This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	**SECP_66_1503_14**
Action:	**For Decision**

SECMP0058 Modification Report

1. Purpose

SECMP0058 'Changes to the governance of the Self-Service Interface' has undergone the Refinement Process and the Working Group has now completed its assessment of the areas requested by the Panel, and prepared the Modification Report. We are recommending that this modification be progressed to the Report Phase and that the Panel approves the Modification Report, the implementation approach, and that SECMP0058 is a Self-Governance Modification.

This paper provides a high-level summary of the key points. Full details can be found in the draft Modification Report in Appendix A.

2. Summary of the proposal

What is the issue?

SEC Appendix AH 'Self-Service Interface Design Specification' sets out the detailed specifications for the Self-Service Interface (SSI). The information set out in Appendix AH is specified at a level of detail which is very prescriptive, and which can only be changed by raising and progressing a SEC Modification. Due to this, the Data Communications Company (DCC) is unable to make rapid changes to the SSI to improve User ability to access DCC services, which is undermining the usefulness of the SSI over time as the needs of Users change.

What is the Proposed Solution?

This modification seeks to remove the low-level detail and functional requirements from Appendix AH and move these to a new technical specification document titled the SSI Baseline Requirements Document (Annex C of the Modification Report), which would be created and maintained by the DCC. The DCC propose that the new DCC managed technical specification document will not be subject to SEC Section D 'Modification Process'. Instead, it would become a document owned and maintained by the DCC with approval of changes being made by the Panel or a Sub-Committee.

It is also proposed that a new governance process is put in place outlining the step-by-step governance rules for managing improvements to the SSI. If SSI Improvement Proposals (SIPs) were to result in changes to the way Services are provided by the SSI without changing how Users connect to the SSI or the access rights granted to Users, they would impact the SSI Baseline Requirements Document instead of Appendix AH. Therefore, the governance process for these types of changes would not require the Modification Process, allowing for a more efficient SSI change process.

3. Proposed progression

The Working Group believes that this modification is now ready to progress to the Report Phase.

Determination approach

The Panel previously agreed on 10 August 2018 that SECMP0058 should be progressed as a Self-Governance Modification Proposal. We do not believe anything has changed that would mean SECMP0058 would require an Authority decision.

Implementation approach

The Working Group recommends an implementation approach of:

- **27 June 2019** (June 2019 SEC Release) if a decision to approve is received by 13 June 2019; or
- **10 Working Days following approval** if a decision to approve is received after 13 June 2019.

4. Recommendations

The Panel is requested to:

- **AGREE** that SECMP0058 should be progressed to the Report Phase;
- **APPROVE** the Modification Report;
- **APPROVE** the implementation approach; and
- **AGREE** that SECMP0058 should be progressed as a Self-Governance Modification.

Joe Hehir

SECAS Team

8 March 2019

Attachments:

- **Appendix A:** SECMP0058 Modification Report
  - **Annex A:** SECMP0058 Legal Text
  - **Annex B:** SECMP0058 SEC Appendix AH Legal Text
  - **Annex C:** SSI Baseline Requirements Document
  - **Annex D:** SSI Change Governance Process
  - **Annex E:** SSI Improvement Proposal Form
  - **Annex F:** SECMP0058 first Working Group Consultation Responses
  - **Annex G:** SECMP0058 second Working Group Consultation Responses

SEC
Smart Energy Code

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Smart Energy Code

SECMP0058

‘Changes to the governance of the Self-Service Interface’

Modification Report

Version 0.6

About this document

This document is the Modification Report for SECMP0058 'Changes to the governance of the Self-Service Interface'. It provides detailed information on the background, issue, solution, costs, impacts and implementation approach. It also summarises the discussions that have been held and the conclusions reached with respect to this Modification Proposal.

Contents

1. Summary 3
2. Background 4
3. Solution 6
4. Impacts 8
5. Costs 9
6. Implementation approach 10
7. Discussions and development 11
8. Conclusions 16

Appendix 1: SSI change governance process map 18

Appendix 2: Glossary 19

This document also has seven annexes:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the proposed solution.
- **Annex B** contains the redlined changes to SEC Appendix AH required to deliver the proposed solution.
- **Annex C** contains the proposed Self-Service Interface (SSI) Baseline Requirements Document.
- **Annex D** contains the proposed SSI Change Governance Process.
- **Annex E** (attached separately) contains the SSI Improvement Proposal Form.
- **Annex F** contains the full responses received to the first Working Group Consultation.
- **Annex G** contains the full responses received to the second Working Group Consultation.

1. Summary

SEC Appendix AH 'Self-Service Interface Design Specification' sets out the detailed specifications for the SSI. The information set out in Appendix AH is specified at a level of detail which is very prescriptive, and which can only be changed by raising and progressing a SEC Modification. Due to this, the Data Communications Company (DCC) is unable to make rapid changes to the SSI to improve User ability to access DCC services, which is undermining the usefulness of the SSI over time as the needs of Users change.

This modification seeks to remove the low-level detail and functional requirements from Appendix AH and move these to a new technical specification document titled the SSI Baseline Requirements Document (Annex C), which would be created and maintained by the DCC. The DCC propose that the new DCC managed technical specification document will not be subject to SEC Section D 'Modification Process'. Instead, it would become a document owned and maintained by the DCC with approval of changes being made by the Panel or a Sub-Committee.

It is also proposed that a new governance process is put in place outlining the step-by-step governance rules for managing improvements to the SSI. If SSI Improvement Proposals (SIPs) were to result in changes to the way Services are provided by the SSI without changing how Users connect to the SSI or the access rights granted to Users, they would impact the SSI Baseline Requirements Document instead of Appendix AH. Therefore, the governance process for these types of changes would not require the Modification Process, allowing for a more efficient SSI change process.

This modification will impact the DCC as the new SSI Baseline Requirements Document will need to be developed, maintained and administered by the DCC, but will not impact on DCC Systems. This modification will also impact the SEC Panel or a delegated Sub-Committee as they will be required to oversee SSI improvements at certain stages in the SSI improvement governance process. Implementation costs are limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort in updating the SEC, and this change is targeted for the June 2019 SEC Release.

2. Background

What is the SSI?

The SSI is a web-based portal which allows Users to obtain information about, and interact with, DCC Services. This includes raising and monitoring the status of incidents and viewing the smart metering inventory. SEC Sections H8.15-H8.18 set out the obligations for the SSI whilst SEC Appendix AH currently sets out the minimum design specifications for the SSI.

What is the issue?

The DCC has received feedback from Users stating that, whilst the SSI is compliant in its current form, it has insufficient functionality to fully support them as effectively as required. As a result, the DCC need to make a number of improvements to the SSI to ensure it is the channel of choice for the DCC service management function and to optimise it for effective and efficient delivery of service.

SEC Appendix AH currently sets out the detailed specifications and functionality for the SSI. This information is specified at a level of detail which is very prescriptive and, as a result, any change that a SEC Party wishes to make to the SSI but that impacts one of its Functional Components, requires a Modification Proposal to be raised and progressed. This governance mechanism isn't the most appropriate form of governance for the SSI as it doesn't allow for the level of flexibility required to make timely and cost-effective improvements to the SSI in order to improve User ability to access DCC services, which is undermining the usefulness of the SSI over time as the needs of Users change.

SECMP0058 was raised by the DCC on 2 August 2018 to resolve this issue.

What discussions were held before the modification was raised?

Discussions with the Operations Group

The DCC initially informed the SEC Operations Group on 27 March 2018 of the feedback they had received from Users about the SSI within Appendix AH, outlining the improvements that the DCC would like to make to the SSI for it to work more effectively. It was noted that the functionality provided by the SSI was set in Appendix AH and that its prescriptive detail was preventing improvements being made to the SSI as any changes affecting SSI functionality would have to undergo the Modifications Process. The Operations Group discussed the issue and agreed that improvements to the SSI were needed, and that an agile approach might be considered, but noted that it would still need to include appropriate governance under the SEC.

The DCC presented slides to the Operations Group on 24 April 2018 covering their proposals for improvements to the SSI and the governance around it. They proposed to remove the detailed specifications from Appendix AH, replacing these with a set of high-level requirements and principles. The low-level detail and Functional Components would be moved from Appendix AH to a technical specification document. The technical specification document would only be referenced within the SEC, meaning a Modification Proposal would not be required each time the document required a change. It was noted however, that a modification would initially be required to make these changes to Appendix AH and its governance.

As an alternative approach the DCC also proposed leaving Appendix AH as the detailed specification but that a new change governance process specifically for Appendix AH could be introduced to enable swift and timely improvements to the SSI.

The DCC advised the Operations Group on 26 June 2018 that they would be raising a Modification Proposal to replace the detailed SSI specification in Appendix AH with a technical specification document that would not be subject to the Section D Modifications Process, in line with the original proposal.

Panel input and revised Planned Maintenance allowance

The DCC advised that there would be two types of change to the SSI and its supporting systems, which included both non-functional change and functional change. Non-functional change would not remove functionality that is currently in place, but enhance the usability of the system. Functional change would include the updating or replacement of fundamental screen/interface changes, or removal of existing functionality. The DCC advised the Panel that it would like to move to a more agile, enduring approach to maintaining and managing the functionality of the SSI so that it could be rapidly amended to meet SSI Users' needs.

On 11 May 2018 the DCC presented to the Panel a proposal to deploy non-functional changes to the SSI that would not impact Appendix AH, through SSI-only Planned Maintenance windows without requiring Modification Proposals. Due to the backlog of SSI changes awaiting implementation, the DCC asked the Panel for a temporary revised Planned Maintenance schedule to support the implementation of these non-functional changes to the SSI. As a result, the Panel agreed to the DCC's proposal of a revised Planned Maintenance schedule and to further explore suitable governance of Appendix AH impacting functional changes going forward. This revised Planned Maintenance schedule would remain in place until SECMP0058 was either rejected or implemented.

Summary of discussions prior to SECMP0058

Pre-modification discussions	
Date	**Summary of discussions**
24 Apr 18	The DCC advised the Operations Group of their proposal to remove the detailed specifications and functional requirements from Appendix AH and move these to a new technical specification document.
11 May 18	The Panel agreed to the DCC's proposal of a revised Planned Maintenance schedule to support changes to the SSI, and to further explore suitable governance of Appendix AH going forward. This revised Planned Maintenance allowance would later be extended to remain in place until SECMP0058 was either rejected or implemented.
26 Jun 18	The DCC advised the Operations Group that they would be raising a Modification Proposal to replace the detailed SSI specifications in Appendix AH with a technical specification document that would not be subject to the Section D Modifications Process.

