many installed inverter-based DER connecting to the network do not have the mandated standard AS4777 settings applied and this adversely impacts local network voltage management. Other than analysing historical smart meter data (where that exists), I have no way of knowing whether the installed system is compliant view inverter settings of registered DER and initiate changes (within appropriate permissions) adapt network DER connection assessments and DOE calculations to accurately reflect the existing installed DER status	view inverter settings of registered DER and initiate changes (within appropriate permissions)	view inverter settings of registered DER and initiate changes (within appropriate permissions)

How the Standing Data Use Case is enabled within the Point to Point approach, as compared to the Data Hub approach, has been shown in the following diagrams.

Figure 23 Standing Data Use Case in Point to Point architecture

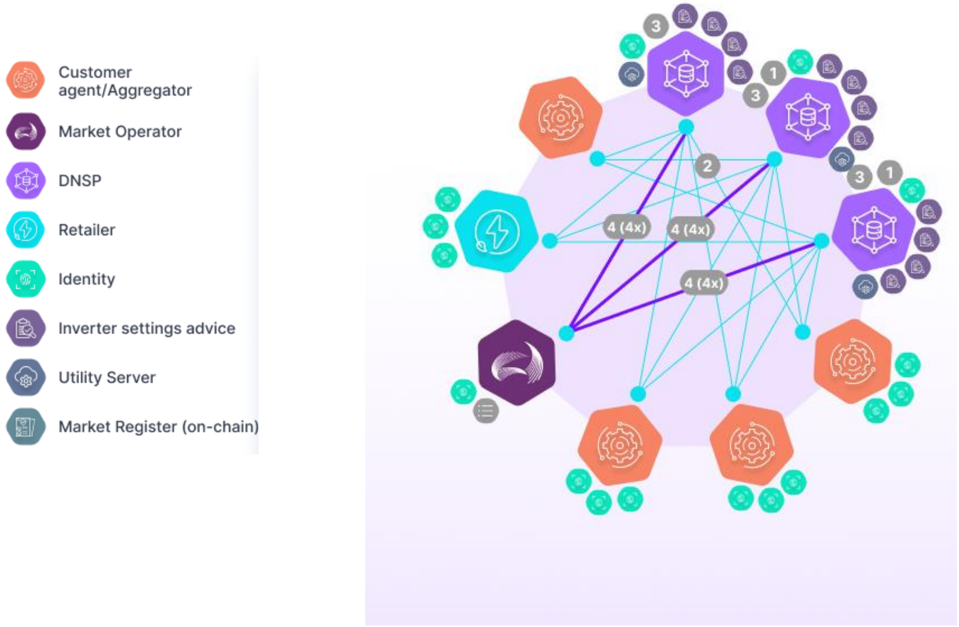
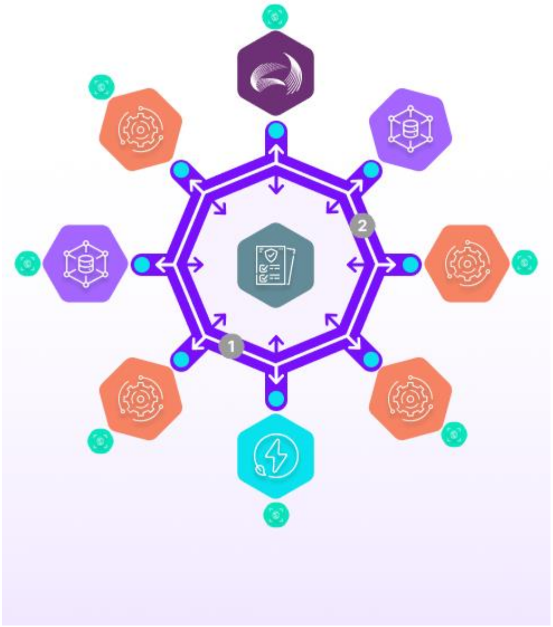


Figure 24 Standing Data Use Case in Data Hub architecture



Note: In the Point-to-Point architecture, all lines represent Point-to-Point integrations. Purple-coloured lines highlight an example of 1x agent/aggregator integration for the use case shown, however, this integration would need to be replicated for each agent/aggregator:DNSP pair

These steps outline the Point to Point integrations process for the Standing Data use case shown above:

1. Each DNSP establishes a 2030.5 Utility Server.
2. Every aggregator and OEM, or other third party agent, authorised to advise changes to inverter settings integrates with each DNSPs 2030.5 Server
   a. *Note: the Identity verification process may not be standardised across actors. Multiple identities will be created and be required to be managed by each aggregator / OEM / customer agent.*
3. As inverter settings are changed, relevant customer agent communicates with each relevant DNSP's Utility server to advise change
   a. *An audit trail of which agent made which update is NOT available via this solution*
4. DNSPs update DER register to advise AEMO of inverter setting change

These steps outline the Data Hub process for the Standing Data use case shown above:

1. Each market participant and third party actor (e.g. OEMs) integrates with Data Hub
2. Based upon assigned roles and permissions, utilising their DIDs and associated credentials, DER standing data is updated by all parties for their relevant meta-data of devices, with records of changes "hashed" on chain utilising agreed Consensus protocols to ensure verified and secure changes can be made to the single source of truth.
   a. *An audit trail of which agent made which update IS available via this solution, which supports enforcement and compliance endeavours*

5.1.9 Cyber Security

As the power system becomes increasingly decentralised with DER uptake, it is imperative to maintain secure and reliable communication infrastructure that extends to DER devices directly and / or via aggregators. With multitudes more devices and access points, ensuring market infrastructure can manage the risk of threat actors that may target vulnerable points across a wide and expanding ecosystem of DER supply chains is a critical capability.

EY was engaged to conduct a cyber security threat assessment on the different approaches to data exchange being tested in Project EDGE[62]. Specifically, a data hub (either centralised or decentralised) and Point-to-Point methods for scalable data exchange. A total of 12 cyber security risks (two (2) critical-rated, six (6) high-rated and four (4) medium-rated) were identified during their assessment.

Key mitigating controls that would enhance the security of DER data exchange infrastructure were identified by EY. By applying a more comprehensive application of DIDs across the DER Marketplace ecosystem, beyond only market actors as in the EDGE field trial, EY's assessment identified that the following benefits could be derived:

[62] AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

- Secure integration with the DER ecosystem: by ensuring that all devices and entities associated with the DER Marketplace had a DID, this would enable each to seamlessly control and upload their standing data and credentials to a DER Register when they initially come online, saving time, effort and errors in manually uploading data;
- End to end visibility and auditability: With DIDs and Verifiable Credentials (VCs) at each level of the supply chain, this would support greater integrity checking and enable the isolation of operation (via revoking VCs) if and when a security threat has been identified.
- Secure interoperability across the DER ecosystem: Correct DIDs and VCs (and customer consent) enable any organisation (e.g. retailer / aggregator) to send control signals to compatible devices. This capability provides security with the flexibility to enable consumers to seamlessly switch between market service providers, as well as support aggregators and VPP operators to simply coordinate numerous device types across their portfolio.
- Compliance with industry standards: DIDs, VCs, and DLT can provide the traceability of settings and firmware upgrades against compliance to industry standards.

6 Lessons Learned

To test the hypothesis that a data hub model provides a scalable and long-term approach for DER Marketplace data exchange, Project EDGE conducted field trials between May 2022 and March 2023. The EDGE data exchange platform was initially deployed in May 2022, with AEMO, AusNet, and Mondo as the initial trial participants. Further platform updates were released throughout Q3 2022, and as of September 2022 two additional aggregators were on-boarded into the field trial.

In addition, the data exchange platform is being utilised by Project Symphony[63], Western Australia's largest DER Orchestration Pilot, where WEM-based DER are being co-ordinated as part of a Virtual Power Plant (VPP) to unlock economic and environmental benefits for customers and the wider community.

Key elements of the field trial's operation included:

- To demonstrate DER wholesale energy market integration, AEMO established sandboxed wholesale markets (WEM and NEM) for the Projects' field trials. Three participating aggregators, enrolled portfolios of battery storage, controlled loads and rooftop solar assets. To operate the EDGE wholesale market, aggregators submitted bi-directional (i.e. export or import) offers to AEMO via the dedicated "EDGE" topic for each 5-minute market interval. In addition, as the DNSP, AusNet communicated daily Dynamic Operating Envelopes (DOE) per NMI to AEMO, who partitioned (sorted) the NMI-based envelopes back to aggregators so that they could adjust their portfolio schedules and future offers[64].
- To run the sandboxed markets, a simplified dispatch engine was developed that applied both business logic (i.e. offer validation based on market rules) as well as the aggregated DOE limits to each interval and solved for each aggregator's dispatch target based on those constraints.
- Similar to the existing wholesale market, AEMO communicated dispatch instructions and future price forecasts to the aggregators every five minutes, who in turn were responsible for sending the appropriate control signals to their portfolio assets to achieve the desired outcome for the current interval and as necessary, revising offers for future intervals.
- To demonstrate the local services function set, AusNet used the dedicated "LSE" topic to communicate directly with aggregators and procure local network services on a bilateral basis. When aggregators receive event triggers from AusNet for local network services, they send the appropriate control signals to participating assets, and subsequently revise offers in the EDGE wholesale marketplace to reflect any changes in availability of their entire portfolio resulting from LSE pre-service engagement and delivery.

[63] See WA DER Program: Project Symphony

[64] Initially, DOEs were submitted and partitioned on a daily basis. Subsequent phases of the trial will increase the frequency of DOE partitioning to four times per day (six hour intervals).

Through the field trial, and the accompanying stakeholder engagement sessions and independent analysis, Project EDGE developed a robust evidence base to evaluate the hypothesis and inform further development of a data hub model that is fit-for-purpose and capable of supporting emerging DER use cases. The remainder of this section summarises the key lessons learned from using the Data Hub throughout the operational trials.

Lessons are categorised in the following sections by the time horizon within which they require AEMO's attention, namely:

- Near Term Lessons to Incorporate: immediate steps that AEMO and industry stakeholders can apply within the next 6-18 months
- Medium Term Lessons Requiring Further Evaluation: areas that warrant further consultation and evaluation, to be conducted within the next 2-3 years
- Longer term Lessons for Consideration: potential strategies relevant to the long-term evolution of DER management in the NEM post-2025

6.1 Near-Term: Lessons to Incorporate

This section contains lessons which should be applied as soon as possible, and inform further development of DER data exchange solutions in the next 6-18 months (through 2023 & 2024).

Lesson 1: There is industry support for implementing a DER data hub concept, although further work is required to determine the optimal design

Project participants indicated that, while point-to-point integrations are generally suitable at current levels of DER adoption, there is support for implementing an industry-wide data hub concept in anticipation of a DER-rich future[65].

The primary appeal of the hub concept is the ability for AEMO, DNSPs, aggregators and customer agents to exchange a wide variety of information – including real-time data, encrypted data, and bulk data – in a secure and standardised fashion via a single integration. Project participants indicated that a data hub model would improve efficiency and reduce operational complexity – critical requirements as DER continues to proliferate in both wholesale markets and local network support services.

While evidence suggests a hub solution offers security and efficiency benefits compared to point-to-point integrations, there is not clear consensus about the optimal hub implementation strategy – centralised or decentralised.

Each approach has relative strengths and weaknesses. For example, a centralised model may offer certain advantages with respect to scalability, however, it may introduce bottlenecks at scale and heighten risks in the event of a single point of failure. A decentralised model may offer certain efficiency and resilience benefits but likely requires more total resources to achieve similar scalability.

[65] A data hub model also ranked higher in EY's theoretical evaluation, as per their Technology and Cybersecurity Assessment report, Section 3. Additional feedback in support of a DER data hub came directly from project participants, as well as stakeholder forums, including the DER Market Integration Consultative Forum (MICF), the Demonstrations Insights Forum (DIF), and the Networks Advisory Group (NAG)

At present, the Data Hub architecture deployed leverages both conventional centralised infrastructure - a message broker hosted by AEMO - as well as decentralised technologies and architectures. As a hybrid, it is considered a balanced approach capable of delivering many of the benefits from both centralised and decentralised models.

As described in the following section, further engagement and governance participation among industry stakeholders will be required to determine an appropriate framework for implementing a hub beyond the scope of the trial.

Lesson 2: A production DER data hub solution must offer the flexibility of multiple integration mechanisms while maintaining standardisation

Project participants indicated support for the Data Hub solution architecture, but the experiences of several project participants indicate that the current container-based integration method is likely to be considered too complicated for widespread adoption, and does not offer sufficient flexibility. Extending a DER data hub beyond the scope of The Projects into a market-wide solution will require further development of additional integration methods that remain aligned with a common technical standard.

In the current implementation, participants and DNSPs must download and run a container-based application[66] and deploy it in a hosting environment of their choice (i.e. cloud provider or on-premise server), using Kubernetes (an emerging system for orchestrating and managing container-based applications). Using containers and Kubernetes can help organisations improve efficiency, scalability, and performance when deploying complex applications across multiple environments[67], but both technologies are relatively novel in the global IT landscape, and the Australian energy market in particular. As these tools and technologies are not yet ubiquitous, there is significant variation across organisations with respect to their knowledge, proficiency, and support levels to use them.

The installation process of the containerised integration application required participants to specify connection details to the Message Broker utilised by AEMO. Due to natural heterogeneity in each organisation's host environment and varying in-house technical resources and capabilities, the initial deployment and integration of participant client gateways was more complex than anticipated. One barrier was the need for each participant to configure and maintain a custom deployment pipeline based on their specific host environment and implementation parameters. Project participants indicated preference for a more streamlined, standardised deployment model similar to other web-hosted applications - for example, the ability to download and run an installation wizard, or the ability to configure and run components via an administrator user interface instead of executing custom deployment pipeline workflows.

As participants all self-hosted containerised gateway applications, coordinating the release of new versions was challenging, especially when updates resulted in incompatibility with prior versions. Unlike with other web applications – whether hosted in an app store, or accessed via Software-as-a-Service (SaaS) – where updates and modifications are automatically pushed to all end users, in the container-based approach all project participants had to proactively download

[66] A container is a unit of software that bundles code and associated dependencies into a cohesive, executable package that can be easily deployed in different environments. See https://www.docker.com/resources/what-container/ for additional context.

[67] See https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-kubernetes/#overview for additional details.

a new client version and execute their deployment pipeline. Communicating and coordinating updates (and subsequently troubleshooting errors that arose during deployments) was time-consuming albeit manageable at the scale of the trial (involving five organisations), however, it will not scale to an industry-wide solution involving hundreds (or more) of organisations. Project participants indicated that having a standard DevOps type solution to automate the distribution and deployment of updates and new versions could mitigate this challenge.

6.2 Medium-Term: Lessons Requiring Further Evaluation

This section contains lessons which should inform further analysis and stakeholder engagement over the next two years to align development work on a DER data exchange solution related to market reforms.

