Flexibility Service System Interoperability

Comparative Analysis of Solutions for the Dispatch of Flexibility Services

Open Networks
October 2024 | Version 1.0

DOCUMENT CONTROL

Authorities

Version	Issue Date	Authorisation	Comments
1	Mar-24	Open Networks Steering Group	Date of publication Oct-24

Related documents

Reference 1	***Flexibility Service System Interoperability –*** *Review of options around APIs and Standards for the Dispatch of Flexibility Services*

Change history

Version	Description
1.0	First distributed version

TABLE OF CONTENTS

Contents

Introduction

About ENA

Energy Networks Association represents the companies which operate the electricity wires, gas pipes and energy system in the UK and Ireland.

We help our members meet the challenge of delivering electricity and gas to communities across the UK and Ireland safely, sustainably and reliably.

Our members include every major electricity and gas network operator in the UK and Ireland, independent operators, National Grid ESO which operates the electricity system in Great Britain and National Grid which operates the gas system in Great Britain. Our affiliate membership also includes companies with an interest in energy, including Heathrow Airport and Network Rail.

We help our members to:

- Create smart grids, ensuring our networks are prepared for more renewable generation than ever before, decentralised sources of energy, more electric vehicles and heat pumps. Learn more about our Open Networks programme.
- Create the world's first zero-carbon gas grid, by speeding up the switch from natural gas to hydrogen. Learn more about our Gas Goes Green programme.
- Innovate. We're supporting over £450m of innovation investment to support customers, connections and more.
- Be safe. We bring our industry together to improve safety and reduce workforce and public injury.
- Manage our networks. We support our members manage, create and maintain a vast array of electricity codes, standards and regulations which supports the day-to-day operation of our energy networks.

Together, the energy networks are keeping your energy flowing, supporting our economy through jobs and investment and preparing for a net zero future.

About Open Networks

Britain's energy landscape is changing, and new smart technologies are changing the way we interact with the energy system. Our Open Networks programme is transforming the way our energy networks operate. New smart technologies are challenging the traditional way we generate, consume and manage electricity, and the energy networks are making sure that these changes benefit everyone.

ENA's Open Networks programme is key to enabling the delivery of Net Zero by:

- opening local flexibility markets to demand response, renewable energy and new low-carbon technology and removing barriers to participation
- opening data to allow these flexible resources to identify the best locations to invest
- delivering efficiencies between the network companies to plan and operate secure efficient networks

We're helping transition to a smart, flexible system that connects large-scale energy generation right down to the solar panels and electric vehicles installed in homes, businesses and communities right across the country. This is often referred to as the smart grid.

The Open Networks programme has brought together the nine electricity grid operators in the UK and Ireland to work together to standardise customer experiences and align processes to make connecting to the networks as easy as possible and bring record amounts of renewable distributed energy resources, like wind and solar panels, to the local electricity grid.

The pace of change Open Networks is delivering is unprecedented in the industry, and to make sure the transformation of the networks becomes a reality, we have created three workstreams under Open Networks to progress the delivery of the smart grid.

2023 Open Networks programme Workstreams

- Network Operation
- Market Development
- Planning and Network Development

Our members and associates

Membership of Energy Networks Association is open to all owners and operators of energy networks in the UK.

- Companies which operate smaller networks or are licence holders in the islands around the UK and Ireland can be associates of ENA too. This gives them access to the expertise and knowledge available through ENA.
- Companies and organisations with an interest in the UK transmission and distribution market are now able to directly benefit from the work of ENA through associate status.

ENA members

BUUK infrastructure
Cadent Your Gas Network
electricity north west Bringing energy to your door
ESB NETWORKS
ESO
national gas
nationalgrid
Northern Gas Networks
Northern Ireland Electricity Networks
NORTHERN POWERGRID
Scottish & Southern Electricity Networks
SGN
SP Energy Networks
UK Power Networks Delivering your energy
WALES&WEST UTILITIES

ENA associates

- Chubu
- EEA
- Guernsey Electricity Ltd
- Heathrow Airport
- Jersey Electricity
- Manx Electricity Authority
- Network Rail
- TEPCO

Executive Summary

The ENA's Open Networks programme currently has a stream of work focused on interoperable flexibility service dispatch. The intention of this work is to deliver an interoperable protocol for the dispatch of flexibility services, to reduce barriers to entry for flexibility service providers seeking to offer flexibility services across different network operators. A common API (Application Programming Interface) is an important aspect of this, and work has been carried out to identify the requirements of such an API, and to explore available options. There was no straightforward best option to adopt identified during that work – many approaches from previous research projects were codifying particular market structures and processes into their standards, or were based around the concept of implicit, rather than explicit, dispatch, meaning they did not meet the needs of this work.

As such, 5 options for delivering interoperable dispatch were identified, and these were reported to the Open Networks Programme steering group in October 2023. Since then, a process of carefully evaluating the options for an interoperable flexibility dispatch system has been carried out. This has been informed by the previous stakeholder engagement, and a detailed technical evaluation of standards options.

The main conclusion is that there is no immediate "off the shelf" solution that can be adopted in the immediate term to deliver a fully interoperable solution. Existing solutions either do not meet the requirements to dispatch each of the five ENA flexibility services, or there would be other very significant trade-offs to their adoption (i.e. major commercial downsides to, for example, selecting a single vendor solution for every network operator to adopt).

A range of technical standards were explored as well; it is important to note that standards generally only normalise the data structures and forms of message payloads to be communicated. Significant time and effort would then be needed to turn a standard into a specification that GB network operators could adopt and then implement.

International standards alignment was also considered; having a standard with an established international presence is a positive feature because it saves significant time and effort (when compared to building a new standard from scratch). It would also allow for a GB solution to benefit from potential future economies of scale, as well as leverage existing knowledge and experience gained from active real-world deployments.

One specific challenge identified in this process is that many flexibility projects launched to date, in particular those in Europe, have not explicitly considered dispatch (i.e. where a network operator sends an ahead-of-time or near-real-time message requesting a given asset begins to provide a particular flexibility service). Instead, "implicit dispatch" or "self-dispatch" based on observed network properties is common. In addition, some flexibility research projects did not use Application Programming Interface (API) based dispatch. This limited the number of existing credible implementations available to be explored.

Stakeholder input from FSPs and market participants, gathered in earlier stages of this work, confirmed that stakeholders are keen for us to follow a modern approach that makes use of web standards like Representational State Transfer (REST) based APIs, as opposed to more legacy technologies like Simple Object Access Protocol (SOAP). Our stakeholders advised that is harder to find suitably experienced software developers to work with legacy ways of operating.

Consequently, OpenADR 3.0 appears to present a credible international standard that meets the needs of interoperable services flexibility dispatch. This is based around a modern REST-based API, which appears to be sufficiently versatile to support the communication of both the current and future data parameters needed to enable the dispatch of flexibility services. This position will be validated through ongoing work to compare the OpenADR 3.0 standard and its features with the ENA's standard flexibility products.

Subject to the continued availability of ongoing stakeholder engagement and input, the steering group is asked to **endorse** our proposal to continue to **progress the transition , at pace, to the technical delivery and implemention of OpenADR 3.0 as a specification and implementable means of providing an interoperable dispatch solution**.

(Note: when our original standards analysis was carried out in 2023, OpenADR 3.0 had not yet been formally launched; its release took place in late November 2023.)

Background Context

As part of the ENA's Open Networks Programme work on the interoperability of flexibility dispatch, this report (October 2024) provides an update on the work carried out to date in evaluating a set of options previously presented to the ENA Open Networks Steering Group in October 2023, to deliver flexibility dispatch interoperability through a commonly adopted API. The aspiration for this work is to open up the flexibility market, and make it easier for providers to sell into multiple markets, without different dispatch APIs becoming a barrier to adjacent market entry.

This report follows a report (Titled Flexibility Service System Interoperability - Review of options around APIs and Standards for the Dispatch of Flexibility Services), and documents subsequent analysis carried out, which was informed by the gap analysis and minimum requirements work carried out on that document.

In this report, the work to date on reviewing different technical standards has been set out. It is important to review this alongside the previous reports including, in particular, the outcomes of stakeholder engagement with FSPs and other flexibility stakeholders, and around some of the interoperability gaps identified, since that work is critical in underpinning the approach taken here, as well as the conclusions reached.

Options-Informed Recommendations

Four options were presented to the ENA Open Networks steering group in October 2023, informed by the previous phase of this work. This report summarises our recommendations around these options, based on further analysis carried out to explore these, and their feasibility and other requirements which would emerge from them.

The underlying rationale for this work is to deliver flexibility systems interoperability. Improved interoperability can reduce barriers to market participation and increase liquidity and choice in flexibility markets, delivering improved value for bill-payers.

