Data Communications Company

# Future Service Management

## DCC conclusions on the code required documents

**Date: 25 September 2025**
**Author: consultations@smartdcc.co.uk**
**Classification: DCC Public**

# Table of Contents

# 1. Background and context

1. The purpose of this document is to conclude the Data Communication Company's (DCC's) recent consultation on the new and updated documents required by the Smart Energy Code (SEC) to support the delivery of the Future Service Management (FSM) Programme.[1]

2. DCC has previously consulted on the transitional and enduring changes to the SEC that are required to deliver the FSM solution.[2] The changes to the SEC introduce two new 'code required documents' and require updates to the existing SSI Baseline Requirements Document to align this to the solution being implemented by the FSM Programme. SEC Appendix AU 'Network Evolution Transition and Migration Approach Document' (NETMAD) requires the changes to these documents for the FSM solution to be consulted upon by DCC and approved by the SEC Panel by 3 November 2025.

## 1.1. The FSM Programme

3. The DCC Service Management System (DSMS) is a critical part of DCC's infrastructure, used to track and resolve issues across the smart metering network. Customers use the 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.[3] However, the tool on which the DSMS is currently built is now coming to the end of its life and a new solution is required to mitigate service and security risks to the smart meter network.

4. The FSM Programme was initiated in June 2023 to competitively procure and implement a replacement tool ahead of the new DSP service commencing in 2028. The scope of this programme is to:

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

5. 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 has procured and is implementing a new platform as a replacement for the existing DSMS. After it was recommended by all bidders during the 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.

6. Following engagement with its customers, DCC decided 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 solution. Any future technologies could also be incorporated into the ServiceNow solution in the same way. DCC has also decided to include the functionality to return all SMETS2+ CHs within the scope of the programme. Please note that the existing OMS solutions

[1] FSM consultation on the code required documents | Smart DCC
[2] FSM conclusions on the transitional and enduring regulatory changes | Smart DCC
[3] 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.

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.

7. 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 multi-factor authentication (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). Customers indicated that the DCCKI certificates were not user friendly, and that MFA would both be more secure, and easier for users.

8. Finally, DCC is developing a simplified process to allow a user to attach an Anomaly Detection Threshold (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. This will reduce or remove some manual steps and result in an improved user experience.

## 1.2. Consultation responses and next steps

9. The consultation, which ran from 1 August 2025 to 29 August 2025, sought views on:

- The new SSI Functions and Roles Policy, which will set out in detail the structure and definition of Job Type Roles within the SSI;
- The new DCC Internet Access Policy, which will set out the procedure to be followed before a User will be able to access the SSI via the internet, including technical details and rules that the User must continue to comply with; and
- An updated version of the SSI Baseline Requirements Document, to reflect the solution being delivered by the FSM Programme.

10. A summary of the comments received and DCC's responses to these are set out in Section 2 of this document. DCC has made some updates to the code required document drafting that it consulted upon, and its conclusions on this are set out in Section 3 of this document.

11. Changes to these documents require the approval of the SEC Panel following consultation with the industry. As such, DCC submitted these documents to the SEC Panel for approval at its meeting on 23 September 2025.

# 2. Analysis of responses

12. DCC received three responses to this consultation: one from a Large Supplier, one from the SEC Panel and one from the SEC Operations Group (OPSG).

13. DCC has analysed the feedback provided. This section sets out an overview of the responses received to this consultation and DCC's response.

## 2.1. Question 1

14. DCC sought views on the proposed drafting for the new SSI Functions and Roles Policy.

| | |
|---|---|
| **Q1** | Do you agree with the proposed SSI Functions and Roles Policy for the FSM Programme? |

### Respondent views

15. Two respondents were supportive of the proposed changes, with one of those respondents welcoming the clarity this document provided. The third respondent provided no view on this question.

16. One respondent stressed the importance of ensuring that changes to user roles and workflows are supported by clear guidance and training, as this would help to avoid operational disruption for Parties who would be required to adapt internal processes.

17. One respondent noted they would require more than one administrator role for their organisation and sought clarity on whether they would be able to create more administrators or if DCC would be able to create more on their behalf.

### DCC response

18. DCC notes that clear guidance on the new roles and functions is contained in the SSI Functions and Roles Policy. DCC will also be providing full training and guidance on the new functions and roles as part of the training awareness sessions, training material and guidance being provided ahead of FSM go-live, which will all be made available on a secure remote location. DCC will be providing training first for User Integration Testing (UIT), and then for go live. Supporting drop-in sessions will also be available during the transition period. There will also be 'tours' available in the system to support users with the various processes. Training is scheduled to begin in early November 2025 and will continue until after FSM go-live.

19. DCC can confirm that it will create one administration role for each organisation on the new platform. That user will then be able to create as many additional administration roles for their organisation as they require, and it will be up to them to do so.

