

# Flexibility Digital Infrastructure

## System Use Case exercise

### Icebreaker One Response

December 2023, Version 2.0

#### Notes:

- This copy of a doc is hosted independently of govt and contents do not represent govt policy
- Deadline 19th Jan for feedback

*Disclaimer: The materials in this Template comprise Ofgem's current thinking around a Flexibility Digital Infrastructure (FDI). This Template is purely an information gathering exercise to enable a more informed discussion on FDI governance and technical design. It is not an indication of any minded-to positions on an FDI in Ofgem's Future of Distributed Flexibility workstream.*

## Contents

1.	SUC Template for BUC.4	3
	Brief introduction to IB1, Trust Frameworks and Open Energy	3
	Technical approach recommendations	3
	FDI vs DSI vs Trust Framework	3
	Trust Framework Features	4
	DSI Features	4
	Trust Framework & DSI Operation as part of BUC 4	5
2.	SUC Template for BUC.2	11

Version	Date	Author(s)	Notes
2.0	4 <sup>th</sup> December 2023	Ofgem	Emailed to participants.

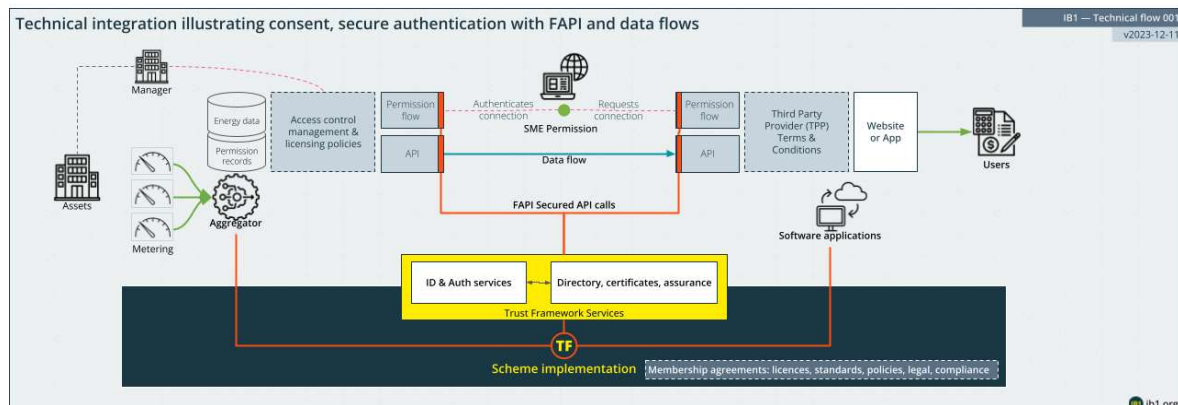
## 1. SUC Template for BUC.4

Please use this template (based on [IEC standards](#)) to set out your SUC proposals which deliver the BUC narrative and KPIs, and address the scenario provided above. You may find the [PlantUML website](#) tool useful for making sequence diagrams (tutorial seen [here](#)), but diagrams created in Word/PowerPoint (or equivalent) are entirely acceptable.

