Data Communications Company

Future Service Management

Consultation on the code required documents

Issued: 1 August 2025
Respond by: 17:00 on 29 August 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 following new and updated documents required by the Smart Energy Code (SEC) to support the delivery of the Future Service Management (FSM) Programme:

   - The new Self-Service Interface (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.
   - An updated version of the SSI Baseline Requirements Document, to reflect the solution being delivered by the FSM Programme.

2. We are seeking your responses to the questions set out in this consultation by **17:00 on Friday 29 August 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.[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.

4. 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 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 and DCC has procured a new platform as a replacement for the existing DSMS. Following it being recommended by all bidders during our procurement exercise, DCC 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. The OMS functionality for 4G CHs is included within the 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 would also be incorporated into the ServiceNow solution in the same way.

[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.

The functionality to return all SMETS2+ CHs is also included 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.

7. In addition to replacing the tool, DCC will be retiring the use of User Interface (UI) DCC Key Infrastructure (DCCKI) personnel certificates to access the DSMS and replacing 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).

1.2. Requirement to develop the code required documents

8. DCC has previously consulted on the transitional and enduring changes to the SEC required to deliver the FSM solution, and its conclusions were published on 25 April 2025.[2] The changes to the SEC will be delivered following Direction from the Department using powers under Condition 22 of the Smart Meter Communications Licence and SEC Section X5 'Incorporation of Certain Documents into this Code'.

9. The changes to the SEC introduce two new 'code required documents':

   - The SSI Functions and Roles Policy, which will set out in detail the structure and definition of Job Type Roles within the SSI.
   - The 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.

10. Changes will also be required to the existing SSI Baseline Requirements Document to align this to the solution being implemented by the FSM Programme.

11. SEC Appendix AU 'Network Evolution Transition and Migration Approach Document' clause 11.3 requires DCC to have developed and consulted upon these documents and then have these changes approved by the SEC Panel no later than 20 Working Days prior to the start of User Integration Testing (UIT) for the FSM Programme. UIT is currently scheduled to begin on 1 December 2025, and so these documents need to be approved by the Panel no later than 3 November 2025.

12. In its conclusions on the SEC changes required for the FSM Programme, DCC confirmed that it would develop and consult on the detailed drafting for the two new documents and the updates to the SSI Baseline Requirements Document required for the FSM solution in a further consultation. These documents are the subject of this consultation.

13. Prior to issuing this consultation, DCC presented overviews of the draft documents to the Operations Group (OPSG), the Security Sub-Committee (SSC) and the Technical Architecture & Business Architecture Sub-Committee (TABASC) to inform them on the content and drafting that is being consulted upon.

1.3. Scope and structure of this consultation

14. This consultation seeks your views on the documents set out in section 1.2:

   - Section 2 of this consultation document summarises the new SSI Functions and Roles Policy. The detailed drafting is available in Attachment 1.

[2] FSM conclusions on the transitional and enduring regulatory changes | Smart DCC

- Section 3 of this consultation document summarises the new DCC Internet Access Policy. The detailed drafting is available in Attachment 2.
- Section 4 of this consultation document summarises the changes to the SSI Baseline Requirements Document. The redlined changes to this document are available in Attachment 3.

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

16. This consultation will close at **17:00 on Friday 29 August 2025**. Following this, DCC will provide the responses received to this consultation and the updated versions of these documents to the SEC Panel for its approval. DCC will also publish its conclusions on this consultation on the DCC website.

2. The SSI Functions and Roles Policy

17. This section sets out the structure and content of the new SSI Functions and Roles Policy. The full document is available in Attachment 1.

18. This policy will set out the Business Functional Domains and Job Type Roles available to SSI users. It describes the Functional Components that are available to each of the Functional Domains and which Functional Components a user with a specific Job Type Role is permitted to access.

19. Much of the information in this policy is currently contained in SEC Appendix AH 'Self-Service Interface Access Control Specification'. This is being moved to the SSI Functions and Roles Policy and updated accordingly as part of the agreed SEC changes for the FSM solution. 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.