20. DCC has not made any changes to the proposed SSI Functions and Roles Policy drafting in response to the comments received on this question.

## 2.2. Question 2

21. DCC sought views on the proposed approach set out in the SSI Functions and Roles Policy whereby DCC would not provide any validation for changes made by administrators to their organisation's SSI user accounts.

| | |
|---|---|
| Q2 | Do you agree that, except for the set-up of an organisation's initial administration account, DCC will not provide any validation for changes to any accounts made by administration users? |

### Respondent views

22. Two respondents were supportive of the proposed approach, with one of those respondents agreeing that each organisation's administrators should be accountable for the changes needed to user accounts and roles. The third respondent provided no views on this question.

23. One respondent recognised DCC's rationale for this and agreed that activities should not be duplicated once accounts are established. However, they highlighted that the risks associated with misconfigured accounts needed to be managed. They considered this would require appropriate training, clear accountability, and proportionate audit arrangements to give Parties confidence in the process.

24. One respondent welcomed the ability to be able to download reports on the frequency and last login for each of their organisation's user accounts. They asked if additional fields could be added to an account, such as department or line manager.

### DCC response

25. As noted above, DCC can confirm that a full suite of training and support will be provided to Users on the new FSM platform. Please see paragraph 18 above for full details. DCC can also confirm that any changes made by an administration user will be subject to audit and logging arrangements and will be managed according to the Security Management Plan.

26. Administration users will be provided with the facility and visibility to be able to manage their user base. Users will not be able to add fields to user accounts (noting that this feature is also not available to users in Remedy).

27. DCC has not made any changes to the proposed SSI Functions and Roles Policy drafting in response to the comments received on this question.

## 2.3. Question 3

28. DCC sought views on the proposed drafting for the new DCC Internet Access Policy.

| | |
|---|---|
| Q3 | Do you agree with the proposed DCC Internet Access Policy for the FSM Programme? |

### Respondent views

29. Two respondents supported the introduction of this policy and the principle of controlled access. The third respondent provided no views on this question.

30. One respondent stressed that the operational impact for Users must be carefully considered. They considered that internet-based access and MFA would represent a significant change for many Parties, and adequate training, support and phased migration would be essential to ensure security objectives are met without causing disruption.

31. One respondent suggested that DCC should also recognise Google Authenticator as an approved option for MFA.

### DCC response

32. As noted above, DCC can confirm that a full suite of training and support will be provided to Users on the new FSM platform. Please see paragraph 18 above for full details. Regarding phased migration, there will be no dual-running period between the new FSM platform and the current DSMS system, and therefore this is not possible. DCC will complete as much preparatory work as possible in advance of go-live to de-risk this.

33. DCC recommends that users use Microsoft Authenticator due to the close and extensive proven integration with Microsoft Entra. However, users are free to use their preferred authenticator applications, such as Google Authenticator. Please note that all authenticator applications sit outside the DCC estate; any support will be provided on a reasonable endeavours basis and ultimately the support will sit with the provider of the application. This has been clarified in the DCC Internet Access Policy.

## 2.4. Question 4

34. DCC sought views on the intended approach set out in the DCC Internet Access Policy that connecting to the SSI via the internet would only be made available to Users without a DCC Gateway Connection.

| | |
|---|---|
| Q4 | Do you agree with the position that internet connectivity should only be made available to Users without a DCC Gateway Connection? |

### Respondent views

35. One respondent agreed with DCC's position, provided clear communication was given to Users and that no legitimate operational use cases were excluded. They considered that where exceptions emerge (e.g. where contingency arrangements require internet-based access in parallel with a Gateway Connection), these should be considered on a case-by-case basis.

36. One respondent disagreed with DCC's position. They considered that each DCC User organisation should have the choice of using an application programming interface (API) or 'hard-wired link', depending on their organisation's needs and expected future usage requirements.

37. The third respondent noted that not all users can access SSI via their DCC Gateway Connection, and suggested DCC consider users also being allowed to connect via the internet. As an example, a User's call centre teams may not be in or have access to the same premises as the DCC User System which makes use of the DCC Gateway Connection. Users may also wish to segregate their Smart Metering System (SMS) operational traffic to their SSI traffic.

### DCC response

38. The feedback received from respondents concurs that if there are valid use cases for internet access for DCC Gateway Parties then this should be permissible. Legitimate use cases have also been identified in the feedback. DCC has therefore updated the DCC Internet Access Policy to reflect the position that requests by DCC Gateway Parties for internet access to the SSI will be considered on a case-by-case basis. DCC highlights that using a DCC Gateway Connection is the preferred option that it would advise users to use. This adheres to the 'secure by design' security principle, whereby if the business use case does not justify it then the most secure option must be used.