3. Solution

Proposed Solution

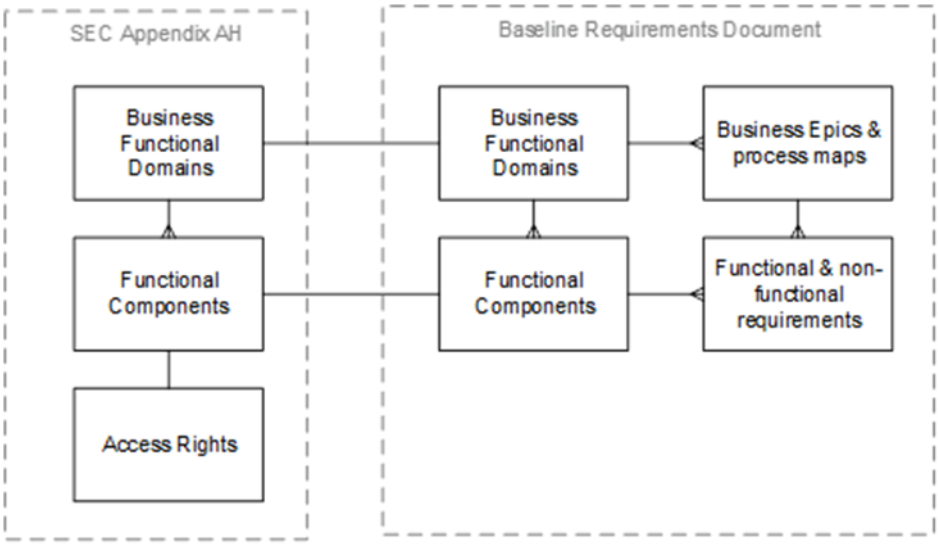
This modification seeks to remove the low-level detail and functional requirements from Appendix AH and move these to a new technical specification document titled the SSI Baseline Requirements Document (Annex C), which would be created and maintained by the DCC. In addition, new governance arrangements will be introduced to ensure flexibility, efficiency and transparency, whilst incorporating an agile approach to improving the SSI.

The DCC propose that the SSI Baseline Requirements Document will not be subject to the Section D Modification Process and instead can be amended by the DCC following consultation with Parties, and with the agreement of the SEC Panel (or a Sub-Committee to which the Panel has formally delegated the required decision-making power). The SSI Baseline Requirements Document will allow full traceability of the requirements outlined in SEC Sections H8.15(c) and H8.16 to the lowest level of detail, ensuring the DCC maintain the SSI and that SSI Users have access to certain categories of information (access control rules). It will also reflect the requirements of Appendix AI 'Self Service Interface Code of Connection'.

The technical details of each Functional Component will be contained in the new SSI Baseline Requirements Document, along with details of how Functional Components will be used to provide services to Users via the SSI. It is proposed that these aspects should be subject to a new governance process which allows the DCC to make changes following consultation with Parties and subject to agreement from the Panel (or a Sub-Committee to which the Panel has formally delegated the required decision-making power).

The purpose of Appendix AH will be focussed on providing detailed rules around access control, rather than being a technical specification document, and it is proposed that it should be re-named to the 'Self-Service Interface Access Control Specification'. The detailed step-by-step governance rules which will apply when making changes to the SSI Baseline Requirements Document will be contained in the SSI Change Governance Process (Annex D) which will be a document referenced within the SEC, with any changes to the process being managed by the SEC Panel or a delegated Sub-Committee. This will allow the DCC to make changes to the Functional Components within the SSI without having to raise a Modification Proposal but still with industry oversight, ensuring agile, flexible and efficient governance over the SSI. A diagram summarising the steps of this process is provided in Appendix 1.

The amended version of Appendix AH and the SSI Baseline Requirements Document are structured to provide direct traceability of regulatory requirements between the two documents. Appendix AH establishes Business Functional Domains, which define the capabilities provided by the SSI in terms of groupings of one or more Functional Components. Both the Business Functional Domains and Functional Components are included in the SSI Baseline Requirements Document and are linked to Epics, which describe User activities and are associated to Process Maps. The relationship between different elements of each document are illustrated in the diagram below:



Legal text

The changes to the SEC required to deliver the proposed solution can be found in Annexes A and B.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
	Large Suppliers		Small Suppliers
	Electricity Network Operators		Gas Network Operators
	Other SEC Parties	✓	DCC

This modification will impact the DCC as they will need to develop, maintain and publish the SSI Baseline Requirements Document. There are no impacts on any other SEC Parties identified.

DCC System

This modification will not impact DCC Systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section A 'Definitions and interpretations';
- Section H 'DCC Services';
- Appendix I 'CH Installation and Maintenance Support';
- Appendix T 'DCCKI Interface Design Specification';
- Appendix W 'DCCKI Registration Authority Policies and Procedures';
- Appendix AA 'Threshold Anomaly Detection Procedures';
- Appendix AH 'Self Service Interface Design Specification'; and
- Appendix AI 'Self Service Interface Code of Connection'

Other industry Codes

This modification will not have an impact on any other Industry Codes.

Greenhouse gas emissions

This modification will not have an impact on Greenhouse Gas Emissions.

5. Costs

DCC costs

This modification will not incur any one-off implementation costs on the DCC nor will there be any additional costs for the DCC to administer the proposed governance arrangements.

SECMP0058 is only an enabler for change to the SSI; the ongoing costs to make changes to the SSI using this process would be included in the DCC's forecast for each sprint, the decision on which to approve resting with the SEC Panel or a delegated Sub-Committee. Furthermore, there will be no additional costs on the DCC to administer the proposed governance arrangements as these costs would be covered in their current operating costs model and would not require any additional resource on top of what they were already using to manage the SSI. As such, there will be no additional DCC costs associated with the modification following its implementation.

SECAS costs

The estimated SECAS implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

Other than their share of the central costs, there are no specific costs anticipated on any SEC Parties to implement SECMP0058.

Some SEC parties noted in their consultation response that there would be costs for them to assess and respond to the SSI improvement consultations on an enduring basis, though these costs would be minimal.

6. Implementation approach

Recommended implementation approach

The Working Group is recommending an implementation date of:

- **27 June 2019** (June 2019 SEC Release) if a decision to approve is received on or before 13 June 2019; or
- **10 Working Days following approval** if a decision is made after 13 June 2019.

The June 2019 SEC Release is the earliest SEC Release that this modification could be implemented in. The Proposer and the Working Group are keen for this process to be implemented as soon as possible, due to the need to move from the current interim approach to an enduring approach.

If the Change Board approves this modification under Self-Governance at the April 2019 Change Board meeting, the DCC would take a proactive approach and aim to consult the industry on its first batch of SIPs in the backlog prior to this modification's implementation date.

7. Discussions and development

How will the SSI improvement process be governed?

The SSI Change Governance Process (Annex D) documents the end-to-end process for making improvements to the SSI via the SSI Baseline Requirements Document and the governance rules around this. The Working Group discussed how it could be ensured that the document was legally binding, with some members suggesting that the entirety of the document should be included within the SEC. However, other Working Group members felt that the SEC wasn't necessarily the most appropriate place for the detailed end-to-end process and governance of the SSI Baseline Requirements Document.

It was suggested that the SSI Change Governance Process should be referenced within the SEC, along with the requirement for any updates to this to be consulted upon before being signed-off by the Panel or a Sub-Committee. This would give the SSI Change Governance Process greater flexibility as it wouldn't require a Modification Proposal in order to change. However, any changes to the document would undergo a consultation with all SEC Parties and ultimately any decision pertaining to it would be made by the SEC Panel or a delegated Sub-Committee. This approach was supported by the Working Group.

How will SSI improvement consultations work?

The Panel noted that the costs of subsequent changes to the SSI should be consulted upon by the DCC, enabling consideration by all SEC Parties. The Panel also raised a query over whether these costs could be signed off outside of the Modification Process, as this would require clear governance and appropriate documentation. They asked the Working Group to ensure appropriate governance around costs was clearly defined and included within the solution of this modification.

The Working Group discussed the SSI Governance Process in depth. Initially the Proposer raised the idea of consulting on SSI impacting changes with the Customer Working Group (a DCC-led forum) and the Operations Group. However, Working Group members advised that the Customer Working Group is not formally recognised under the SEC and nor does it contain enough representation across SEC Parties to be able to form a sufficient consultation. Members also advised that issuing SSI improvement consultations to the Operations Group would not be adequate due to the potential cost impact considerations for all SEC Parties. The Working Group agreed that an industry SSI improvement consultation issued to all SEC Parties would have to occur during the process and that this would last for a minimum of 15 Working Days, allowing SEC Parties to consider the SIPs within the consultation and provide responses in a reasonable timeframe.

There were discussions over the frequency of the SSI improvement consultations, and it was agreed that these would occur quarterly following the implementation of the modification and would include batches of SIPs that had been amalgamated over the previous months. The Working Group suggested that, eventually, the frequency of SSI improvement consultations could be reviewed and could occur less frequently, focusing on the packages of SIPs to be completed in several sprints over a subsequent defined time period (which would always lie within a single Regulatory Year).

The level of detail in the SSI improvement consultations were discussed and it was agreed they should include the following details:

- The proposer of each SIP;

- A description of each SIP;
- The benefits of each SIP;
- The SEC Parties impacted;
- Whether each SIP is seeking to add, amend or remove functionality;
- The anticipated cost range; and
- The anticipated timescales to develop and deploy.

Prioritisation of SSI changes

A member of the Working Group advised that although user requirements should be prioritised, from their experience this had not been the case with the current 'sprints' process under Planned Maintenance of the SSI. Another Working Group member agreed and advised that to ensure transparency, the DCC needed to explain why certain SSI changes are prioritised over others. The DCC acknowledged this feedback and will investigate this as part of the SSI improvement consultation.

Communicating the SSI improvement consultation

The level of communication was highlighted as a key factor in relation to the SSI improvement consultation and it was agreed that the scope and scale of the SSI improvements would be clearly communicated. It was proposed that SECAS could communicate the SSI improvement consultations on behalf of the DCC and that having an agreed list of suitable contacts at the start of the process would ensure relevant individuals would receive the consultations.

How will SEC parties be informed on the costs of each SIP?

Throughout the refinement of SECMP0058, the Working Group stressed the importance of SSI improvement consultations containing a suitable level of information, especially on the anticipated costs of SIPs, in order to make an informed judgment on each set of sprints. The idea of the DCC carrying out their Impact Assessments for SIPs prior to the SSI improvement consultation was discussed but was not a popular choice for the Proposer or the majority of the Working Group. The DCC advised that Impact Assessment pre-consultation would increase the risk of cost-wastage if SIPs that were Impact Assessed were subsequently removed due to the feedback received from the SSI improvement consultation. The DCC also advised that it would raise difficult questions on who would pay for any subsequent cost-wastage with agreement amongst SEC Parties unlikely. The majority of the Working Group agreed with this assessment and agreed that it would be more cost effective for everyone involved if SSI Impact Assessments were to occur after the SSI improvement consultation.