There are two relevant key factors to interoperability that should be considered in reviewing these options and recommendations.

A well-standardised API can help to improve interoperability, by making it easier for market participants who have worked with one network operator to begin to offer services to another.

Also, an **API in itself is simply a means of communicating structured information to others.** To achieve genuine interoperability, there is a requirement to have **alignment and standardisation of those messages, their meaning, and wider business processes and implementations**, so that each message exposed by a network operator through an API has the same meaning, regardless of which network operator issues it. This means that to deliver interoperable dispatch, there is both a requirement to converge on a **standardised structure of messaging and protocols (i.e. an API)**, as well as to converge on **standard interpretations, controls and requirements around how that API is used**, so that each network operator imposes the same expectations on FSPs, creating an interoperable ecosystem.

Background to Flexibility Service Products

The ENA Open Networks Programme originally defined four flexibility service products – secure, dynamic, sustain and restore. There has also been work to deliver MW Dispatch (ESO dispatching assets via network operators) to manage constraints using installed assets of > 1 MW, through a "turn to zero" curtailment, to reduce real power export to zero.

While work is ongoing as part of other Open Networks working groups to update these definitions, the interoperability TWG has carried out an analysis of communications requirements for dispatch, and set out the parameters required for this in the analysis (**Enclosed,** as **Appendix A**). At a very high level, dispatchable flexibility services are dispatched near to real-time, or ahead of time (e.g. day-before), and are dispatched with either fixed or variable "quantities" of demand/generation. This introduces a degree of complexity when seeking out a standardised, interoperable approach, especially where different network operators have different approaches to the technical specifics of the implementations of these services.

This document reviews each option from a technical, as well as a commercial risk perspective, and also proposes a new, fifth option, which came to light during technical review of existing specifications and options in the market. This document also sets out a **series of steps** which need to be **taken, regardless of the option selected**, to deliver interoperability of flexibility dispatch.

In describing interoperability, this refers to the idea that the process and experience for an FSP being dispatched will be the same, irrespective of which network operator they are providing services to. This means that, from an FSP perspective, the systems, protocols, communications requirements, and expectations should be aligned, to avoid ambiguity or different interpretations of message semantics.

The consequence of not having this alignment in interpretation of messages would be the **emergence of network operator-specific conventions**, which would sit outside of the API semantics and specifications, and would **risk the creation of overlaid specifications that result in a series of similar, but non-interoperable, dispatch ecosystems**, from the perspective of an FSP.

Options Proposed to Steering Group in October 2023

Four options were proposed to the Open Networks Steering Group in October 2023, reflecting on the ambition to deliver a solution promptly, while also recognising the range of options which were previously explored.

Option ID	Name	Summary
A	Adopt one of the existing dispatch platforms	An existing flexibility dispatch platform would be adopted by all network operators
B	Adopt existing dispatch vendor API as a common standard	An existing flexibility dispatch platform vendor's API would be adopted and implemented by all other vendors as a common standard
C	Adopt existing industry standard as a new common standard	An existing industry standard would be selected and adopted as the new dispatch interoperability standard

D	Framework for enduring solution	Take no tactical steps, and work towards a longer-term strategic enduring solution
E	Collaborate with the industry to develop a new UK standard	Working collaboratively with stakeholders to develop a new UK-specific dispatch standard, building on the learnings from existing flexibility dispatch platform vendors

In light of the desire to deliver a solution in the shorter term, the fourth option (Option D), which would have resulted in a shift in focus towards only delivering a longer-term strategic solution, was not considered to be viable. A fifth option was proposed in the event that it was necessary to develop a new standard, if none of the other options provided viable.

In exploring options for a tactical solution, the focus and rationale for this evaluation was to consider **viability of solutions which would take less time to be adopted**, rather than one which would be replaced quickly.

Recap of FSP Stakeholder Feedback and Insights

As a recap of some of the key insights gained from previous stakeholder engagement feedback (as set out in the earlier October 2023 report), a number of general sentiments were noted:

- FSPs were often indifferent about the specifics of a dispatch platform, but were keen on it being **consistent**, having **longevity**, and being **simple to deploy**.
- There was a strong preference to deploy a solution now which can be **iterated upon**, rather than waiting to develop a "perfect" solution.
- FSPs were keen on a **common digital life-cycle** across all DSOs to cover more than just the dispatch phase of flexibility services.
- FSPs preferred to **employ modern technologies** (HTTP REST over XML SOAP), given a more established ecosystems of developers being available to them.
- FSPs were keen on **examples and sandboxes to be available**, to allow them to explore and experiment, and some even preferred this over documentation, on the basis that documentation can be interpreted differently.

Summary of Options

A - Mandate adoption of existing platform as common industry solution

Since multiple network operators have already adopted interim dispatch platform API solutions, this option explores selecting one existing platform and adopting it (as a platform) as a common industry solution for dispatch.

B - Mandate adoption of existing vendor API implementation as new common standard

In this option, an interim dispatch platform API would be selected as the common standard, the vendor of the chosen API would sign over intellectual property rights to their API specification, and it would be adopted by all network operators and dispatch platform vendors as the GB dispatch standard.

C - Mandate adoption of established industry/formal standard

This option explores a range of different existing standards, evaluating their appropriateness for use in an interoperable GB dispatch standard, informed by the earlier gap analysis and minimum data parameter requirements.

D - Investigate further and recommend the framework for an enduring solution

In this option, a team would be resourced to carry out further investigation and focus on an enduring solution. As set out above, this option was not considered to be viable, given the desire from industry to see an interoperable dispatch API solution in the short term.

E - Work with industry to develop an enduring solution collaboratively taking input from vendors

This option was proposed as an additional option, which is similar to Options C and D, while learning lessons from existing dispatch platform API vendors' experiences.

Detailed Options Analysis

In this section, detailed technical and commercial analysis for each option is presented.

Option A – Mandate Adoption of Existing Platform

Commercial Implications

One clear initial downside of this approach is that it creates a **dependency on a single chosen vendor** and requires all network operators to adopt their software and platform. This would grant a **single vendor an effective monopoly position** on both network operator dispatch of flexibility resources, as well as on FSP participation in the flexibility market, on the basis that unless a given participant had access to this flexibility platform (which, in some deployment architectures, may require FSPs to interact directly with the platform provider, rather than the network operator), participation could be on arbitrary or variable commercial terms.

To make the approach of adoption of a single existing platform (as a platform provided by the vendor) a viable option, **very careful consideration would need to be taken as to the commercial arrangements for this**, specifically in ensuring **open market access, and equal and transparent pricing for all market participants**, etc. Otherwise, there is a risk that a platform operator could use their control over the ecosystem to directly or indirectly exclude or include participants, or use their position to control the economic viability of different flexibility providers from entering the market.

In particular, since the chosen platform vendor would become a single-source natural monopoly for technical advice and guidance on their existing API implementation, it is likely that those implementing their API would require advice, guidance and support from them.

Similarly, there may be other commercial aspects to be addressed around access by aggregators, to ensure that direct provision of flexibility services, as well as provision of services through an aggregator, are treated in a non-discriminatory manner. If a platform was able to charge more to aggregators, they may prefer to nudge FSPs to participate via aggregators through structuring their pricing with higher onboarding and fixed charges. Similarly, if a platform preferred to interact with more FSPs to maximise revenues in offering adjacent consulting services on integrations (which would not be required by a smaller number of aggregators), they could develop a pricing model which would discourage larger aggregators from participating.

Carefully constructed contracts and commercial agreements could reduce some of these risks**, but network operators and FSPs would have few credible options were they to seek to part ways with a platform provider** – the incumbent platform provider would have significant bargaining power in such negotiations, as the ecosystem has adopted their platform and interfaces, and there would be costs on all parties to move away. In stakeholder engagement, it was a clear view from flexibility providers that they were keen for stability and agreement on an enduring API. This would likely present a substantive barrier to switching platform vendor (and thus API) in future.

It would therefore **not appear to be feasible to have an effective and productive commercial negotiation for subsequent contract renewals**, based on **sunken cost and FSP and wider industry investment** in integration with the chosen platform. This would likely give rise to under-priced bids to provide the platform, with a view to gain dominance, then raise prices in future periods, once the sector has adopted the platform. Similarly, such a market position would make the selected platform provider an attractive takeover target by external investors, seeking to raise the platform price at subsequent contractual re-negotiation periods.

