Data Communications Company

Future Service Management

Consultation on the transitional and enduring regulatory changes

Issued: 23 January 2025
Respond by: 17:00 on 6 March 2025
Contact: consultations@smartdcc.co.uk
Classification: DCC Public

Table of Contents

1. Background and context

1. This consultation sets out and seeks your views on the regulatory approach to the delivery of the Future Service Management (FSM) Programme. It sets out the regulatory changes required to support the delivery of the replacement tool for the current DCC Service Management System (DSMS), including:

   - Changes to User access and identity management for the new platform, including the introduction of multi-factor authentication (MFA)
   - Enabling an improved process for Anomaly Detection Threshold (ADT) and other file submissions
   - Aligning Order Management System (OMS) functionality with the Self-Service Interface (SSI)

2. It also sets out the changes needed for the transitional arrangements, including the migration of data onto the new platform and the activities and testing Users will be required to undertake before they can access this.

3. We are seeking your responses to the questions set out in this consultation by **17:00 on Thursday 6 March 2025**.

1.1. The FSM Programme

4. The DSMS is a critical part of DCC's infrastructure, used to track and resolve issues across the smart metering network. Customers use DSMS to request DCC services, raise incidents, and access reporting and diagnostics information. This system handles a high volume of activity, with around 25,000 separate requests or incidents raised through it each month. The current DSMS service is supported under the existing Data Service Provider (DSP) contract.[1] However, the tool on which the DSMS is currently built is now coming to the end of its life and so a new tool is required to mitigate service and security risks to the smart meter network.

5. The FSM Programme was initiated in June 2023 to competitively procure and implement a replacement tool ahead of the new DSP service commissioning in 2026. The scope of this programme is to:

   - Replace the existing scope of DSMS including the SSI and the Self Service Management Interface (SSMI);
   - Replace the underlying Service Management tool which is used by the DCC Service Desk; and
   - Incorporate OMS capabilities, including the ordering of 4G Communications Hubs (CHs) and the returns of all Smart Metering Equipment Technical Specifications 2+ (SMETS2+) CHs.

6. The current DSMS service is built upon a BMC Remedy platform, which is an IT Service Management tool. The support contract for Remedy is due to expire in October 2025 and DCC is working to procure a new platform as a replacement for the existing DSMS. Following it being recommended by all bidders during our procurement exercise, DCC has selected ServiceNow as the platform to be used for FSM. ServiceNow is a flexible cloud-based 'software as a service' tool offering several Service Management aspects either 'out-of-the-box' or via configuration or customisation.

7. DCC has concluded to include the OMS functionality for 4G CHs within scope of the FSM Programme, leveraging the same ServiceNow solution as for Service Management. The 4G OMS will therefore be delivered through the replacement tool at the same time, replacing the existing

[1] The DSP and other services delivered under the data services contract sit right at the heart of the smart metering infrastructure.by providing data services that connect DCC Users (such as Energy Suppliers, Network Operators and Other Users) to Devices at their consumers' premises.

solution. Any future technologies would also be incorporated into the ServiceNow solution in the same way. DCC has also concluded to include the functionality to return all SMETS2+ CHs within the scope of the programme. Please note that the existing OMS solutions for ordering 2G/3G and long-range radio (LRR) CHs will not be replaced within this programme. Each will instead be retired independently in the future as they reach their final dates for ordering the respective products.

8. In addition to replacing the tool, DCC is intending to retire the use of User Interface (UI) DCC Key Infrastructure (DCCKI) personnel certificates to access the DSMS and replace them with MFA. MFA is a widely used and trusted approach to authenticating the person logging in to a site by requiring them to provide two or more pieces of evidence (for example entering a password, using a security token or authenticator device, or using biometrics).

1.2. Approach to regulatory change

9. DCC needs to identify and set out any regulatory changes which correspond with any changes to the current arrangements required to deliver the new FSM platform. The Joint Industry Plan (JIP) for FSM includes a key milestone which requires DCC to have concluded on the detailed regulatory changes required for FSM no later than 30 March 2025. This consultation sets out DCC's view on the regulatory changes required, and our conclusions on this consultation will form the conclusions required by this JIP Milestone, which we are planning to publish by 25 April 2025. We note that our planned publication date is after the current date of the JIP Milestone. On 18 December 2024, DCC was directed to produce an updated delivery plan for the FSM Programme and is planning to issue its consultation on this in February 2025. We will be consulting on a revised date for this JIP Milestone as part of that separate consultation.

10. DCC has developed the proposed amendments to the SEC Subsidiary Documents (SSDs) which are required to deliver the FSM solution. No material changes are required to the main body of the SEC (the SEC Sections) to deliver this solution. However, DCC has identified some consequential changes to the main body of the SEC that would be beneficial to make in response to the SSD changes. These proposed amendments are also included in this consultation, and there will be no parallel consultation issued by the Department for Energy Security & Net Zero (DESNZ) (the Department).

11. The changes to the SEC Subsidiary Documents will be delivered following Direction from the Department using powers under Condition 22 of the Smart Meter Communications Licence and SEC Section X 'Transition'. As the main body changes are consequential changes only, the Department considers the changes to the main body of the SEC can be delivered under the provisions of Licence Condition 22.30 and SEC Section X5.6, rather than needing to be enacted by the Secretary of State using the powers conferred under Section 88 of the Energy Act 2008.

1.3. Industry engagement to date

12. DCC engaged with the industry (including DCC Users) during the competitive procurement via a series of workshops and with Smart Energy Code (SEC) Panel and Sub-Committees between March and June 2024. It used this engagement to understand DSMS users' business needs and the features and functionality that they would like to see in the new solution. Users ratified that DCC needed to deliver a modern and secure Service Management System which is easy for customers to use and allows for maintenance and future growth. It was agreed that the toolset should enable improvements and automation whilst meeting customers' existing needs, including having regard to the existing SEC requirements for the DSMS.

13. The initial engagement involved working with customers to identify pain points for existing users by conducting deep dives and learning sessions to understand user needs for a Service Management tool. Users considered the high-level problem statements and scope and were supportive of the overall approach, provided that the core functionality of the DSMS was

protected. Additionally, customers were supportive of updating the SEC where necessary to keep the solution as close to the out-of-the-box tool as possible to drive optimal cost benefits.

14. DCC shared the business requirements with the Operations Group (OPSG) and the Technical Architecture & Business Architecture Sub-Committee (TABASC), both of which were initially comfortable that the business needs identified would be achieved. They also agreed that DCC would set up a working group which consisted of a small group of DSMS users from Supplier Parties and Network Parties (known as the Service Management Working Group (SMWG)).