Lesson 3: Decentralisation of hub architecture and identity management systems may offer benefits compared to a centrally administered hub, but raises questions regarding support and maintenance

Analyses by both Project Participants and EY indicated that there are resiliency benefits to implementing a hub with a more decentralised architecture[68] due to inherent redundancies and failover / recovery mechanisms. However, operating such a hub at scale will require a thoughtful approach to ongoing support. Whereas a more conventional, centralised hub has a clear relationship between the service provider / administrator (e.g. AEMO) and users (e.g. participants) those lines may become blurred in a hub that empowers all market stakeholders with greater autonomy to manage their own identities and credentials, host their own applications that integrate with common messaging infrastructure, and establish bilateral and bespoke communication channels without relying on a central broker.

Roles and responsibilities for providing technical support as well as ongoing maintenance and upgrades will need to be clearly defined via a robust governance mechanism. Once defined, service providers that can deliver these requirements can then be engaged by shared governance mechanisms. The potential benefits and practical considerations for implementing a decentralised hub are further described in EY's report[69].

Lesson 4: A DER data exchange hub must be designed with capacity for DER coordination during Unexpected Events

As outlined in EY's Technology and Cybersecurity report[70]aggregators are able to follow AEMO intervention targets when directed during unexpected events, however, coordination among participants will be needed to ensure targets are achieved within dynamic network limits.

With the NEM market suspension occurring in June 2022, Project EDGE established a test plan to learn from this exceedingly rare event. Multiple tests were conducted by AEMO to help elucidate the required considerations when directing a highly saturated DER market where a substantial proportion of supply and demand is managed by aggregator Virtual Power Plants (VPPs). These tests highlighted several key findings relevant to market infrastructure, including:

[68] AEMO - Project EDGE - Technology and Cybersecurity Assessment, EY, June 2023
[69] Ibid, see Section 6
[70] Project EDGE Lesson Learnt Report #2, December 2022

- When formulating directions to VPPs, coordination is required between AEMO and DNSPs to ensure that dispatch targets are able to be achieved within the DOEs provided by the network;
- Such coordination is facilitated through capabilities such as AEMO having visibility of DER through the DOEs published into the data hub.
- Given the nature of market operations during such an event, the efficiency enabled by coordinating directions with DNSPs via a data hub, compared to multiple point to point integrations, is significant, especially considering the anticipated large number of VPPs and DNSPs likely to be operating in such a DER-rich future.

Lesson 5: AEMO's Technology Strategy and IT Architecture teams should conduct a more extensive comparison of the Data Hub implemented in EDGE and the existing e-hub to identify gaps, overlaps, and an optimal path forward

The Data Hub solution developed in Project EDGE & Symphony features some enhancements relative to the current capabilities of the e-Hub, but also lacks certain capabilities that exist in e-Hub. These are summarised in the table below.

A detailed evaluation by AEMO's Technology Strategy and IT Architecture teams would result in a more accurate estimate of the time and effort to either develop the existing e-Hub features in a data hub, augment e-hub to enable the relevant capabilities of the Data Hub or map out a convergence between a DER data hub and the e-Hub.

.

Table 11 Attribute and Functionality Comparison between e-Hub and Data Hub Solution

Attributes and Functionalities	Description
Common to the Data Hub and e-hub	• For information sharing between participants and AEMO, both solutions provide similar functionality and implement common security patterns (certificates, ports, payload integrity). • From an identity and access management perspective, both solutions have similar approaches to authenticating participants and authorising specific transactions / permissions via role-based access control. • Both solutions support API's, File Transfer, Schema Validation, and Response message formats.
Data Hub enhancements to the current e-Hub capabilities	• Messages can be sent between participants and DNSPs without configuration by or the involvement of AEMO - a central broker administrator is not required. The Data Hub solution also supports broadcast patterns to multiple subscribers, such as distributing forecast prices from AEMO to all aggregators. Further, The Projects architecture creates an opportunity for participants and DNSPs (or another third party) to host their own transport layer, supporting enterprise resilience as well as independence; • The general-purpose, open-access messaging infrastructure makes the Data Hub highly adaptable to new use cases and requirements. For example, it has the ability to enable B2B/B2C schemas and transactions quickly, as well as the ability to use

Attributes and Functionalities	Description
	Portfolio Management data to partition and inform select / required recipients as required; • The complexity of the eHub integration and some functionalities are removed, and within solution becomes a part of the Container. For example: o Enables API, File transfer, and Message Queue (all in one) capability; o Validates schema prior to it being sent; o Caching of incoming payload; • Integration efficiency is enhanced with: o a single endpoint to connect to industry integration, so that it requires only one firewall port to be opened; o a single credential to talk to multiple parties (regardless of which party hosts the Transport Layer); o a single port whitelisted to enable communications (to each Transport Layer); and o Security requirements met with a single MTLS certificate (per Transport Layer); • AEMO is not responsible for administering identities or certificates for external organisations - public / private Certificates are self-managed by participants and DNSPs; • Certificates are tied to an identity/role, and a role has visibility for only those channels/topics to which it has permission (i.e. not every channel/topic is visible to everyone); • Large messages (payloads) are broken up by the container for transport (and reconstructed); • Each Payload is encrypted/decrypted by a one-time use key, enhancing security; • the Data Hub solution supports publish / subscribe patterns (the current e-hub implementation requires configuration changes for this); • Participants can self-service for child certificates (for development and test purposes); • Deploying containers with a Kubernetes service have horizontal scalability (with Pods being spun up on demand) • Multiple containers can be setup in an organisation to cater for different environments (development, test, staging) • Containers (if required) can be set up on a user's machine for development purposes; • The EDGE solution can facilitate event-based transactions being "passed through" - AEMO isn't required to partition (sort) messages / data for the "correct" recipient.

Attributes and Functionalities	Description
e-Hub capabilities not currently implemented in EDGE[71]	• Synchronous transactions capability • Schema version (n-1) compatibility • Improvements required in logging, alerting & monitoring • Store Messages that are passed between participants (if a requirement) • Store and forward capability (between Initiator and Recipient) • Stop file mechanism (if a requirement)

6.3 Long-Term: Lessons for Consideration

This section contains lessons which should be considered by policymakers and factored into long-term planning (>2 years) and NEM reforms.

Lesson 6: Decentralised Architectures align well with collective governance, which could better support innovative business models

Given the nature of the trial, Project EDGE did not explore in any detail the potential governance arrangements for the solution options it considered. However, it noted that the nature of the architecture of the progressed solutions lend themselves to alternative and more flexible governance arrangements than those in place for point-to-point or augmented e-hub solutions.

Particularly with respect to the decentralised solution option - with participants (and others) hosting market infrastructure and being enabled to support direct one-to-one communications and distributed applications support - the governance arrangements to support this infrastructure would likely entail shared responsibilities across industry participants and key actors (DNSPs, and AEMO). Such governance arrangements would then potentially drive and support shared financing and cost recovery fee structures to support the shared market infrastructure.

Project participants and EY's Theoretical Evaluation[72] indicated that a more decentralised hub architecture allowed for more flexible governance, as delegated responsibilities are matched with the technical ability to administer direct communications (e.g. bilateral exchange between DNSPs and aggregators) and distributed applications (e.g. Local Services Exchange). Further decentralising the hub architecture, as well as using a role-based permission system defined through collective governance, has the potential to offer operational efficiencies and enable more rapid innovation, as participants could develop new applications and implement new DER use cases based on their role, rather than requiring a central administrator to do so.

As a current day example of "shared industry governance", AEMO's Information Exchange Committee[73] provides a proven mechanism that could be extended to support and evolve a shared energy industry data hub solution. Determining an appropriate governance model that

[71] These features would likely need to be developed for future use beyond the EDGE trials. While detailed requirements would need to be documented to support these features, the Project Team estimates that delivering these capabilities would require an additional six months of development effort.
[72] AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023, Section 3
[73] See more about the Information Exchange Committee AEMO's Information Exchange Committee

includes all industry participants and balances flexibility with stability will require thoughtful consideration and industry engagement.

Lesson 7: A Decentralised Hub Architecture Aligns with National Electricity Objective (NEO)[74]

EY's Technology and Cybersecurity Assessment report for Project EDGE includes a theoretical evaluation of various data exchange options which ranked a decentralised DER data exchange approach as the most suitable architecture for a secure, scalable, two-sided market, while also aligning closely to the assessment's success criteria and the NEO. The report noted that while current volumes of DER data exchange are relatively small, there is less distinction between centralised and decentralised options. However, there may come a tipping point where the advantages of decentralised approaches start to outweigh the costs and complexities of transitioning towards decentralised technologies. Introducing a production DER data hub across the entire NEM must be done thoughtfully and will require more focused work to address important design decisions and practical considerations. For example, building in the flexibility to decentralise the initial DER data exchange approach so that the associated benefits can be captured should this option become feasible. Beyond the technology itself, NEM stakeholders must convene to align on operational requirements, ownership and commercial structures, governance models (including roles and responsibilities), and legal framework[75]. The AEMO Engineering Framework[76] should also be consulted in the design phase. Continued stakeholder engagement is required to reach consensus on a path forward that will result in a data hub that can scale and adapt to evolving industry requirements over time.

6.4 Evaluating Project EDGE Research Questions & Hypotheses

Project EDGE's Research Plan[77], developed by the University of Melbourne, has guided the delivery of Project EDGE to create a pathway to generating an empirical evidence base. It applied the design thinking approach adopted by Project EDGE, beginning with the National Electricity Objectives (NEO) and cascading through multiple steps to guide the Project's design.

The Project EDGE Lessons Learnt Report #2 covered research questions (RQ.) 1, 4 and 6 in detail, and should be read in conjunction with this report. This Lessons Learnt report mainly addresses results and recommendations relating to RQ.6. Appendix A4 outlines a high level assessment against key research questions given the activities outlined in this report have relevance to other research hypotheses associated with RQ.3, RQ.4, RQ.5 and RQ.7.

[74] AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[75] See Section 6.1, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[76] AEMO Engineering Framework documents (various) available at: https://aemo.com.au/en/initiatives/major-programs/engineering-framework

[77] Project EDGE, Master Research Plan

7 Recommendations for a Future DER Data Hub

Project EDGE established a robust evidence base to support the hypothesis that a DER data hub is a more efficient and scalable data exchange solution to support emerging DER use cases than existing point-to-point connections.

Accordingly, the overarching recommendation based on the lessons learned through Project EDGE is that the NEM should move forward with scoping, designing, and ultimately implementing a DER data hub in anticipation of a DER-rich future.

Moving forward, AEMO should continue to engage industry stakeholders to evaluate and align on data hub technologies and capabilities, operational requirements, ownership and commercial structures, governance models (including data exchange roles and responsibilities), and legal frameworks.[78]

This section offers recommendations for the future of an industry DER data hub solution informed by the technical development and operation of the Projects' Data Hub and its application in more than 11 months of round the clock operational field trials. The lessons described are provided to inform considerations of high-level models for DER integration and data exchange, and are intended to be technology-agnostic so that they can be applied regardless of any technology solution choice made for a future DER data hub. The Project Participants do not endorse or intend to prescribe any technology choices or vendors based on this report.

7.1 Assess Opportunities to Leverage EDGE & Symphony Technology Investments

One of the objectives of Project EDGE was to demonstrate new technical capabilities required to meet emerging DER use cases such as Dynamic Operating Envelopes and Local Services Exchange. Several of the novel software components that were developed specifically to meet these requirements and currently underpin the EDGE Data Hub solution – including the Self Sovereign Identity (SSI) technologies, the DLT-based identity data registry, DDHub client gateway, and Decentralised Logic Execution – were based on open standards and made available under an open-source license, meaning that AEMO or any other actor in the NEM is free to utilise and modify the source code without paying license fees. Accordingly, these components could be further augmented or repurposed for a future data hub implementation. AEMO should incorporate these components in an evaluation of its long-term technology strategy, determine which, if any, capabilities are relevant to a production-grade data hub solution, and identify DER use cases where they may add value to industry going forward.

[78] See Section 6.1, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

7.2 For a Production-Grade DER data hub Deployment, it should be a requirement to develop Various Integration Mechanisms to Promote standardisation while maintaining flexibility for Industry

A practical lesson that holds significant value for market participants, and overall solution efficiency, relates to the integration mechanism required for participants to interact with a DER data exchange hub. Within Projects EDGE & Symphony, participants were required to manually download, configure, and deploy a containerised software solution (i.e. the DDHub Client Gateway) within an environment of their choosing. For a future production-grade deployment of a DER data hub, integration must be further streamlined via automation and support multiple additional options so participants can manage the integration without key specialised IT skills or resources. For any future data hub implementation, additional integration methods should be developed to provide maximum flexibility for participants. Recommended integration methods include:

- Enhanced containerised approach: The existing container-based approach can be enhanced with improved documentation and tooling.
- Enterprise cloud marketplace: Cloud marketplaces such as Azure and AWS are a popular way to offer cloud-native applications in a simple user interface that automates back-end deployment processes, similar to existing enterprise cloud services. This method could enable DNSPs and aggregators to *subscribe* to the data hub through their existing cloud provider rather than manually configuring and deploying a containerised application on their own. One potential limitation to this approach is that it requires participants to commit to a paid subscription to a specific cloud provider (if they don't already have an existing partnership, and/or prefer to run this type of solution on-premise).
- Standalone platform (web or desktop application): Another potential approach is to enable participants to integrate with the hub as well as administer all data exchange processes (e.g. configure channels and topics) through a standalone application (similar to existing software- and platform-as-a-service models). Offering integration as a standalone application with a user interface to manage both infrastructure and business operations tasks would replace the manual development tasks that are currently required (e.g. executing scripts, deploying software packages downloaded from a repository), and would allow a wider range of business users (e.g. software architects, IT analysts, program managers) to interact with the data hub and manage integrations with other systems.
- APIs: Many participants are familiar with APIs from experience with existing market systems (e.g., retail transactions via e-Hub), so similar APIs and associated front-end user interfaces could be developed to enable access between the hub and external systems.

7.3 Prioritise Development of Functional Capabilities to Support DER Use Case with No Incumbent Solution

EY's report outlines a conceptual roadmap[79] for a phased rollout of a DER data hub. In this approach, the DER data hub would be initially implemented for one DER use case for which there

[79] See Section 1.5, AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

is no existing widespread solution, such as DNSPs publishing DOEs to DER agents and endpoints. Once the hub is adopted by all relevant stakeholders for the initial use case, additional DER use cases where no current solution exists can be implemented within the hub.