From a commercial and contractual perspective, it **does not appear that Option A presents a viable or attractive option** as a tactical solution. This is for the following reasons:

- The need to negotiate contractual and commercial terms very carefully with a chosen platform provider, to avoid unintended consequences or barriers to participation being imposed by a platform provider. This would, in itself, likely take several months of in-depth legal review before it would be clear whether or not a viable agreement could be reached.
- The clearly foreseeable challenges in carrying out commercial re-negotiations having adopted a platform, which deliver value for money to billpayers, given the high cost-to-switch for all participants in the flexibility ecosystem, and the limited bargaining power available to network operators once a provider is chosen.
- The significant risk that the selected platform provider would be acquired or taken over by an entity with a view to either significantly raising prices to deliver profits at billpayer expense (given the high costs of switching once a platform is adopted), or with a view to an overseas entity gaining a foothold in a portion of the GB energy sector to impact the stability of UK CNI.
- Stakeholder feedback has expressed a focus on the importance of delivering longevity on an API selected for the GB flexibility market – this would limit the credibility of changing platform in future, and potentially create a vendor lock-in scenario, or hinder the ability to negotiate competitive pricing in future for platform access.

Technical Implications

From a technical perspective, by adopting an existing platform that is already able to be used for dispatch by a network operator today, some of the technical risks around being able to deliver the requisite functionality are reduced. Network operators are, today, using platforms like these to dispatch flexibility services, although **not in a manner which would necessarily allow FSP-side interoperability across network operators**.

It is important to note that current dispatch API platforms have not necessarily been designed to deliver interoperability across different network operators, and that findings in this section are therefore not intended as criticism of existing products or solutions on the market, but rather a technical assessment of whether a straightforward “lift-and-shift” approach would work in all scenarios.

There would still be significant work to be carried out once a preferred dispatch platform vendor was selected, to establish if each network operator was able to carry out dispatch using the available fields in an API. This is because different dispatch platforms currently implement very different API functionality.

As an example, the Flexible Power dispatch platform API[1] dispatch message contains a message timestamp, an indication of region, the category of flexibility service being dispatched, and the meterable units to be dispatched. That API contains no indication of quantity of service being dispatched (precluding partial dispatch), nor any specific reference to a contract or agreement which would allow an FSP to disambiguate dispatch messages for differentiated service delivery levels.

In contrast, a Piclo API dispatch message[2] contains fields to stipulate dispatched quantities, directions, real or reactive power, and times (allowing for ahead-of-time dispatch, rather than near-real-time dispatch).

In addition to specific API semantics, there would also be a requirement to validate the security architecture and model of the existing platform being adopted, to assess whether the solution will provide a straightforward route for participation of FSPs. This includes options for software that FSPs can use as clients or "FSP-side implementations" to connect to the API, and how they can connect their dispatch implementation to the assets in question, to provide flexibility services. This will require technical integration work to be carried out, and will require a skills-base of developers and engineers to carry out these integrations. While this is not a requirement unique to this option, there would likely be a more limited range of experience and capability to develop against a vendor's own proprietary API, and this is likely to limit the potential providers of such services.

There are also some potentially more fundamental architectural differences between existing dispatch API platform vendors' solutions, which would need to be explored. **Both Flexible Power and SGS require FSPs to host an API server facing towards a Network Operator**, to receive dispatch messages. Piclo has the ability for an FSP to host an API server to receive web-hook dispatch messages, but also has an API which could be polled for new dispatch messages.

From a technical perspective, it is important to keep in mind that, while Option A may appear a simple and straightforward solution to delivering something quickly, **multiple network operators would need to procure and implement an integration between their back-end systems and a new platform**, which would be time-consuming. Given there are several platforms already in use in the UK, it would not be possible to converge on a solution through Option A without several network operators needing to change platform.

The platforms available also **do not necessarily support all of the API functions that the TWG considers to be necessary to deliver a wider interoperable dispatch and flexibility ecosystem**. For example, neither Flexible Power nor Piclo have the concept of an "availability declaration" that is submitted after a contract is awarded. SGS' platform has the concept of availability status reporting, although it is optional for FSPs on all services other than MW Dispatch.

Similarly, Flexible Power does not have the ability to schedule future service delivery (i.e. providing notice ahead of time of delivery), as their API only provides an ENA service name, and dispatched units. Such an API call would therefore be most simply interpreted as an immediate dispatch (incorporating ramp-up time), although one cannot preclude that some users may have agreed "out-of-standard" interpretations of such a message to indicate an ahead-of-time dispatch. **This is the kind of variation that an interoperable standard needs to avoid, to ensure that API semantics communicate the necessary information without other specific behaviours based on non-standardised information.**

Recommendations

The following recommendations and observations are made, based on the above:

Commercial/Risks:

[1] https://flexiblepowerportal.co.uk/docs/public/participant.html
[2] https://docs.picloflex.com/#tag/dispatch/paths/dispatch_webhook/post

- If an existing platform was to be adopted, there should be a way for the "platform" or server implementation to be hostable by network operators, or a pathway to this being feasible before deployment, as opposed to relying on vendor-hosted (and risk-aggregated) centralised platform servers being provided as a service.
- For a tactical solution, while it may be possible to run a single platform instance in the short term (i.e. a multi-tenant architecture), there should be a smooth migration pathway planned towards a single-tenant architecture. This will require routes to identify service URLs and their discoverability, in order to allow for network operators to operate their own platform instances in future.
- Careful consideration should be given to commercial implications, and how to ensure value for money, since this approach would effectively select a "winner" in the market. This will reduce competition, and likely have a negative impact on other suppliers, and potentially introduce significant barriers to switching platform vendor in the future.

Technical:

- **No one platform currently meets the ENA TWG's minimum service parameter requirements** – while SGS and Piclo meet more of the minimum data field requirements than Flexible Power, Piclo appears to issues all dispatch messages with a level of ambiguity over whether they are absolute or relative values[3]; and some products are currently dispatched using absolute values. While SGS implements a subset of ENA services, the API semantic around Dynamic dispatch is currently day-ahead scheduling without near real-time dispatching.
  Option A is being considered for direct adoption of an existing commercial solution, and the currently available options do not appear to necessarily deliver an interoperable solution across network operators.
- For a tactical dispatch solution, to reduce the burden on FSPs and facilitate market entry for small providers, as well as individual 'pro-sumers', and reduce requirements on FSPs to have their own server infrastructure or substantive cloud footprint, **there should be a viable route for an FSP to provide services by polling a network operator-provided API as a client**, without having to provide and expose server or web-hook APIs to the internet. This is explained in more detail later under "Technical Architecture Considerations".
- A tactical dispatch solution should still offer sufficient security to reduce the risk of exploitation of a single internet-connected component and limit the attack surface. This would need to be explored for each platform in more detail, were this option considered further.

Option A (adoption of an existing platform) would likely not present an immediate technical solution to delivering interoperable dispatch, given that none of the options explored currently meets all of the minimum requirements from the TWG, and given the commercial risks of this approach highlighted above. In particular, selecting a single platform vendor to be adopted by all network operators is likely to deliver poor outcomes for the market, and increase pricing over time, as well as introducing barriers to switching platform vendor.

[3] https://docs.picloflex.com/#tag/dispatch/paths/dispatch_webhook/post - while it is somewhat ambiguous from the documentation, it is likely that since a dispatch event considers power type (real/reactive), capacity (MW) and need direction as being either import or export to grid, an implementer may consider this as a dispatch of a relative (i.e. delta) quantity of power.

Option B – "Mandate adoption of existing vendor API implementation as new common standard"

This option is similar to Option A, but where only the API specification from a vendor would be adopted as a common standard. The vendor's platform implementation would not necessarily be adopted, but their API semantics would be adopted as the GB dispatch standard. Other dispatch API platform vendors would be able to implement the API specification, in order to allow for competition in service provision, while adopting one vendor's API.

The TWG has conducted initial exploratory conversations with vendors in the sector to assess their willingness and interest around this, and felt it was worth exploring this option.

Commercial Implications

Similar to Option A, this option has commercial implications that should be explored carefully. In Option B, a vendor would sign over intellectual property rights to their API specification, and it could then be adopted as a GB dispatch standard.

Assuming a vendor was willing to do this, there are likely to be commercial implications, since this vendor will be most experienced with their own API, and may seek to capitalise on this position by offering consulting and integration services in a manner that results in the ENA selecting an API as granting one vendor a preferential position in the market. If time was of the essence in adopting an API, it is highly likely that this vendor would have a significant advantage compared with others, who would effectively be starting from scratch in adopting that API specification.

Secondly, for this to not create a vendor lock-in scenario similar to Option A, there would need to be a plan for other vendors to implement the selected vendor API into their own products, to create a market for competitive service provision. This would take time, as other vendors would need time to develop new products that support this API (both for Network Operator-side and FSP-side systems). The other vendors would need to see a prospect for their product (implementing this API) to be adopted, rather than their network operator customers adopting the product of the vendor whose API specification was selected, otherwise there would be little case to invest in developing support for the new API.