15. The SMWG supported DCC in understanding how the current tool works from customers perspective and how they would use the new solution by prioritising any customisations of the tool according to users' needs. DCC reviewed over 50 configurations and customisations to ServiceNow and presented these to the SMWG. It asked the group to score each potential customisation on benefit, risk and criticality for DCC to understand a full picture of implementing any potential customisation. The outcomes of these sessions were presented monthly into governance at OPSG and TABASC meetings, and the DCC delivered an industry wide briefing session to inform customers of the proposals and gather feedback on user impact and any costs associated with the proposals. In addition to the SMWG, DCC also held a working group for the security-based configurations and customisations and highlighted the need for potential changes to the SEC.

16. DCC's assessment and the outputs of the SMWG and the security working group were presented back to the SEC Panel and its Sub-Committees in June and July 2024. Overall, the industry was supportive of the outcomes from this work. This engagement has informed the solution that DCC is taking forward. For most areas that were discussed with the industry, it was agreed that the solution should include configurations or small customisations to meet current SEC provisions.

17. However, to provide benefits to DCC and users by modernising Service Management and access to a Service Management System, DCC has identified a small number of SEC changes that would be needed. It is proposing to introduce the following changes to the SEC:

- Changes to User access and identity management: DCC is intending to retire the use of User Interface (UI) DCC Key Infrastructure (DCCKI) personnel certificates and replace them with MFA. UI DCCKI certificates are only used for accessing SSI and SSMI and have no other use or purpose under the SEC. Additionally, these are separate to Enterprise Information Integration (EII) and Infrastructure Key Infrastructure (IKI) DCCKI certificates, which are not affected by the FSM solution. The changes for this are summarised in Section 2.1 of this document.

- Enable improved process for ADT and other file submissions: DCC is developing a simplified process to allow a user to attach an ADT file directly within a service request and utilise a workflow to process it. This would remove the current manual process using SharePoint. This process also relates to Quarantine Command Action files and could also be extended to other file upload requests. The changes for this are summarised in Section 2.2 of this document.

- Aligning OMS functionality with SSI: DCC is also intending to incorporate OMS functionality within the scope of FSM. Specifically, this will cover the ordering of 4G CHs (and any later products) and the returns of all SMETS2+ CHs (both existing 'legacy' CHs and 4G CHs). Consequently, the access rules for OMS user security will need aligning with those for SSI. Please note that the existing OMS platforms for existing 2/3G and LRR CHs will be left as-is and will continue to operate until such time that those types of CHs are no longer able to be ordered. Consequently, there are also some small wording changes within the SEC documentation to better accommodate the new processes as well as the legacy processes. The changes for this are summarised in Section 2.3 of this document.

1.4. Scope and structure of this consultation

18. This consultation seeks your views on the proposed changes to the SEC Subsidiary Documents to support the delivery of the FSM Programme:

    - Section 2 of this consultation document sets out our proposed changes to the SEC (both main body and subsidiary documents) to deliver the enduring arrangements. These changes have been grouped and discussed by the topic areas set out in section 1.3 above. The redlined changes to each affected document are available in Attachments 1-15.
    - Section 3 of this consultation document sets out our proposed changes to SEC Appendix AU 'Network Evolution Migration & Transition Approach Document' (NETMAD) covering the transitional arrangements during the delivery of the FSM Programme. The redlined changes to the NETMAD are available in Attachment 16.

19. This consultation also seeks your views on the proposed designation dates for these changes. Section 4 of this consultation document sets out the proposed dates and the rationale for this.

20. Section 6 of this consultation document lists the questions that we seek your views on and how you can respond to this consultation.

21. This consultation is expected to impact all SEC Parties that use the DSMS or that use the OMS for 4G CHs.

22. This consultation will close at **17:00 on Thursday 6 March 2025**. Following this, DCC will provide a report to the Department by 25 April 2025 containing its consideration of the responses and its conclusion on the regulatory changes required for the FSM Programme. We will publish this conclusions document on the DCC website.

2. Enduring regulatory changes for FSM

23. This section sets out the areas of the FSM solution where we consider SEC changes will be needed to deliver the enduring solution. These have been grouped by topic area. A summary of all the proposed changes listed by document can be found in Appendix A.

24. DCC takes seriously its objectives of continually improving service to our customers whilst also driving down the costs incurred from doing so (which are ultimately recharged to those customers). Service Desk best practice is to enable customers to efficiently 'self-serve' as far as possible. We believe the FSM solution can both substantially improve existing self-serve processes, and progressively enable self-service to customers for more processes or interactions that have historically used manual processes such as email or SharePoint file transfers.

25. Therefore, throughout the changes detailed under the following topics or sections, we have endeavoured to make small improvements to procedures which follow this principle. You will observe such details within the SEC drafting, even where they may not always be called out in this summary document.

26. Furthermore, DCC proposes that the SSI should become the primary tool for all interaction with DCC support services and that alternative means such as email and voice calls shall be limited only to cases where Users are unable to access or correctly use the SSI. In such cases, DCC's support shall be targeted upon resolving the access or usage issue, and the User shall be expected to submit any other matter via the standard service request, incident or other methods provided within the SSI.

27. As part of this, DCC is aiming to use the SSI when it contacts Users. This is reflected in proposed minor wording changes to various workflows where we have amended references to how DCC should contact Users. If notifications are made via SSI, then a User could be allowed to choose

whether it wants to receive email notifications (or other methods that may be added in the future). Alternatively, it may want to simply see any incidents or notifications within the SSI itself, which may be more convenient if it uses the SSI frequently. One important consequence of allowing Users to make this choice is that DCC would consider that it has met any obligation it has to notify a User if it has created the relevant transaction or event in SSI, regardless of whether the User has chosen to leave email notifications enabled or has disabled them. We seek your views on this as part of this consultation.

28. SEC Modification Proposals MP239 'Enduring Solution for Resolving SMETS2 Device Certificate Misalignment Issue'[2] and MP246 'DCC User access to metadata via the DCC Self-Service Interface (SSI)'[3], which have been approved for implementation in the June 2025 SEC Release, will affect the SSI. DCC will be accounting for these changes in the FSM solution. The only SEC document that these modifications and the FSM changes both affect is SEC Appendix AH 'Self-Service Interface Access Control Specification'. As these modifications are due to be implemented before the changes for FSM, DCC has drafted the changes to Appendix AH against the current baseline updated for the changes that will be made by these two modifications.

2.1. Changes to User access and identity management

29. The FSM solution will introduce MFA as the mechanism for enabling user access to the FSM platform. This will require multiple changes from the current arrangements:

- The scope of the DSMS (including SSI) and the OMS will be combined into a single ServiceNow platform
- The DCCKI User Interface personnel certificate mechanism will be replaced with MFA
- An ID and Access Management Platform will be introduced that will be suitable for Single Sign-On (SSO) across multiple DCC systems
- A consolidated role/access/authorisation function will also be created, which will be suitable to support SSO at a later date
- Secure Internet-based access will be enabled for Parties that do not have DCC Gateway connections

30. Each of these areas are discussed in more detail in the following subsections, summarising the technical changes, the implications of these on users, and the areas of the SEC that will need updating to enable this.