Narrative of the System Use Case
<p>Short description</p> <p><i>Written description of your SUC implementation of the BUC. Describe the SUC operation and what new/existing systems are involved and what system functions are used to deliver the BUC. Describe any aspects of the BUC narrative or KPIs or scenario that your SUC implementation does not meet. Optionally, please also include any overall architectural diagrams.</i></p> <p><b>Brief introduction to IB1, Trust Frameworks and Open Energy</b></p> <ul style="list-style-type: none"> <li>• IB1 is not a tech vendor</li> <li>• We promote a common approach to designing and implementing trusted data ecosystems to build confidence, accelerate rollout, and ultimately decarbonise sectors of the economy more quickly. We call these ecosystems <a href="#">Trust Frameworks</a>.</li> <li>• We led the 2+-year project to co-create the <a href="#">Open Energy Trust Framework</a> alongside industry stakeholders</li> <li>• Our technical approach is informed by Open Banking             <ul style="list-style-type: none"> <li>◦ Identity and authorization implemented with Financial-Grade API (FAPI)-compliant OpenID</li> </ul> </li> <li>• Consequently our response in this document is less about the implementation of the features of the Flex market, and more about how the market is governed and its operation is trusted by participants. This manifests itself in the technical architecture by being more about the “arrows between boxes” than the “boxes”.</li> </ul> <p><b>Technical approach recommendations</b></p> <ul style="list-style-type: none"> <li>• Distributed systems scale and adapt more quickly</li> <li>• Data is exchanged peer-to-peer - trust is managed separately from data &amp; services</li> <li>• Open standards encourage innovation</li> <li>• Metadata describing data and services, and their licence terms, should be openly available so potential participants can assess the cost and effort required to integrate</li> </ul> <p><b>FDI vs DSI vs Trust Framework</b></p> <ul style="list-style-type: none"> <li>• Our response characterises three layers of functionality that come into play within the business use cases             <ul style="list-style-type: none"> <li>◦ Open Energy Trust Framework features</li> <li>◦ Data Sharing Infrastructure features</li> <li>◦ Flex digital infrastructure features</li> </ul> </li> <li>• In our thinking, FDI is a “Scheme” within the Open Energy Trust Framework             <ul style="list-style-type: none"> <li>◦ Member organisations register at a TF level and are verified</li> <li>◦ They request to participate in the FDI Scheme</li> <li>◦ They execute contracts at the TF and Scheme level</li> <li>◦ They are provided capabilities (roles and scopes) within the FDI scheme</li> </ul> </li> <li>• We think that there are elements of the Flex BUCs beyond those already noted in BUC1/BUC1.1 that could be implemented with DSI or as general TF capabilities rather than as Flex-specific</li> </ul>

## Trust Framework Features

pto



The diagram above illustrates the role of the Trust Framework in a scenario where meter data (on the left) is being shared, with permission from the meter owner, with a Third Party Provider (on the right). Note this is not the FDI use case - just an example use case to show where the TF is involved.

One a technical level, the Trust Framework has the following components:

- Member organisation management (managed by TF operator - including KYC)
- Scheme management (managed by TF or scheme operator - organisations register at a TF level but are granted capabilities at a scheme level)
- (Optionally) Contract execution workflow - for the TF and, if required, on joining schemes
- Organisation user management (including KYC)
- Organisation scheme assignment (by TF operator)
  - Organisation capabilities (permitted roles and scopes) within scheme assignment
- MTLS client certificate issuance with claims
  - Claims selected from permitted roles and scope assigned to the org in the scheme
- Financial Grade API (FAPI)-compliant OpenID Identity Server
  - Certificate introspection for client certificates
  - Push access requests
- FAPI-compliant OAuth2 authorisation server
  - Support for “code id\_token” OAuth flow
- Public registry of member organisations
  - Contact info
  - Organisation ID in the TF
  - Scheme membership
  - Data and service catalogues in DCAT format
  - Organisational assurance level
- Public registry of licences
  - Scheme membership
  - Scheme scopes covered
- Data and service monitoring
- Member and end-user customer services

## Features

As currently envisaged, the DSI is likely to add the following technical features or relevance to FDI:

- Service architecture for Data Preparation Nodes (DPNs host APIs & apps that send or receive data on the infrastructure)

- FAPI-compliant APIs as part of the Open Energy TF
- Security and access control
- Local logging and monitoring
- Data schema checking
- (Optional) Data & metadata hosting
- DSI Services
  - Registering DPNs
  - DPN service monitoring
  - Data catalogue
  - Transaction logging & auditing
  - Repository of permitted schemas

## Trust Framework & DSI Operation as part of BUC 4

### User verification and uploading commercial information:

1. First time User, FSP-1, has their organisation verified by the system (or systems).
  - Consider how FSP-1 will verify who they are to the system.

**Trust Framework:** Organisations register and are assigned roles as part of TF/Scheme onboarding. The FDI should consider what is necessary for KYC and subsequent enforcement, auditing, and issue resolution.

2. The system issues a unique identifier (ID) associated with FSP-1's organisation.
  - Consider how issuing multiple unique IDs will be avoided if FSP-1 tries to register again.
  - If multiple systems are able to issue unique IDs, consider how IDs remain coordinated and unique across multiple systems.