There is a risk that other vendors may not want to implement the chosen vendor API, especially if they provide services internationally, and were keen to avoid intellectual property issues with their own products (as it is likely that any agreements around IPR would be GB-specific). If each Network Operator were to place a requirement on their existing or future prospective vendors to adopt and implement an ENA-selected standard, this would likely mitigate this risk, at least from the perspective of non-adoption in GB.

Technical Implications

With the exception of specific implications around a vendor running a platform (since for Option B to be materially distinct from Option A, network operators would need to have a choice of multiple vendors implementing the selected common API), many of the technical considerations of Option B are as set out for Option A.

In particular, it is important to note the findings when reviewing Option A around there being no single option which would meet the technical requirements for an interoperable dispatch platform across all network operators, as these apply equally to Option B, since Option B simply considers a different method of adoption of the same underlying technology of Option A, in the short term.

Recommendations

Option B does not present a materially distinct option from Option A, in the context of a tactical solution. This is because the key distinction between Option B is that there would be multiple vendors offering products using the selected dispatch standard, which is selected from existing vendors' commercial offerings. Given the timescales in place on the Open Networks Programme**, it does not appear feasible for there to be multiple vendors offering compatible products** (which are tested and robust enough to be used in production for dispatch of flexibility resources in the live network) available in a short time window for delivery of competitive options for a tactical solution.

This would result in **Option B potentially shifting more towards resembling Option A, with similar commercial risks** – Option B would **effectively select a "winner" in the market** of dispatch platform vendors, with a product already available that matches the new standard.

This vendor would then be **afforded a privileged market position to win many available contracts with network operators and FSPs**, as they would inherently have a more stable, better-tested, proven implementation available before their rivals. As such, **in tactical time-scales, Option B shares most of the same risks as Option A,** albeit with potentially reduced longer-term risks through intellectual property transfer or licensing.

The **importance of ensuring that IPR arrangements are robust** should not be under-estimated – while a transfer would likely deliver better billpayer value than a licensing arrangement (which would be subject to future licensing negotiations), there should be consideration as to whether or not it is likely that a provider would be willing to fully transfer their own IPR, as this may impact their own ability to offer services in other markets. Similarly, other vendors may not be willing to implement the selected API, if they are concerned that they could implement protected IPR from the chosen GB solution that would put them at risk of legal action in other markets.

Specialist legal, commercial and IPR licensing input should be obtained before exploring Options A or B, to understand options to mitigate these risks, as well as assess the feasibility of there being viable agreements reached, before further time is expended in exploring them.

Option C – "Mandate adoption of established industry/formal standard"

Under this option, a number of different existing standards have been explored, to evaluate their appropriateness for use in a GB dispatch standard. This work sits alongside the earlier long-listing and short-listing carried out for the October 2023 options report.

OpenADR 2.0 and 3.0

OpenADR is a standard for communication of information to trigger a demand response action from energy-using devices. It features functionality which could be used for dispatch of flexibility resources. The 2.0 version of the standard is based around an HTTP/SOAP architecture or XMPP communications, and the newer 3.0 version of the standard is based around HTTP/REST. In stakeholder engagement with the team behind OpenADR, they explained that SOAP was perceived by many FSPs to be a barrier to adoption, hence a transition towards REST-based APIs with version 3.0. When the original standards analysis was carried out in 2023, OpenADR 3.0 had not formally launched – the release took place in late November 2023[4].

OpenADR 3.0 is not designed to replace the previous 2.0 version of the standard, and 3.0 is designed to provide an extra, simplified way to add OpenADR functionality to devices. It is important for context to note that

[4] https://www.openadr.org/index.php?option=com_content&view=article&id=211:openadr-alliance-launches-openadr-3-0&catid=21:press-releases&Itemid=121

OpenADR is intended to be used to send demand response signals to consumer equipment in the household (for example, electric vehicle chargers or water heaters).

OpenADR 3.0 opens up more opportunities for expansion and extension within the confines of the standard (which is not particularly relevant to this comparison), through extensibility in API fields, as well as in adding new values to existing enumerated-type fields. **Taking advantage of such extensibility features is effectively creating a new bespoke standard**, as the expectation of, and use of, such additional fields will require standardisation and adoption by the industry.

One important learning from OpenADR was the **importance of having an agreed single testing specification**, rather than allowing for a proliferation of different test specifications by different test houses – resulting in products passing their respective tests but not being truly interoperable. They also reflected on the lesson of offering too much flexibility (such as supporting XMPP-based transports in addition to HTTPS-based transports in OpenADR 2.0), and how this ultimately resulted in multiple parallel implementations of the same logic being required to deliver a usable system.

From a standards selection perspective, it is worth noting that **OpenADR 3.0 is explicitly not backwards compatible with 2.0** in terms of protocol layer data, due to the changes in communications layers and architectures (i.e. removal of XMPP, introduction of HTTP-based PUSH via webhooks, removal of whole-message signatures of the XML payloads, and removal of mandatory client certificates for TLS sessions, introduction of an OAuth2 client credential flow for authentication).

From a technical perspective, either version of OpenADR appears capable of supporting dispatch communications, although there would need to be standardisation and agreement of which API messages are used to communicate which messages, since OpenADR 3.0 is extensible, and there are a number of different “events” which can be announced to FSPs through OpenADR, and **these would need to be common across network operators to deliver dispatch API interoperability**.

It is important to note the areas of a dispatch process which are not covered by specifications and APIs, and which OpenADR has called out as being excluded from scope, as these are a helpful reference in evaluating other options and considering additional work that would be required to support these.

For example, OpenADR does not define various requirements for HTTP client and server capabilities, such as compression algorithms supported and TLS cipher options which must be supported. OpenADR does not define how a network operator-side implementation should validate content, and this is left as an implementation detail for those implementing OpenADR. Similarly, content validation of messages received by clients is considered outside the scope of the specification, and the service provider hosting the OpenADR platform needs to maintain a secure web platform, including updating TLS ciphers as required.

Significantly, OpenADR also points out the need for out-of-band business processes to onboard FSPs, and agree specific details of “programs” or “tariffs”, and then issue credentials to a FSP so they can participate. This will be a requirement for any option ENA considers, and therefore becomes a common requirement for any solution.

On balance, OpenADR 3.0 appears to be more appropriate than 2.0, based on the previous stakeholder feedback indicating a preference for more modern use of web technologies, rather than legacy XML/SOAP-oriented protocols.

USEF & UMEI

Based on previous discovery work looking for standards, as well as stakeholder feedback and input through a dissemination event, USEF and UMEI were also reviewed as potential standards for dispatch.

The UMEI project was part of the EU-funded EUniversal project, aiming to develop a universal approach to the use of flexibility by network operators. Similarly, the USEF project was developed as part of the USEF Foundation, and has since transitioned to part of the Linux Foundation Energy project, and been rebranded as ShapeShifter.

The USEF standard (version 3.0, latest available as of December 2023)[5] sets out a flexibility trading protocol, which is focused around the delivery of a "market structure, roles, rules and tools for the commoditization and trading of flexible energy usage work with existing energy markets." In the USEF phased paradigm, the "Operate" phase is the most relevant one to flexibility dispatch, as this is the phase in which actual flexibility is delivered.

The USEF protocol however for this is highly complicated, and does not directly expose a straightforward paradigm for flexibility dispatch – Section 2.1 of the standard defines the Operate phase, where "The actual assets and appliances are dispatched and the AGR adheres to its D-prognoses. When required, network operators can invoke additional flexibility from AGRs to resolve unexpected congestion.".

The USEF standard itself does not describe a semantic through which dispatching is carried out – indeed, the documentation describes the Operate phase as exchanges of updated D-prognoses, the revocation of flexibility offers, and the exchange of flexibility orders. Absent any mechanism through which flexibility services can be dispatched independently of other complex processes, **USEF would not be a viable tactical dispatch API solution, as it does not define a method to dispatch an FSP**.

The USEF standard appears to make an implicit assumption that acceptance of a FlexOrder is akin to an (ahead of time) dispatch instruction, but this is not expressly stated in the standard, and ambiguity like this would create complexity for implementers to understand and reach a clear understanding as to an instruction.

The UMEI standard is also a specification designed around market constructs – while a "Reservation Market" is defined for ahead-of-time offers of flexibility services before dispatch, the standard states "The actual dispatching can be done outside the market or in a consecutive activation market." The standard does not define an activation market or dispatch method, beyond setting out an activation market as a "Flexibility market where the assets are dispatched for the period covered by a trade." **No details is given as to how dispatch should be carried out in UMEI**.