2.1.1. SSI and OMS consolidation

31. The current SSI and OMS functionality will be implemented as modules within a single ServiceNow platform. This will enable users to use a single account to access one or both areas (as their permissions allow) via a single portal.

Changes to the SEC

32. **SEC Appendix H** 'CH Handover Support Materials' includes the details around the OMS accounts through which users access the service. These will need to be updated to align with the new accounts on the FSM platform.

33. **SEC Appendix AH** sets out the requirements for accessing SSI and authentication of users. This will need to be updated to clarify the scope of SSI will include the OMS.

[2] MP239 'Enduring Solution for Resolving SMETS2 Device Certificate Misalignment Issue' - Smart Energy Code
[3] MP246 'DCC User access to metadata via the DCC Self-Service Interface (SSI)' - Smart Energy Code

2.1.2. Replacing DCCKI UI certificates with MFA

34. MFA will be introduced as the method for authenticating the user logging in to an account. MFA is a widely used and trusted approach to authenticating the person logging in to a site by requiring them to provide two or more pieces of evidence (for example entering a password, using a security token or authenticator device, or using biometrics). It is already used elsewhere in the industry, for example when logging in to the Switching Portal under the Retail Energy Code (REC).

35. The most popular form of MFA is for a user to confirm their identity using an authenticator app. The FSM solution will formally support Microsoft Authenticator, and DCC recommends this tool. However, we understand that Users may already have other authenticator apps or have other preferences. As such, DCC proposes to also support one or two further authenticator apps on a best-efforts basis (i.e. it will test that SSI works with these and provide some customer support for any basic queries, but it cannot take any responsibility if there are complex or fundamental issues with those apps). Other authenticator apps will also be allowed and should also be compatible, but DCC will not provide any formal support for these, and their use will be entirely at the User's risk. In all cases, DCC cannot accept liability should an authenticator app not work as it should, and any recourse for Users would be directly towards the providers of those applications. We are seeking views from respondents on this approach, including views on what specific apps you would like DCC to support.

36. If a user cannot or does not have an authenticator app, or it fails to work on an occasion, the platform will support other mechanisms such as receiving a one-time password via email or SMS or using a phone-based validation.

37. The introduction of MFA means that DCCKI UI certificates will no longer be needed, as these are only used for accessing SSI. Therefore, DCCKI administration tokens will be revoked and retired. Consequently, administrators and users will no longer need to manage these certificates. To be clear, only DCCKI UI certificates will be removed; all other types of DCCKI certificates will be unaffected by the FSM solution and will continue to be used and managed as they are today.

Changes to the SEC

38. The MFA mechanisms will be included in **SEC Appendix AH** and **Appendix AI** 'Self Service Interface Code of Connection'. Changes within these two documents are quite substantial, due to the degree of change within the underlying technologies and methods, but in summary:

- Text relating to UI DCCKI Certificates has been removed, including the relationship with SEC Appendix W 'DCCKI Registration Authority Policies and Procedures'. This includes removing the dependency upon Appendix W for the process to create Organisational Administrators.
- New content has been added which sets out the technical details on establishing and supporting MFA will be included in a supporting 'Code Required Document', referred to as the 'DCC Internet Access Policy'. This document is then referred to in various contexts within Appendices AH and AI. The intention here is for the policy to contain more specific technical details which are expected to be maintained to keep track with evolving technology industry developments, e.g. new authentication techniques, product changes etc. without requiring further changes to the SEC documents (please note that changes to this policy will be subject to industry consultation and SEC Panel approval – see below).

39. **SEC Appendix S** 'DCCKI Certificate Policy', **Appendix T** 'DCCKI Interface Design Specification', **Appendix V** 'DCCKI Code of Connection and DCCKI Repository Code of Connection' and **Appendix W** 'DCCKI Registration Authority Policies and Procedures' are part of the 'DCCKI Document Set' which contains all the provisions relating to the DCCKI. All references to DCCKI UI certificates will be removed from these Appendices. Note that only DCCKI UI certificates are being removed, and references to all other types of DCCKI certificate will be unchanged.

40. **SEC Appendix W** will also be updated to remove the process for establishing Organisation Administrators for SSI and DCCKI UI tokens, as this is being reimplemented in the SSI as noted above.

41. The new DCC Internet Access Policy will be a SEC required document that will be owned by DCC. Any changes that DCC proposes to this will need to be consulted upon with the industry before being approved by the SEC Panel (the Panel may choose to delegate this responsibility).

42. We have attached an early draft of the DCC Internet Access Policy to this consultation, to provide context on what this will contain – you can find this in Attachment 17. The details of this policy are still being developed, and a further consultation on this will be issued in due course to seek your views on this once it has been completed. This policy will then need to be approved by the SEC Panel before it comes into effect, which will be required to happen before the start of User Integration Testing (UIT).

2.1.3. ID and access management platform and SSO

43. The FSM solution will change the platform on which the SSI is built, from Remedy to ServiceNow. As part of this change, the ID and access management platform will change from the existing DSP Entrust platform, which will be retired, to Microsoft Entra. This change provides a platform for other elements of the solution. The new platform also has the capability for integration with other DCC systems beyond ServiceNow in the future.

44. The DCC's use of Microsoft Entra potentially introduces a new connectivity requirement for users, which is that they need to allow access for a standard Microsoft login page, ideally via the internet. This will involve users allowing the Microsoft URLs. If there are any header injection or tenant restrictions, then the two FSM tenants (assuming production and non-production access is required) will need to be put on the allowed lists. We consider that it is preferable for organisations to be able to provide the connectivity to Microsoft via their own internet (or other) routes. If an organisation is not able or willing to do this, then DCC may be able to provide an alternative solution, which we are currently developing. To help us establish whether such an alternative is needed, we are seeking your feedback on this matter via this consultation.

45. As DCC has developed the detailed design of the FSM solution, it has identified that the ability to federate the authorisation (validating what someone can do, directly within their own corporate ID management systems) is more complicated than anticipated and would at best require a large amount of customisation. DCC has confirmed this is the case with all leading identity provider products and that it is not specific to the one selected for FSM. The product being utilised within the FSM programme will allow the federation of authentication (validating who you are), but this will need setting up and configuring for each User. As this feature is available now but has never been taken up, we are proposing removing the federation ability as part of these changes. If there is future demand, DCC will look to bring it in via a SEC Modification Proposal, during which we will be able to confirm the costs to set up individual parties and the process for billing them for this.