The Working Group noted that they still needed an idea on the costs for each SIP in order to make an informed judgment on the consultation. As a result, the DCC decided to take a t-shirt sizing approach to establishing the costs of SIPs in their initial assessment. These would be set out into three categories:

- Small (below £50k);
- Medium (£50k-£100k); and

- Large (exceeds £100k).

The cost brackets within these boundaries raised concern with a Working Group member, who realised the potential for multiple SIPs exceeding £100k in costs. The member believed that any improvements to the SSI would be small and that the scope should not impact the wider DCC Total Systems and should therefore not be exceeding £100k. The DCC understood the member's view and advised that any risks of wider impacts to the DCC Total Systems found at Impact Assessment would be fed back to the Panel or any delegated Sub-Committee for consideration before implementation.

The member then advised that this risk could be alleviated up front whereby SSI Improvement Proposers would be clear on the types of SIPs they were submitting and which DCC Systems they would impact. The idea of proposer ownership was emphasised with proposers being expected to provide enough information along with their SIP to enable the DCC to carry out a thorough assessment. It is hoped that will prevent the SSI from potentially becoming a dumping ground for complex changes with a wider scope than just the SSI and Remedy systems. Other members of the Working Group acknowledged that this would be hard to achieve as SSI Users don't have a clear enough understanding of the DCC Total Systems in order to properly assess the wider impacts of their own SIPs but agreed with the principle of SIP proposer ownership. The Working Group considered whether some guidance on this could be provided by the DCC, although stressed any guidance should not be seen as an exhaustive list of what could or could not qualify.

Will there be an impact on Sub-Committee terms of reference?

It was agreed that the SEC Panel or a delegated Sub-Committee would have to consider SSI improvement consultation responses and manage work requiring sign-off such as the development and deployment of SSI improvements. The Working Group recommended that this work should be delegated to the Operations Group as they currently consider SSI improvements under the current 'sprints' process utilised by the DCC. Furthermore, the Panel, or the delegated Sub-Committee, would manage and approve any changes to a package of work consulted upon (e.g. the addition of new items or changes to deployment dates) without any further consultation with the industry.

A member of the Working Group advised that the Operations Group formed decisions by the consensus of the group and that the meetings themselves (excluding those where a vote would take place) required no level of quorum over their attendance. The Working Group agreed that the Operations Group Terms of Reference would require amendments to include conditions on decisions regarding changes to the SSI.

The Operations Group Terms of Reference have since been amended to include a provision for specific matters that have been delegated to the Operations Group by the Panel that require a determination. These decisions will be decided by a simple majority of voting Operations Group Members. In the circumstance of a tie amongst voting Operations Group Members, the Chair shall have a casting vote.

For clarity, the relevant Sub-Committee's terms of reference and operation of the SSI improvement process may be reviewed by the Panel at any time, ideally at least annually, to ensure that they remain appropriate to reflect the duties and requirements of the SEC. Amendments to these terms of reference will be approved solely by the Panel.

Is the proposed SSI improvement process agile?

Once the Working Group agreed on the governance rules for proposing improvements to the SSI, SECAS and the DCC developed a view of the end-to-end process and the worst-case timescales at each stage of the process, taking the governance rules into account. The Working Group established that it could take up to seven months from the point of proposing an SSI improvement to its implementation. Concerns were raised over these timescales and it was noted that one of the aims of this modification was to maintain an 'agile' approach towards SSI Improvements.

The Working Group explored ways of reducing the end-to-end process, with a shortened consultation window and increased consultation frequency both suggested. However, it was deemed that a shortened consultation window would not give Parties enough time to analyse the SIPs, whilst an increased frequency of consultations would be inefficient when considering the other industry consultations that Parties are asked to respond to.

The estimated 20 Working Days for the DCC to validate, prioritise and triage SIPs was questioned by one Working Group member who believed that this timespan was too long for the work that was being undertaken. The DCC advised that this timescale was not set in stone and that it was dependent on the scope of each individual SIP. The DCC used timescales for SIPs already undergoing the improvement process, with some being validated and prioritised within a matter of days. The Working Group also noted that the rules within the SSI Change Governance Process could be changed once the process is implemented and improvements are realised, and felt 20 Working Days was an appropriate starting figure.

The Working Group member suggested a more effective use of the validation and prioritisation stage of SIPs would be to bring forward SSI Impact Assessments to this stage, prior to the SSI improvement consultation. The Working Group member believed that this would speed up the end-to-end process and would also provide SEC Parties with a clear view of the costs of each sprint. However, as noted above, the majority of the Working Group were opposed to this idea as it would increase the risk of cost wastage if SIPs that were Impact Assessed were subsequently removed due to the feedback received from the SSI improvement consultation.

The Working Group agreed that the end-to-end timescales were a consequence of the need for a robust governance process over SSI improvements including an industry consultation and set points whereby sign-off is required. It was felt that the proposed solution was a suitable balance between robust governance and an 'agile' approach and noted that while the proposed process may not be that much quicker than a Modification Proposal, the efficiencies of being able to batch changes, and the greater flexibility with their assessment and implementation outweighed this. One member also noted the likelihood of forming quorate Working Groups to assess each individual SIP was very small.

How should changes to the SSI Baseline Requirements Document be shown?

The SSI Baseline Requirements Document is intended to contain the business and technical requirements that will be removed from Appendix AH. It was initially proposed that the SSI Baseline Requirements Document would not show the changes to the SSI but that a 'delta document' would be periodically released showing the latest changes to the SSI. Some members of the Working Group strongly opposed this due to a perceived lack of efficiency and transparency and advised that there had to be a live version of the SSI Baseline Requirements Document. Following this feedback, the DCC agreed to maintain and publish a live version of the SSI Baseline Requirements Document and a redlined version showing the changes being made to it for each sprint.

What parts of Appendix AH should remain within the SEC?

Initially the DCC had proposed to remove Appendix AH in its entirety and that the SSI Baseline Requirements Document would form its replacement. However, the majority of the Working Group were opposed to this and advised that both DCC and User obligations had to remain in the SEC. They noted that SEC Parties would not be legally bound to comply with the SSI Baseline Requirements Document if it fell outside the SEC. Other Working Group members then suggested that, rather than completely removing the content from Appendix AH, it could be left with just a set of core principles and requirements. This was still not adequate to some Working Group members and so the idea of a 'slimmed down' Appendix AH was agreed upon which would include all DCC and User obligations, access controls, and the core principles that the SSI is expected to meet. Following on from this, the DCC opted to remove all Interface Transactions from Appendix AH and move these to the SSI Baseline Requirements Document.

The proposed changes to the SEC to deliver the proposed solution can be found in Annexes A and B.

What impact will this modification have on Planned Maintenance?

Currently the SEC allows for no more than four hours per month for Planned Maintenance of the SSI. However, a temporary arrangement is now in place (more information can be found in Section 2 of this document) that allows the DCC a window of six hours per week to carry out Planned Maintenance to the SSI, which will remain in place until SECMP0058 is either rejected or implemented.

In the SECMP0058 Modification Proposal form, the DCC advised that future improvements to the SSI will affect the levels of Planned Maintenance required to implement them and, as such, the Panel and the Working Group raised concerns as to how the DCC would meet their Planned Maintenance allowance in the future. The DCC clarified that the window for system maintenance covers the deployment phase of changes to the SSI and they are unlikely to exceed their current allowance of six hours per week. On the rare exception that they may need to exceed this, they would have to consult with the Operations Group first, who have been delegated the responsibility by the Panel to oversee improvements to the SSI.

The DCC have confirmed that SECMP0058 will not be making any amendments to the SEC impacting Planned Maintenance allowance and that any changes to these allowances would be proposed under a separate Modification Proposal. For the avoidance of doubt, when the temporary SSI Planned Maintenance arrangements end following the rejection or implementation of SECMP0058, the DCC will adhere to SEC Sections H8.3 and H8.4 for any Planned Maintenance activities.

8. Conclusions

Benefits and drawbacks

The Proposer and the Working Group have identified the following benefits and drawbacks in implementing this modification:

Benefits

- The Working Group agreed that this modification would result in stronger and more efficient governance being in place for changes to the SSI.
- This modification would result in unnecessary low-level detail being removed from the SEC. This would contribute to a more efficient SSI change process as proposed changes would have less chance of impacting the legal text in the SEC and would therefore not require a Modification Proposal to change these.
- The use of a redlined version of the Business Requirements Document would allow for greater control of SSI changes through to delivery as well as an audit trail for SEC Parties to have an ongoing view of changes to the SSI.
- Considering the anticipated benefits that this modification should bring, the DCC will be able to make improvements to the SSI fast enough to meet the changing needs of SSI users. Improving the SSI will encourage more SEC Parties to use it and there will therefore be a reduction of interaction outside of the SSI and increase efficiency in the DCC responding to queries.

Drawbacks

A drawback identified by the Working Group was that in order to contain the level of detail required in the SSI improvement consultations, the DCC would have to carry out more development prior to the consultation, which would increase the risk of cost wastage if any of the SIPs did not come to fruition. However, this risk was not considered to increase significantly compared to the existing Section D Modification Process. The DCC advised that the more detail Parties require in the SSI improvement consultations, the more it will cost the DCC to provide this detail as they will have to carry out more development up-front.

Another drawback was noted in the speed of the end-to-end process, with SIPs possibly taking as long as seven months from the point they are proposed through to implementation. However, it was noted that, despite these timescales, the proposed governance process still offered more in terms of efficiency and flexibility compared with the Modifications Process.

Proposer's rationale against the General SEC Objectives

Objective (a)[1]

The Proposer believes that SECMP0058 will better facilitate SEC Objective (a) as this modification will provide Users with an improved means of accessing DCC Services directly, including information which could be critical to resolving issues related to the provision, installation and operation of Smart Metering Systems.

Objective (b)[2]

The Proposer also believes that SECMP0058 will better facilitate SEC Objective (b) as this modification will better enable the DCC to meet the Interim General Objective in its licence, specifically it will support improved co-ordination of the activities, systems, and procedures of SEC Parties by providing better access to DCC Services and information.

Working Group members' views

The majority of the Working Group agreed that this modification facilitates SEC Objective (a), though the other members felt that it would facilitate SEC Objective (g)[3] instead of (a), noting that these two objectives can sometimes be misinterpreted for one another. In either case, the Working Group agreed that this modification will provide Users with an improved means of accessing DCC Services directly, including information which could be critical to resolving issues related to the provision, installation and operation of Smart Metering Systems.

The majority of the Working Group agreed that this modification facilitates SEC Objective (b) for the same reasons as given by the Proposer, by enabling the DCC to comply, at all times, with the General Objectives of the DCC (as defined in the DCC Licence), and to efficiently discharge the other obligations imposed upon it by the DCC Licence.