2.1. Business Functional Domains, Functional Components and Job Type Roles

20. Section 3 of the policy sets out the Business Functional Domains[3] and the Functional Components[4] for the SSI.

21. Section 4 of the policy sets out the Job Type Roles available to be assigned to SSI Users. Each Job Type Role will enable the user to access to one or more Functional Components, as set out in the policy.

2.2. Management of Job Type Roles

22. Section 5 of the policy sets out the mechanism for DCC to manage the initial set-up of an SSI user for a new SEC Party as part of the onboarding process. This initial user would be granted administration rights for their organisation and would be responsible for creating, amending and deactivating other users within their own organisation.

23. Section 6 of the policy sets out the processes whereby an administrator user can create further user accounts for their organisation, update the details and Job Type Roles assigned to these, or deactivate these accounts when they are no longer needed.

24. In its original consultation on the regulatory changes required for the FSM Programme, DCC removed the need for it to validate any changes to the Job Type Roles assigned to a user. DCC

[3] A Business Functional Domain is a grouping of one of more Functional Components which is used to describe and deliver the functional requirements of SSI users.
[4] A Functional Component is a specific item or a set of functionalities provided by the SSI which is subject to the access controls set out in the policy document.

considered this validation provided no value as it would not know if the change was valid or not. It originally considered an exception for the creation of or change to an administration or other senior role. Since that consultation, DCC has further concluded that it would not be able to determine if it was appropriate for an individual within an organisation to be assigned an administration or other senior role. As such, DCC has determined that, other than the set-up of an organisation's initial administration account, it will not provide any validation for changes to any accounts made by administration users.

3. The DCC Internet Access Policy

25. This section sets out the structure and content of the new DCC Internet Access Policy. The full document is available in Attachment 2.

26. This policy will set out the eligibility and technical requirements for gaining access to the SSI. It will also cover the access and authentication processes that are applicable to Users accessing the SSI via public internet and to Users accessing the SSI via a DCC Gateway Connection.

3.1. Eligibility and technical requirements

27. Section 2 of the policy sets out the eligibility and technical requirements for accessing the SSI via the internet

28. The policy states that only Users that do not have a DCC Gateway Connection would be eligible to set up a connection to the SSI via the internet. This would apply to both the User Integration Testing (UIT) and the Production environments.

29. DCC's rationale for this position is that access via a private network (i.e. the DCC Gateway Connection) is more secure than access via the public internet, and so if access via a private network is possible this should be the default position for User access. Please note that the security posture for internet connectivity has been deemed sufficient by the Security Sub Committee (SSC), and so this does not imply that internet connectivity with the controls proposed is insecure, but that a private network is more secure.

30. The policy also sets out the technical requirements for accessing the SSI via the internet, including accessing via a fixed range of Internet Protocol (IP) addresses, the use of a secure protocol, and the use of custom Uniform Resource Locators (URLs). Note that the security controls and hardening within ServiceNow will be exactly the same as connectivity via the DCC Gateway private network.

31. Section 5 of the policy sets out the internet browsers that the ServiceNow platform is supported on.

3.2. Authenticating to SSI

32. Sections 3 and 4 of the policy set out the provisions for authenticating to SSI, which applies to Users accessing the SSI via a DCC Gateway Connection as well as Users accessing via the internet. Section 3 sets out the process when using the DCC Identity Provider Service, while Section 4 sets out the process when using the local ServiceNow user identity.

33. MFA will be used to authenticate the user's identity, and this will need to be set up the first time a user logs in to the SSI following the cutover to the ServiceNow platform.

34. The policy sets out the MFA options that DCC will make available to Users, which will be via an authenticator application or via one-time passwords. A user will be required to choose which option to use upon set-up and can change this later:

- When using the DCC Identity Provider Service (Microsoft Entra), DCC's recommended authentication application is Microsoft Authenticator, which is fully tested by Microsoft for compatibility. Microsoft does not test Entra with any other applications, but supports them on an underlying 'soft token protocol' basis. As such, DCC will allow any other authenticator application to be used, but DCC support would be provided on a 'best endeavours' basis and so would be at the User's own risk.
- When authenticating via the local ServiceNow user identity service, DCC has no specific authenticator application it recommends, but has set out a series of applications that ServiceNow tests against. DCC will allow any other authenticator application to be used, but DCC support would be provided on a 'best endeavours' basis and so would be at the User's own risk.
- When using a one-time password, a one-time password will be emailed to the user for each authentication request. This will be sent to the email address the user configured at the point of their credentials being created, which should be a corporate email address to align with relevant security controls.