Further reviewing other adjacent documentation about UMEI, including technical presentations given in 2022, LongFlex (i.e. future activation of service) contracts are set out as being activated either through ShortFlex, or "bilateral[ly] through other means", which is presumed to mean outside of the scope of the standard. ShortFlex is defined as being "activated based on trade confirmation" (which is presumed to mean considered dispatched upon the order being placed), and InstantFlex is "activated based on automatic power settings (frequency, voltage or reactive)", which is presumed to mean self-dispatch.

In Deliverable 2.6 of the EUniversal Project, the API interfaces are defined in Section 3, and they move straight from the "Pre-trading phase" to the "trading phase" (i.e. posting and reading orders), without considering the dispatch or activation method. While "Flexibility activation" was claimed to be in the present version of UMEI in that report, no further details could be found of their flexibility activation method in that report.

The glossary of UMEI states that, in a Reservation Market, "**The actual dispatching can be done outside the market or in a consecutive activation market.**"

[5] https://github.com/shapeshifter/shapeshifter-specification/blob/main/USEF%20Flex%20Trading%20Protocol%20Specifications%203.0.0.pdf

It is therefore concluded that neither USEF or UMEI presents a viable GB dispatch solution, as neither includes dispatch functionality as would be required to directly dispatch FSP resources. The complexity of these projects is also likely to introduce challenges for smaller market participants to interact or engage, or even understand the semantics and paradigms used – being rooted from research projects, they appear to be more focused on innovative holistic market design patterns and structures, rather than straightforward and unambiguous industry-ready standards development. Partial adoption would introduce a range of areas of friction, such as a lack of explicit dispatch messages.

As a general observation of both USEF and UMEI, these options appear to be designed to implement a full flexibility marketplace. This is a very different goal to implementing a dispatch protocol. There is significant complexity and breadth in these standards, and the extent to which participants and implementers would need to understand complex market dynamics and functions (such as D-prognoses in the case of USEF) in order to deliver even basic functionality. This is likely to present a significant barrier to entry for new FSPs, as opposed to a simpler and more functional dispatch API focused around clear issuance of unambiguous dispatch instructions. Clear and unambiguous instructions are likely to result in better outcomes for customers, through correct dispatch of flexibility resources where they are required.

In addition, by attempting to encompass wider market dynamics and functions, such protocols would likely, were they usable and viable for dispatch (which they do not appear to be) limit future directions of travel of the wider flexibility market by being built around a range of assumptions in how a flexibility market is expected to operate.

The GB approach to flexibility with explicit dispatch differs from many of the assumptions and structures used elsewhere, where implicit approaches to dispatch (i.e. where market participants take actions of their own accord, based on observed network parameters or through price signals) may be favoured.

For example, an explicit dispatch message is one that is targeted to one or more specific assets, and conveys the technical parameters of a service to be provided, either ahead of time or close to real-time – flexibility services themselves are exposed to energy markets as products, and specific flexibility contracts are invoked and dispatched to manage the network. In some cases, with the emergence of closer to real-time procurement of flexibility services, there may be reduced distinction between a network operator accepting an offer, and a dispatch event occurring.

In an implicit dispatch system, on the other hand, indirect signals are used to create market or pricing-based incentives for load shifting or usage adjustment – as a simple example, time-of-use pricing can be used as a means of implicit dispatch to encourage users to reduce usage in a time of local constraint on consumption in a given area of the network.

In selecting a tactical dispatch API solution however, it is important to assess standards' fitness for purpose against current flexibility products and service definitions, which do not operate in this way at present.

IEC CIM (Common Information Model)

CIM is a common information model for the exchange of information about an electrical network, based around a “wires” model. CIM itself is a UML (Universal Modelling Language) model providing a common data vocabulary and an ontology of data, describing data formats, structures, and relationships.

CIM itself, as a data model and structure/ontology, does not define a communications protocol itself – other standards or communications protocols are required to then communicate information. For example, IEC 61970 is a set of standards that define APIs (application program interfaces) for energy management systems, and enables communications from the control centre out to external assets. IEC 61970 encompasses CIM.

It is also important to note that CIM is not, in itself, a fully defined data model – a series of CIM profiles are then used, which are subsets of the overarching CIM UML model. A profile is a self-contained data model, which can be used to generate exchangeable artefacts that others can process. CIM profiles are themselves standardised – for example, IEC 61970-452 defines an Equipment Profile; IEC 61970-453 describes a Schematics Layout Profile, and IEC 61970-456 defines an Analog Measurements Profile, Discrete Measurements Profile, State Variable Profile, and Topology Profile.

One challenge encountered in attempting to review CIM-based dispatch models is that, since CIM represents a data model and ontology, there is not one single representation or protocol to review – CIM is not representing a specific API-based approach or similar, and therefore an additional standard is required, to overlay the concepts of dispatch on top of a CIM data model.

OpenADR 2.0 is aligned with the CIM information model, and is interoperable with IEC 61968 (Distribution Management) and IEC 61970 (Energy Management). OpenADR 2.0 is based on SOAP/XML and XMPP-based transports[6], which are now generally considered to be obsolete in modern IT systems, in favour of RESTful APIs, which OpenADR 3.0 makes use of.

Given that stakeholder feedback to date has pointed towards a preference for the use of modern web-standards like HTTP/REST (which have a greater available number of developers familiar with the technologies concerned, as opposed to legacy options like SOAP/XML APIs), implementing a CIM-based API solution facing FSPs is likely to present barriers to adoption, due to FSPs needing to work with both IT and web standards, as well as legacy technologies.

There is also a significant burden likely to be encountered by FSPs, even if other approaches were taken, and there are indicators to suggest that a number of standards for CIM-compatible dispatch have limited support.

For example, IEC 62325-301:2018 presents a CIM extension for markets, including dispatch functionality. It constitutes 446 pages of standard document, featuring more than 750 tables. In contrast, Appendix A of this document sets out the minimum data parameter requirements for flexibility dispatch, demonstrating that such a standard would add very significant complexity. The standard itself is based on 4 packages, comprising common, management, and operations aspects of markets, plus environmental considerations. This would present a significant burden for FSPs to interact with or implement, and gaining familiarity with it would take a significant amount of time. This standard is also XML-based, built upon CIM, and much of the standard is not necessary for flexibility dispatch. Where functionality is designed for flexibility, it is very limited – for example, the DispatchInstReply (i.e. a reply to a dispatch instruction) defined in Section 6.5.8.17 is defined to support only dispatches of active (i.e. real) power, measured in Megawatts. A requirement to be able to communicate

[6] https://www.openadr.org/index.php?option=com_dailyplanetblog&view=entry&id=62:update-to-the-openadr-specification

both real and reactive power has been identified from the minimum dispatch requirements, alongside the ability to use relative or absolute values for dispatches.

According to EPRI's CIM Primer (8th Edition)[7], most guidance on CIM uses XML examples, as IEC 61968-100's main focus was on SOAP, rather than HTTP APIs. It is possible to convey CIM information over JSON, as well as over REST, but this would entail adopting a divergent version of a significant suite of standards, which would place significant burden on FSPs and implementers.

While there have been other attempts to standardised CIM communications over HTTP, such as IEC 62325-504, which defines a framework for web services communication of CIM data, this was withdrawn in 2023[8] and there does not appear to be a newer revision of this standard. This was a SOAP-based API, which is again in contrast with the approach that FSPs indicated a clear preference towards.

Despite this, CIM is likely to be used by network operators and dispatch platform vendors as a model for interchange of underlying information "behind the scenes" of a dispatch system, and could certainly prove useful for ancillary information exchange about network schematics – this work has explored the use of CIM in the FSP-facing interface facing for dispatch of flexibility services. In this context, adopting CIM would effectively lead to creation of a new standard by default, and a standard which is likely to be considerably more complex for FSPs to implement than other options. It therefore does not offer a credible technical solution at this time for flexibility dispatch, even if it is used in the wider information exchange of network information internally.

NG ESO Dispatch-Relevant Specifications

In exploring relevant existing options, it was identified that National Grid ESO has existing dispatch systems for their own transmission flexibility services. Since these are already in use in the GB market, these were explored these for completeness, as if usable, there could be advantages in alignment of flexibility dispatch interfaces between DSO and ESO markets, in order to reduce barriers to entry in adjacent markets.

National Grid ESO shared information about their existing relevant dispatch systems for the Balancing Mechanism for evaluation. EDL and ASDP were explored, and had a preliminary discussion about the Wider Access API (WAAPI).

Electronic Dispatch Logging (EDL) is a legacy ASCII-based text control protocol, and is not applicable to HTTP APIs, and would not be suitable for adoption in a web-based API.