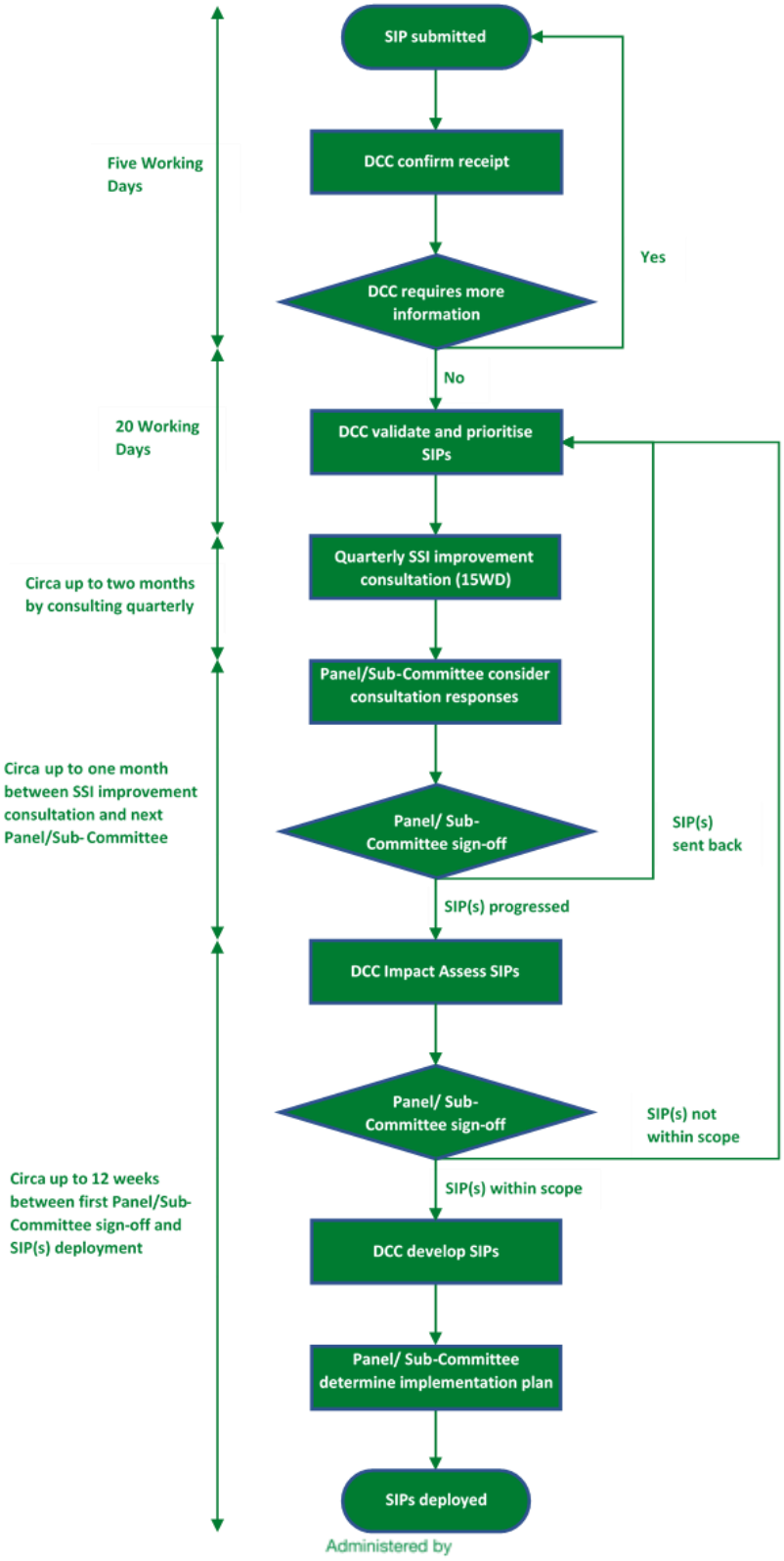
[1] Facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain.

[2] Enable the DCC to comply at all times with the General Objectives of the DCC (as defined in the DCC Licence), and to efficiently discharge the other obligations imposed upon it by the DCC Licence.

[3] Facilitate the efficient and transparent administration and implementation of this Code.

Appendix 1: SSI change governance process map

This process map summarises SSI Change Governance Process and presents a high-level view of the potentially longest timescales at each stage of the process.



Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary – Acronyms	
Acronym	**Full term**
DCC	Data Communications Company
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIP	SSI Improvement Proposal
SSI	Self-Service Interface

This table lists key terms used in this document and their definitions.

Glossary – Terms	
Term	**Meaning**
Epics	High level story that encapsulate business requirements in a solution neutral manner.
Functional Component	Means a specific item or set of functionality provided by the Self-Service Interface which is subject to the access controls set out in Appendix AH.
Planned Maintenance	Means, in respect of a month, Maintenance of the DCC Systems planned prior to the start of that month and which will disrupt, or poses a Material Risk of disruption to, provision of the Services (and, where it will disrupt, or poses a Material Risk of disruption to, the provision of the Services in relation to Devices associated with Communications Hubs, at least 100,000 Communications Hubs are affected).
Regulatory Year	Means a period of twelve months beginning at the start of 1 April in any calendar year and ending at the end of 31 March in the next following calendar year.
SSI Baseline Requirements Document	A technical specification document maintained by the DCC containing the specifications and Functional Components for the Self-Service Interface.

If you have any questions on this modification, please contact:

Joe Hehir

020 7770 6874

joe.hehir@gemserv.com

Smart Energy Code Administrator and Secretariat (SECAS)

8 Fenchurch Place, London, EC3M 4AJ

020 7090 7755

sec.change@gemserv.com

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0058 'Changes to the governance of the Self-Service Interface'

Annex A

Legal text – version 0.5

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

These changes have been drafted against SEC Version 6.5.

Section A 'Definitions and Interpretations'

Add the following new definitions to Section A1 in alphabetical order:

SSI Baseline Requirements Document	means a document produced and maintained by the DCC in accordance with the Self-Service Interface Access Control Specification.
SSI Change Governance Process	means a document established under Section H8.15A (Self-Service Interface) and contains the governance arrangements for making changes to the Self-Service Interface.

Amend the following definitions in Section A1 as follows:

Self-Service Interface ~~Design~~ Access Control Specification	means the SEC Subsidiary Document of that name set out in Appendix AH.
Technical Code Specifications	means the Technical Specifications, the GB Companion Specification, the DCC Gateway Connection Code of Connection, the DCC User Interface Code of Connection, the DCC User Interface Specification, the Self-Service Interface ~~Design~~ Access Control Specification, the SSI Baseline Requirements Document, the Self-Service Interface Code of Connection, the Registration Data Interface Documents, the Message Mapping Catalogue, the Incident Management Policy, the DCC Release Management Policy, the Panel Release Management Policy, the SMKI Interface Design Specification, the SMKI Code of Connection, the SMKI Repository Interface Design Specification, the SMKI Repository Code of Connection, and the SMETS1 Supporting Requirements.

Section H 'DCC Services'

Amend Sections H8.15 and H8.16 and add new Section H8.15A as follows:

Self-Service Interface

H8.15 The DCC shall maintain and keep up-to-date an interface (the **Self-Service Interface**) which:

(a) complies with the specification required by the Self-Service Interface ~~Design~~ Access Control Specification and the SSI Baseline Requirements Document;

(b) is made available to Users in accordance with the Self-Service Interface Code of Connection via DCC Gateway Connections; and

(c) allows each User to access the information described in Section H8.16 as being accessible to that User (and also allows other Users to access that information to the extent permitted by the first User in accordance with the Self-Service Interface ~~Design~~ Access Control Specification).

H8.15A Any changes to the Self-Service Interface shall be processed by the DCC in accordance with the "**SSI Change Governance Process**". Any changes to the SSI Change Governance Process shall be prepared and consulted upon by the DCC and approved by the Panel.

H8.16 The Self-Service Interface must (as a minimum) allow the following categories of User to access the following:

(a) the Smart Metering Inventory, which shall be available to all Users and capable of being searched by reference to the following (provided that there is no requirement for the DCC to provide information held on the inventory in respect of Type 2 Devices other than IHDs):

(i) the Device ID, in which case the User should be able to extract all information held in the inventory in relation to (I) that Device, (II) any other Device Associated with the first Device, (III) any Device

Associated with any other such Device; and (IV) any Device with which any of the Devices in (I), (II) or (III) is Associated;

(ii) the MPAN or MPRN, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meter to which that MPAN or MPRN relates, or in relation to any Device Associated with that Smart Meter or with which it is Associated;

(iii) post code and premises number or name, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked to that postcode and premises number or name, or in relation to any Device Associated with those Smart Meters or with which they are Associated;

(iv) the UPRN (where this has been provided as part of the Registration Data), in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked by that UPRN, or in relation to any Device Associated with those Smart Meters or with which they are Associated;

(b) a record of the Service Requests and Signed Pre-Commands sent by each User, and of the Acknowledgments, Pre-Commands, Service Responses and Alerts received by that User (during a period of no less than three months prior to any date on which that record is accessed), which shall be available only to that User;

(c) a record, which (subject to the restriction in Section I1.4 (User Obligations)) shall be available to all Users:

(i) of all 'Read Profile Data' and 'Retrieve Daily Consumption Log' Service Requests in relation to each Smart Meter (or Device Associated with it) that were sent by any User during a period of no less than three months prior to any date on which that record is accessed; and

(ii) including, in relation to each such Service Request, a record of the type of the Service Request, whether it was successfully processed, the time and date that it was sent to the DCC, and the identity of the User which

sent it;

(d) the Incident Management Log, for which the ability of Users to view and/or amend data shall be as described in Section H9.4 (Incident Management Log);

(e) the CH Order Management System, which shall be available to all Users;

(f) any and all information in respect of the SMETS1 SM WAN as the DCC is required to make available under the Self-Service Interface ~~Design~~ Access control Specification and the SSI Baseline Requirements Document, which shall be made available to all Users; and the following information in respect of the SMETS2+ SM WAN, which shall be available to all Users (and which shall be capable of interrogation by post code and postal outcode):

(i) whether a Communications Hub Function installed in a premise~~s~~ at any given location:

(A) is expected to be able to connect to the SM WAN;

(B) is expected to be able to connect to the SM WAN from a particular date before 1 January 2021, in which case the date shall be specified; or

(C) cannot be confirmed as being able to connect to the SM WAN before 1 January 2021;

(iii) any known issues giving rise to poor connectivity at any given location (and any information regarding their likely resolution); and

(iv) any requirement to use a particular WAN Variant (and, where applicable, in combination with any particular Communications Hub Auxiliary Equipment) for any given location in order that the Communications Hub will be able to establish a connection to the SM WAN;

(g) additional information made available by the DCC to assist with the use of the Services and diagnosis of problems, such as service status (including information in respect of Planned Maintenance and Unplanned Maintenance)

and frequently asked questions (and the responses to such questions), which shall be available to all Users; and

(h) anything else expressly required by a provision of this Code.