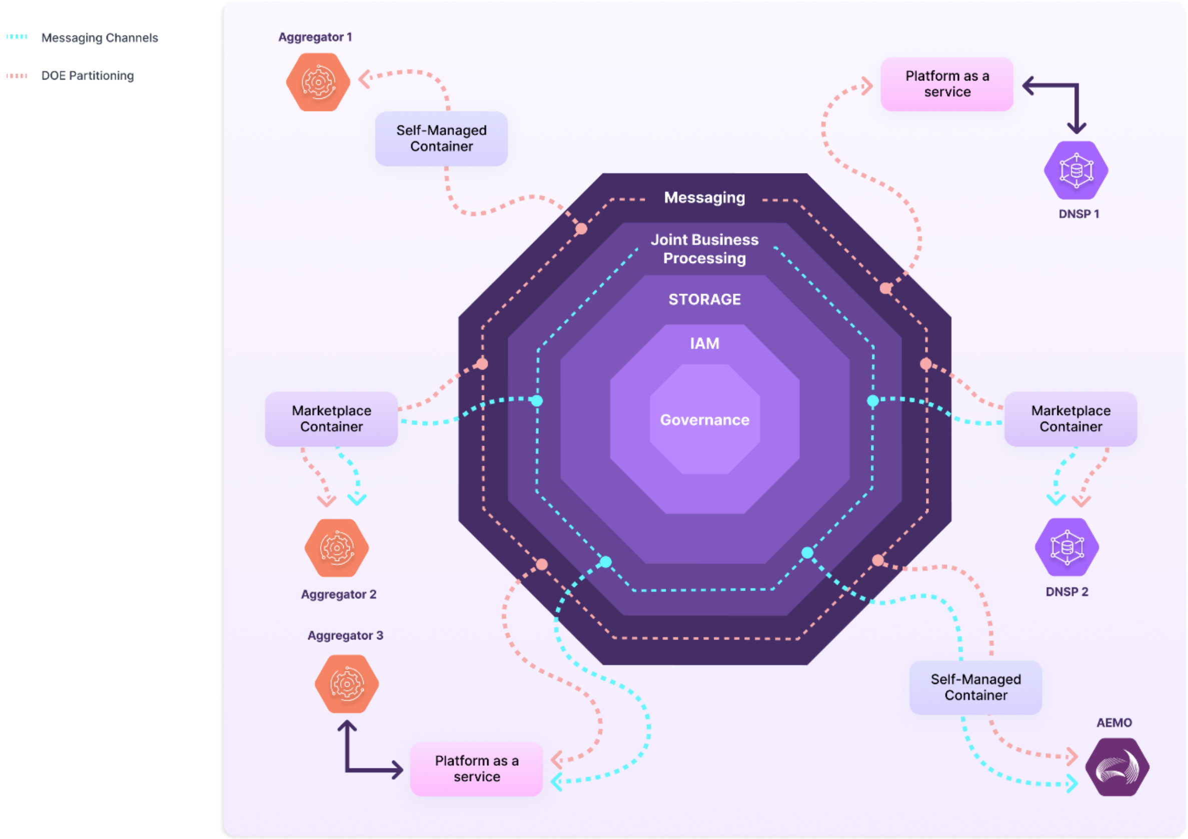
One benefit of this approach is that functional and technical capabilities can be developed in a similarly phased approach in order to reduce overall complexity, achieve technical proof points incrementally, and meet market needs as they emerge.

Identifying the precise functional capabilities to be developed will depend on the initial use case(s) selected. However, there are several generic capabilities that facilitate all use cases in a production solution. These include:

- Expanded integration methods: as described above in Section 7.2.
- Federated Identity: The IDAM component within the hub should link SSI systems with existing enterprise IDAM solutions (e.g. ActiveDirectory, AWS IAM) used by participants for administering users, roles, and permissions within their own organisation. Implementing a federated identity system would enable individual users within DNSPs, aggregators, and AEMO to use existing organisational credentials to log into the hub, where SSI components could be used for inter-organisational IDAM processes. It would use the key vault on each user’s machine for authentication, so users can use DIDs to interact with any service within the hub while using external key vaults (e.g. Azure, HashiCorp, AWS) for key management.
- Enhance Storage Configuration: For use cases requiring larger volumes of data storage (such as a dynamic DER register), the hub should provide the ability for administrators to configure where data from hub operations - outputs, messages, logs - is stored (e.g. Azure, AWS etc.) as well as how data is read / ingested from existing external private databases.
- Enable Joint Business Processing Configuration: Some emerging DER use cases may require the capability to execute parallel processing of sensitive business operations, the capability to transmit complex datasets amongst three or more parties in a way that does not reveal all data to all parties, and/or the capability to provide public verification of outputs while maintaining privacy and integrity of inputs (e.g. DOE partitioning use case described in Section 5.1.1). Accordingly, the hub should offer the ability to customise and configure this type of joint business processing (see Appendix A3).
- Option for Multi-tenant hosting of hub infrastructure: Decentralisation of hosting, ownership, and governance may offer multiple benefits to industry. The hub should be designed in such a way that hosting configuration and responsibilities can evolve over time in response to changing industry needs. For example, to begin the hub could initially be operated as demonstrated in the trials - AEMO would host the core messaging infrastructure, while DNSPs and aggregators would integrate with the hub using multiple integration methods but over time additional parties could become authorised to host messaging infrastructure for scalability and/or resiliency purposes.

By way of example, a high-level conceptual architecture showing some of the above capabilities that would be implemented for a phased rollout approach is shown in the figure below.

Figure 25 Conceptual Architecture of EDGE Data Hub Enabling DOE Use Case, with Multi-Integration Approach



Hub Components*

- Governance: Rules, roles, and responsibilities defined via formal decision-making process and encoded within the hub.
- IAM (Identity and Access Management): Tools to enable participants to acquire roles and authenticate actions within the hub via self-managed identity.
- Storage: Tools to enable participants to configure integrations with existing storage solutions.
- Joint Business Processing: The ability to customise and configure Decentralised Logic Execution (see Section 4.1.4) of business operations that require consensus (i.e. public / independent validation) on a particular operation that relies on datasets that can NOT be made public.
- Messaging: Message broker as described in Section 4.1.3

These components are common capabilities to a DER data exchange hub, irrespective of the delivery model.

7.4 Integrate Technology Evaluations and Demonstrations with Governance, Legal, and Commercial Workstreams

EY's independent report[80] outlines a number of important governance, legal, and commercial questions that must be addressed through continued stakeholder engagement. That report (as well as Section 6 of this report) highlights unique attributes of decentralised technologies that enable opportunities for new business to business services, business to market services, and market infrastructure funding models.

Market digital infrastructure design should ideally be driven by the desired outcome(s) nominated by industry and policy makers. A continuous feedback loop, between stakeholder discussions / decisions and technology designs, should be enabled to evaluate how technological capabilities – including those with respect to decentralised architectures - can align with the desired outcomes of those stakeholder and policy decisions. For example, if policy makers decide that co-investment and joint ownership and/or operation of a data hub amongst AEMO, DNSPs and other third parties is appropriate, it should be possible to find ways to test technology in parallel, such that technical capabilities should inform non-technical decisions, and vice versa.

7.5 Consider Further Decentralisation of the Hub Architecture and Hosting, including Shared Ownership

Enabling a decentralised architecture offers benefits with respect to resilience, scalability, interoperability, and innovation[81]. Once a production grade hub is operational for a single use case for all participants and territories, core hub components should be considered for release (via multiple integration methods) to be hosted by other authorised organisations.

Governance mechanisms and associated fee structures for decentralised service provision would need to be agreed and finalised to support effective decentralisation of data hub components. While these technology approaches are still relatively new and emerging, considerable experience and proven models exist that could be adopted by AEMO and the industry at large[82].

As an indicative example of how this could work in practice, a production hub could initially be made operational in a centralised environment (like EDGE & Symphony) with an initial cohort of DNSPs and aggregators for the first use case. Additional participants from other jurisdictions could be progressively onboarded enabling the hub solution to be available for all participants and territories. When the hub is fully operational at scale for the initial use case, industry governance bodies could facilitate stakeholder discussions and prioritisation about other DER use cases that can be adopted by the hub, as well as delegation of hosting responsibilities to participants who are already onboarded, including investment and cost recovery frameworks. Plans can then be designed and implemented that align with industry priorities. To enable decentralised hosting, the software components underpinning the hub would be made available to authorised participants, who would in turn deploy them and integrate them with the hub via the established IDAM processes.

[80] AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

[81] Ibid

[82] See Toward a collaborative governance model for distributed ledger technology adoption in organizations for an extensive literature review investigating decentralised governance issues and presenting state-of-the-art governance practices to offer a comprehensive understanding on key governance issues in organizations

7.6 Consider Options to Expand Scope Beyond DER Use Cases

Projects EDGE and Symphony tested the concept of a shared data exchange hub in support of DER use cases. However, this same architecture could be potentially applied to a wider range of energy market processes and use cases.

Over the long term as DER become increasingly prevalent and play a larger role in wholesale market operations as well as distribution network operations, there are many potential benefits for harmonising DER data and workflows with non-DER operations such as transmission and distribution system planning, renewable generation transmission connection, and electric transport planning and operations[83]. This process would be evolutionary and span many years, as the scope of work required to design and implement these additional use cases is significant.

Nevertheless, the concept of a holistic "Digital Spine", acting as a common digital layer for transactions and interoperability for *all actors and processes* in an energy system, is already being developed in other energy markets globally, most notably the UK. Thus, when designing a DER data hub for Australia it is advised to design as many components to be extendable, as scalable as possible, and able to be used for functionality beyond the original requirement.

[83] Data sharing is a key element of the National Charge Link initiative

8 Conclusion

Project EDGE has been a productive collaboration between AEMO, AusNet Services, Mondo, and various aggregators, technology providers (including Energy Web Foundation) and expert consultants, with extensive stakeholder engagement from across the energy industry.

With the prospect of substantial DER growth in the coming decade and beyond[84], it is essential to enabling the flexibility inherent in DER devices that their service be coordinated across AEMO, DNSPs, retailers, aggregators, customer agents and other third parties in all markets. Such coordination is founded upon an effective identity and data exchange infrastructure that can meet and evolve with the requirements of a DER-rich landscape.

EDGE's working hypothesis that a data hub is a more efficient market infrastructure for the emerging DER landscape has been field tested and assessed by project proponents as well as through the engagement of EY with their independent Technology and Cybersecurity Assessment report[85].

Based on practical evidence provided in this lessons learnt report as well as EY's independent analysis, it is recommended that AEMO and the broader industry move to develop a production-grade data hub in collaboration over the next 12-24 months, utilising select participants and focusing upon enabling a single use case. Once proven, this infrastructure can be extended to all participants for the same use case, before being considered for extension to support other use cases.

[84] See AEMO 2022 Integrated System Plan for details.

[85] AEMO Project EDGE Technology and Cybersecurity Assessment, EY, June 2023

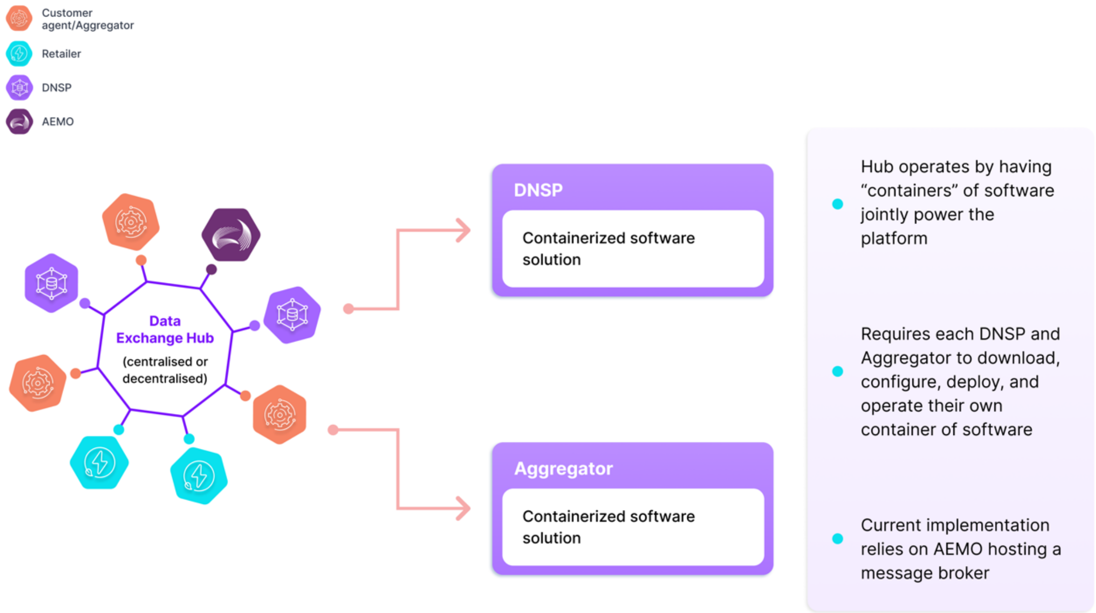
A1. Detailed DER Data Hub Solution Architecture

A1.1 Overview

Project EDGE trialled shared messaging infrastructure which combined proven messaging technologies with a novel architecture and approach to identity and access management to enable AEMO, DNSPs, and market participants to exchange diverse datasets, ranging from real-time telemetry to bulk file uploads, and via a single, standardised integration mechanism with a central messaging infrastructure hosted by AEMO.

In contrast to the existing AEMO e-Hub Shared Market Protocol, which does provide the ability for participants to exchange messages bilaterally, the messaging component in the DER Data Hub is a shared transport layer hosted by AEMO upon which DNSPs and market participants establish their own communication channels and run their own independent applications (such as trade of local network support services) based on their respective roles. This flexibility to support first movers is enabled by the DER Hata Hub's distributed governance structure. This is a key distinction from the existing AEMO e-Hub in which participants are more tightly coupled in updates. DNSPs have the capability to establish bilateral communication channels with aggregators which in turn enable Local Services Exchange applications. In production, this architecture could support a wider array of DER applications such as e-mobility solutions (e.g. green tariffs, dynamic charging), customer switching, or clean energy procurement (e.g. 24x7 matching).

Figure 26 Conceptual Architecture of EDGE Decentralised Data Hub Implementation with Container-based integration

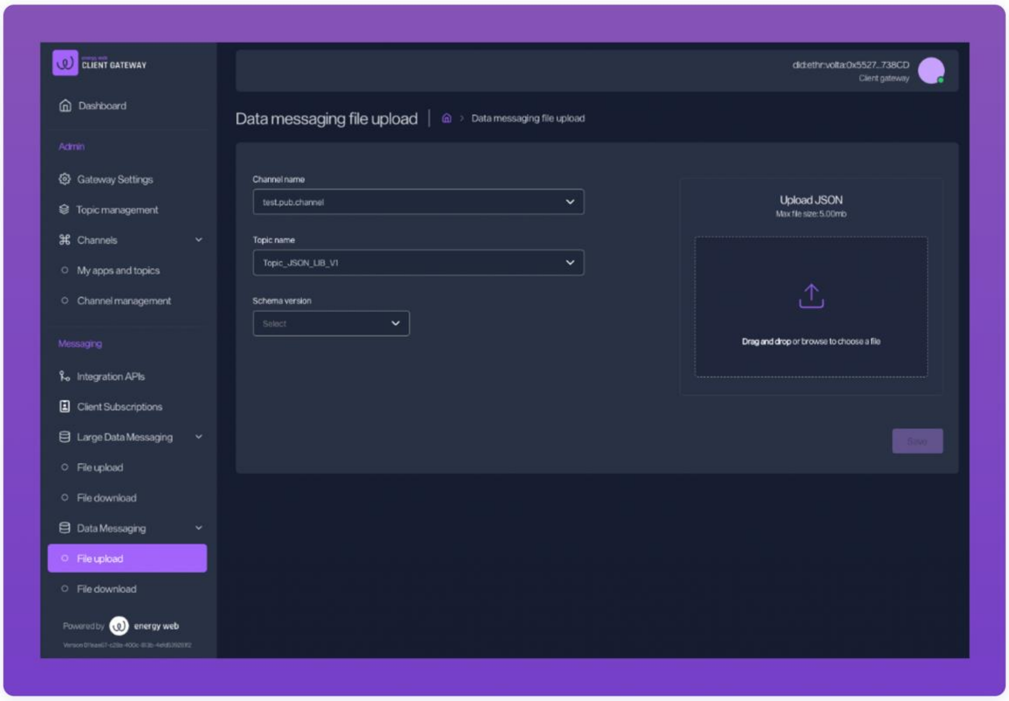

Customer agent/Aggregator
Retailer
DNSP
AEMO
Data Exchange Hub
(centralised or decentralised)
DNSP
Containerized software solution
Aggregator
Containerized software solution
Hub operates by having "containers" of software jointly power the platform
Requires each DNSP and Aggregator to download, configure, deploy, and operate their own container of software
Current implementation relies on AEMO hosting a message broker

The primary innovations in the trials were related to the participant integration method and identity and access management framework. In contrast to relying on API-based integrations between siloed systems, Project EDGE's solution enabled participants and DNSPs to integrate with shared messaging infrastructure hosted by AEMO via a containerised application.