46. The ID and access management platform being utilised for the FSM solution will also enable SSO to all DCC Services which are integrated with it. This will incorporate ServiceNow and the new 4G OMS, and then later will include SharePoint and the incoming Reporting tool. Any future services would also look to use the same identity. DCC is working to identify the best date for the delivery of the future integration of SharePoint, to ensure it does not incur costs on the existing platform now that would need to be repeated when the SharePoint sites are migrated in the future.

47. Meanwhile, DCC is also looking across the full scope of usage of SharePoint to identify opportunities where a migration of content or purpose to ServiceNow would provide a better experience for users. As part of the FSM programme DCC is moving some high-traffic processes to ServiceNow, such as Nominated Contacts and the ADT file management process (see section 2.2 below for more details of this) alongside investigating the possibility to move some other processes either for the launch of FSM or at a later date. This will also be supported by the

migration of all knowledge held within the 'Information for SEC Parties' site from SharePoint into a central location accessible through ServiceNow.

48. DCC acknowledges the desire from Users for a single sign-on experience across DCC systems. We expect to share a more detailed plan for how we will deliver this with the industry in the first quarter of 2025. We also welcome views from respondents to this consultation on any further benefits Users may want DCC to deliver on the FSM platform in the future.

Changes to the SEC

49. **SEC Appendices AH and AI** set out the requirements for accessing the SSI and authentication of users. This will be updated to reflect the changes to the login and account management approach arising from this change.

50. Removing the alternative Identity Provider Service element (i.e. the federation) means that much of the technical detail underlying authentication can be managed solely within the DCC's service provision and need not be presented within the SEC itself. Specifically, this means we can remove most of the detail around Security Assertion Markup Language (SAML), leaving only the key concepts such as the need for a user to allow a token to be placed into their browser.

2.1.4. Consolidating accounts and roles across DCC

51. Currently, SSI users are provided access to features based on the Job Type Roles that they are assigned. Each organisation has one or more Administration Users approved by DCC, who can create, change and delete other user accounts within their organisation. The FSM solution will simplify this process in two ways:

- Removal of DCC validation of changes to non-administrator roles: Currently, any changes to a user's assigned role by an administrator need to be validated by DCC. This step will be removed for the creation of new user accounts or changes to most roles assigned to an existing account. This is because DCC would not know if the change to a user's role is valid or not, and so its validation of the change provides no value. The exception is the creation of or change to an administration or other senior role (of which we anticipate more varieties in the future), which will continue to need to be validated by DCC. These roles will now be managed within the SSI platform, including new procedures and workflows to support a self-serve request with additional DCC validation.
- Simplification of assignable roles: The current SSI is set up to provide access to systems and features to each user based on the role that they are assigned by the DCC. These roles and the systems each gives access to is documented in SEC Appendix AH. With OMS being added to the platform, the number of roles will need to increase. Furthermore, the systems or features needed by a given role may vary from one organisation to another. Therefore, the roles approach will be simplified such that an administrator will simply give access to the relevant systems or features a given user account requires.

52. This change in structure also has the potential to be built upon further and expanded to other parts of the DCC systems. However, that is outside the scope of the FSM Programme. Any such proposals to expand upon this functionality will be progressed and consulted upon via separate projects in the future.

Changes to the SEC

53. **SEC Appendix AH** currently contains the rules relating to Business Functional Domain specifications and SSI Job Type Role definitions. These will be removed from Appendix AH and moved to a 'Code Required Document' sitting underneath this Appendix called the '**SSI Functions and Roles Policy**'. This will enable changes to these low-level details (e.g. the addition of new functions) to be progressed and approved in a more streamlined approach than via the SEC Section D 'Modification Process' mechanism. Appendix AH will be updated to refer to this document and its governance.

54. The initial version of this Policy will comprise slightly amended versions of the Business Functional Domain and Job Type Roles tables from the existing Appendix AH. Amendments will cover new roles to support OMS, and some small refinements to other roles to reflect slight differences in the way that ServiceNow will provide functionality versus how the legacy SSI provides it. It will also include the procedures and processes for creating all roles, including the more senior roles such as Organisational Administrator. As we progress, we anticipate that a few additional Job Type Roles may be created to support other functions or processes which are not currently provided within SSI, but which could be better provided in this manner in future.

55. This new SSI Functions and Roles Policy will be a SEC required document that will be owned by DCC. Any changes that DCC proposes to this will need to be consulted upon with the industry before being approved by the SEC Panel (the Panel may choose to delegate this responsibility).

56. The details of the initial version of this document are dependent on the final detailed design of the FSM solution, which is still in development. We have attached an early draft to this consultation, to provide context on what this will contain – you can find this in Attachment 18. A further consultation on this will be issued in due course to seek your views on this once this has been fully developed. This policy will then need to be approved by the SEC Panel before it comes into effect, which will be required to happen before the start of UIT.

2.1.5. Enabling internet access

57. The incorporation of OMS into ServiceNow (see section 2.3 below) will require some Parties that don't currently access SSI to be able to do so in the future. Currently, SSI is accessed via a DCC Gateway connection only, but some smaller Parties won't have such a connection, having instead procured a third-party provider to carry out the associated activities that would require one in their stead. The FSM solution will enable these users to be able to access the OMS functionality within ServiceNow. Furthermore, the choice of Microsoft Entra as the Identity Provider Service platform requires user personnel to access a Microsoft URL to authenticate. DCC will therefore configure both ServiceNow and Microsoft Entra to be accessible via the internet.

58. DCC intends that the internet connectivity to ServiceNow should only be used by Parties that do not have a DCC Gateway connection which can be used for such purpose. As such, we will be including requirements for Parties with a DCC Gateway connection to only access the ServiceNow platform via this connection.

59. For Parties wishing to use the Internet option, we will require that they have already registered their desire to use such a connection with DCC, and agree to comply with some basic security measures (e.g. notifying a connection IP address for their outbound connection, which can be whitelisted by DCC). The details will be defined within the new 'DCC Internet Access Policy' introduced in section 2.1.2 above.

Changes to the SEC

60. **SEC Appendix AI** sets out the requirements for connectivity. The rules will be updated to remove the restriction of using a DCC Gateway only and reflect the ability to access ServiceNow via an internet connection.

61. To support this dual connectivity model, and in keeping with a general approach to remove unnecessary technical detail, we will also remove some of the technical details which can reasonably be assumed to be covered by general industry standards (such as server-side TLS support for web browsers) or the broader DCC Gateway connectivity requirements and policy.