Appendix I 'CH Installation and Maintenance Support Materials'

Amend Section 5.2 as follows:

5 **COMMUICATIONS HUB DIAGNOSTICS**

5.1 Where, following successful installation of a Communications Hub and Commissioning of the related Communications Hub Function, a Supplier Party identifies a potential Communications Hub fault, pursuant to Section H9.6 of the Code, that Supplier Party shall take all reasonable steps to complete the Communications Hub Availability and Diagnostics Check procedure prior to raising an Incident with the DCC.

Communications Hub Availability and Diagnostics Check

5.2 A Supplier Party may undertake a Communications Hub Availability and Diagnostics Check, by either:

(a) utilising the Self Service Interface to complete the Communications Hub availability and diagnostic check as defined in the Self-Service Interface ~~Design~~ Access Control Specification and the SSI Baseline Requirements Document; or

(b) sending Service Requests 6.13: (Read Event or Security Log) for the CHF event log and Service Request 8.9: (Read Device Log) for the CHF Device Log, in accordance with DUIS and interpreting the Service Responses received.

Appendix T 'DCCKI Interface Design Specification'

Amend references to 'Self Interface Design Specification' as follows:

Submission of Personnel Authentication Certificate Applications and Issuance of Personnel Authentication Certificates

2.4 Prior to submitting an initial -Personnel Authentication Certificate Application, (but not for any subsequent application), a Party that is a DCCKI Eligible Subscriber in respect of Personnel Authentication Certificates shall submit an Administration User Credentials Request via the approved mechanisms set out in the DCCKI RAPP.

2.5 The DCC shall make a Personnel Credentials Interface accessible via the Self Service Interface for the purpose of accessing DCCKI Services in order to obtain a Personnel Authentication Certificate. The DCC shall ensure that:

(a) the -Personnel Credentials Interface uses the HTTPS protocol;

(b) the Personnel Credentials Interface uses Java 7, update 6 (or greater);

(c) the Personnel Credentials Interface supports JavaScript, CSS and images;

(d) initial access to the -Personnel Credentials Interface will be authorised through use of username and single use password, the provision of which shall be detailed in the DCCKI RAPP and shall be secured by server side authentication using TLS 1.2;

(e) subsequent access to the Personnel Credentials Interface is secured by mutual authentication using TLS1.2 between the Supported Browser being used by the DCCKI Eligible Subscriber and the Personnel Credentials Interface;

(f) DCCKI -Certificates are used for the TLS authentication and shall support the following cipher suites:

i. ECDHE-RSA-AES256-GCM-SHA384

ii. ECDHE-RSA-AES128-GCM-SHA256

iii. ECDHE-RSA-AES256-SHA384

iv. ECDHE-RSA-AES128-SHA256;

(g) access to the Personnel Credentials Interface is denied without a valid credential for Authentication; and

(h) User Personnel are provided with the means to view and update their password and user account information as set out in the Self Service Interface ~~Design~~ Access Control Specification.

Issuance of Personnel Authentication Certificates to Administration Users

Initial Issuance of a Personnel Authentication Certificate to Administration Users

2.6 In order to obtain an initial Personnel Authentication Certificate, an Administration User shall log onto the Personnel Credentials Interface via the Self Service Interface using the supplied username, and single use password as provided in accordance with the DCCKI RAPP.

2.7 Upon initial login, the SSI Administration User shall be required to:

(a) change the password for the user account from that provided; and

(b) provide answers to security questions that will subsequently be used to confirm the identity of that Administration User if their password is forgotten, their Personnel Authentication Certificate has expired or the Smart Card Token provided to that Administration User is lost or stolen.

2.8 On successful change of the user account password, the Administration User shall be able to request initialisation of the Smart Card Token which will result in a Personnel Authentication Certificate Application.

2.9 In order to initialise the Smart Card Token, the Administration User shall:

(a) connect the Smart Card Token to the system that the Administration User is using to access the Personnel Credentials Interface. The system shall be configured in accordance with sections 2.5 (b) and (c) of this DCCKI IDS; and

(b) request initialisation of the Smart Card Token by following the instructions

displayed on the Personnel Credentials Interface.

2.10 Following a successful request for initialisation of the Smart Card Token the DCC shall ensure that, where the Smart Card Token generates a Personnel Authentication Certificate Application, this shall automatically be submitted to the UI DCCKICA.

2.11 The Administration User shall be notified via the Personnel Credentials Interface as soon as reasonably practicable of the Issuance of a Personnel Authentication Certificate for that Administration User.

Subsequent Issuance of a Personnel Authentication Certificate to Administration Users

2.12 Prior to the expiry of a Personnel Authentication Certificate Issued to an Administration User, that Administration User may:

(a) log onto the Personnel Credentials Interface via the Self Service Interface, using their Smart Card Token, username and password; and

(b) reinitialise the Smart Card Token by following the steps set out in section 0 of this DCCKI IDS, which will result in the Issuance of a new -Personnel Authentication Certificate.

2.13 In the event that a Personnel Authentication Certificate Issued to an Administration User has expired prior to their obtaining a new Personnel Authentication Certificate, that -Administration User may:

(a) log onto the Personnel Credentials Interface via the Self Service Interface and obtain a new Personnel Authentication Certificate by:

(i) using their -Administration User username and password; and

(ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(b) reinitialise the Smart Card Token by following the steps outlined in section 0 above which will result in the Issuance of a new Personnel Authentication

Certificate.

2.14 In the event that the Smart Card Token is lost or stolen, an Administration User may:

(a) obtain a new Smart Card Token from their DCCKI ARO in accordance with the DCCKI Code of Connection;

(b) log onto the Personnel Credentials Interface via the Self Service Interface:

(i) using the Administration User's username and password; and

(ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(c) initialise the Smart Card Token by following the steps outlined in section 0 of this DCCKI IDS which will result in the Issuance of a new Personnel Authentication Certificate.

Issuance of Personnel Authentication Certificates to other User Personnel

Initial Issuance of a Personnel Authentication Certificate to other User Personnel

2.15 The initial Issuance of a Personnel Authentication Certificate to a User Personnel shall be via the Personnel Credentials Interface following the creation of an account for that User Personnel by an Administration User.

2.16 In order to provide Authentication credentials to User Personnel, (which shall comprise a single use password and a username) an Administration User may:

(a) log onto the Self Service Interface using their Smart Card Token, username and password in accordance with the Self Service Interface ~~Design~~ Access Control Specification and Self Service Interface Code of Connection;

(b) create additional user accounts for other User Personnel; and

(c) provide details to those User Personnel including a username and single use password that allows them to log onto the Personnel Credentials Interface via the Self Service Interface.

2.17 In order to obtain an initial Personnel Authentication Certificate, User Personnel of a DCCKI Eligible Subscriber, shall log onto the Personnel Credentials Interface via the Self Service Interface using the agreed username and single use password, as established by the relevant Administration User.

2.18 Upon first login, those User Personnel shall be required to:

(a) change the password for their account; and

(b) provide answers to security questions that will subsequently be used to confirm the identity of that individual if the password is forgotten, their Personnel Authentication Certificate has expired or their Personnel Authentication Certificate is destroyed or, no longer has access to their Personnel Authentication Certificate or Private Key associated with their Personnel Authentication Certificate.

2.19 Upon successful login, the User Personnel shall be able to submit a Personnel Authentication Certificate Application by following the instruction displayed on the Personnel Credentials Interface.

2.20 Following a Personnel Authentication Certificate Application request:

(a) the User Personnel shall be requested to create a password in accordance with the instruction displayed on the Personnel Credentials Interface, to protect the credentials to be generated by the DCCKICA and transferred to the User Personnel's browser;

(b) the DCCKI Eligible Subscriber shall ensure that the systems of its User Personnel are configured to allow the credentials to be transferred to the User Personnel's browser and in accordance with sections 2.5 (b) and (c) of this DCCKI IDS;

(c) the DCCKICA shall generate the credentials consisting of a Key Pair along with a Personnel Authentication Certificate that is specific to that User Personnel and the systems that User Personnel is using to access the Personnel Credentials

Interface and shall make it available to the browser in the form of a PKCS#12 file protected using the password created by the User Personnel;

(d) the User Personnel shall unprotect the PKCS#12 file using the password created by that User Personnel; and

(e) the User Personnel shall download, verify and install the PKCS#12 file in a location accessible to a Supported Web Browser, when requested by the Authentication Credentials Interface.

Subsequent Issuance of a Personnel Authentication Certificate to other User Personnel

2.21 Prior to the expiry of a Personnel Authentication Certificate assigned to a member of User Personnel, in order to obtain a new Personnel Authentication Certificate, that individual:

(a) may log onto the Personnel Credentials Interface via the Self Service Interface, using their existing Personnel Authentication Certificate, username and password; and

(b) follow the steps outlined in sections 0 and 0 of this DCCKI IDS.

2.22 In the event that their Personnel Authentication Certificate has expired prior to obtaining a new Personnel Authentication Certificate, a member of User Personnel may:

(a) Log onto the Personnel Credentials Interface via the Self Service Interface:

(i) using their username and password; and

(ii) provide answers to the security questions as selected -when obtaining their initial Personnel Authentication Certificate; and

(b) follow the steps outlined in sections 0 and 0 of this DCCKI IDS.

Appendix W 'DCCKI Registration Authority Policies and Procedures

Amends Section 3.18

Procedure for providing credentials to DCCKI AROs in order to allow Administration Users to use the Self Service Interface

3.18 In order to obtain access to the Self Service Interface (SSI) in accordance with the Self Service Interface ~~Design~~ Access Control Specification, each DCCKI Authorised Subscriber that is a DCCKI Eligible Subscriber in relation to Personnel Authentication Certificates may submit an Administration User Credentials Request in order to obtain credentials for a member of the User Personnel of that organisation nominated to become an Administration User via the procedures set out immediately below.

Submission of Administration User Credentials Requests

3.19 A DCCKI ARO of a DCCKI Authorised Subscriber that meets the conditions set out in section 0 of this DCCKI RAPP may submit an Administration User Credentials Request to the DCCKI Registration Authority using the form provided for the purpose on the DCC Website, which shall be substantively in the form set out in Annex A (A5) to this DCCKI RAPP.

3.20 In submitting an Administration User Credentials Request, a DCCKI ARO of a DCCKI Subscriber shall provide the required details of the User Personnel who are to be provided with Smart Card Tokens, single use passwords and usernames for the purposes of establishing access to the Personnel Credentials Interface, and submitting a Personnel Authentication Certificate Application as Administration Users.

DCCKI Registration Authority processing of Administration User Credentials Requests

3.21 On receipt of an Administration User Credentials Request, DCCKI Registration Authority Personnel shall;

(a) confirm via the DCC Service Desk to the DCCKI ARO that submitted the request that such request has been received, where this notification may be made via telephone or in writing using the contact details established as part of enrolment to the DCCKI Services;

(b) ensure that the submitting organisation meets the conditions set out in section 0 of this DCCKI RAPP; and

(c) ensure that all required information has been provided.