The containerised application was published for participants to download and run independently within an environment of their choosing. During installation, participants specified connection details to the message broker hosted within and utilised by AEMO. Once integrated via the containerised application, participants and DNSPs utilised self-determined identity (i.e. digital identity that is fully controlled and administered by participants themselves rather than administered by AEMO on their behalf) to perform authentication and authorisation processes, which govern access and abilities within the shared messaging infrastructure. AEMO acted as the primary issuing authority to grant participants and DNSPs with credentials and assign them roles that reflected their respective functions within the market. These credential-based roles defined the permissions for each organization and govern their ability to:

- create and configure data exchange channels;
- send messages to other participants using the transport layer through channels;
- if desired, restrict who they receive messages from and/or send messages to; as well as authenticate messages to ensure they are valid.

Figure 27 Example UI of EDGE Data Exchange Hub



Data messaging file upload

Channel name: test.pub.channel

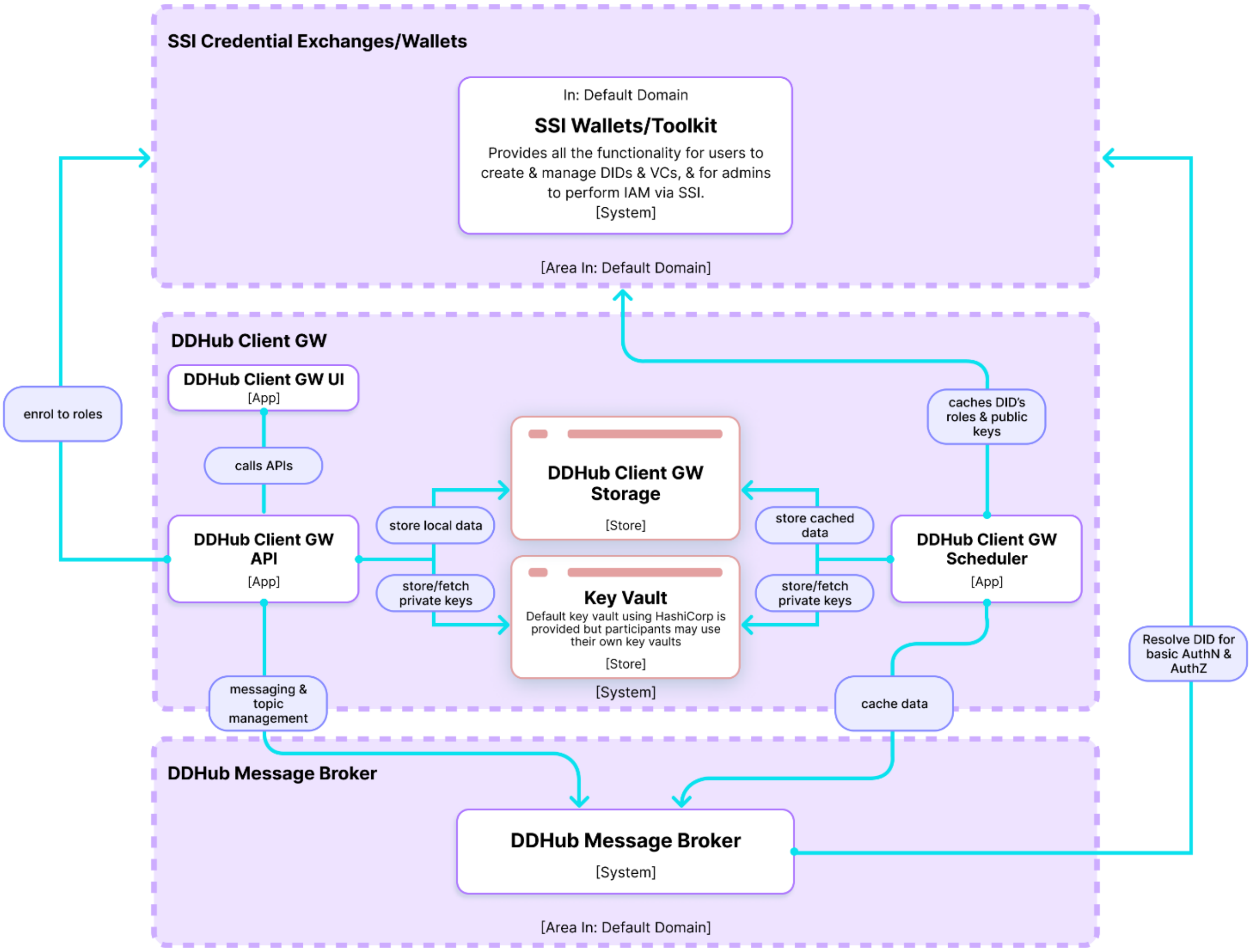
Topic name: Topic_JSON_LIB_V1

Schema version: Select

A1.2 Data Hub Client Gateway Architecture

Each participant client gateway is an independent application that runs in its own isolated runtime environment (i.e. container). The client gateway is published as an application available to all participants, who then deploy it within the environment of their choice. To initiate the integration with the Data Hub, participants first download the container image (i.e. preconfigured “template”) from GitHub and install their unique instance within a dedicated Azure Kubernetes Service (Microsoft’s cloud system for orchestrating containerised applications) environment. The deployment of the client gateway results in a connection with the common messaging transport layer hosted within AEMO’s environment, establishing a standard single integration method that enables each participant to communicate with AEMO or any other organisation.

Figure 28 EDGE Client Gateway Architecture

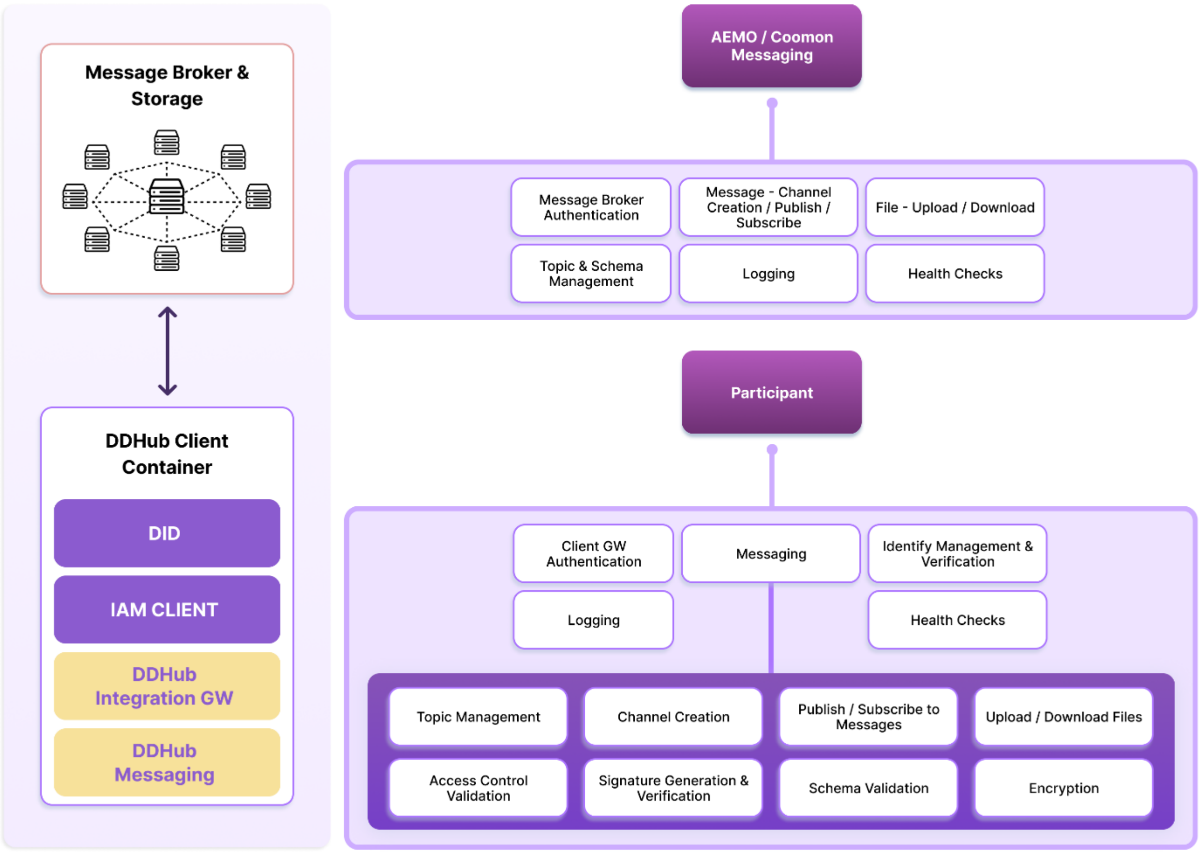

SSI Credential Exchanges/Wallets
In: Default Domain
SSI Wallets/Toolkit
Provides all the functionality for users to create & manage DIDs & VCs, & for admins to perform IAM via SSI.
[System]
[Area In: Default Domain]
DDHub Client GW
DDHub Client GW UI
[App]
calls APIs
DDHub Client GW API
[App]
enrol to roles
store local data
store/fetch private keys
DDHub Client GW Storage
[Store]
Key Vault
Default key vault using HashiCorp is provided but participants may use their own key vaults
[Store]
[System]
store cached data
store/fetch private keys
caches DID's roles & public keys
DDHub Client GW Scheduler
[App]
Resolve DID for basic AuthN & AuthZ
messaging & topic management
cache data
DDHub Message Broker
DDHub Message Broker
[System]
[Area In: Default Domain]

Legend:

- DDHub Client GW UI: the main interface for admins to manage their DDHub Client GWs
- DDHub Client GW API: exposes RESTful and Web Socket APIs for integration
- DDHub Client GW Scheduler: contains scheduler jobs for caching data including but not limited to channels, topics, and decryption keys
- DDHUB Client Gateway Storage: a postgres DB used to store configuration data.
- Key Vault - store private keys and other secrets
- DDhub Message Broker: The component that routes messages between Client gateways (using API to control NATS messaging).
- SSI Toolkit: Libraries and components that implement identity and access management functionalities as described in Section 4.3

The figure below provides an overview of participant's integration with the messaging transport and its linkage to the centralised hub.

Figure 29 Overview of Participant Integration with Common Messaging Transport Layer



Once initiated, each participant's container provides the capability to send/receive messages asynchronously with other peers within the common messaging infrastructure. The use of Self-Sovereign Identity (SSI) technologies enables participants to maintain their own credential certificates for accessing the hub. Secure communications between participants and AEMO is managed by IP Whitelisting and MTLS certificates.

A1.3 Managing Identities and Permissions

As described in the preceding section, the data exchange solution developed in EDGE & Symphony comprises a shared messaging transport layer as well as independent participant client gateways. Identity and Access Management (IDAM) in EDGE serves three primary functions:

- Authorising participant client gateways to interact with the common messaging transport layer;
- Authorising participants to access and read / write information within dedicated topics (i.e. individual communication channels dedicated to specific use cases / processes);
- Authenticating messages to ensure that both sender and recipient are known and trusted.

As implemented in EDGE, Identity and Access Management functionalities are enabled using Self-Sovereign Identity (SSI) technologies based on World Wide Web Consortium (W3C) standards, namely Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs). Appendix A2 explains these concepts in more detail.

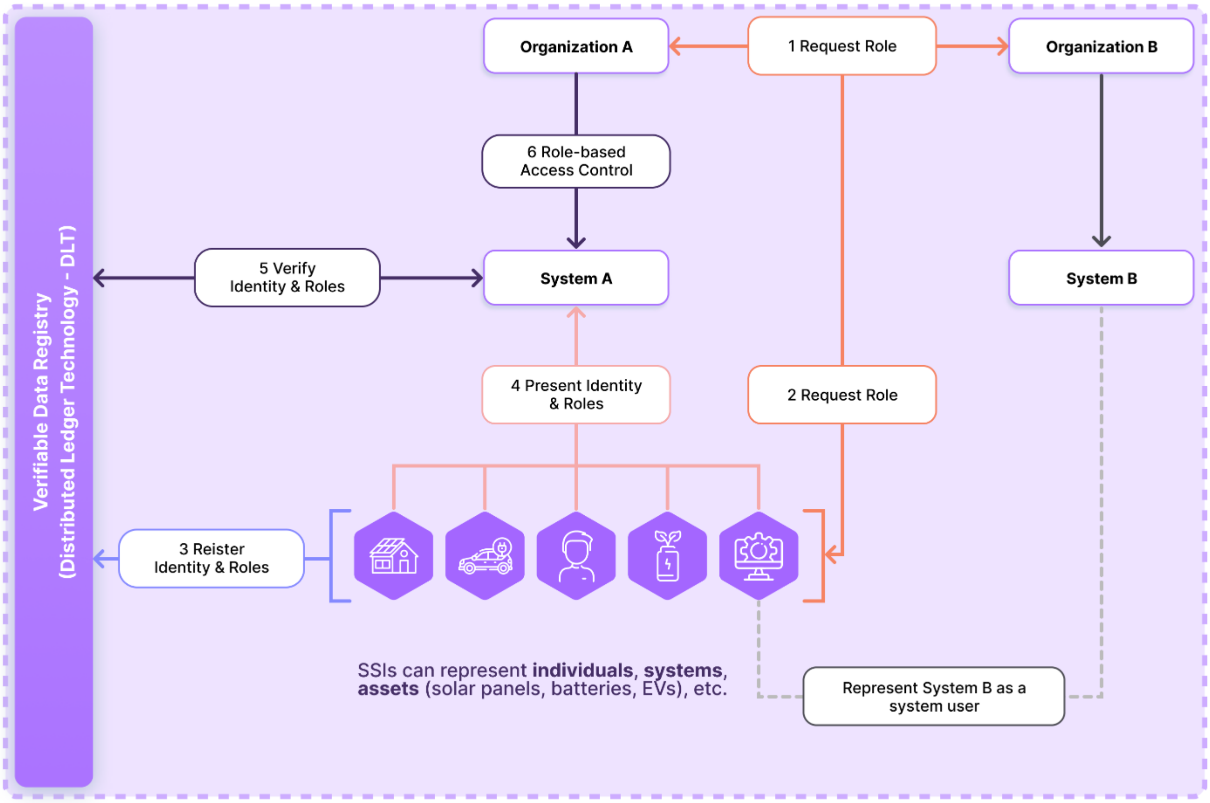
An IDAM verifiable data registry using Distributed Ledger Technology. The registry defines a hierarchy of roles for aggregators and DNSPs. In the current implementation, role hierarchy is defined with AEMO being the parent organisation, under which there are four applications to which roles are assigned. This means that AEMO is currently the primary issuing authority for all roles for all participants. However, the functionality exists for DNSPs to create their own separate organisations, applications, and roles in the future.