2.2. Improved process for ADT and other file submissions

62. The FSM solution will introduce an improved process for handling ADT submissions and quarantine notifications and resolutions. While the use of file signing will remain unchanged, both the submission and the notification processes will be improved through leveraging ServiceNow

functionality. This will result in an improved user experience, reducing manual steps, and will also remove some manual steps within DCC. This should also reduce the overall handling time. In essence, the change will remove the current use of SharePoint in submitting these files, allowing all activity to happen in the ServiceNow workflow.

63. Figure 1 below illustrates the processes for submitting ADT files currently, and as proposed under the FSM solution. The diagram shows the steps carried out by the User in red, with a single purple step performed by DCC. The DCC step comprises approximately ten lower-level steps today, which will reduce by about half under the proposed solution, providing further benefit.

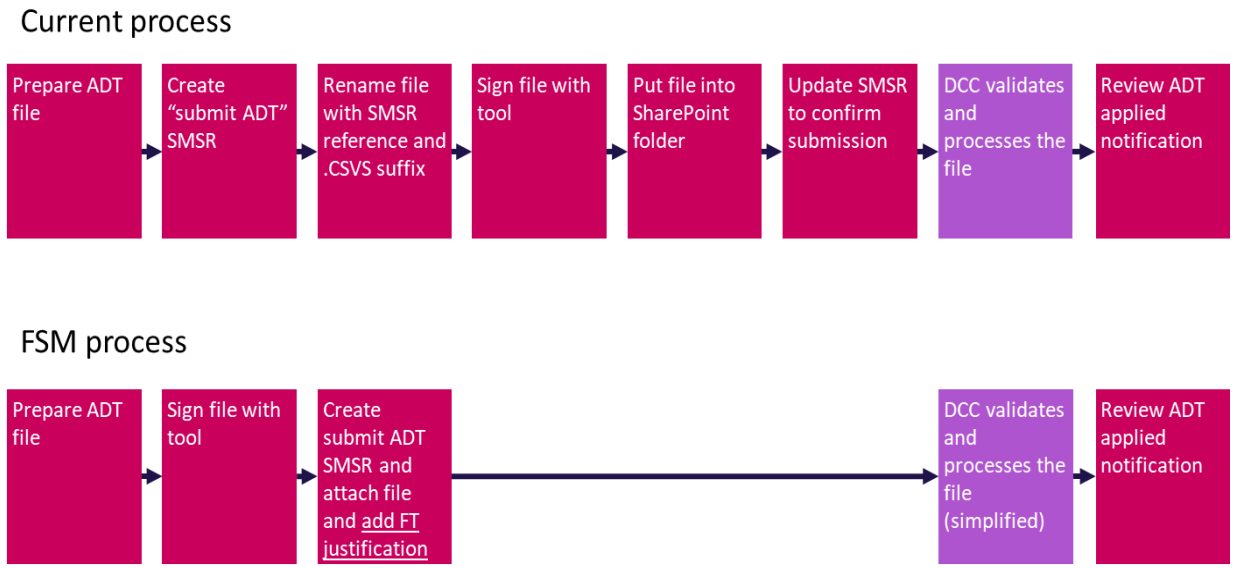

Figure 1: Comparison of existing and proposed steps for submitting ADT files

64. This approach illustrated for ADT files would also be followed for Quarantine Command Action files, with only the DCC step varying behind the scenes. For quarantine files, the workflow begins with DCC raising an incident and assigning this to the relevant User, which then leads to this file process in response. That basic workflow is not proposed to change, but we have proposed some minor edits in the SEC drafting to clarify and align wording and slightly simplify the steps to complete the procedure.

65. DCC will also follow the same approach for submission of other file types, whereby a file is attached directly within a Service Management Service Request, instead of placed in SharePoint. Many of these other processes are not explicitly defined in the SEC, so we do not need to make further changes specifically in relation to them. However, we have taken the opportunity to amend all other references to using SharePoint for transferring files in any context to allow for the alternative option of using the SSI. This will enable individual processes to be improved in due course without requiring a further set of SEC changes.

66. DCC has also reviewed the usage of quarantine files and concluded that this usage is very low. Early feedback from Users is that the time it takes them to release messages means the auto delete timeout would have already triggered by the time they access these. As such, many Users already have workarounds to resend these messages. DCC is therefore investigating whether to remove the ability to release quarantine files from the FSM solution, which would simplify the solution and reduce the delivery cost. Quarantine files would still be created, and Users would still receive an alert that a file had been quarantined so they would be aware this had happened. However, Users would not be able to request these be released. The creation of quarantine files would then be removed from the new DSP solution (although alerts would still be provided). We are seeking feedback from Users on this proposal as part of this consultation to inform whether we take this forward. If Users support this, we will develop and consult on this change separately.

Changes to the SEC

67. **SEC Appendix AA** 'Threshold Anomaly Detection Procedures' details the procedures for ADTs, including where ADTs have been exceeded, and the requirements for quarantined communications. The processes set out in this document will be updated to reflect the above revised process for submitting files. We have also restructured these sections slightly to better align the phrasing across the quarantined file scenarios.

68. SEC **Appendix D** 'SMKI Registration Authority Policies and Procedures', **Appendix H**, **Appendix J** 'Enduring Testing Approach Document', **Appendix K** 'SMKI and Repository Test Scenarios Document', **Appendix R** 'Common Test Scenarios Document' and **Appendix W** will be amended to replace references to the use of SharePoint in transferring information to or from DCC. In most cases we have simply substituted a phrase similar to "via the DCC's delivery method of choice (as from time to time specified on the SSI)" to allow future flexibility. However, in some cases where the broader workflow is specifically within the SSI then we have simply stated that it shall be used.

2.3. Aligning OMS functionality with SSI

69. The FSM solution will incorporate the OMS functionality relating to the ordering of 4G (and later) CHs and the return of all SMETS2+ CHs (both legacy and 4G). Integrating these features into the ServiceNow platform will provide users with a comprehensive self-service capability across the entire CH lifecycle. Through the platform, users will be able to directly action the following activities:

- Submit CH forecasts
- Create and confirm CH orders and manage tolerance exceptions for all future CHs
- Track consignments
- Amend and confirm CH deliveries
- Manage delivery acceptance and rejection
- Initiate in-life returns
- Manage return management acceptance (RMA) and track the delivery of returned CHs
- Monitor the progress of returns, including visibility of any triage activities

Changes to the SEC

70. **SEC Appendix H** details the provisions of forecasting, ordering and delivery of CHs to Suppliers and to Meter Asset Providers (MAPs). This document will need to be modified to include changes for the new user access, authentication and account profiles within the FSM solution. Key changes include:

- Documenting the new user identification (ID), login and access rules, which will reflect the single sign-on and MFA aspects delivered by FSM
- Small amendments to account profiles to align with the SSI structures and to reflect the enhanced functionality
- Minor changes to some processes to accurately reflect the new self-serve capabilities (for example contacting the Service Desk via the SSI rather than by other means) to reduce delay and manual effort

71. A particular example of the process streamlining is the CH transfer process. This will be redefined to take advantage of the FSM functionality, meaning that Service Requests with defined workflows, status tracking and transparency can be exploited to deliver a more efficient and effective process for all Parties.