3.22 Where the Administration User Credentials Request is valid, the DCCKI Registration Authority shall in relation to that request:

(a) ensure that single use passwords and usernames are generated for each member of User Personnel whose details are provided;

(b) provide, via a secured electronic means as set out on the DCC Website, the usernames to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface;

(c) provide, via secure post, the single use passwords to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface; and

(d) provide one Smart Card Token for each member of User Personnel identified:

(i) to the DCCKI ARO that submitted the request or their named alternative, whose details have been provided by that DCCKI ARO at the time the request was made. This delivery may be in person, via a nominated employee, or via a commercial courier service. (Any person delivering the materials shall have information that enables verification of the materials and the sending organisation, and allows Authentication of that person's identity); and

(ii) ensure that the DCCKI ARO that submitted the request (or their named alternative) is advised in advance of any such delivery, including the means of delivery, and the name of the person that shall be making that delivery. This notification may be made via telephone or in writing using the contact details established as part of enrolment to the DCCKI Services.

3.23 If the Administration User Credentials Request is not valid, the DCCKI Registration Authority Manager shall ensure that a DCCKI SRO of the submitting organisation and the DCCKI ARO who submitted that request is notified of the reasons for its rejection.

Establishment of Administration User credentials

3.24 On receipt of the Smart Card Tokens, usernames and single use passwords from the DCCKI Registration Authority, the DCCKI ARO shall ensure the distribution of the required materials to the relevant User Personnel within their organisation. Those User Personnel may then use the materials to access the Personnel Credentials Interface for the purposes of submitting a Personnel Authentication Certificate Application and obtaining a Personnel Authentication Certificate in accordance with the procedures set out in the DCCKI Interface Design Specification.

3.25 Following successfully obtaining a Personnel Authentication Certificate, the User Personnel nominated by that DCCKI ARO shall be an enabled Administration User who may then create usernames and single use passwords for other User Personnel within their organisation in accordance with the DCCKI Interface Design Specification.

3.26 In the event that, following provision of Smart Card Tokens, usernames and single use passwords by a DCCKI ARO, relevant User Personnel are unable to successfully obtain a Personnel Authentication Certificate, that DCCKI ARO shall raise an Incident in accordance with the Incident Management Policy, in order to resolve the matter.

Appendix AA 'Threshold Anomaly Detection Procedures'

Amend references to 'Interface Transaction' as follows

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below.

Anomaly Detection Thresholds File	means a CSV file submitted by a User for the purposes of notification of ADT and Warning Thresholds to be applied by the DCC.
Authorised Responsible Officer (ARO)	means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP.
Comma Separated Values (CSV)	means a tabular set of data records in text format in which the data fields within each data record are delimited using commas, and where data fields are not enclosed with opening and closing double quotation marks.
DCC Service Management System (DSMS)	means the Service Desk system used to manage Incidents and Service Management Service Requests.
Fast-Track Notification	means submission from a User to the DCC of an Anomaly Detection Thresholds File that is submitted with the intention of being applied in shorter timescales than standard processing timescales, where such timescales are set out in clause 3 of this document.
File Signing Certificate	means an IKI Certificate issued to a Party in accordance with the SMKI RAPP and associated with a Private Key that is used for the purposes of Digital Signing of CSV files.

~~Interface Transaction~~Functional Component	has the meaning ascribed to this term in the Self Service Interface ~~Design~~Access Control Specification.
Quarantined Communications Action File	means a CSV file submitted by a User for the purposes of notifying the DCC of the actions to be taken by DCC in respect of quarantined communications.
Quarantined Communications Report File	means a CSV file issued by the DCC to notify a User that communications have been quarantined.
Senior Responsible Officer (SRO)	means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP.
Service Management Service Request (SMSR)	means the request raised by the User to facilitate management of a Service Desk call.
Warning Threshold	in respect of a User, a number of communications within a period of time which, if exceeded, will result in the DCC notifying the User. Where both that number and the period of time are set by the User.

1. Introduction

1.1. The Threshold Anomaly Detection Procedures (TADP) document makes provision for such matters as are described in Section G6.1 and G6.4 (b) (i) of the Code, and provides further processes and detail required to facilitate those matters.

2. DCC Anomaly Detection Threshold Guidance

2.1. Pursuant to Section G6.4 (b) of the Code, each User shall take into account any guidance issued by the DCC as to the appropriate level for their Anomaly Detection Thresholds (ADTs) giving regard to their Service Request forecast and expected pattern of demand for each Service Request.

2.2. DCC shall:

(a) provide guidance to support Users in setting appropriate ADT and Warning Thresholds;

(b) provide a template for the User to provide its ADT and Warning Thresholds in the format set out in clause 6.3 of this document; and

(c) provide the guidance and template referred to above via the Self Service Interface (SSI).

3. Notification of Anomaly Detection Thresholds

User and DCC Responsibilities: ADT submissions

3.1. Prior to sending the DCC any Anomaly Detection Thresholds File, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC, where such reference number will be generated by the SSI automatically.

3.2. Each User shall use reasonable steps to organise its business processes in such a manner that obviates the need for it to rely on the use of Fast-Track Notifications.

3.3. Where a User wishes to submit a Fast-Track Notification it shall, prior to doing so, contact the Service Desk and provide a justification for why it is necessary for them to do so.

3.4. A User shall, in each User Role in relation to which it is required (or elects) to set ADTs, provide an Anomaly Detection Thresholds File to the DCC via an email to the Service Desk. The email shall include:

(a) the SMSR reference number in the subject line of the email; and

(b) the Anomaly Detection Thresholds File (of the form set out in clause 6.3 of this document), Digitally Signed by a Private Key associated with a File Signing Certificate and provided to an Authorised Responsible Officer (ARO) in accordance with the SMKI RAPP.

3.5. The User shall update the SMSR corresponding to the Anomaly Detection Thresholds File submission on the SSI. On receipt of an SMSR and accompanying Anomaly Detection Thresholds File, the DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file;

(b) check that the format of the Anomaly Detection Thresholds File is correct; and

(c) for Fast-Track Notifications, assess whether the justification provided is valid.

3.6. Following the checks above the DCC shall verify that the ADT and Warning Threshold values provided are consistent with guidance issued by DCC. Where the DCC considers this not to be the case it shall contact a Senior Responsible Officer (SRO) acting on behalf of the User, by telephone using the contact details held by the DCC. The DCC shall request confirmation from the SRO as to whether the submitted Anomaly Detection Thresholds File should be applied. The SRO shall either:

(a) provide confirmation to the DCC to apply the ADT and Warning Thresholds that it has submitted in which case the DCC shall apply the ADT and Warning Thresholds included within the Anomaly Detection Thresholds File and close the relevant SMSR; or

(b) resubmit Anomaly Detection Thresholds File having had further regard to the guidance.

3.7. The DCC shall validate and process Anomaly Detection Thresholds File submissions and shall either apply the ADT and Warning Thresholds or reject the submission, in accordance with the timescales set out immediately below:

(a) for a notification of an Anomaly Detection Thresholds File that is not a Fast-Track Notification, within 72 hours of receipt of an Anomaly Detection Thresholds File by the DCC; or

(b) for a Fast-Track Notification, within 24 hours of receipt of an Anomaly Detection Thresholds File by the DCC.

3.8. Where the ADT and Warning Thresholds have been successfully applied, the DCC shall update and close the relevant SMSR. Where any of the checks outlined at clause 3.5 fail, the DCC shall not apply the ADT and Warning Thresholds and shall update the SMSR to reflect this and notify the User of the reason for the failure.

4. Exceeding Anomaly Detection or Warning Thresholds

User and DCC Responsibilities: User Warning Threshold

4.1. Where the number of communications has exceeded the Warning Threshold, the DCC shall raise an Incident and send an email notification to the User's registered contact address on the DSMS.

4.2. Following any such notification, a User shall use the "View Service Management Incident" ~~Interface Transaction~~Functional Component within the SSI to obtain details on the Warning Threshold exceeded using the SMSR reference number provided within the email notification.

4.3. Each User shall investigate, and then update and assign the Incident to the Service Desk using the "Update Service Management Incident" ~~Interface Transaction~~Functional Component within the SSI.

User and DCC Responsibilities: User Set Anomaly Detection Threshold

4.4. Where the DCC has quarantined communications in accordance with the Service Request Processing Document the DCC shall raise an Incident and send an email notification to the affected User's registered contact address on the DSMS to inform the User of the ADT that has been exceeded.

4.4A In respect of each quarantined communication, the DCC shall also send a DCC Alert to the User who sent the communication to inform then that the communication has been quarantined.

4.5. The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the

communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time period has elapsed, the DCC shall archive all quarantined communications relating to the event for audit purposes and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident.

4.6. Each User shall use the "View Service Management Incident" ~~Interface Transaction~~Functional Component within the SSI to obtain details on the ADT exceeded using the Incident reference number provided within the email notification. The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" ~~Interface Transaction~~Functional Component within the SSI, which shall include the list of quarantined communications in a CSV format.

4.7. Each User shall investigate and resolve the ADT exceeded event. Each User shall provide an email to the Service Desk indicating the action to be taken on each of the quarantined communications. The email shall include:

(a) the Incident reference number in the subject line of the email; and

(b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

4.8. Each User shall update the Incident using the "Update Service Management Incident" ~~Interface Transaction~~Functional Component within the SSI and assign to the Service Desk for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

(b) check that the format of the data is correct.

4.9. Upon successful validation of all of the above checks the DCC shall perform the actions on the quarantined communications, notify the User, update and close the Incident.

4.10. Where any of the above validation steps fail the DCC shall update the Incident, reassign it to the User and notify the User of the reason for the failure.

User and DCC Responsibilities: DCC Set Anomaly Detection Threshold

4.11. Pursuant to Section G6.6 of the Code the DCC shall set ADTs. Where a DCC set ADT has been exceeded, the DCC shall:

(a) quarantine the communication(s) that have exceeded the ADT;

(b) raise an Incident in accordance with the Incident Management Policy;

(c) determine the reasons for the Incident and take appropriate remedial action; and

(d) in respect of each quarantined communication, send a DCC Alert to the User who sent the communication to inform them that the communication has been quarantined.

4.12. DCC shall contact the User(s) impacted by the event by raising an Incident to notify them that their communication(s) have been quarantined. At an appropriate point during the investigation, DCC shall advise Users of the action that should be taken in respect of quarantined communications, which will be one of the following:

(a) that quarantined communications must be deleted;

(b) that the User may decide whether quarantined communications should be processed or deleted; or

(c) that no action should be taken by the User in respect of quarantined communications, which will result in the quarantined communications being archived for 30 days and subsequently deleted by the DCC.