**Trust Framework:** Organisations can have only one ID. Roles and claims are provided as part of client certificate issuance. OpenID identity tokens include the ID and the issuer, ensuring uniqueness (federation mechanisms ensure federated identity servers - issuers - cannot have duplicate IDs). It's unlikely that FDI will need federated servers.

3. FSP-1 provides relevant commercial information using their unique ID.
  - Consider how FSP-1 will understand if their commercial information is relevant, compliant and necessary.

### FDI Feature

4. FSP-1 configures relevant data- and entity- assurance agreements (defined in BUC.1/1.1 and BUC.8).
  - Consider how the assurance agreements can be operationalised, using FSP-1's defined user rights (see KPIs) and wider permissions logic, based on the unique IDs provided by the system.
  - Consider how FSP-1 will configure assurance agreements via the interfacing with the system.

**Trust Framework:**

1. Provides a standard mechanism for associating organisations (like FSPs) with roles and permitted scopes and generating signed certificates for their applications to assert their claims.
2. Provides a standard mechanism for service providers to publish the licence terms (access conditions and purposes) for their services.
3. Leaves it to service providers to implement the access controls they publish

#### **Searchable directory:**

5. FSP-1 searches directory of other users to identify MO-1, MO-2 and MO-3 IDs and express interest in market exploration.
  - Consider how permissions-based secure messaging channels for user notifications could be enabled by the system.

**Trust Framework:** Publishes directory of participating organisations with roles & permitted scopes

**FSI:** Implements messaging channels (I don't think they're planned as a DSI feature either)

#### **Commercial interoperability across markets:**

6. The system provides MO-1, MO-2, and MO-3 a means for accessing pre-authorised shared FSP-1 data used for initiating the Registration stage.
  - Consider how controls on the commercial information MOs are authorised to access could be introduced.
  - If multiple systems are able to issue unique IDs, consider how MOs know which system the FSP information is held on.

**FSI:** A few possible mechanisms here: a required FAPI-secured API on the FSP (more complex but scalable). A FAPI-secured central service for registered FSPs (single point of failure but reduces complexity for FSPs).

7. FSP-1 is notified of further action needed on their behalf to then initiate contractual agreements.

**Trust Framework:** Ideally contractual agreements would standardised for FSPs and MOs as part of the scheme design. So participation as a FSP in the FSI scheme on the Trust Framework would include all the contractual agreements necessary. This means no additional bilateral contracts are needed between MOs and FSPs, allowing FSPs to participate in multiple MOs without friction.

#### **Seamless integration with BUCs:**

8. The system is able to seamlessly use and integrate all user unique ID outcomes (described in Steps 1-7) into the system used to deliver BUC.2 (Common Asset Registration) and wider BUCs.

**Trust Framework:** This is provided as part of the identity service

**FDI:** Consider operational elements of monitoring etc e.g.

- Market-specific technical assurance of registered endpoints
  - Availability
  - Correctness of metadata for FDI participation\

○ ...

- Market-specific logging of correct operation
- Market-specific redress mechanisms

[illegible]



**Diagram(s) of the Use Case**

*Please include sequence diagram(s) working through the scenario steps to show how they are implemented in the SUC proposed.*



## 2. SUC Template for BUC.2

Please use this template (based on [IEC standards](#)) to set out your SUC proposals which deliver the BUC narrative and KPIs, and address the scenario provided above. You may find the [PlantUML website](#) tool useful for making sequence diagrams (tutorial seen [here](#)), but diagrams created in Word/PowerPoint (or equivalent) are entirely acceptable.