35. When using the DCC Identity Provider Service, Users will need to be able to connect to a series of URL domains via the internet, which are set out in the policy. If this is not possible, then Users will need to use the local ServiceNow user identity service. Please note that using this local option will limit the ability for Users to take advantage of potential future extensions to the single sign-on capability.

4. Updates to the SSI Baseline Requirements Document

36. This section sets out the key updates being made to the SSI Baseline Requirements Document to deliver the FSM solution. The full redlined changes to this document are available in Attachment 3.

4.1. Updates to Business Functional Domains

37. Section 2 of the document describes each of the Business Functional Domains as referenced in the SSI Functions and Roles Policy. The following changes have been made to reflect the FSM solution:

- Business Functional Domains BFD05 'Forward Schedule of change', BFD09 'Service Requests', BFD10 'Communications Hub Availability & Diagnostics' and BFD12 'Knowledge Management Search and FAQs' have been consolidated into BFD01 'Service Management'. These Business Functional Domains are no longer in use and have been defined as basic, fundamental requirements within the User Cases. Therefore, they have been integrated into BFD01, enabling users to have effective incident handling, visibility of planned changes, access to diagnostic tools, streamlined service requests, and self-service knowledge resources. These have subsequently been marked as no longer in use. Other references to these have been updated accordingly throughout the rest of the document.
- BFD08 'DCC Service Alerts & Portal Access' has been updated to include the integration of MFA and Entra.

4.2. Updates to the baseline SSI platform requirements

38. Section 4 of the document sets out the baseline functional and non-functional requirements for the SSI. The following changes have been made to reflect the SSI solution:

- New functional requirements SSI-FR-82 to SSI-FR-85 have been added to reflect the MP252 solution.
- New non-functional requirement SSI-NFR-36 has been added to detail the enforcement of MFA to access the platform and the integration of Entra and Microsoft Authenticator.
- Changes have been made to multiple other non-functional requirements to reflect the replacement of the existing Security Assertion Markup Language (SAML) authentication and DCC Key Infrastructure (DCCKI) Senior Responsible Officer (SRO) with the new MFA solution for authenticating a user.

5. Next steps

39. Following the closure of this consultation, DCC will assess respondents' views and amend the draft documents as required. DCC will then submit the full responses received to this consultation and the amended versions of these documents to the SEC Panel for approval.

40. DCC will also publish a report containing its consideration of the responses to this consultation and its amendments to the draft documents. DCC will publish this conclusions document on its website.

6. Consultation questions and how to respond

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

Q1	Do you agree with the proposed SSI Functions and Roles Policy for the FSM Programme? *Please indicate any areas of disagreement and your rationale for this*
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? *Please provide your rationale for your response*
Q3	Do you agree with the proposed DCC Internet Access Policy for the FSM Programme? *Please indicate any areas of disagreement and your rationale for this*
Q4	Do you agree with the position that internet connectivity should only be made available to Users without a DCC Gateway Connection? *Please provide your rationale and, if you disagree, please include any use cases that you consider may require Users with a DCC Gateway Connection to access the SSI via the internet*

Q5	Do you agree with the authentication methods and security controls that are set out in the DCC Internet Access Policy? *Please provide your rationale for your response*
Q6	Do you agree with the changes to the SSI Baseline Requirements Document for the FSM Programme? *Please indicate any areas of disagreement and your rationale for this*

42. Please provide responses using the attached response form by **17:00 on Friday 29 August 2025** to DCC at consultations@smartdcc.co.uk.

43. 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.

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

7. Attachments

45. This consultation includes four attachments (Attachments 1-3 are 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
- Attachment 4: Consultation response template