The Ancillary Service Dispatch Platform (ASDP) API was reviewed, which is an XML SOAP-based API, rather than REST-based API. ASDP was stated to be end of life from NG ESO's perspective, and not something they would recommend implementing at this point.

A preliminary discussion took place about the Wider Access API (WA API), which NG ESO stated is being transitioned to a new platform as part of a move to a new balancing platform, and built with some platform assumptions that mean it is carrying technical debt that would not be viable to deploy as a new initiative.

NG ESO highlighted that their Open Balancing Platform (OBP) work aims to replace each of these components, and that it is not yet ready to be adopted at-scale, but may be in a few years' time.

On this basis, there did not appear to be an existing available API standard/specification from NG ESO that would be appropriate at this time for interoperable flexibility dispatch functionality.

[7] https://www.epri.com/research/products/000000003002006001
[8] https://webstore.iec.ch/publication/22465

Recommendations

In conclusion, OpenADR 3.0 should be considered as potentially viable candidates for a dispatch standard under Option C, with the important caveat that (like with any approach) they will require further work and standards development to support flexibility dispatch as is envisaged to be required for the GB market.

It is important to note that OpenADR 3.0 is not directly backwards-compatible with OpenADR 2.0, since version 3 was designed to be easier to implement, and move away from some legacy technology choices made in 2.0 (such as use of SOAP/XML-based APIs, with the option for XMPP transport). It is also important to note that OpenADR 3.0 contains features which can be used to describe the desired power parameters for a flexibility event, but that OpenADR 3.0 is not in itself designed around GB flexibility products – there will therefore be a need to define these in the implementation of the standard itself. This means that there is an inherent requirement for implementers to understand GB specifics of implementation.

In OpenADR, the "event" construct is that which is used to signal an energy event, and would likely be best put to use as a dispatch construct. An event has a type, and can supply information specific to that type – it would be necessary to agree which "type" of event would be used for dispatch as part of a GB standard, and how to interpret this. For example, a "SIMPLE" event can be used to send a basic demand response signal with 4 possible values. There are also price-based options, as well as options for communicating relative and absolute setpoints for dispatch to control consumption of load. To use OpenADR effectively in a dispatch API context, there would need to be wraparound context, by way of a standard or documentation, to set out exactly how the API would work, and what would be communicated, in order that FSPs and other implementers understand what to expect, and how to react to these messages.

There will also be testing requirements, once such a specification is agreed upon – The OpenADR Alliance sets out in the documentation for the release of 3.0 the potential for a certification profile to be created in future for demand flexibility, but it is not yet defined, and remains just a possibility. This indicates that, in addition to testing of the GB API semantics for dispatch, there would likely be wider requirements to test overall functionality in the context of dispatch.

Similarly, OpenADR does not handle the process of establishing user identities, and therefore there would need to be architecture and design of a wider framework (in common with all other solutions) to support onboarding of users, and handling of authentication, authorisation and accounting, as well as identity management.

Finally, since OpenADR is a specification, network operators would need to implement (or procure the implementation of) their side of the OpenADR standard (called a VTN) to face towards FSPs, who would need to implement an OpenADR client (and potentially websocket server, depending on PUSH/PULL posture adopted).

Option D – "Investigate further and recommend the framework for an enduring solution"

No specific technical analysis has been carried out of this option, as it effectively proposes to establish a resourced team to carry out further investigation and focus on an enduring strategic solution. This option is not considered to be feasible, given the desire from FSPs and network operators to deliver a workable interoperable flexibility dispatch solution on a tactical basis.

Option E - "Work with the industry to develop an enduring solution collaboratively taking input from vendors"

This option was proposed to consider how best to capture learnings from existing providers of flexibility dispatch solutions, while also recognising that there are significant commercial risks if an existing solution or specification is adopted. This option reflects the need to ensure that the scope of a standard is wide enough to enable FSPs and others to easily participate in the market, and that this requires definitions and agreements of parameters, architectures and factors which often go beyond those included in any one vendor specification, to create the necessary touchpoints to enable interoperability. This approach allows for learning lessons from existing specifications, and building consensus (which is a key part of standardisation), by convening relevant stakeholders to develop a standard, informed by those who have already developed such platforms, and are best-placed to share lessons learned from their own experiences.

As a specific example around interoperability gaps, dispatch APIs have generally been designed around the concept of FSPs having a relationship with a single network operator, and the process of onboarding an FSP to a new network operator will need to be designed to consider an FSP already providing services to another network operator. This will be a business process, which ultimately needs to establish a technical dispatch API connection to the FSP. Therefore while a standard may cover some aspects of this, to deliver true interoperability in the market, there will be extra requirements over the top of a standard to enable the interoperability sought by the Open Networks Programme.

The main disadvantage of this approach is that it is not likely to benefit from the ability for FSPs and other market participants to benefit from international harmonisation and standardisation of some of the lower-level principles and message flows that an existing international standard may offer, like Option C would offer. In addition, starting the development of any standard from scratch will take significant time, and there are risks that more iterations of development are required before a functional standard is realised.

By developing a standard based on industry input and learnings, significant time gains could likely be made by leveraging learnings from vendors' experience in this sector. This is based on the fact that, in the technical analysis of Option A, it was clear that some of the existing industry options are close to delivering an interoperable dispatch solution, but that specific aspects of certain products are limiting factors in delivering interoperability. It would therefore make sense under this option to explore how input from industry could support this task. There would be a need to carefully manage stakeholder input to this process however, to ensure that no one party dominates development of a new specification, and that there is no undue preference towards selection of approaches taken by any one vendor – this can be handled in technical standards development through a clearly defined problem statement and "best technical solution" approach, but these kinds of discussions are likely to add delays to development of a new standard, if stakeholders seek to see aspects of their own solutions included in a standard.

Attempting to develop a new standard without the benefit of this input from the sector would take considerably longer, and be unlikely to gain their confidence and backing. As part of this recommendation that it would be **important for network operators to work closely with vendors, as part of a collective endeavour to holistically reach agreement and expedient decisions** around API semantics, with a view to **either eliminating, or reducing and making explicit in API messages any network operator-specific variations**, to **ensure interoperability** of dispatch functionality across the GB market. If this option is selected, a **governance framework with independent technical input, as well as open participation from vendors of flexibility platforms, FSP-side implementations, network operators, ESO, and other relevant stakeholders should be convened**, with **clear and robust terms of reference** to provide guiding principles for development and implementation of the API specification.

In addition to this, there will be other "next steps" that need to be taken irrespective of which option is selected. These will be important, and would **rapidly become pre-requisites for development of an interoperable specification**, since a key part of delivering dispatch system interoperability will be **alignment of wider business processes**, as well as **capturing and making explicit the implicit assumptions that sit within dispatch APIs** as used today.

From a commercial perspective, this approach should alleviate risks of a single vendor receiving a preferential market position as a result of decisions around a dispatch standard, thus reducing commercial concerns. There would need to be careful consideration around intellectual property rights, and an approach such as that taken in other standards bodies (such as 3GPP[9]) would be required, to ensure that relevant IPR holdings are declared by participants when providing input to standards development.

Governance of this process will be key, in particular to ensure that the design delivers an interoperable solution which does not result in standards bifurcation with different network operators, and which does not overly advantage or disadvantage any market participant.

Common Next Steps and Recommendations

Irrespective of which approach is taken, there are going to be some common next steps, which should not vary too significantly between options. These include some potential gaps, or common areas of work, which are necessary to be explored regardless of which option is selected – even adoption of an existing international standard, or adopting of an existing vendor solution, will likely require many of these to be carried out.

- **Developing business process and business system integration to network operator back-end systems** (which is likely to take slightly different amounts of time depending on what is selected as a dispatch architecture). In order to deliver a workable flexibility dispatch system which can be used to dispatch actual services, there will need to be **sufficient integration into network operator business processes** to allow it to be used as part of a wider system involving pre-qualification and settlement.
- **Definition of the high-level system architecture** (i.e. pan-network operator) of the dispatch solution selected, including whether it is single-tenant or multi-tenant, and how FSPs will discover network operator endpoints, and whether these endpoints can be moved. This should also include planning around disaster recovery endpoint movement, where applicable.
- **Conducting a detailed security architecture review and threat modelling exercise** against the proposed solution, to document and establish what are considered acceptable risks, and the levels of mitigations required. This should include factors around resilience, if the selected approach results in a third-party platform sitting between network operators and FSPs. Ideally, each network operator would agree on a common posture to this, such that security does not present barriers to interoperability.
- **Ascertaining the extent to which this dispatch system constitutes or may constitute CNI within network operator systems**, and whether any thresholds are exceeded by any platform or infrastructure.
- Establishing the wider network operator-side posture towards flexibility resources and communications requirements – for example, **whether heartbeats are required**, and **how network operators will handle edge-cases and scenarios where an FSP cannot be reached** (in order to standardise this across all network operators). This will be important if an interoperable API is to be designed as part of Option E, such that **these requirements can be clearly and explicitly documented for all flexibility services**.