As currently implemented, AEMO is the only organisation with a role of Topic Creator due to the nature of the trial. However, the functionality exists to issue the Topic Creator role to other entities, which would allow them to create new topics for other specific use cases, and ultimately establish bespoke message exchange features on the shared messaging transport layer.

Although AEMO is an issuing authority of roles, AEMO does not store or manage identities and credentials (e.g. usernames, passwords, roles, permissions) on behalf of participants. Each participant creates a unique and persistent identifier (i.e. DID) that they maintain full control over.

In the Projects, each participant is issued an initial credential with a role to authorise interactions on the Hub; a role credential contains the digital and Decentralised Identity (DID) of the participant, for authentication purposes. When a participant needs to send or receive messages via the shared message broker, the participant's client gateway application obtains the public key of the participant's role credential from the Distributed Ledger Technology (DLT) to authenticate each message, ensuring that participants are only allowed to exchange data within topics for which they are qualified.

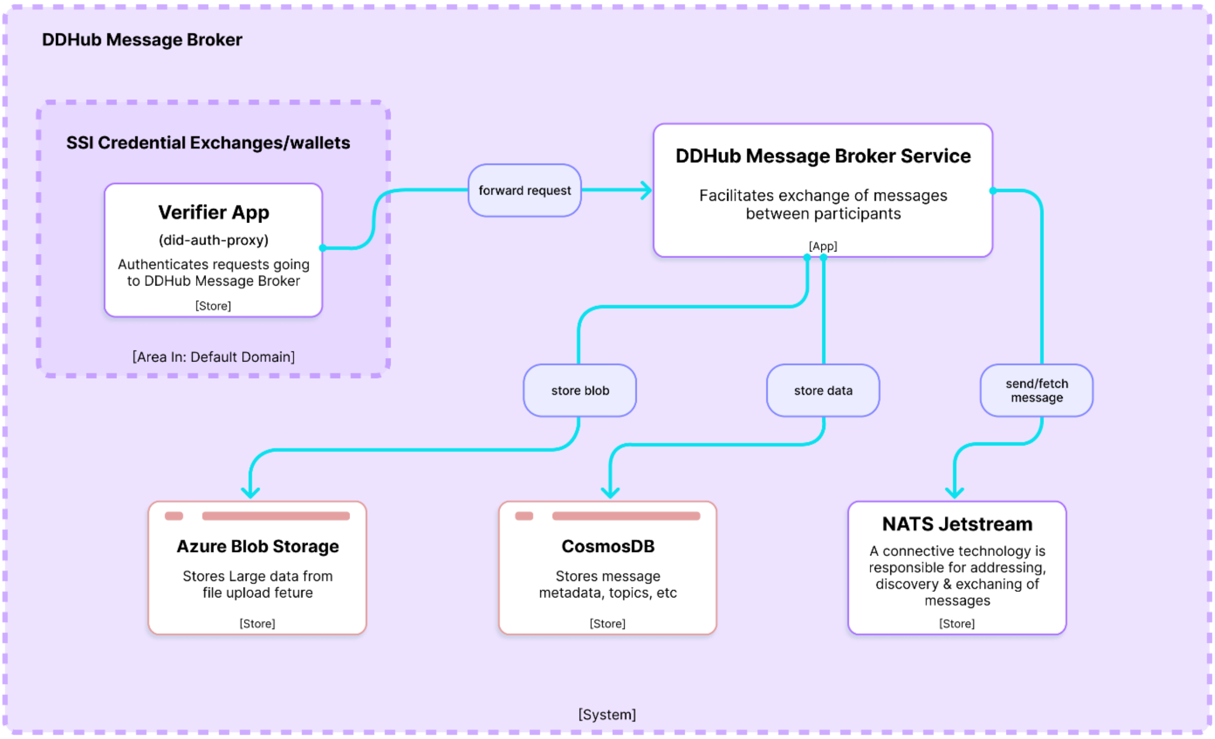
Figure 30 Conceptual Overview of SSI Role-Based Access Control


Verifiable Data Registry
(Distributed Ledger Technology - DLT)
Organization A
1 Request Role
Organization B
6 Role-based Access Control
5 Verify Identity & Roles
System A
System B
4 Present Identity & Roles
2 Request Role
3 Reister Identity & Roles
SSIs can represent individuals, systems, assets (solar panels, batteries, EVs), etc.
Represent System B as a system user

A1.4 Maintaining Information Integrity via Shared Messaging and Mutual Authentication

Messaging in EDGE & Symphony is accomplished via a secure, open-access transport layer that is hosted in a dedicated Azure cloud environment by AEMO, as shown in the figure below. As currently implemented, this means all messages and message requests ingress into AEMO's environment, however, this is a design choice to expedite the completion of the trial. In a future state, and as outlined in Section 6, AEMO and/or multiple other third parties could be delegated the responsibility of hosting the transport layer.

Figure 31 Message Broker Architecture


DDHub Message Broker
SSI Credential Exchanges/wallets
Verifier App
(did-auth-proxy)
Authenticates requests going to DDHub Message Broker
[Store]
[Area In: Default Domain]
forward request
DDHub Message Broker Service
Facilitates exchange of messages between participants
[App]
store blob
store data
send/fetch message
Azure Blob Storage
Stores Large data from file upload feture
[Store]
CosmosDB
Stores message metadata, topics, etc
[Store]
NATS Jetstream
A connective technology is responsible for addressing, discovery & exchaning of messages
[Store]
[System]

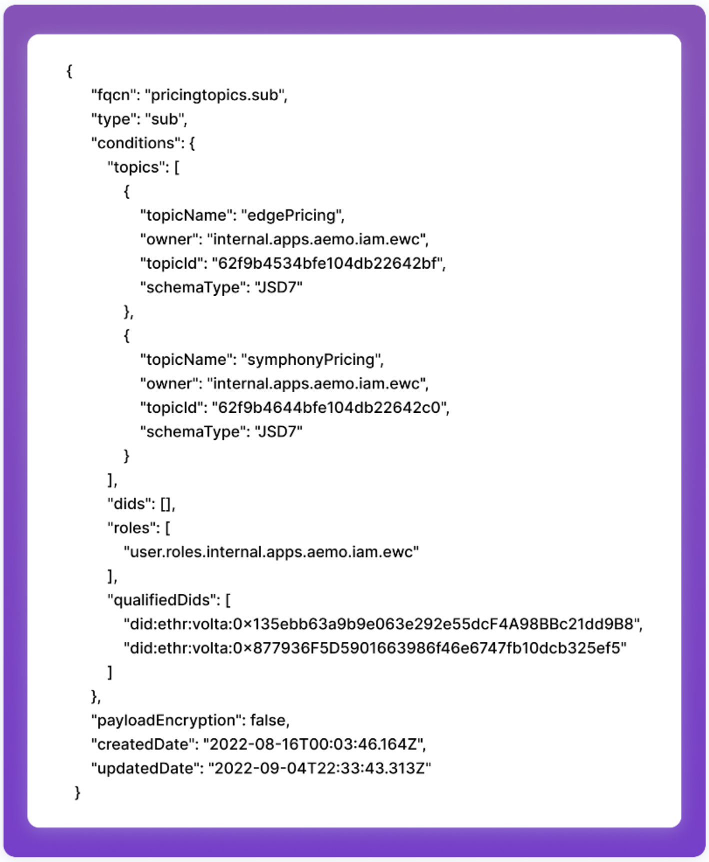
As described in the preceding sections, once participants are integrated with the transport layer they must acquire one or more roles to access one or more channels, and topics within channels.

Channels are defined at the client gateway, and are what messages are sent and received on. Participants define a channel as:

- Type: Publish/Subscribe
- Topics: Any that the DID has visibility of
- Restrictions: Who will receive a message on a publish channel, or who I will receive a message from on a sub channel. Channels can be restricted by DID or role

An example of a channel definition object is provided below. In this example, the channel will receive edgePricing or symphonyPricing from any DID with the role: *user.roles.internal.apps.aemo.iam.ewc* and does not specify that payload encryption is required.

Figure 32 Channel Definition Object



```
{
   "fqcn": "pricingtopics.sub",
   "type": "sub",
   "conditions": {
      "topics": [
         {
            "topicName": "edgePricing",
            "owner": "internal.apps.aemo.iam.ewc",
            "topicId": "62f9b4534bfe104db22642bf",
            "schemaType": "JSD7"
         },
         {
            "topicName": "symphonyPricing",
            "owner": "internal.apps.aemo.iam.ewc",
            "topicId": "62f9b4644bfe104db22642c0",
            "schemaType": "JSD7"
         }
      ],
      "dids": [],
      "roles": [
         "user.roles.internal.apps.aemo.iam.ewc"
      ],
      "qualifiedDids": [
         "did:ethr:volta:0×135ebb63a9b9e063e292e55dcF4A98BBc21dd9B8",
         "did:ethr:volta:0×877936F5D5901663986f46e6747fb10dcb325ef5"
      ]
   },
   "payloadEncryption": false,
   "createdDate": "2022-08-16T00:03:46.164Z",
   "updatedDate": "2022-09-04T22:33:43.313Z"
 }
```

In the current EDGE implementation, there are three Topics that correspond to three different use cases being evaluated in the trial:

- “EDGE”: dedicated to facilitating messaging between participants and AEMO (i.e. offers and dispatch instructions) as well as between DNSPs and AEMO (Dynamic Operating Envelopes, which inform DER dispatch).
- “Local Services Exchange”: dedicated to facilitating messaging between participants and DNSPs to enable DER to provide local network services either bilaterally or via a market mechanism.
- “Internal”: used primarily for testing purposes.

Topics are data schemas that define the payload of a message within a channel. They are grouped under owners that are used as an authorisation unit for visibility. For example, the EDGE application under the AEMO organisation owns a number of topics including:

- boffer
- operatingEnvelope *(AEMO owns the distribution of the transaction, not its generation)*

AEMO as an organisation provisions a user role (via credential) to the application for participants (via their DIDs) that allow them to see these topics. Topics are versioned, e.g. boffer version: 1.0.0, 2.0.0, etc

With each participant hosting their own Container in their environment, the Hub environment is composed of multiple Messaging Client Nodes interacting with each other through the transport layer (Message Broker). Each node (or couple of nodes) in the cluster is identified with a unique digital and Decentralised Identifier (DID) and is issued with a Hub Messaging Client role. Each node contains an Identity and Access Management (IDAM) Client that ensures legitimacy of users interacting within the messaging cluster by checking their identities, and issued role or set of roles.

The IDAM Client and DIDs provide a layer of protection against unauthorised access to Hub functionalities. Data exchanged within the cluster is secured in transit using mTLS.

A2. Self-Sovereign Identity Overview

A2.1 SSI Concepts

'Self-Sovereign Identity' is a growing paradigm that promotes an individual's control over their identity and their data. This is in contrast to the current paradigm where most official identifiers (driver's license, birth certificate, usernames, etc.) are given to users and maintained by a central authority, and where user data can be shared without their knowledge or consent (especially in the event of a cybersecurity breach) and where roles, access, and permissions can be centrally revoked without user knowledge.

A DID is an identifier that can be generated and controlled by individuals or organizations without an external authority. It can be used to identify any subject, such as a non-tangible asset, a customer, or an organisation. A user can create a DID for themselves or an asset using cryptographic or other means. A DID for a given system resides in a verifiable DID registry[86], which is developed according to W3C standards. Most DID registries live on a decentralised ledger to ensure no one party can unilaterally change its parameters, but they can also be hosted in conventional servers or networks. In this implementation, the DID registry is built on Distributed Ledger Technology (DLT).

A Verifiable Credential is a secure and machine-verifiable digital credential which respects a standard data model. The use of digital signatures makes verifiable credentials more tamper-evident and more trustworthy than many conventional role-based digital identifiers. Much like a physical credential (e.g. a passport, or driver's license), a VC typically contains:

- Information related to identifying the subject of the credential (unique identifier)
- Information related to the issuing authority (for example, AEMO or another trusted party)
- Information related to the type of credential this is (for example, a Retailer/Aggregator license, or a DNSP-specific credential)
- Information related to specific attributes or properties being asserted by the issuing authority about the subject
- Evidence related to how the credential was derived
- Information related to constraints on the credential (for example, expiration date, or terms of use).

Together DIDs and VCs can be used to implement Identity and Access Management solutions that provide users and organisations with greater control over their identities and associated data.

[86] See https://www.w3.org/TR/did-spec-registries/ for a formal specification.

Instead of an external authority maintaining control over an identifier and its associated identity data, any individual or asset can create an identity, and then acquire credentials over time through interactions with peers or authorities (similar to how real-world credentials such as passports are acquired via citizen interactions with an issuing authority).

To implement Identity and Access Management, organisations can define roles, which grant access to certain features or functionalities of a given application or service. In order to be granted a specific role, a user must acquire and hold one or more specified VCs, which they present to the role issuer. Just like conventional IDAM solutions, roles are nested in a hierarchy under an organisation or a specific application.