4.13. Upon being advised of the action to be taken, Users shall submit an email and Quarantined Communications Action File which specifies actions in respect of each quarantined communication and shall, where relevant, correspond with the actions as advised by the DCC. Such email shall be submitted to the Service Desk and shall include:

(a) the DSMS Incident reference number notified in the subject line of the email; and

(b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

4.14. The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time period has elapsed, the DCC shall archive all quarantined communications relating to the event and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident.

4.15. The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" ~~Interface Transaction~~Functional Component within the SSI which shall include the quarantined communications(s) in a CSV format. Each User shall update the Incident using the "Update Service Management Incident" ~~Interface Transaction~~Functional Component within the SSI and assign the Incident to DCC for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

(b) check that the format of the data is correct.

4.16. Within 24 hours of receipt of a Quarantined Communications Action File, the DCC shall validate that Quarantined Communications Action File and shall either:

(a) where the checks are successful, perform the actions on the quarantined communications and notify the User of successful completion of the notified actions once completed, via the SSI; or

(b) where the checks are unsuccessful, update and reassign the Incident and notify the User of the reason for the failure.

Appendix AH 'Self Service Interface Design Specification'

For full Appendix AH redlining please see Annex B

Appendix AI 'Self-Service Interface Code of Connection'

Amendments to definitions in Appendix AI:

Definitions

In this document, except where the context otherwise requires:

- expressions defined in section A1 of the Code (Definitions) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- any expressions not defined here or in section A1 of the Code have the meaning given to them in the Self-Service Interface ~~Design~~ Access Control Specification, the SSI Baseline Requirements Document or the DCC User Interface Specification.

Updates to references in Appendix AI

Communications Authentication

1.13 Each User shall install a valid Root DCCKICA Certificate, UI DCCKICA Certificate and Personnel Authentication Certificate in its User Personnel's browser prior to establishing a TLS1.2 connection to the Self-Service Interface in accordance with the Self-Service Interface ~~Design~~ Access Control Specification, where such DCCKI Certificates shall be obtained as set out in the DCCKI RAPP.

1.14 The User shall secure the connection between its User Personnel browser and the Self Service Interface or the Identity Provider Service used by the User, using TLS 1.2 in accordance with RFC5246 and will make use of:

(a) for the Identity Provider Service, mutual authentication using PKCS #3 Ephemeral Diffie Hellman key exchange to generate a shared secret for communications encryption, utilising one of the following cipher suites:

(i) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDHE-RSA-

AES128-SHA256;

(ii) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDHE-RSA-AES256-SHA384;

(iii) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256; or

(iv) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDHE-RSA-AES256-GCM-SHA384; or

(b) for the Self Service Interface, server-side authentication.

Technical Infrastructure

1.15 The DCC shall provide the User, via secured electronic means, with details of a Uniform Resource Locator (URL) to access the Self Service Interface, corresponding with each applicable IP address provided in accordance with clause 1.7.

1.16 The DCC shall give reasonable advance notification to each User of any changes to the Self-Service Interface URL.

1.17 The DCC shall ensure that the IP addresses of the Self-Service Interface shall remain static.

Use of DCC Identity Provider Service

1.18 Each User using the DCC Identity Provider Service shall follow the processes set out in the DCCKI RAPP in order to obtain Personnel Authentication Certificates for its User Personnel prior to accessing the Self-Service Interface.

1.19 Each User that elects to use the DCC Identity Provider Service may create, modify or remove accounts for its User Personnel using the Self-Service Interface as further set out in the Self-Service Interface Specification, save that in the case of accounts for an Administration User, the DCCKI Registration Authority shall, upon receiving an Administration User Credentials Request as set out in the DCCKI RAPP, create, modify or remove the accounts.

1.20 The DCC shall provide an Identity Provider Service that shall, pursuant to clause 1.26, store secure cookies on each User Personnel's browser(s) to validate login sessions and shall ensure that such cookies do not include storage of information that permits personal identification.

Use of an Identity Provider Service that is not the DCC Identity Provider Service

1.21 The DCC shall only permit the use of an Identity Provider Service which conforms to the Identity Provider Service requirements set out in the Self-Service Interface ~~Design~~ Access Control Specification. The DCC shall not provide access to the Self-Service Interface where a User uses an Identity Provider Service that does not conform to such requirements.

1.22 When using an Identity Provider Service that is not the DCC Identity Provider Service, a User shall provide to the DCC the following details of its authentication arrangements:

(a) identity provider – <name of external Identity Provider Service>; and

(b) identity provider - <External Identity Provider Service URL>

and shall inform the DCC if the details change.

1.23 Each User that elects to use an Identity Provider Service that is not the DCC Identity Provider Service shall ensure that the SAML assertions, as set out in the Self-Service Interface ~~Design~~ Access Control Specification, are applied to access requests prior to establishing a TLS session.

1.24 Where a User elects to operate an Identity Provider Service that is not the DCC Identity Provider Service, the DCC shall regard an authentic signature on the SAML token for a member of User Personnel as confirmation that the User has appropriately performed verification, validation, role assignment and authentication of that member of User Personnel.

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0058 'Changes to the governance of the Self-Service Interface'

Annex B

Legal text – SEC Appendix AH

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

These changes have been drafted against SEC Version 6.5.

Version AH 1.1

Appendix AH

Self-Service Interface ~~Design~~ Access Control Specification

DRAFT

Definitions

In this document, except where the context otherwise requires:

- expressions defined in Section A1 of the Code (Definitions) have the same meaning as is set out in that Section;
- the expressions in the ~~left hand~~left-hand column below shall have the meanings given to them in the ~~right hand~~right-hand column below; and
- any expressions not defined here or in Section A1 of the Code have the meaning given to them in the DCC User Interface Specification or the Self-Service Interface Code of Connection.

SSI Baseline Requirements Document	means a document which sets out the design specification of the Self-Service Interface, and which is maintained by the DCC in accordance with Section 1 of this Appendix AH.
Buseiness Functional Domain~~DCC Service User Organisation ID~~	~~means a displayed field which will follow the following format: "<(<User ID>)>< Party >/<User Role Reference> <(< Service User Descriptor >)>". NOTE: User Role Reference is as detailed in the DCC User Interface Specification.~~ means a grouping of one or more Functional Components which is used to describe and deliver the functional requirements of Self-Service Interface Users.
Functional Component ~~RequirementInterface Transaction~~	means a specific item or set of functionality provided by the Self-Service Interface which is subject to the access controls set out in this Appendix AH.~~means one of the interactions with the Self-Service Interface as detailed in clause 1.10.~~
Job Type Role	means one of the functional roles as set out in the table contained in clause 1.5.2~~1.9.2~~

DRAFT

Order Management System (OMS)	as defined in the CH Handover Support Materials
Security Assertion Markup Language (SAML)	an open, published framework for exchanging security information between online business partners
~~**Service User Descriptor**~~	~~means an optional free text field of up to 30 characters set by a User when a User ID is registered. Once this field is set it can only be changed via a request to the DCC Service Desk.~~

1 SELF-SERVICE INTERFACE ~~DESIGN~~ ACCESS CONTROL SPECIFICATION

The DCC shall ensure that, where the DCC receives a request to access the Self-Service Interface, it shall direct that request to the appropriate URL for dealing with that request, and that such URL shall be implemented and maintained such that communications across it can be authenticated.

1.1 Authorisation

The DCC shall ensure that each user of the Self-Service Interface shall only be permitted to access a~~n Interface Transaction~~Functional Component if it is entitled to do so pursuant to clause 1.5.1 and 1.5.2 given the User ID(s) and Job Type Role(s) that are supplied as attributes of the SAML assertion.

1.2 SAML Authentication

The DCC shall provide to Users a SAML-capable Identity Provider Service for the purpose of authentication of User Personnel to the Self-Service Interface (the "DCC Identity Provider Service").

Each User may use an Identity Provider Service that is not the DCC Identity Provider Service for the purpose of authentication of its User Personnel to the Self- Service Interface.

To authenticate each request from a User Personnel that seeks to access the Self-Service Interface, the DCC shall use either:

a) a SAML assertion provided by the DCC Identity Provider Service (as defined in clause 1.3); or

a SAML assertion provided by an Identity Provider Service provided by the User (as defined in clause 1.4).

After an Identity Provider Service provides the User Personnel's SAML assertion, the DCC shall store a secure cookie in the User Personnel's browser. Such secure cookie shall be set to expire 8.5 hours after initial authentication by:

a) the DCC, for the DCC Identity Provider Service; or
b) the User, where such User is using an Identity Provider Service that is not the DCC Identity Provider Service.

If this cookie exists during subsequent authentication, the DCC shall bypass SAML authentication. Where using either the DCC Identity Provider Service or any other Identity Provider Service, if a User wishes to change the rights of that User Personnel to access the Self-Service Interface, the User shall delete the cookie from the User Personnel's browser cookie store.

The User shall ensure that its browser uses HTTP POST to transfer SAML between its Identity Provider Service and the Self-Service Interface.

Each User shall ensure that SAML assertions are applied when requesting access to the Self-Service Interface.

Each User must, when using any Identity Provider Service, present the Job Type Role(s) for which access to the Functional Component~~Interface Transaction~~s ~~are~~is being requested in the SAML assertion sent to the DCC.

Each User shall ensure that each SAML assertion includes a Digital Signature produced by a DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate in accordance with the FIPS 186-4 Digital Signature Standard using SHA-256 hashing algorithm. The User shall ensure that a SHA-256 hashing algorithm is applied to the SAML assertion.

1.3 SAML Authentication via the DCC Identity Provider Service

Where a User Personnel attempts to access the Self-Service Interface and a non-expired cookie is not stored in the User Personnel's browser cookie store:

1. The DCC shall send a SAML assertion request to the DCC Identity Provider Service via the User Personnel's browser;
2. When requested, the User shall provide the requested credentials (username, password, and certificate) to the DCC Identity Provider Service;
3. As set out in clause 1.1, the DCC shall grant or deny that person's access to the Self-Service Interface by providing a cookie enabling such access to be stored in the User Personnel's browser cookie store. If access is denied, the DCC shall provide a browser message which requests that the User Personnel resubmits their credentials.

The DCC shall ensure that, where a User is using the DCC Identity Provider Service, access to the Self-Service Interface is only provided once a User Personnel performs a login and generates a new password the first time that it uses that Identity Provider Service.

1.4 SAML Authentication via an Identity Provider Service that is not the DCC Identity Provider Service

When using an Identity Provider Service that is not the DCC Identity Provider Service, the User shall comply with this clause 1.4.

1.4.1 Authentication Requirements

A User providing a SAML assertion when seeking to access the Self-Service Interface via an Identity Provider Service that is not the DCC Identity Provider Service, shall ensure that its Identity Provider Service:

- prompts the User Personnel to provide their credentials (username, password, and certificate); and
- validates the User Personnel's credentials and (only where successfully validated) sends a SAML response including a SAML assertion to the Self-Service Interface.