[9] https://www.3gpp.org/about-us/legal-matters/call-for-ipr

- Establish, where network operators host their own platforms, their **security posture around communicating with multiple FSPs, and if they will shard or otherwise sub-divide their platform** to avoid exposing a single attack surface to multiple FSPs (i.e. creation of multiple single-tenant instances of a dispatch API service, rather than a single shared one that all FSPs interact with).
- **Definition of "exemplar" methods of utilisation of the selected dispatch API** – for example, which modes, methods, and API endpoints and messages will be used.
- **Definition of the "direction" of the API** (i.e. 'Push' vs 'Pull' from an FSP perspective), since some of the API options allow for both options to be used.
- **Definition of standard cross-network operator (where possible) security requirements to be flowed down to FSPs for inter-connection,** in order to, as much as possible, streamline the process and avoid creating an interoperable API that sits atop 6 different non-interoperable onboarding processes.
- **Definition of an approach to "identity" in dispatch**, in order that there is pathway for an FSP to "enter" the ecosystem, as well as "widen" their participation in the ecosystem to supply more than one network operator. This is **important to enable interoperability**, and avoid creating a series of **similar, but different, per-network operator dispatch onboarding processes**, which are substantively different from the perspective of an FSP. In the event that certain flexibility services have different technical requirements (i.e. around restoration/black start resilience), a common identity layer would allow attributes such as restoration-eligibility to be assigned to FSPs in an interoperable manner based on an attribute on their certificate.
- Validating and de-risking the FSP-side integration between the dispatch API and their own infrastructure, and ensuring there are suitable implementations available that do not create vendor lock-in scenarios or similar.
- **Understanding and modelling information exposed to FSPs**, to ensure that FSPs (or their technology providers) have access to the information in a dispatch message needed to understand what to dispatch, and with which parameters.
- **Harmonise and make explicit any potentially ambiguous aspects of dispatch API terminology**, including **drafting with formal standards-level precision**, functions and wider **requirements and definitions** for terms like (as one example) "acknowledgement", and eliminate ambiguity around whether a request is acknowledged on receipt, as opposed to successful and acknowledged receipt by the unit being dispatched, and that the answer to this is consistent across all network operators.
- Carry out **alignment with other ENA Open Networks workstream activities**, to ensure that the **API is developed alongside work defining the wider technical and non-technical controls**. There needs to be a clear and robust understanding of terminology and required behaviours and actions before an interoperable API can be implemented (since if such information cannot be communicated clearly through an API, it will block interoperability), since **API documents will need to communicate this information to implementers**, and **an interoperable API standard/specification will require this to be defined** if a failure to implement it correctly would hamper interoperability.
- **Consider how a dispatch API will align with other ENA Open Networks work** seeking to standardise and harmonise market engagement, contracting, and procurement and settlement functions.
- Ensure that the solution aligns more broadly with the direction of regulatory and policy travel holistically across the dispatch ecosystem, and that it has a pathway to evolve to deliver future flexibility services which may be introduced, with pathways for backwards and forwards compatibility, while avoiding ambiguity around which service is being dispatched against a given unit.

Technical Architecture Considerations

Three key architectural considerations have been highlighted based on the technical analysis work carried out, on the basis that these are likely to inform wider requirements around an API or specification for interoperable dispatch functionality, regardless of which option is progressed.

Levels of network operator-side isolation of different FSPs

Depending on network operators' security posture, a network operator-hosted dispatch server could be implemented in a single-tenant (i.e. one backend service per FSP) or multi-tenant (one common backend service for all FSPs to share) manner. From a security and resilience perspective, there may be some benefits in being able to limit the exposure of a network operator to a security issue affecting a dispatch server, through splitting FSPs across separately hosted server backends, meaning that an issue affecting one backend dispatch server would not affect other FSPs.

Other architectures could also be developed, and should be explored, around failover, hot spares, and similar resilience measures, including use of disaster recovery sites or facilities. Given that most FSP resources are unlike to be connected to restoration/black start-resistant telecoms infrastructure, restoration/black start considerations for cloud-hosted components are likely to be less of a concern than in some other scenarios. Nonetheless, isolated cloud failure or outage scenarios should be considered for causes other than power outage, in order to establish and communicate suitable resilience requirements or expectations to FSPs, and align these across the flexibility market to ensure interoperability and consistency.

FSP requirements to host an internet-facing API server

Many existing platforms (including Flexible Power, Piclo and SGS) make provision, or indeed require (in the case of Flexible Power and SGS) a FSP to host a web-facing API from a server instance, to enable the "pushing" of dispatch messages to an FSP from a network operator or platform-hosted dispatch client. This means that the API for dispatch is provided by the FSP towards the network operator.

The advantage of an "FSP hosts a server" approach is that it allows for a network operator to initiate communications with an FSP when there is a dispatch message to be sent, rather than have the FSP regularly poll the network operator for any available dispatch messages. This is likely to be slightly more efficient, by reducing the workload on the network operator-side servers interacting with FSPs. Given that some flexibility services (such as MW dispatch) currently expect a heartbeat signal to indicate availability, and some flexibility dispatch platforms (such as SGS) implement optional status heartbeat APIs, this does not appear to present a major advantage, as such polling messages could contain heartbeat and availability/status information.

The disadvantage of this approach is that it places a number of non-trivial technical burdens on FSPs, which present impediments to market participation. Firstly, in order to host APIs like this, an FSP needs to have a public domain name registered, with DNS records hosted on their behalf, pointing towards a server implementation. This server will require a public IP address, either requiring use of a cloud-based virtual server, or an on-premises server with a business-grade internet connection with a static public IP address.

There was no specific clear mention from any of the flexibility platforms explored around whether or not their implementations support IPv6, so it is presumed that this would depend on their software, as well as network operator and other intermediate network configurations. On this basis, it is assumed that an FSP would require a publicly routable IPv4 address. These are increasingly difficult to obtain from ISPs, due to regional allocations having been exhausted many years ago. Once this is in place, the FSP would need to securely host an API, through a web service, running a web server, and obtain a trusted TLS certificate to enable secure communications using HTTPS. Network operators would need to stipulate which root and intermediate

certificate authorities they trust. FSPs would need to manage certificate lifespans, and ensure they renew certificates before they expire, or risk failing to receive dispatch messages.

While there are avenues to obtain free certificates, these generally require levels of automation of certificate issuance that are likely to present knowledge barriers for those not familiar with such services. Such certificates are also generally of much shorter lifespans (as they are assumed to be used by technically savvy users who have automated their certificate handling infrastructure).

FSPs would also need to manage and maintain the security of their internet-facing infrastructure, as well as any other enabling or supporting infrastructure enabling their services, and ensure that they have a suitable security response strategy, given they are hosting an internet-exposed web API that is likely accessible to the whole internet. While they could add extra protections here, such as IP whitelisting, this would again add technical burden, as FSPs would need to maintain and update these whitelists to avoid losing connectivity to their dispatching network operators. In addition, where network operators are authenticating to an FSP-provided server through an API, the FSP will have a responsibility to ensure their logging and other monitoring infrastructure does not reveal network operator-controlled API tokens in logs (as bearer tokens are widely used in these APIs), as these can be replayed by an attacker and used to issue false dispatch requests to an FSP.

Finally, the FSP needs to understand and maintain this infrastructure as required, and have the knowledge to secure it and the various accounts required. While this is not a significant burden for people who are well-versed in managing web services and internet domains, it requires a wide breadth of learning before a market participant is able to even begin to offer a service.

Another disadvantage of “FSP as server” is that it requires both the FSP and network operator to maintain and operate web-facing API servers, and each act as an API client. This adds complexity to API specifications, and introduces potential ambiguity around which service exposes which API endpoints.

On balance of the above considerations, a technical recommendation is made that, **to facilitate ease of market access, reduce barriers to participation, and reduce the technical burden on FSPs, pull-based APIs hosted by network operators should be adopted**. By avoiding the requirement for FSPs to host internet-facing web services, they are not required to expose (and secure) web services on the public internet. This approach allows an FSP to act as a client to the network operator(s) dispatching them, initiating outbound connections to network operators, and making a regular polling request to seek any applicable dispatch messages. This heartbeat poll message also allows network operators to detect a loss of communications to an FSP, and receive any status or availability information that a communications protocol specifies to be included in heartbeat messages.