Figure 33 Example of Organisational Role Hierarchy

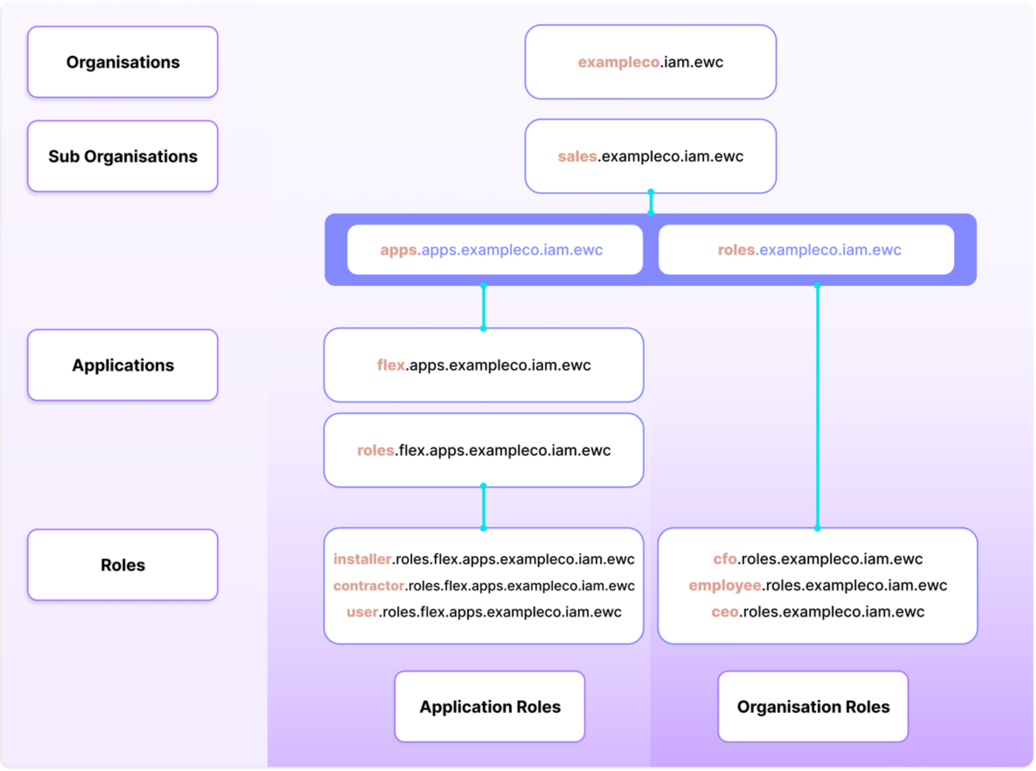
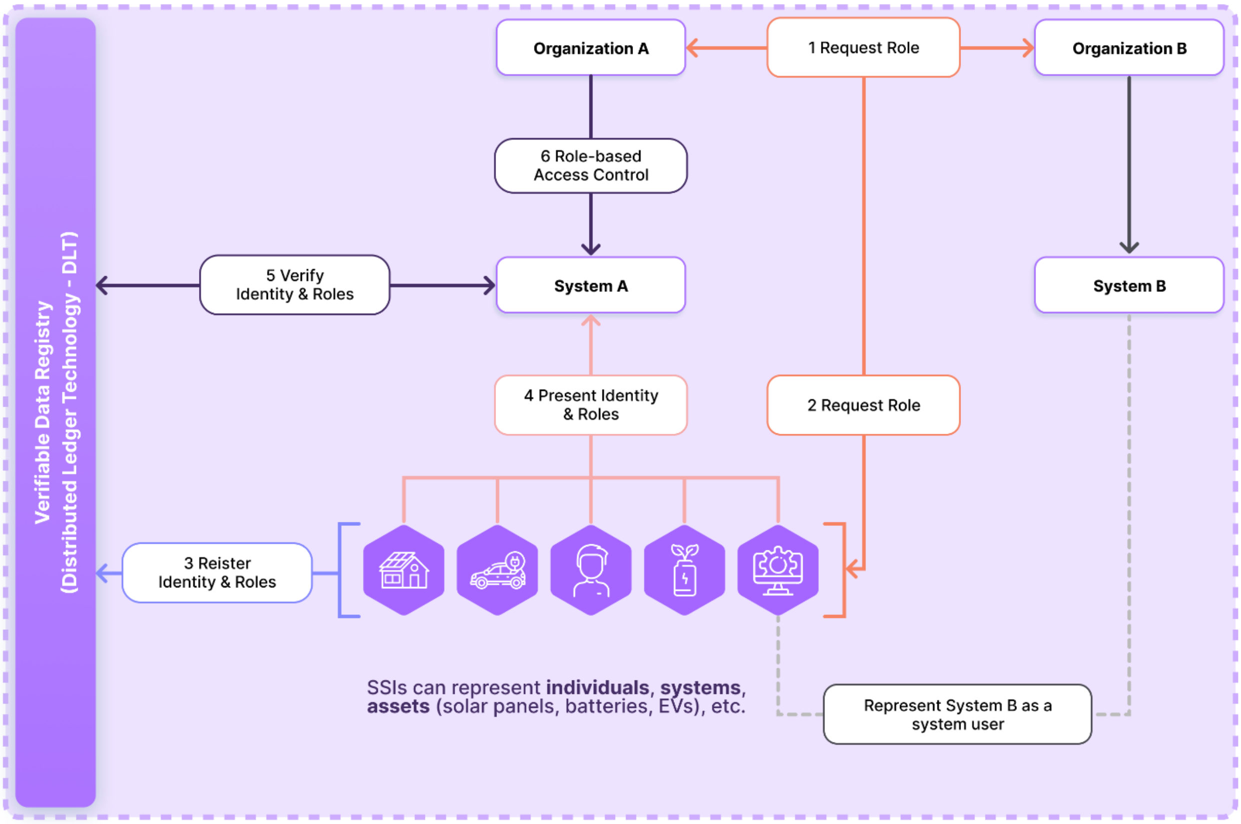

Organisations
exampleco.iam.ewc
Sub Organisations
sales.exampleco.iam.ewc
apps.apps.exampleco.iam.ewc
roles.exampleco.iam.ewc
Applications
flex.apps.exampleco.iam.ewc
roles.flex.apps.exampleco.iam.ewc
Roles
installer.roles.flex.apps.exampleco.iam.ewc
contractor.roles.flex.apps.exampleco.iam.ewc
user.roles.flex.apps.exampleco.iam.ewc
cfo.roles.exampleco.iam.ewc
employee.roles.exampleco.iam.ewc
ceo.roles.exampleco.iam.ewc
Application Roles
Organisation Roles

Figure 34 Conceptual Overview of SSI Role-Based Access Control



Both DIDs and VCs are specifications of the W3C. The W3C is an organisation which provides core technical specifications to establish guidelines and best practices for an open, inclusive and trustworthy web.

A2.2 SSI FAQ

Question	Answer
Where does one get an identity from?	A user can create a DID for themselves or an asset using cryptographic or other means. In EDGE, participants create DIDs in the process of deploying the client gateway application.
Where do participants get certificates associated with that identity (so that it can be stored on the ledger)?	In EDGE, certificates are issued in the form of Verifiable Credentials. Participants undergo existing KYC / onboarding processes, but instead of AEMO issuing a standard certificate, a credential is issued to the participant DID in the verifiable data registry.
Where are the roles stored?	Roles and credentials are stored in a verifiable data registry. In EDGE the data registry was implemented on DLT, but registries can use any storage solution. Importantly, the verifiable data registry only stores the role definition and the credentials associated with DIDs; private data that is associated with a given credential or DID is stored in existing systems.
How does the solution deal with the situation when a credential is compromised (i.e. a private certificate is leaked)?	SSI presents a fundamentally different paradigm (and attack surface) than conventional IDAM, where a central administrator has access to and control over all identities and associated credentials. In SSI there is no central user database or administrator to hack; each party controls their own identity independently, and credentials are controlled by / authenticated with these identities. If a given user's credential (i.e. private key) were compromised then only that that specific user is impacted and there are no cascading impacts (e.g. no other credentials or identities would be compromised as a result). For example, if an issuing authority (e.g. an organization or user who has a role that grants ability to issue credentials to other entities) had their private key compromised, an attacker may be able to temporarily issue new credentials (or revoke existing ones) but they would not have the ability to expose or otherwise compromise identity or data of other participants.

A3. Supporting Emerging DER Use Cases

A3.1 Use Case Solutions

Project EDGE's operational phase has deployed a PoC Data Hub to support testing a market model for efficient and scalable integration of DER into the wholesale energy market (while remaining within the technical limits of the distribution network), as well as enabling the trading of local network services that DNSPs can procure from aggregators representing customers and their DER devices.

In addition to the above use cases, vendors were asked to consider the potential for the digital infrastructure to support several other use cases, including:

- Direct DOE Distribution: enabling the DOE sent out by DNSPs (by NMI) to be partitioned and sent to relevant aggregators without the involvement of the central broker (AEMO);
- ZEL Requests: enabling Retailers to issue zero export limit requests to third-party customer agents (e.g. during periods of negative wholesale market pricing); and
- Portfolio Management: enabling aggregators to update their DER portfolios via a single registry, which both AEMO and DNSPs would leverage.

While each of these additional use cases have their own specific requirements, at a high level they are all variations of the capability for any given entity to directly and securely broadcast and/or selectively disclose sensitive data to multiple counterparties (i.e. a one:many messaging scheme) without necessarily needing to continuously maintain a recipient list or rely on a third party (like AEMO) to perform routing. Delegating responsibilities and capabilities to participants and enabling them to self-manage certain technical functions via a collective governance mechanism has the potential to offer operational efficiencies.

Within scope of the existing project, the ZEL and DOE use cases were tested in early March 2023. The Portfolio Management scope was considered in a design exercise but could not be included within the EDGE project timeline.

As described previously, in the current EDGE implementation all parties have the ability to broadcast messages to multiple counterparties on a shared messaging infrastructure. However, the current architecture still relies on AEMO as the sole hosting provider, meaning all messages and message requests ingress through AEMO's host environment. This was a deliberate design choice for the trial, but in the future the solution can be designed such that messaging infrastructure and routing could be performed by other entities as well. Moreover, in the EDGE trial, AEMO maintains the participant registry, including their DID, roles, and associated NMIs (with respect to aggregators), and utilises this registry to ensure DOEs are routed to the correct aggregator (aka, "partitioning").

Delivering this partitioning functionality can also be achieved through an approach called Decentralised Logic Execution (DLE). DLE is a generic concept that allows a network of independent worker nodes (i.e. a cluster of computing resources operated by separate hosting providers, aka “worker nodes”) to process messages and compute any result in parallel. DLE borrows concepts from public distributed ledger solutions, namely distributed consensus protocols which reward nodes which compute a provably correct and timely result, and punish those that attempt to tamper with data or logic execution.

In contrast to conventional DLT consensus protocols, which are designed to solve arbitrary mathematical computations in an adversarial environment, DLE implementations enable custom business logic (i.e. pre-defined input, computation, and output) within the protocol that is executed by a network in which nodes are vetted. In other words, the parameters of the consensus mechanism are to be configurable - a DLE solution defines the inputs required for the computation and how they are obtained, the computation itself, and the submission and mathematical validation of the computation result between peer nodes.

Any business operation that requires consensus (i.e. public / independent validation) on a particular operation that relies on a dataset that can NOT be made public – such as Direct DOE Distribution, Portfolio Management, and ZEL Requests – can benefit from DLE.

An indicative example of DLE nodes performing DOE distribution is shown in the figures below:

Figure 35 Block Diagram of DLE Nodes interacting with the OE Process

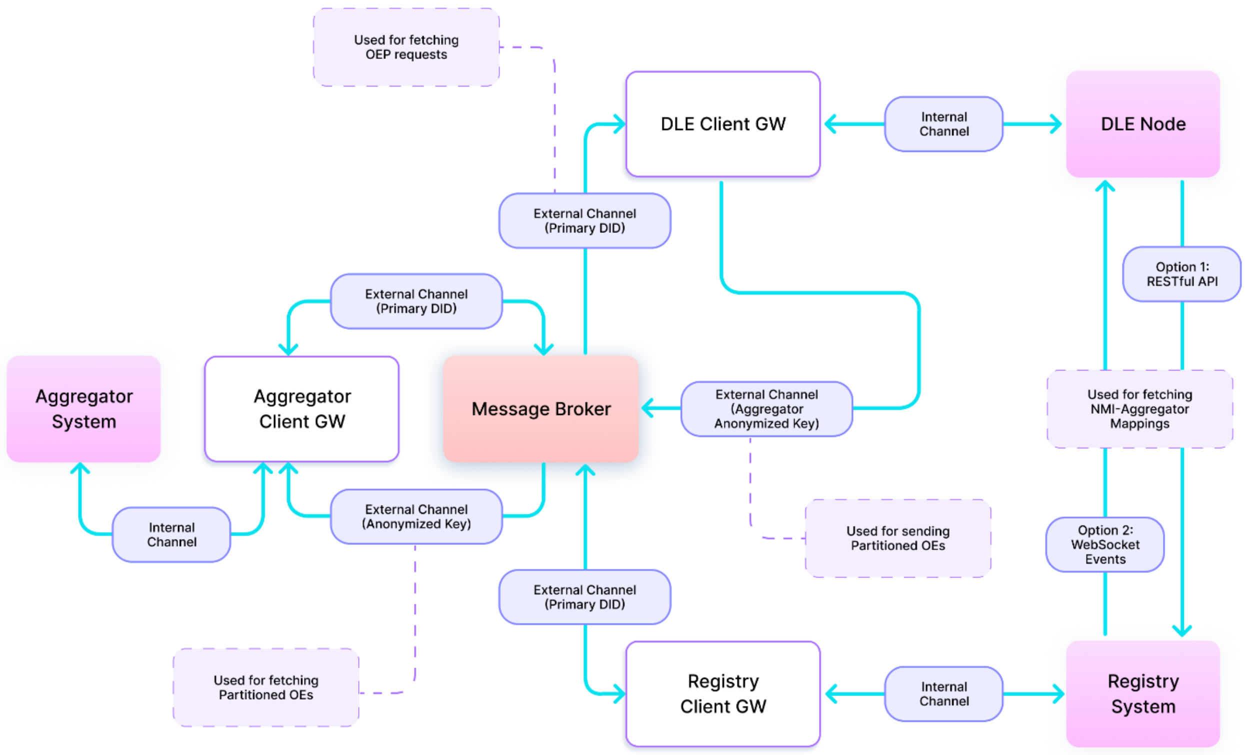
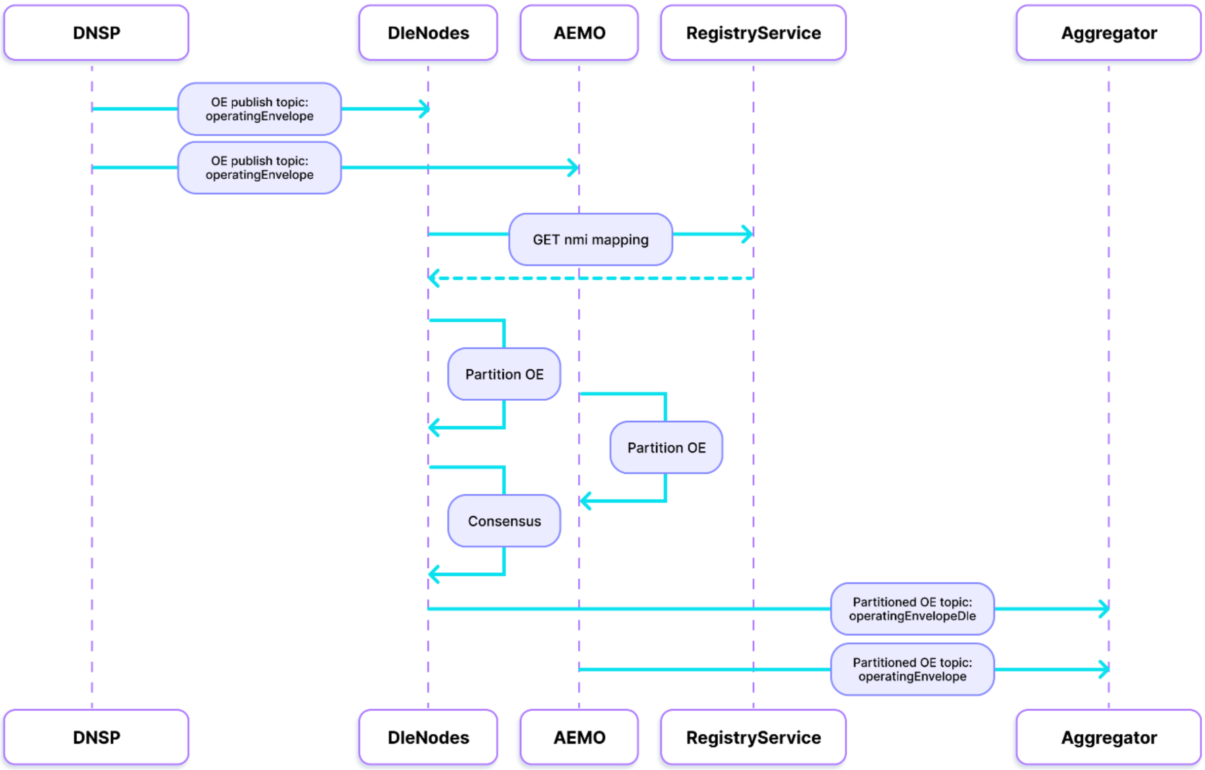
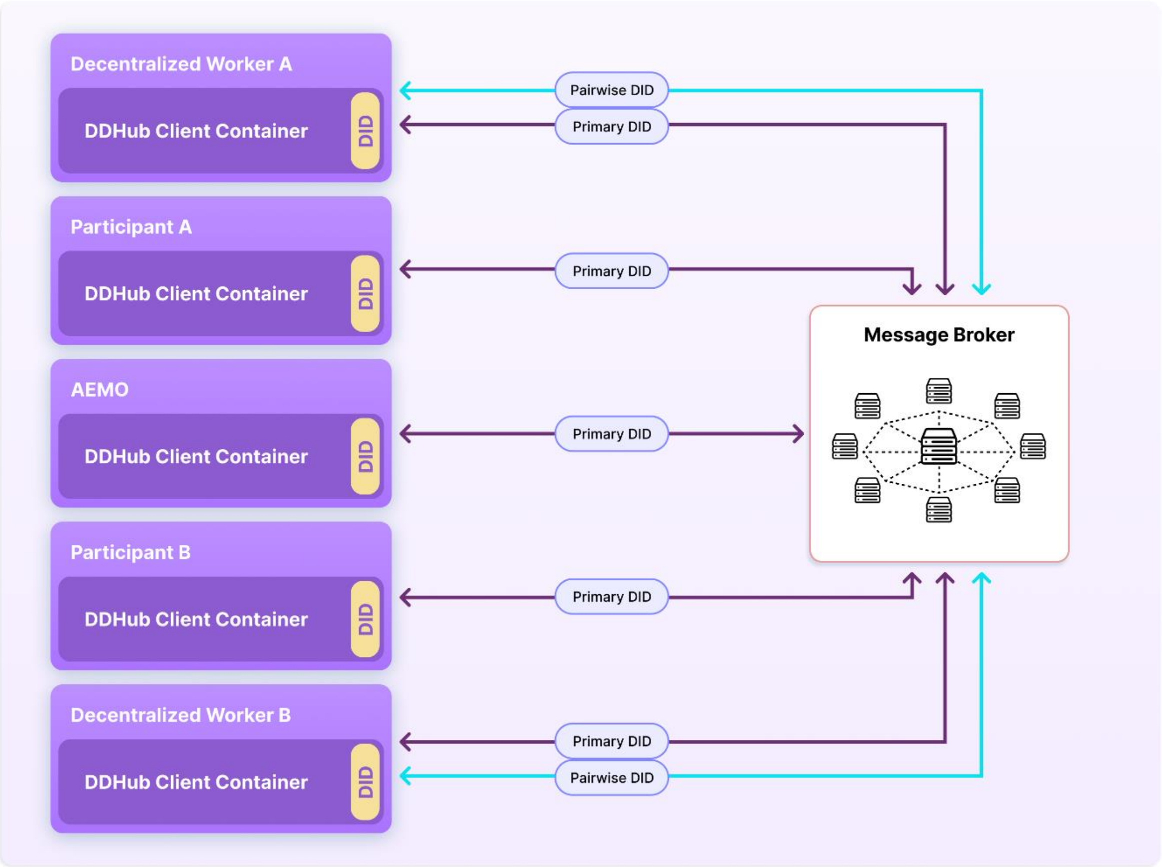