Narrative of the System Use Case
<p>Short description</p> <p><i>Written description of your SUC implementation of the BUC. Describe the SUC operation and what new/existing systems are involved and what system functions are used to deliver the BUC. Describe any aspects of the BUC narrative or KPIs or scenario that your SUC implementation does not meet. Optionally, please also include any overall architectural diagrams.</i></p> <p>We don't see any specific role for the Trust Framework in this use case, but there are potential features of the DSI that may be considered - noted below. Where we haven't commented, we consider the feature to be purely FDI functionality.</p> <p><b>Asset validation and registration</b></p> <ol style="list-style-type: none"> <li>1) FSP-1 provides asset data to the system (or systems).             <ol style="list-style-type: none"> <li>a. Consider how the system is integrated with the system(s) necessary to deliver common user registration (BUC.4) outcomes for FSP-1.</li> <li>b. Consider how the system can 'signpost' the necessary data requirements until pre-qualification, for a given MO.</li> <li>c. Consider how interactions across multiple potential data access points (i.e. asset owners, installers) or databases (i.e. technology vendors, existing FSP or MO registries) will be supported.</li> </ol> </li> <li>2) The system validates the technical parameters for the data provided by FSP-1.             <ol style="list-style-type: none"> <li>a. Consider how validation using multiple trusted asset databases (e.g. OEM cloud platforms) will be handled.</li> <li>b. Consider how assets can demonstrate valid data (e.g. by virtue of existing participation in flexibility markets) and circumvent/expedite this step.</li> <li>c. Consider how validation of planned assets could be supported.</li> </ol> </li> </ol> <p><b>DSI: For 1&amp;2</b> The DSI will have standards for asset schemas. Whether they are necessary or useful to the FDI is unclear at this stage.</p> <ol style="list-style-type: none"> <li>3) The system validates the contractual parameters (i.e. right to operate for a given period) for the data provided by FSP-1.             <ol style="list-style-type: none"> <li>a. Consider how the system could surface data needed to reconcile conflicting contractual claims by multiple FSPs to the asset and ensure only one operator for it at a given moment.</li> </ol> </li> <li>4) The system registers the validated data to the dedicated asset record, ensuring each asset has a unique identifier.             <ol style="list-style-type: none"> <li>a. Consider how the unique asset ID paradigm would be maintained should another Registered User, FSP-n, attempt to provide data for an existing validated asset.</li> </ol> </li> </ol>

- b. If multiple systems are used throughout steps 1-4, consider how 4a can reliably be achieved.
- 5) The system confirms the registration of validated data with FSP-1.
  - a. Consider how FSP-n is then notified of attempted duplicated asset registration.

**Asset record accessed by MOs:**

- 6) Registered Users MO-1, MO-2 and MO-3 are able to access the registered asset data for use in their procurement systems.
  - a. Consider how FSP-1 could be notified if a given market operator, MO-n, accesses data of an asset that they operate.
  - b. If multiple systems are used throughout steps 1-5, consider how MO-n identifies and accesses the system that the registered data is held on.

**DSI:** Data access logging is anticipated to be a feature of the DSI. It may be sufficient or be enhanced for the FDI. Or the FDI's requirements may be sufficiently different that it has its own mechanisms.

**Asset record updated by FSPs:**

- 7) FSP-1 provides updated asset data to the system.
  - a. Consider how interactions across multiple potential data access points (i.e. asset owners, installers) or other databases (i.e. technology vendors, existing FSP or MO registries) will be supported.
  - b. Consider how the system would handle a situation where FSP-1 and FSP-n provide updated asset data simultaneously? Consider how the system would reconcile divergent asset data provided simultaneously?
  - c. If multiple systems are used for asset validation and registration, consider how the unique asset ID paradigm would be maintained if an asset was updated from a different access point than was originally registered from.

**Unexpected system downtime:**

- 8) The system faces unexpected downtime during a process such as validation and registration of FSP-n.
  - a. Consider what measures need to be in place for data recovery and system resilience?
  - b. If multiple systems are being used and they have technical interdependencies, consider what additional features need to be in place.,

**DSI:**

- Non-repudiation (proof that requested data was received) is being considered as a core DSI feature
- Resilience is a key design tenet of the DSI

**Seamless integration with BUCs:**

- 9) The system is able to seamlessly use and integrate all of user common asset registration outcomes (described in Steps 1-8) into the system used to deliver wider BUCs.



**Diagram(s) of the Use Case**

*Please include sequence diagram(s) working through the scenario steps to show how they are implemented in the SUC proposed.*