72. The existing 'legacy' OMS platforms for forecasting and ordering 2/3G and LRR CHs will not be included in the FSM solutions and will be left as-is. These platforms will continue to operate until such time that these types of CHs are no longer able to be ordered. As such, Appendix H will need to retain the rules for these platforms. Therefore, Appendix H will contain text which is worded to cater for both the continued use of these two 'legacy' ordering systems and for the new 4G solution within the SSI. Please also note that the number of OMS Accounts provided to each Party at no additional charge will remain unchanged at four per Region.

73. Additionally, we are proposing some minor housekeeping edits to correct minor points or errors which affect both the legacy and the new solutions. The aim is to maintain consistency between them as far as practicable to minimise any User confusion.

74. **SEC Appendix I** 'CH Installation and Maintenance Support Materials' details the provisions for returning CHs to DCC. The FSM solution incorporates the current SEC requirements for CH returns of all types, using the SSI. Key changes being proposed include:

- Small amendments to account profiles to align with SSI structures and to reflect enhanced functionality
- Minor changes to the returns processes to accurately reflect the new self-serve capabilities (for example communicating with the Service Desk via the SSI tool rather than by other means) to reduce delay and manual effort
- Changes to utilise SSI in respect of CH Transfers

75. **SEC Section F** 'Smart Metering System Requirements' will also require a small consequential change within Section F6A to reflect the use of SSI for CH Transfers.

76. Please note that the changes within this consultation do not include any changes related to proposed SEC Modification Proposal MP252 'Amending the process for Communications Hub returns'[4], which will proceed according to the SEC Modification Process. Some of the changes required for that modification would be enhancements to the changes proposed here, so the FSM design will provide some of the underlying capability required.

3. Transitional arrangements for FSM

77. Delivering the FSM solution will require some transitional and migration activities to be carried out by DCC and by Users. The provisions for these will be set out in the NETMAD. This section summarises the transitional and migration activities needed for the FSM Programme. A summary of all the proposed changes listed by document can be found in Appendix A.

3.1. Migrating SSI user account data

78. DCC will migrate all SSI user accounts from the current DSMS platform to the new FSM platform. The data that will be included in this migration will be:

- Foundation data from DSMS
- All historical and active Service Desk tickets from DSMS
- All historical and active CH returns data from DSMS
- All historical and active CH orders and associated records from the interim OMS for 4G CHs
- User identity data from the existing DCC Identity Provider Service (Entrust IDP)

[4] MP252 'Amending the process for Communications Hub returns' - Smart Energy Code

79. DCC will transfer all user accounts to the ServiceNow platform, irrespective of whether a user is still considered to be active or not. This is to ensure data integrity by allowing all historical records to be associated with the user that raised that request.

80. For each User organisation, Administration Users will be given early access to an instance of the new SSI, in which they will be able to see and manage all the individual user accounts ('SSI Accounts') for their User IDs. All these accounts will be marked as inactive. The Administration User will be expected to review each account and determine whether it should be reinstated, and if so what access permissions (Job Type Roles) it should be assigned. This process will ensure that individual SSI Accounts are ready to be utilised by the User Personnel as soon as the new FSM platform goes live. The process for doing this is contained within **SEC Appendix AU** (the NETMAD) and will be supported by user training and user guide materials that will be provided nearer to go-live.

81. DCC will set up a series of online training sessions in the weeks prior to the start of UIT. These sessions will cover topics including how to navigate the FSM platform, how to raise and review an Incident, and how to raise and review a Service Management Service Request. Users will not be required to attend these sessions, but if they do then they should contact DCC to request to join a given session, and DCC will be able to add them to the invite.

82. Over the subsequent weeks until the cut-over to the new FSM, DCC will take one or more incremental snapshots of the user account data in the live environment and incorporate these into the data in the new FSM environment. Administrators will then be able to revise the affected accounts to complete the preparation at or before the final cut-over.

3.2. User testing to access the FSM platform

83. DCC has reviewed lessons learnt from when the previous SSI was introduced. One notable lesson was the number of Users with limited understanding of how to use the system, leading to many issues arising at go-live.

84. As a mitigation, DCC will be enhancing the User Entry Process Testing (UEPT) process to include additional tests related to logging in to the new platform (including using MFA), raising and updating Incidents, managing user credentials, and testing the basic OMS functionality. New Users will need to complete this testing as part of UEPT before they will be able to access the ServiceNow platform. These new tests have been included in **SEC Appendix R**.

85. DCC also considers that all existing Users will need to complete this additional testing before they can access the ServiceNow platform. This additional testing is intended to give both DCC and Users the confidence that at FSM Go-Live Users will be able to access the new platform and will know how to use it effectively. This will mitigate the risk of a potential overload of requests for User support during the early days of FSM, which could adversely impact all Users. Therefore, the scope of additional testing is also included with **SEC Appendix AU**.

86. Any existing Users that have not completed this testing by the FSM Go-Live date, and therefore would not be eligible to access the ServiceNow platform, will still be able to raise Incidents via email or telephone. DCC will review the existing Users that have not completed this testing and the potential volume of Incidents they may raise as part of its go/no-go decision. If this number is materially high, DCC may choose to delay go-live to mitigate the impact on operations that would arise from the anticipated increase in the number of telephone calls or emails that the Service Desk would need to manage.

4. Designation of the SEC changes

87. The enduring FSM solution will be delivered in a 'big bang' approach on the Go-Live date. At that point, the existing DSMS will be deactivated and the ServiceNow platform will be activated. The enduring changes to the SEC have all been drafted on the basis they will be implemented on Go-Live to reflect this replacement taking effect.

88. We are therefore proposing that, subject to the timely receipt of DCC's conclusions report on this consultation, the Department will designate the enduring SEC changes on 25 October 2025, or as soon as reasonably practicable within one month thereafter as a contingency measure if required. A draft direction for the designation of the SEC documents can be found in Appendix B of this consultation document.

89. The transitional measures set out in the NETMAD will need to be delivered sooner, to enable these to be effective during the transition period. The earliest transitional activity listed in the NETMAD would need to be completed by the start of June 2025, six weeks prior to UIT commencing, and so this is the latest date by when the NETMAD changes would need to be implemented. However, there is no reason these changes cannot be delivered sooner.