Used for fetching OEP requests
DLE Client GW
Internal Channel
DLE Node
External Channel (Primary DID)
Option 1: RESTful API
External Channel (Primary DID)
Aggregator System
Aggregator Client GW
Message Broker
External Channel (Aggregator Anonymized Key)
Used for fetching NMI-Aggregator Mappings
Internal Channel
External Channel (Anonymized Key)
Used for sending Partitioned OEs
Option 2: WebSocket Events
External Channel (Primary DID)
Used for fetching Partitioned OEs
Registry Client GW
Internal Channel
Registry System

Figure 36 Sequence Diagram of DLE Nodes interacting with the OE Process


DNSP
DleNodes
AEMO
RegistryService
Aggregator
OE publish topic: operatingEnvelope
OE publish topic: operatingEnvelope
GET nmi mapping
Partition OE
Partition OE
Consensus
Partitioned OE topic: operatingEnvelopeDle
Partitioned OE topic: operatingEnvelope
DNSP
DleNodes
AEMO
RegistryService
Aggregator

As shown in the conceptual diagram below, the primary DID is used as a message channel on normal communications between participants or to decentralised workers and a pairwise DID is used as message channel on communications by Decentralized Workers to the participants (the pairwise DID is used to anonymise correlation between any standing data and the participant).

Figure 37 DLE Component messaging architecture



In these situations:

- Only the standing data curator (e.g. AEMO or other 3rd party) and the identity owner can associate the primary and pairwise DIDs, thus enabling secure service delivery to correct identity owners.
- The recipient of a message authenticates using credentials public key stored on the Distributed Ledger Technology (DLT) and processes the message.
- In addition, it is possible to deploy third party actors to provide services which are provided by a centralised broker (e.g. AEMO) in other models. For example, Dynamic Operating Envelopes are distributed by DNSPs via NMIs only. Utilising the standing data registry as a reference, an external "worker" component(s) can partition DOE files, and send all relevant DOEs to the correct Aggregator (as a "NMI bundle").
- This activity generates a "hash" record on the DLT (data is never stored on the DLT, however, hash records are made on the DLT to indicate the "current state" of the data record, wherever it may be stored). The DLT operates via a consensus function called Proof of Work. As the DOE partitioning activity generates its hash record, the first "worker" that completes the activity is paid, while other workers are used to validate the accuracy of the activity.

- Decentralised workers, a network of nodes that perform messaging between participants, will have read-only access to the subset of standing data which will be used for executing specific workflows and business logic based on the roles and responsibilities of different participants (e.g. DOE partitioning among DNSPs and aggregators).

Pseudonymisation is key to ensuring that the decentralised workers can appropriately execute business logic and establish public consensus (outputs) based on private inputs (i.e. datasets). As an example, for DOE partitioning the decentralised workers would only map each NMI to a list of pseudonyms representing aggregators that are generated and encrypted using each aggregator's private key. At regular intervals (e.g. daily), aggregators can generate a new pseudonym and publish it to a verifiable data registry (hosted either in a conventional database or on DLT), thereby updating the mapping of NMIs to pseudonyms. Aggregators can "listen" for DOE partitioning results on a dedicated channel using their pseudonym as the identifier / endpoint, and only the aggregator can unencrypt the mapping using their private key, but all parties can verify that mapping and thus DOE partitioning are performed correctly.

For client gateways receiving messages generated by a DLE node, there is little difference between these messages and any other message that is received. In order to receive a message generated by a DLE node, the topic will need to be added to an internal channel at the client gateway. From there, it can be ingested in the same way as any message generated by a direct sender, with the exception that messages sent from a DLE node cannot be on the same client gateway channel as messages sent directly. It is important to note that the identity of DIDs receiving messages is anonymised to the DLE nodes. This is the reason why a different channel must be set up on the client gateway. To achieve anonymized message sending and receipt, the client gateway will establish an anonymised external channel that is associated with a rotating key (public key) generated by the gateway.

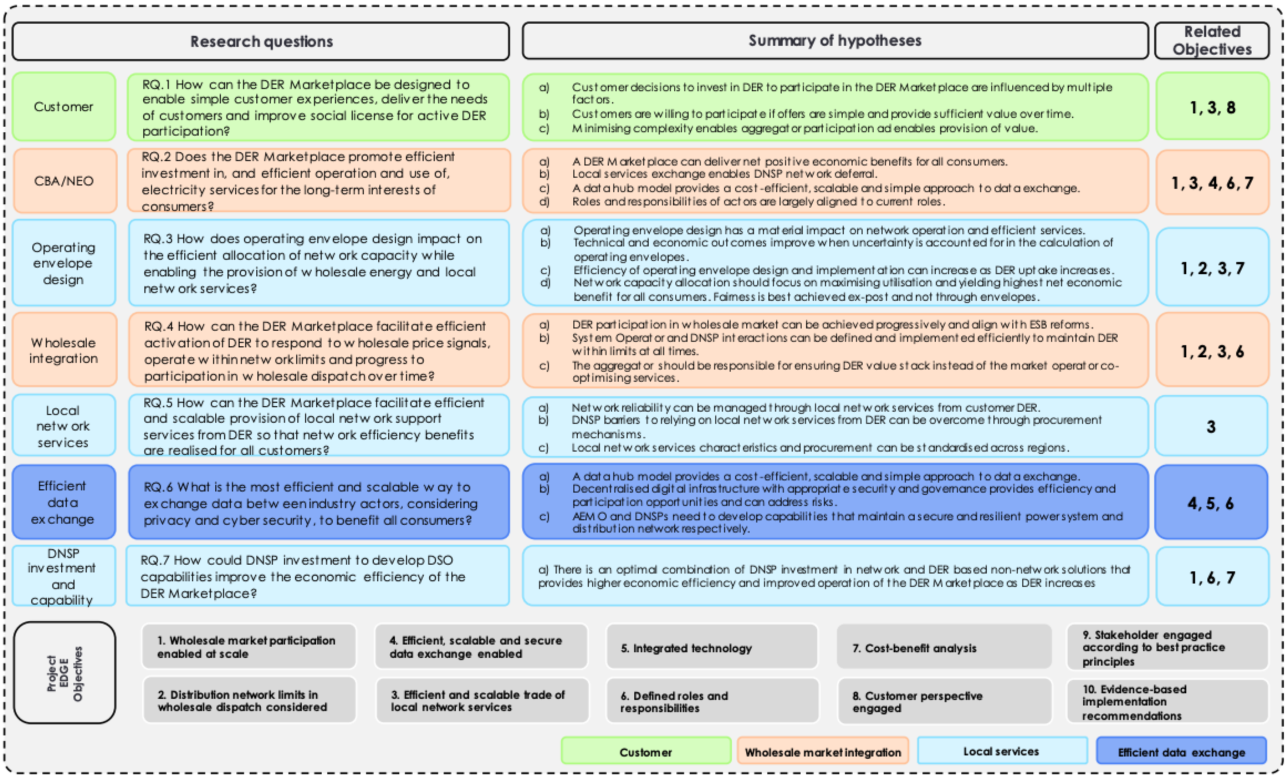
The section above outlines significant detail about the solution deployed within Project EDGE. Through regular engagement by Project team members with AEMO stakeholders, particularly those within AEMO's Technology Strategy and IT Architecture teams, a series of queries about how the solution operates, its constituent parts, and how it might function in the future have been raised.

These queries have been addressed in the form of a Frequently Asked Questions (FAQ) listing found in Appendix A5.

A4. Assessment Against Key Research Questions

As shown in the figure below, Project EDGE tested a number of hypotheses in order to address seven key research questions[87], which are in turn critical to achieving ten objectives in support of the National Electricity Objective.

Figure 38 Summary of EDGE objectives, research questions, and hypotheses



Research questions		Summary of hypotheses	Related Objectives
Customer	RQ.1 How can the DER Marketplace be designed to enable simple customer experiences, deliver the needs of customers and improve social license for active DER participation?	a) Customer decisions to invest in DER to participate in the DER Marketplace are influenced by multiple factors. b) Customers are willing to participate if offers are simple and provide sufficient value over time. c) Minimising complexity enables aggregator participation ad enables provision of value.	1, 3, 8
CBA/NEO	RQ.2 Does the DER Marketplace promote efficient investment in, and efficient operation and use of, electricity services for the long-term interests of consumers?	a) A DER Marketplace can deliver net positive economic benefits for all consumers. b) Local services exchange enables DNSP network deferral. c) A data hub model provides a cost-efficient, scalable and simple approach to data exchange. d) Roles and responsibilities of actors are largely aligned to current roles.	1, 3, 4, 6, 7
Operating envelope design	RQ.3 How does operating envelope design impact on the efficient allocation of network capacity while enabling the provision of wholesale energy and local network services?	a) Operating envelope design has a material impact on network operation and efficient services. b) Technical and economic outcomes improve when uncertainty is accounted for in the calculation of operating envelopes. c) Efficiency of operating envelope design and implementation can increase as DER uptake increases. d) Network capacity allocation should focus on maximising utilisation and yielding highest net economic benefit for all consumers. Fairness is best achieved ex-post and not through envelopes.	1, 2, 3, 7
Wholesale integration	RQ.4 How can the DER Marketplace facilitate efficient activation of DER to respond to wholesale price signals, operate within network limits and progress to participation in wholesale dispatch over time?	a) DER participation in wholesale market can be achieved progressively and align with ESB reforms. b) System Operator and DNSP interactions can be defined and implemented efficiently to maintain DER within limits at all times. c) The aggregator should be responsible for ensuring DER value stack instead of the market operator co-optimising services.	1, 2, 3, 6
Local network services	RQ.5 How can the DER Marketplace facilitate efficient and scalable provision of local network support services from DER so that network efficiency benefits are realised for all customers?	a) Network reliability can be managed through local network services from customer DER. b) DNSP barriers to relying on local network services from DER can be overcome through procurement mechanisms. c) Local network services characteristics and procurement can be standardised across regions.	3
Efficient data exchange	RQ.6 What is the most efficient and scalable way to exchange data between industry actors, considering privacy and cyber security, to benefit all consumers?	a) A data hub model provides a cost-efficient, scalable and simple approach to data exchange. b) Decentralised digital infrastructure with appropriate security and governance provides efficiency and participation opportunities and can address risks. c) AEMO and DNSPs need to develop capabilities that maintain a secure and resilient power system and distribution network respectively.	4, 5, 6
DNSP investment and capability	RQ.7 How could DNSP investment to develop DSO capabilities improve the economic efficiency of the DER Marketplace?	a) There is an optimal combination of DNSP investment in network and DER based non-network solutions that provides higher economic efficiency and improved operation of the DER Marketplace as DER increases	1, 6, 7

Project EDGE Objectives

1. Wholesale market participation enabled at scale
2. Distribution network limits in wholesale dispatch considered
3. Efficient and scalable trade of local network services
4. Efficient, scalable and secure data exchange enabled
5. Integrated technology
6. Defined roles and responsibilities
7. Cost-benefit analysis
8. Customer perspective engaged
9. Stakeholder engaged according to best practice principles
10. Evidence-based implementation recommendations

🟩 Customer 🟧 Wholesale market integration ⬜ Local services 🟦 Efficient data exchange

The results and recommendations in this report primarily address RQ.6, but are also relevant to some of the hypotheses associated with RQ.3, RQ.4, RQ.5 and RQ.7. The Project EDGE *Lessons Learnt Report #2*[88] addressed in detail research questions 1, 4 and 6, and should be read in conjunction with this report.