## 2.5. Question 5

39. DCC sought views on the authentication methods and security controls set out in the DCC Internet Access Policy.

| | |
|---|---|
| **Q5** | Do you agree with the authentication methods and security controls that are set out in the DCC Internet Access Policy? |

### Respondent views

40. All three respondents were broadly supportive of the proposed authentication methods.

41. One respondent noted it would be important that these controls are implemented consistently and that Users are given adequate time and support to adapt for these. They considered that the balance between security and useability must be carefully managed to avoid unintended barriers to access. Another respondent noted they would need support from DCC to ensure the change in authentication remains as robust as under the current arrangements.

42. One respondent repeated their request that Google Authenticator should be added as an approved option for MFA.

### DCC response

43. The balance between useability and security were the key factors DCC applied in defining this approach. DCC has adopted a quick, easy and useable authentication mechanism in MFA that most users will be familiar with (e.g. from banking applications). MFA is an industry standard for authentication and is deemed sufficiently robust by industry security experts and the Security Sub-Committee (SSC). As noted above, DCC can confirm that a full suite of training and support will be provided to Users on the new FSM platform. Please see paragraph 18 above for full details.

44. As noted above, DCC recommends the use of Microsoft Authenticator, but users are free to use other authentication applications, such as Google Authenticator. Please see paragraph 33 above for full details.

45. DCC has not made any changes to the proposed DCC Internet Access Policy drafting in response to the comments received on this question.

## 2.6. Question 6

46. DCC sought views on the proposed updates to the SSI Baseline Requirements Document.

| | |
|---|---|
| Q6 | Do you agree with the changes to the SSI Baseline Requirements Document for the FSM Programme? |

### Respondent views

47. One respondent supported the changes but emphasised the importance of aligning these with the wider FSM implementation. In particular, the respondent noted the introduction of the new code required documents and the updates to the NETMAD needed to be synchronised to ensure clarity for Parties and support a smooth transition.

48. One respondent disagreed. They considered there to be missing details on the CH ordering & forecasting and ADT functionality in the baseline requirements, which would need to be added. For example, they sought clarity on whether a user could check the delivery dates and order status in FSM, and whether they could upload ADT files directly into FSM or if these still need to be uploaded via SharePoint.

49. The third respondent provided no views on this question.

### DCC response

50. DCC can confirm that the implementation of the code required documents has been aligned with the wider SEC changes for the FSM Programme. The changes to the NETMAD have already been implemented, which introduced the requirement for DCC to create these documents. These documents will need to be used as part of the subsequent transitional arrangements set out in the NETMAD, and the deadline for their approval was based on when these documents will be subsequently needed.

51. DCC acknowledges the comments on there being details missing from this document. DCC has added additional information to Business Functional Domain (BFD) 04 'Service Audit Trails around uploading ADT files to the new platform and to BFD13 'Forecasting and Ordering' around the OMS functionality. DCC has also added further functional requirements relating to the OMS and the SSI.

# 3. Summary of changes to the documents

52. After reviewing the responses received, DCC has made the following changes to the draft code required documents for the FSM Programme that it consulted on:

- SSI Functions and Roles Policy section 3: Update to BFD04's service capability to clarify that users can upload ADT files directly to ServiceNow.
- DCC Internet Access Policy section 2.1: Update to reflect the position that DCC Gateway Parties may be eligible to access the SSI via the internet, and that such requests will be assessed on a case-by-case basis.

- DCC Internet Access Policy sections 3.2.1 and 4.2.1: Updates to clarify that DCC recommends the use of Microsoft Authenticator but that other authenticator applications can be used and will be supported on a reasonable endeavours basis.
- DCC Internet Access Policy section 4.2.2.1: Update to clarify that the email address used when a user's credentials are set up must be a corporate email address.
- SSI Baseline Requirements Document section 2.1: Update to BDF04 to include additional information around uploading ADT files to the new platform.
- SSI Baseline Requirements Document section 2.1: Update to BDF13 to include additional information on the OMS functionality.
- SSI Baseline Requirements Document section 4.1: Five new SSI functional requirements added in relation to the OMS.

53. The versions of these documents that DCC submitted to the SEC Panel for approval can be found in Attachments 1-3 of this document.

# 4. Next steps

54. DCC is of the view that it has had appropriate engagement and consultation with industry on the code required documents needed for the FSM Programme. As the responses to the consultation and engagement with the industry were broadly supportive of the proposed drafting, DCC has submitted these documents to the SEC Panel for approval.

55. DCC has, where necessary, addressed the comments that have been received from industry. DCC does not believe that the views expressed result in fundamental amendments to the proposed drafting and, as such, further consultation is neither necessary nor appropriate.

# 5. Attachments

56. This document includes three attachments (provided in a single zip folder):

- Attachment 1: Proposed SSI Functions and Roles Policy
- Attachment 2: Proposed DCC Internet Access Policy
- Attachment 3: Proposed changes to the SSI Baseline Requirements Document for FSM