90. We are therefore proposing that, subject to the timely receipt of DCC's conclusions report on this consultation, the Department will designate the changes to the NETMAD on 1 May 2025, or as soon as reasonably practicable within one month thereafter as a contingency measure if required. A draft direction for the designation of the SEC documents can be found in Appendix C of this consultation document.

5. Next steps

91. Following the closure of this consultation, DCC will assess respondents' views and amend the draft SEC changes as required. DCC will then submit an amended version of these documents to the Department that it considers suitable for designation by the Secretary of State.

92. DCC is aiming to provide a report to the Department by no later than 25 April 2025. This report will contain DCC's consideration of the responses to this consultation as well as the proposed updated version of the SEC changes and the proposed date for the designation of these. DCC will publish its conclusions document on its website.

6. Consultation questions and how to respond

93. We are seeking your views on the following questions:

Q1	Do you agree with DCC's proposed amendments to the SEC documents to reflect the changes to User access and identity management being delivered under the FSM solution, as set out in section 2.1? *Please provide any comments you may have on the proposed changes and your rationale for your views*
Q2	Do you agree with DCC's proposed amendments to the SEC documents to enable the improved process for ADT and other file submissions, as set out in section 2.2? *Please provide any comments you may have on the proposed changes and your rationale for your views*

Q3	Do you agree with DCC's proposed amendments to the SEC documents to align the OMS functionality with SSI, as set out in section 2.3? *Please provide any comments you may have on the proposed changes and your rationale for your views*
Q4	Do you agree with DCC's proposed amendments to the NETMAD for the transitional activities, as set out in section 3? *Please provide any comments you may have on the proposed changes and your rationale for your views*
Q5	Do you agree with DCC's proposed approach to relocating detail currently contained in SEC Appendices to the supporting 'SSI Functions and Roles Policy' and 'DCC Internet Access Policy' Code Required Documents, which would be subject to a lighter governance approach to approving updates? *Please provide your rationale for your view*
Q6	Do you agree with DCC's intention that all routine activities, including service requests, incident creation/updates etc, should occur via the SSI, and that email or telephone queries should only be supported for resolving issues related to accessing the SSI? *Please provide your rationale for your views*
Q7	Do you agree with DCC's intention that all DCC contact with and responses to Users should occur via the SSI? As part of your response, we seek your views on whether Users should be allowed to disable email notifications for new notifications within SSI. *Please provide your rationale for your views*
Q8	Do you agree with DCC's proposed approach to MFA set out in section 2.1.2? As part of your response, we also seek your views on which option(s) you expect to use and, if you plan to use an authentication app, whether there is one that you prefer *Please provide your rationale for your views*
Q9	Do you agree with DCC's proposed connectivity requirement set out in section 2.1.3? As part of your response, we would also appreciate your explicit response on whether your organisation can provide the requisite access to Microsoft, or would require DCC to offer an alternative solution for you *Please provide your rationale for your views*
Q10	Do you agree with DCC's proposal to allow internet access to SSI set out in section 2.1.5, including the restriction to allow only parties who do not have a DCC Gateway option and which have been whitelisted? *Please provide your rationale for your views*
Q11	Do you agree that DCC should further develop and consult on its proposal to remove the ability to release quarantined files from the FSM platform set out in section 2.2? *Please provide your rationale for your response*

Q12	Are there any further benefits that you believe DCC should deliver on the FSM platform in the future? *Please provide your rationale for your views*
Q13	Do you agree with the proposed redesignation date for the enduring changes of 25 October 2025 (or as soon as reasonably practicable within one month thereafter)? *Please provide your rationale for your views*
Q14	Do you agree with the proposed redesignation date for the NETMAD of 1 May 2025 (or as soon as reasonably practicable within one month thereafter)? *Please provide your rationale for your views*

94. Please provide responses using the attached response form by **17:00 on Thursday 6 March 2025** to DCC at consultations@smartdcc.co.uk.

95. Consultation responses may be published on our website (smartdcc.co.uk). Please state clearly in writing whether you want all or any part of your consultation to be treated as confidential. It would be helpful if you could explain to us why you regard the information you have provided as confidential. Please note that responses in their entirety (including any text marked confidential) may be made available to the Department and the Gas and Electricity Markets Authority (the Authority). Information provided to the Department or the Authority, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004). If the Department or the Authority receive a request for disclosure of the information, we/they will take full account of your explanation (to the extent provided to them), but we/they cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

96. If you have any questions about this consultation, please contact us at consultations@smartdcc.co.uk.

7. Attachments

97. This consultation includes 19 attachments (Attachments 1-18 are provided in a single zip folder):

- Attachment 1: Proposed changes to SEC Section A for FSM
- Attachment 2: Proposed changes to SEC Section F for FSM
- Attachment 3: Proposed changes to SEC Appendix D for FSM
- Attachment 4: Proposed changes to SEC Appendix H for FSM
- Attachment 5: Proposed changes to SEC Appendix I for FSM
- Attachment 6: Proposed changes to SEC Appendix J for FSM
- Attachment 7: Proposed changes to SEC Appendix K for FSM
- Attachment 8: Proposed changes to SEC Appendix R for FSM
- Attachment 9: Proposed changes to SEC Appendix S for FSM

- **Attachment 10:** Proposed changes to SEC Appendix T for FSM
- **Attachment 11:** Proposed changes to SEC Appendix V for FSM
- **Attachment 12:** Proposed changes to SEC Appendix W for FSM
- **Attachment 13:** Proposed changes to SEC Appendix AA for FSM
- **Attachment 14:** Proposed changes to SEC Appendix AH for FSM
- **Attachment 15:** Proposed changes to SEC Appendix AI for FSM
- **Attachment 16:** Proposed changes to SEC Appendix AU for FSM
- **Attachment 17:** Outline version of the DCC Internet Access Policy
- **Attachment 18:** Outline version of the SSI Functions and Roles Policy
- **Attachment 19:** Consultation response template

Appendix A –Summary of SEC changes for FSM

This table summarises the key changes described in sections 2 and 3 of this document, listed by SEC document, and the part of this document where this is covered in more detail.