[87] Project EDGE | Research Plan

[88] Project EDGE | Lessons Learnt Report #2, see page 15

An evaluation against the hypothesis underpinning research question 6 is outlined in the table below.

Table 12 Evaluation of Research Question 6

RQ.6: What is the most efficient and scalable way to exchange data between industry actors, considering privacy and cybersecurity, to benefit all consumers?	
Hypothesis	**Evaluation**
A data hub model provides a cost-efficient, scalable and simple approach to data exchange.	Project participants indicated support for implementing an industry-wide data hub concept in anticipation of a DER-rich future. The primary appeal of the hub concept is the ability for AEMO, DNSPs, and aggregators to exchange a wide variety of information in a secure and standardised fashion. All project participants indicated that gaining the ability to communicate with multiple other entities via a single integration would improve efficiency and reduce operational complexity - critical requirements as DER continues to proliferate in both NEM wholesale markets and local network support services.
Decentralised digital infrastructure with appropriate security and governance provides efficiency and participation opportunities and can address risks.	Project participants and EY analysis both indicated that there are resiliency benefits to implementing a hub with a more decentralised architecture[89] due to inherent redundancies and failover / recovery mechanisms. However, operating such a hub at scale will require a thoughtful approach to ongoing support, as well as more extensive comparison of the EDGE Data Hub and the existing e-hub to identify gaps, overlaps, relevant capabilities and an optimal path forward. While Project EDGE did not fully explore in detail the potential governance arrangements for the solution options it considered, further decentralising the hub architecture, as well as using a role-based permissioning system defined through collective governance, has the potential to offer operational efficiencies and enable more rapid innovation, as participants could develop new applications and implement new DER use cases based on their role, rather than requiring a central administrator to do so.
AEMO and DNSPs need to develop capabilities that maintain a secure and resilient power system and distribution network respectively.	Project EDGE validated this hypothesis. Several novel capabilities developed in EDGE - including the partitioning of Dynamic Operating Envelopes, the consideration of aggregated DOE limits as a bid validation prior to wholesale energy dispatch, and the establishment of a Local Services Exchange - demonstrated value for all market stakeholders.

While this report does not explicitly address other research questions[90], the table below summarises general comments and insights that are relevant to specific hypotheses in other categories.

[89] AEMO - Project EDGE – 5.3 Technology and Cybersecurity Assessment, EY, June 2023

[90] AEMO - Project EDGE – Technology and Cybersecurity Assessment, EY, June 2023

Table 13 Insights relating to Research Questions

Research Question	Hypothesis	Comments
RQ.3	**Efficiency of operating envelope design and implementation can increase as DER uptake increases.**	Project EDGE has validated that Dynamic Operating Envelopes can be a key enabler of beneficial DER participation in wholesale markets and local services, and demonstrated an implementation mechanism via a shared industry data hub. One potential benefit of leveraging a common DER data exchange solution for DOEs (and other use cases) is that DOE design and logic can evolve over time as needs and conditions change, while the "delivery mechanism" can remain the same. This approach has the potential to improve efficiency and overall outcomes for DER.
RQ.4	**DER participation in the wholesale market can be achieved progressively and align with ESB reforms.**	An industry DER data exchange solution is recommended to be implemented in a phased approach that aligns with progressive growth in DER uptake and market participation.
RQ.4	**System Operator and DNSP interactions can be defined and implemented efficiently to maintain DER within limits at all times.**	Project EDGE demonstrated the capabilities of a shared DER data exchange solution to coordinate the operational activities of AEMO and DNSPs as they perform their respective roles. A key interaction between AEMO and DNSPs in EDGE was the communication and partitioning of Dynamic Operating Envelopes. In the future, a shared data hub could enable additional DER use cases involving interactions between both actors.
RQ.5	**DNSP barriers to relying on local network services from DER can be overcome through procurement mechanisms.**	Project EDGE demonstrated the capability for a DNSP to procure local services from DER aggregators via a shared DER data exchange solution. Enabling multiple DNSPs to leverage a common data exchange technology solution to procure local services from multiple aggregators could facilitate scalable and efficient procurement of such services. Feedback from the participating DNSP was that the provision of a local services exchange assisted with contracting (exchange level) and signalling (leveraging existing identity/portfolio and integration), together with better discoverability of aggregators that are able to participate at a lower price point. There also is potential for automation e.g. pre-registration. Though it was outside the scope of Project EDGE, another potentially beneficial initiative would be the establishment of common service definitions and valuations of specific network services.
RQ.5	**Local network services characteristics and procurement can be standardised across regions**	Project EDGE demonstrated the capability for a DNSP to implement network services procurement through a "Local Services Exchange" (LSE) communication topic. The LSE functionality developed in EDGE could be further augmented into an open-source "template", providing DNSPs with a common technical foundation (e.g. standard integration, re-purposable functionality) but customisable elements

Research Question	Hypothesis	Comments
		that fit needs of each DNSP. This could improve efficiency and lower barriers to entry for aggregators who wish to engage with multiple DNSPs to deliver network services.
RQ.7	**There is an optimal combination of DNSP investment in network and DER based non-network solutions that provides higher economic efficiency and improved operation of the DER Marketplace as DER increases**	It is expected that DER will represent a significant share of total system capacity in the coming decades. Project EDGE has demonstrated basic capabilities to enable DER participation in both wholesale markets and local services in such a way that benefits customers and the system as a whole. One potential path to optimise further investment in DER-based non-network solutions is to enable co-investment among multiple DNSPs (and possibly other NEM stakeholders) in shared industry data exchange solution. Coordinating and aligning investments in an industry standard is likely to minimise total cost to consumers and improve efficiency and lower costs for aggregators.

A5. Frequently Asked Questions and Solution Comparison

These FAQs were generated by Energy Web Foundation through the course of multiple engagements with industry stakeholders. The FAQs relate to the DER data exchange hub concept generally as well as the Data Hub implemented in the Projects.

Question	Response
Is the distributed ledger stored in Australia or globally?	Nodes supporting the distributed ledger can be operated anywhere according to any requirements provided by AEMO or other participants in Australia. For example, nodes supporting the distributed ledger can be restricted to being located within Australia, or eligible for location outside of Australia's borders.
What do we do if DLT for Portfolio Management is successful?	By proving its capabilities for managing portfolios, DLT can be expanded to support an increasing range of Standing Data, both existing and for DER devices. This would create a single source of truth across the market for organisation and device meta-data.

Question	Response
What has been the feedback to date regarding the use of containers?	The experience of several project participants indicates that the current container-based integration method is likely to be considered too complicated for widespread adoption. Containers (and associated technologies like Kubernetes) are relatively new concepts in the IT landscape, and there is significant heterogeneity across participant's host environments and technical resources and capabilities. The initial deployment and integration of participant client gateways was more complex than anticipated. Another challenge with the container-based integration was releasing new versions of the client gateway, especially when updates resulted in incompatibility with prior versions. Project participants have indicated preference for a more streamlined, standardised deployment model similar to other web-hosted applications (e.g. download and run an installation wizard), as well as having a standard DevOps type solution to automate the distribution and deployment of updates and new versions. The recommendation for a production solution incorporates this feedback. We recommend a "platform-as-a-service" (PaaS) model whereby participants connect to the data hub instead of requiring them to download, deploy, and configure their own software containers. This architecture will resolve the challenges faced with the existing architecture.
How scalable is this container?	By moving to a PaaS-based Data Hub solution, the integration pattern is supported by highly scalable cloud infrastructure and services. We foresee no scalability issues with the architecture described.
Who supports the container?	Under the recommended Platform as a Service implementation, service level and support arrangements should be designed and contracted for. Those organisations contracted to provide support would manage all issues. We recommend moving to a PaaS-based integration method to resolve the challenges associated with integrating and supporting participant-hosted Containers.

Question	Response
Who takes ownership if things go wrong?	As part of the enterprise development and deployment of the Data Hub infrastructure, support arrangements would be designed and contracted for. Those organisations contracted to provide support would manage all issues. These organisations would be either contracted by AEMO, or via the collective governance entity utilised to support industry-wide management arrangements.
If we have identities externally managed / hosted, how do we ensure its integrity?	Organisations directly manage their own identities, and only credentials are "anchored" (referenced by) to the DLT.
When would a decision be made to use this hub longer term?	Any longer-term decision would be made in consultation with industry through appropriate governance processes such as the NEM Reform Delivery Committee[91]
Where/who provides the identity so that credentials can hang off it?	There are a growing number of decentralised and digital identity solutions becoming available (e.g. Microsoft have theirs, see here): https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/decentralized-identifier-overview. EWF's DID solution - Switchboard - is also available. It is envisaged that a production-grade data hub solution would be interoperable with current and ongoing digital identity-based solutions. Furthermore, the Data Hub can be configured to trust any Identity and Access Management system, not just one based on decentralized identifiers and self-sovereign identity.
What is the back-up option if Containers fall over in production?	With the PaaS architecture, AEMO (via contractual agreements with solution providers) is in control of the solution's health, eliminating the risk that the solution "falls over" if participant containers go down.

[91] NEM Reform Delivery Committee

Question	Response
How will Demand Respones work with containers?	The PaaS architecture can support a variety of use cases, including enabling DNSPs to procure demand response services from Aggregators connected to the Data Hub
Will containers be available as a Service on AWS and Azure?	Yes, that is the intention to move to a PaaS-based solution, avoiding the need to host containers directly but rather access the Data Hub as-a-service
Is industry tied into EWF (Project EDGE vendor)?	No. By maintaining the infrastructure as open-source technology, the industry avoids becoming beholden to any one provider or developer of the technology. In the same way the Linux Foundation has supported the growth and penetration of open-source operating system technology, the opportunity exists for the Australian energy sector to foster the development of public, open-source technologies and enable services and development to be procured competitively. With a Platform as a Service architecture, AEMO and/or market participants could select at their discretion different service providers to further develop, operate, and maintain the underlying software behind the Data Hub (which is fully open source).
What should be the first use case?	We recommend support for Dynamic Operating Envelope distribution be the initial use case supported by a DER data hub Given industry's rapid progression in this area. Subsequent use cases to support could be ranked in terms of priority / criticality, and adopted from lowest ranked to highest over time.
Is industry ready for DLT for identity?	Digital identities are the present, let alone the future. Enabling identities to roam across the market (in terms of communications with and across participants and operators) should be the objective to avoid having to manage multiple identities. DLT supports this.
Is industry ready for DLT for Standing data?	This use case needs further investigation and testing. Testing EDGE technologies for DER registry data could help industry (and government) assess whether this application of the technology can be safe, effective and efficient for Standing Data.

Question	Response
What data use cases could be appropriate for DLT?	DLTs are slower than centralised databases, as they must not only process transactions like regular databases but also verify signatures, reach consensus across the node network, and require every node to undertake the same computing requirements for each transaction. This makes DLT an inappropriate solution for operational data, like DOEs, bids and portfolio telemetry. Any registry could be applicable for DLT-based data support, depending upon the performance requirement for said data. Registry data that is "highly dynamic" may not be applicable for a DLT. Note that DLT is not a place to store actual data but the immutable proofs such that those data can be traced and verified.
Is industry ready for DLE?	Yes. This approach was demonstrated in Project EDGE and was unnoticed by trial participants. As in Project EDGE, a single node can perform decentralized logic execution which significantly de-risks industry adoption of the solution by making it centralized and operated by one organization initially. Additional nodes performing DLE can be added over time as the verifiability and transparency benefits of the technology are proven. This technology would only be utilised by those hosting nodes.
What is the benefit of the open software model used in Projects EDGE and Symphony?	EWF only builds and deploys open source (freely licensed) software. One benefit of the Australian energy sector maintaining infrastructure as open-source technology is avoiding being beholden to any one provider or developer of the technology. In the same way the Linux Foundation has supported the growth and penetration of open-source operating system technology, the opportunity exists for the Australian energy sector to foster the development of public, open-source technologies and enable services and development to be procured competitively
Does the EDGE/Symphony data exchange model allow participant to participant integration?	Yes. Through integrating with the Data Hub, participants were able to structure 1:1 comms with other participants as they wished.
What patterns were supported in EDGE and Symphony?	File transfer, API's (Synch), Websockets
What file formats were supported in EDGE and Symphony?	JSON, XML, TAB, CSV -- Note schema validation is not currently applied to text file formats (CSV, TAB etc) used in large file transfer

A high-level assessment comparing various characteristics across the solution options considered during Project EDGE is outlined below. This assessment was undertaken by the vendor and solution architecture resources within the AEMO project team, with key aspects validated via direct industry feedback from dedicated stakeholder engagement efforts.

Table 14 Comparison of Data Exchange and Integration Solution Options considered by Project EDGE

Category	Characteristic	Point to Point	Centralised (e-hub)	Decentralised Hub (Single Node) with Container	Decentralised Data Hub
Identity & Access Management	Credential Management Complexity for AEMO	High	Medium	Low	Low
	Credential Management Complexity for Participants and DNSPs	High	Low	Medium	Medium
Integration	Integration complexity for Participants and DNSPs	Medium	Medium	High	Low
Cost	Cost-effectiveness and Operational Efficiency	Low	Medium	Medium	High
	Cost of Ownership (AEMO CapEx + OpEx)	Medium	High	Medium	Medium
Operational Efficiency	Ability to send to messages directly between participants	Possible	No	Yes	Yes
	Support for emerging B2B DER Use Cases	No	No	Yes	Yes
	Barriers to entry	Medium	Medium	Low	Low
Addresses DER Problem Statements	Provides Consistency with DER Standing Data	No	Yes	Yes	Yes
	Reduces High Data Exchange Costs	No	Yes	Yes	Yes
	Enables Visibility of DER	Possible	Yes	Yes	Yes

Category	Characteristic	Point to Point	Centralised (e-hub)	Decentralised Hub (Single Node) with Container	Decentralised Data Hub
	Maintains Cybersecurity in Decentralised System	Yes	Yes	Yes	Yes
Aligns with Design Principles	Reduce Integrations Required	No	Yes	Yes	Yes
	Reduce Reliance on AEMO as Central Administrator / Broker	Yes	No	Yes	Yes
	Shared, accessible, extensible	No	No	Yes	Yes