Security and Authentication

This document is not a full security evaluation of potential solutions, but highlights a concern around the single-factor authentication nature of the platforms and solutions explored here. It is considered best-practice to make use of multi-factor authentication for important systems. Flexibility service dispatch is clearly an important communication, which should have adequate security to protect the stability and integrity of both the power grid, as well as the flexibility marketplace.

Four recommendations are therefore made:

1. **Strong (and multi-factor) authentication should be supported (and ideally mandatory)**

   MFA is an accepted baseline expectation of security in many organisations. Indeed, many cyber-security insurance policies and audits now consider this as a fundamental protective control that should be in place on every possible system, to reduce risks of stolen credentials.

There are, however, inherent challenges in delivering a resilient flexibility dispatch solution using typical MFA technologies used by human users (i.e. SMS passcodes, phone-issued passcodes, and other techniques requiring manual intervention).

Instead, HTTPS with TLS client certificates should be considered as a method to limit the attack surface exposure of dispatch services, as well as to provide a level of strong authentication (which cannot be replayed from a web server log) of instructions issued by network operators. In future, if required, these TLS client certificates could be required to be stored on hardware-protected security to prevent private key extraction and cloning. This would require identity and public key infrastructure, but establishing interoperability between network operators for dispatch of FSP services is also likely to require the establishment of a similar strong identity platform in order to facilitate FSPs to establish new technical connections to network operators in any case, in an interoperable manner.

Careful consideration should be given as to the security posture of FSPs, and the threats/risks posed to FSPs and network operators alike, and where there is a requirement to architect the solution to resist persistent and ongoing concerted efforts to compromise infrastructure or gain a foothold in equipment.

2. **Consideration should be given to the signing of all API messages by keys held only by the market participant, to provide non-repudiation.**

   Since dispatch APIs will be used to communicate market-relevant information, consideration should be given to a requirement for signatures on messages communicated over an API. The Piclo platform API currently includes a field which allows for a signature to be placed on messages, and dispatch messages can be signed by the system operator.

   The signing of messages by keys held only by the relevant party issuing the message (with appropriate timestamps) provides a strong level of confidence, when presented by their counter-party in the market, that such a message was genuinely issued by the party, and can present useful evidence in order to review failures or incidents and market activities, and prove that a message issued by a party was indeed sent by them. This can benefit all parties – an FSP can use it to prove a disputed dispatch request and instruction was signed by a network operator, and therefore they dispatched in good-faith, and a network operator can use it to prove that an FSP declared and confirmed their availability shortly before failing to deliver a contracted service.

   Consideration should therefore be given to the use of enduring asymmetric signatures (using a different key or certificate to that used for TLS communications) in API messages from both network operators and FSPs, such that communications are non-repudiable, and to provide an enduring layer of validation of the integrity and content of API messages, and protect against an issue like compromise of a static API key or Bearer token credential from being used by a malicious party to issue false messages.

3. **An approach to identity, authentication, authorisation and accounting should be agreed at the outset, across network operators.**

   To deliver a genuinely interoperable solution, there will need to be a common approach to identity management and authentication across network operators, otherwise implementations will end up needing bespoke and custom configuration changes per network operator. This would inhibit real-world interoperability and the ability to create a single common implementation that works with any network operator. Standards exist (such as OAuth2), and consideration should be given as to how to make this as interoperable as possible, including making it possible for FSPs to maintain an identity across multiple network operators.

In addition, when considering authentication and identity management, the fact that one FSP may control a large number of assets, which could be deployed at a wide range of geographic locations, where there are limited means for holding of secure cryptographic keys, outside of hardware security devices, should be taken into consideration – credentials at one site should be scoped to that site alone, and not give access or the ability to spoof messages on behalf of other infrastructure that FSP controls, in that or any other region.

4. **The security of FSP-side endpoints should be considered from the outset.**

   There are many examples over time of platform and endpoint security considerations resulting in issues in the longer term for the security of energy infrastructure, such as the poor security posture of many internet-connected electric vehicle chargers[10]. In addition, as set out above, consideration should be given to the secure storage of cryptographic keys, and ensuring that they are scoped and constrained to the flexibility asset or site in question, and that this scoping is technically enforced by the flexibility API itself.

   Historically, many “OT” and energy systems have been deployed with little consideration about their realistic secure lifespan, and how software security updates and maintenance will take place. To have confidence in flexibility assets being available when they are needed, network operators will need to know that devices are maintained, supported, and receiving regular security patches.

   A patching regime that delivers regular security patches to devices will likely also introduce requirements to expedite and enable automation of end-to-end integration testing of the overall solution (including against a network operator’s sandpit or test API), to ensure that updates are suitably tested before being shipped. It is also important that this encompasses the local control mechanisms exerted (if any) by a FSP-side asset – this is to ensure that an FSP-side implementation does not suffer from functional regressions following software updates, which could cause it to deliver incorrect asset control messages in response to flexibility commands (i.e. turning down rather than turning up, or failing to issue a control command having acknowledged a dispatch) – a GB flexibility dispatch approach should set clear requirements around the order of events and requirement for acknowledgement from flexibility assets before acknowledging dispatch, and these behaviours should be tested before software upgrades are shipped to devices.

   This is likely to form part of a wider integration testing and validation regime’s requirements.

[10] https://techcrunch.com/2021/08/03/security-flaws-found-in-popular-ev-chargers/?guccounter=1

APPENDICES

Appendix A – TWG Analysis of Minimum Protocol Communications Requirements for Flexibility Service Dispatch

The following is a summary of the TWG's analysis of the minimum protocol requirements to communicate the information required for dispatch of flexibility services.

It is intended to present a working technical view of the information likely to need communicated from network operators to flexibility service providers, as well as from FSPs to network operators, based on technical analysis of existing dispatch processes, and an understanding of technical options for flexibility dispatch. Some information may be optional or not required in all cases – the purpose of this exercise was to understand the basic envisaged requirements for dispatch of a "run now" or "run at scheduled time" instruction.

(Page intentionally left blank)

Dispatch Information from a Network Operator to an FSP

Hierarchy Level	Field Name	Field Data Type
Top Level	Service start time	UTC Datetime
	Service end time	UTC Datetime
	Dispatch Unit	Unique reference, namespaced by FSP identity
	Contract ID	Foreign key link, namespaced by Network Operator, to a flex services contract
	Instruction time	UTC Datetime
	Network Operator ID	From a well-known list of network operators
	NO Dispatch Ref	Unique dispatch reference, namespaced by Network Operator
	Dispatch Information Revision	Monotonically incrementing integer counter
	Dispatch status	Enumerated type (e.g. pre-notify, run, STOP)
	Signature	Encoded bytes (if required)
		**** Within a given top-level message, between the service start and end time boundaries, one or more "service timing" entries may be presented:**
Service Timing	Setpoint Timestamp	UTC Datetime
	Service Parameters	Structure (defined below)
		**** For each setpoint, a series of service parameters are given. The FSP is expected to turn up/down in line with their ramp rate to deliver these services. All setpoints are given as destination targets (i.e. at the setpoint time, the FSP should be delivering services to the setpoint level)**

Service Parameters	Service Volume	Volume of flexibility service to be dispatched
	Service Units	The units of power conveyed
	Delta or Absolute?	An enum to convey if this is WRT baseline, or an absolute value
	(Price per unit?)	(Define units, then can define price? Once for a window, or per window timeslot?)
	Service Type	Enum - Real or Reactive

Information from an FSP to a Network Operator

Message	Field Name	Field Data Type
FSP Acknowledgement		**** In an acknowledgement, an FSP reads back the dispatch message, as it was interpreted/understood. This means that only fields which were recognised and acted on should be "read back" in the acknowledgement.**
	Dispatch status	Enumerated type (e.g. pre-notify, run, RUN NOW, STOP, EMERGENCY STOP)
	NO Dispatch Ref	Unique dispatch reference, namespaced by Network Operator
	Dispatch Unit	Unique reference, namespaced by FSP identity
	Signature	Encoded bytes

		**** To check for new dispatch messages, an FSP client polls the Network Operator. This provides opportunities for future expansion and use by other TWG areas, such as for declaration of availability, or reporting metering data. This is not within the scope of current work, and would be a future API revision.** ****The below information is the minimum expected from an FSP in a heartbeat message to enable interoperability of dispatch**
Dispatch Poll	Network Operator ID	Unique ID, from a well-known list of network operators
	FSP ID	Unique ID, as defined by the Network Operator to the FSP
	Authentication Parameters	As required and defined by the standard

Visit our website to find out more about Open Networks

Energy Networks Association
4 More London Riverside
London SE1 2AU
t. +44 (0)20 7706 5100

w. energynetworks.org
@EnergyNetworks

The voice of the networks