SEC document	Proposed changes	Section
Section A 'Definitions and Interpretations'	Addition of new definitions used across multiple Appendices Amendment or removal of existing definitions to reflect the changes in the Appendices	-
Section F 'Smart Metering System Requirements'	Consequential amendment to reflect the use of SSI for CH Transfers	2.3
Appendix D 'SMKI Registration Authority Policies and Procedures'	Amendment of references to 'SharePoint' to enable delivery of files via SSI	2.2
Appendix H 'CH Handover Support Materials'	Update details around OMS Accounts to align with the SSI Accounts on the FSM platform	2.1.1
	Amendment of references to 'SharePoint' to enable delivery of files via SSI	2.2
	Updates for the new user access, authentication and account profiles approach, including the new user ID, login and access rules, which will reflect the single sign-on and MFA aspects delivered by FSM	2.3
Appendix I 'CH Installation and Maintenance Support Materials'	Updates to account profiles to align with SSI structures and to reflect enhanced functionality Updates to the returns processes to reflect the new self-serve capabilities	2.3
Appendix J 'Enduring Testing Approach Document'	Amendment of references to 'SharePoint' to enable delivery of files via SSI	2.2
Appendix K 'SMKI and Repository Test Scenarios Document'	Amendment of references to 'SharePoint' to enable delivery of files via SSI	2.2
Appendix R 'Common Test Scenarios Document'	Amendment of references to 'SharePoint' to enable delivery of files via SSI	2.2
	Inclusion of new UEPT tests for accessing and using the SSI	3.2
Appendix S 'DCCKI Certificate Policy'	Removal of text related to UI DCCKI Certificates	2.1.2
Appendix T 'DCCKI Interface Design Specification'	Removal of text related to UI DCCKI Certificates	2.1.2

SEC document	Proposed changes	Section
Appendix V 'DCCKI Code of Connection and DCCKI Repository Code of Connection'	Removal of text related to UI DCCKI Certificates	2.1.2
Appendix W 'DCCKI Registration Authority Policies and Procedures'	Removal of text related to UI DCCKI Certificates Removal of the process for establishing Organisation Administrators for SSI	2.1.2
	Amendment of references to 'SharePoint' to enable delivery of files via SSI	2.2
Appendix AA 'Threshold Anomaly Detection Procedures'	Updates to reflect the revised process for submitting ADT files	2.2
Appendix AH 'Self Service Interface Access Control Specification'	Updates to clarify the scope of SSI will include the OMS	2.1.1
	Removal of text related to UI DCCKI Certificates, including removing the dependency upon Appendix W for the process to create Organisational Administrators Updates to set out the technical details on establishing and supporting MFA via the 'DCC Internet Access Policy'.	2.1.2
	Updates to reflect the changes to the login and account management approach and the removal of the alternative Identity Provider Service	2.1.3
	Delegation of the rules relating to business functional domain specifications and SSI role definitions to sit in the 'DCC Functions and Roles Policy'	2.1.4
Appendix AI 'Self Service Interface Code of Connection'	Removal of text related to UI DCCKI Certificates, including removing the dependency upon Appendix W for the process to create Organisational Administrators Updates to set out the technical details on establishing and supporting MFA via the 'DCC Internet Access Policy'.	2.1.2
	Updates to reflect the changes to the login and account management approach and the removal of the alternative Identity Provider Service	2.1.3
	Updates to remove the restriction of using a DCC Gateway only and reflect the ability to access ServiceNow via an internet connection	2.1.5
Appendix AU 'Network Evolution Transition & Migration Approach Document	Requirements for DCC to migrate data from the current DSMS and OMS to the FSM platform Process for Users to activate and review user accounts ahead of Go-Live Requirement for DCC to provide training to Users	3.1
	Requirement for Users to undergo additional User testing to be eligible to access the FSM platform	3.2

Appendix B –Draft direction text for the enduring changes

This appendix contains the text that the Department plans to use for the approval of the enduring changes to the SEC for FSM.

This direction is made for the purposes of the smart meter communications licences granted under the Electricity Act 1989 and the Gas Act 1986 (such licences being the "DCC Licence") and the Smart Energy Code designated by the Secretary of State pursuant to the DCC Licence (such code being the "SEC").

Words and expressions used in this direction shall be interpreted in accordance with Section A (Definitions and Interpretation) of the SEC.

Pursuant to Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code) of the SEC, the Secretary of State directs that, with effect from 25 October 2025:

- The SMKI Registration Authority Policies and Procedures previously designated and incorporated into the SEC as Appendix D;
- the CH Handover Support Materials previously designated and incorporated into the SEC as Appendix H;
- the CH Installation and Maintenance Support Materials previously designated and incorporated into the SEC as Appendix I;
- the Enduring Testing Approach Document previously designated and incorporated into the SEC as Appendix J;
- the SMKI and Repository Test Scenarios Document previously designated and incorporated into the SEC as Appendix K;
- the Common Test Scenarios Document' previously designated and incorporated into the SEC as Appendix R;
- the DCCKI Certificate Policy previously designated and incorporated into the SEC as Appendix S;
- the DCCKI Interface Design Specification previously designated and incorporated into the SEC as Appendix T;
- the DCCKI Code of Connection and DCCKI Repository Code of Connection previously designated and incorporated into the SEC as Appendix V;
- the DCCKI Registration Authority Policies and Procedures previously designated and incorporated into the SEC as Appendix W;
- the Threshold Anomaly Detection Procedures previously designated and incorporated into the SEC as Appendix AA;
- the Self Service Interface Access Control Specification previously designated and incorporated into the SEC as Appendix AH; and
- the Self Service Interface Code of Connection previously designated and incorporated into the SEC as Appendix AI

are hereby re-designated and incorporated in the form set out in Annex [XX] to this direction.

Pursuant to Condition 22 of the DCC Licence and Section X5 of the SEC, the Secretary of State also directs that, with effect from 25 October 2025, SEC Section A 'Definitions and Interpretations' and SEC Section F 'Smart Metering System Requirements' are hereby modified in the form set out in Annex [XX] to this direction to incorporate the consequential amendments arising from the above redesignations.

For the avoidance of doubt such re-designation of these documents shall be without prejudice to anything done under the DCC Licence or the SEC on or after these documents being re-designated, or the continuing effectiveness of anything done in these documents prior to their re-designation (which shall have effect as if done under the re-designated document).

This direction is also being notified to the SEC Administrator.

Appendix C –Draft direction text for the NETMAD

This appendix contains the text that the Department plans to use for the approval of the NETMAD changes for FSM.

This direction is made for the purposes of the smart meter communications licences granted under the Electricity Act 1989 and the Gas Act 1986 (such licences being the "DCC Licence") and the Smart Energy Code designated by the Secretary of State pursuant to the DCC Licence (such code being the "SEC").

Words and expressions used in this direction shall be interpreted in accordance with Section A (Definitions and Interpretation) of the SEC.

Pursuant to Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code) of the SEC, the Secretary of State directs that, with effect from 1 May 2025 the Network Evolution Transition and Migration Approach Document (NETMAD) previously designated and incorporated into the SEC as Appendix AU is hereby re-designated and incorporated in the form set out in Annex [XX] to this direction.

For the avoidance of doubt such re-designation of the NETMAD shall be without prejudice to anything done under the DCC Licence or the SEC on or after this document being re-designated, or the continuing effectiveness of anything done in this document prior to its re-designation (which shall have effect as if done under the re-designated document).

This direction is also being notified to the SEC Administrator.