The User shall ensure that SAML assertions, provided to the DCC by its Identity Provider Service, comply with the OASIS Standard – Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0.

The User shall ensure that the Identity Provider Service authentication mechanism shall use an appropriate SAML security assertion to demonstrate conformance to UK Government Authentication Framework Level 2.

1.4.2 Enrolment of an Identity Provider Service that is not the DCC Identity Provider Service

Where using an Identify Provider Service that is not the DCC Identify Provider Service, prior to seeking to access the Self-Service Interface for the first time, the User shall obtain at least one DCCKI Infrastructure Certificate in accordance with the DCCKI RAPP, and shall install such DCCKI Certificates on its Identity Provider Service.

The User shall configure their Identity Provider Service as defined in clause 1.4.1 and export and send a copy of the Identity Provider Service metadata to the DCC via secured electronic means, where such metadata shall include the URL of the Identify Provider Service and contact details in respect of the Identity Provider Service. Where the DCC reasonably requires the metadata to include additional information, the DCC shall inform the User of the information required and the User shall provide the information requested.

1.4.3 SAML Profiles, Bindings and Protocols

The User shall ensure that the Identity Provider Service it uses supports the following SAML profile, binding and protocol:

Profile	Web Browser SSO (single sign-on)
Binding	HTTP POST (HTTP/1.1)
Protocol	Authentication Request Protocol

1.4.4 Identity Provider Service SAML Configuration

Where a User notifies the DCC that it wishes to use an Identity Provider Service that is not the DCC Identity Provider Service, the DCC shall upon request provide, to that User via secured electronic means, the following information to be included in each SAML assertion:

- the service provider unique ID to be used by the Identity Provider Service, which is denoted as '[UNIQUE IDENTIFIER SP]' in the SAML attributes list below; and
- the URL formatted identifier of the Self-Service Interface, which is denoted as '[DCC SP URL]' in the SAML attributes list below.

The User shall ensure that their Identity Provider Service:

- shall not sign Authentication Requests (AuthnRequest);
- shall sign SAML Assertions;
- shall not sign Authentication responses;
- shall not encrypt any part of the SAML assertion (other than the Digital Signature);
- shall use persistent and unique nameIDs;
- shall only include NotBefore, NotOnOrAfter or AudienceRestriction in the SAML Condition elements; and
- shall set the SAML assertion nameID to be persistent and unique to the User Personnel.

The User shall ensure that their Identity Provider Service sets the following SAML attributes shown in square brackets, making reference to the information shown after each colon:

- [UNIQUE IDENTIFIER IDP]: a unique ID assigned to the SAML response by the Identity Provider Service.
- [UNIQUE IDENTIFIER SP]: the service provider unique ID for the SAML request, as provided by the DCC.
- [TIMESTAMP]: a timestamp in standard SAML format.
- [DCC SP URL]: the URL formatted identifier for the Self-Service Interface, as provided by the DCC.
- [IDP ISSUER URL]: a URL identifying the Identity Provider Service issuing the SAML assertion.
- [SAML ASSERTION UNIQUE IDENTIFIER]: a unique identifier assigned to the SAML assertion by the Identity Provider Service.
- [MESSAGE SIGNATURE]: a Digital Signature generated by the signing of the SAML assertion message using the DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate.
- [USERNAME]: a unique username assigned to the User Personnel by the Identity Provider Service.

DRAFT

- [SESSION EXPIRY]: a valid SAML date/time object describing the expiry time of the session associated with the user.
- [ASSERTION START]: a valid SAML date/time object describing the start time of the validity of the SAML assertion.
- [ASSERTION EXPIRY]: a valid SAML date/time object describing the expiry time of the validity of the SAML assertion.
- [SAML AUTHENTICATION CONTEXT]: a valid SAML Authentication Context Class describing the authentication that the user has completed with the Identity Provider Service.
- [Role name]: Job Type Role(s) as described in section 1.5. Multiple roles should be specified by separating role names using commas (,).
- [OrgID]: a list of User ID(s) in relation to which the User has been granted permission to access information held on the Self-Service Interface by the other User(s) to whom that information pertains. Such permission having been granted in accordance with clause 1.1.1 and not having been rescinded in accordance with clause 1.5.4. Multiple User IDs should be specified by separating values with commas (,).

~~1.5 Interactive Web Interface~~

~~The DCC may timeout any connection to the Self-Service Interface after a period of inactivity of 15 minutes.~~

~~1.6 File Download Interface~~

~~The DCC shall ensure that the Self-Service Interface provides User Personnel who are downloading files with a prompt to save files.~~

~~1.7 Interaction with Order Management Systems (OMS)~~

~~The DCC shall provide a link from the Self-Service Interface that enables Users to navigate to the OMS. Access to the OMS and capabilities of the OMS are defined in the Communications Hub Handover Support Materials.~~

~~1.8 Error Handling~~

~~The DCC shall present, when an error is detected when a User attempts to either access the Self-Service Interface or access any Functional ComponentInterface Transaction, meaningful error messages containing codes as per HTTP/1.1 standard.~~

DRAFT

~~1.9~~1.5 Roles

~~1.9.1~~1.5.1 DCC defined access

The DCC shall provide to User Personnel of each User access to each ~~Interface Transaction~~Functional Component that the User is eligible to access as set out in Section H8.16 or, where not specified in Section H8.16, as set out in this clause 1.5. Such access shall either be full or conditional, where:

- 'Full' means that the User can access data and use all functions associated with the specific ~~Interface Transaction~~Functional Component; and
- 'Conditional' means that a User's entitlement to access data and use all functions associated with the specific ~~Interface Transaction~~Functional Component is based on the access rules for conditional access set out below.

BFD ID	Business Functional Domain Name	Service capability	Functional Component	DCC Defined Access
BFD01	Service Management	Provide service management capabilities in accordance with H9.4 and the Incident Management Policy, enabling Users to: • Raise, update, view and track I~~i~~ncidents. • Track and view detailed P~~p~~roblem information related to I~~i~~ncidents.	Raise service management I~~i~~ncidents UC_RaiseSMI_001 UC_RaiseSMI_002 UC_RaiseSMI_003 UC_RaiseSMI_004	Full
			Update service management I~~i~~ncidents UC_UpdateSMI_001	Conditional. Access shall be granted as set out in Section H9.

BFD ID	Business Functional Domain Name	Service capability	Functional Component	DCC Defined Access
			View service management I~~i~~ncidents UC_ViewSMI_001 UC_ViewSMI_002	Conditional. Access shall be granted as set out in Section H9.
			Problem management UC_ProblemManagement_001-, UC_ProblemManagement_002	Conditional. Access shall be granted in accordance with Section H9.
BFD02	Smart Metering I~~i~~nventory	Enable Users to search and query current information on Smart Meter Inventory down to individual D~~d~~evices in accordance with H8.16(a). Provide detailed information on a D~~d~~evice and any associated D~~d~~evices.	Smart metering inventory UC_Inventory_001-, UC_Inventory_002	Full
BFD03	DCC Service Status	Provide Users with a dashboard of component availability for ~~the~~ DCC Services in accordance with H8.16(g).	DCC service status UC_ServiceDashboard_001	Full
BFD04	Service Audit Trails	Enable Users to query information on Service A~~a~~udit T~~t~~rails, showing a record of service activity in accordance with H8.16(b). Only the records pertaining to that User will be shown in search and individual message view, where the records pertaining to a User are those for: • the User IDs for that User; and • any User IDs for which that User has been granted permission to access the information in accordance with clause 2.5.3 and such permission has not been rescinded in accordance with clause 2.5.4.	Service A~~a~~udit T~~t~~rails UC_ServiceAudit_001-, UC_ServiceAudit_002	Conditional. Access shall be granted as set out in Section H8.16(b).
BFD05	Forward Schedule of C~~c~~hange	Enable Users to query and view detailed information on Planned Maintenance, changes scheduled or change freezes affecting any of the following elements of DCC Smart Metering ecosystem in accordance with H8.16(g): • Communications Hub firmware.	Forward schedule of change UC_Schedule_001-, UC_Schedule_002-, UC_Schedule_003	Full

BFD ID	Business Functional Domain Name	Service capability	Functional Component	DCC Defined Access
		• Parse & Correlate software. • SMIKI software. • DCC-impacting SEC Releases~~SEC release~~. • Other major DCC releases. • Meter firmware (Meter firmware events will only be visible to Users for Devices for which they are the Responsible Supplier)~~.~~		
BFD06	Meter Read Transactions	Enable Users to query information on Meter Read Transactions for all users in accordance with H8.16(c).	Meter Read Transactions UC_Inventory_001	Full
BFD07	CSP SMWAN Network Coverage	Enable Users to query information on SM WAN network coverage down to premises level across each of the three GB regions in accordance with H8.16(f).	SM WAN network coverage UC_CSPCoverage_001 UC_CSPCoverage_002	Full
BFD08	DCC Service Alerts	Enable Users to view details of any S~~s~~ervice affecting news / A~~a~~lerts and other useful text relating to the quality of service delivery and service management in accordance with H8.16(g).	DCC S~~s~~ervice A~~a~~lerts UC_ServiceAlerts_001, UC_ServiceAlerts_002	Full
BFD09	Service Requests	Enable Users to: • Browse a catalogue of available DCC S~~s~~ervice R~~r~~equests. • Raise and~~,~~ update service management S~~s~~ervice R~~r~~equests with DCC from their service catalogue. Enables~~ing~~ Users to track and update the status of raised requests within DCC service management system. • View full details ~~of the details~~ of the raised S~~s~~ervice R~~r~~equest User Personnel will only be able to access requests raised by the User with which they are associated.	Service catalogue publication and call off UC_ServiceCatalogue_001-, UC_ServiceCatalogue_002-, UC_ServiceCatalogue_003	Full

BFD ID	Business Functional Domain Name	Service capability	Functional Component	DCC Defined Access
BFD10	Communications Hub Availability & Diagnostics	Enable Users to query information on Communication Hub availability and diagnostics down to individual Communications Hubs. Allows Users to attempt to diagnose and resolve Incidents relating to any Communications Hubs for which they are the Responsible Supplier, the Network Party or Registered Supplier Agent, using DCC's remote diagnostic tools.	Communications Hub availability and diagnostics UC_HubStatus_001 UC_HubStatus_002	Conditional. Access shall be granted to the Responsible Supplier, the Network Party or Registered Supplier Agent for any Smart Metering System of which the Communications Hub Function in question forms a part.
BFD11	Reporting	Enable users to access on demand a standard set of pre-defined reports. Allow Users to view and download individual reports from a defined set of published reports.	Reporting UC_Reports_001	Conditional. Users will only be permitted to view reports which pertain to them.
BFD12	Knowledge Management, Search and FAQ's	Enable Users to access the following functionality in accordance with H8.16(g) where applicable: • Knowledge management. This allows Users to view help and support information enabling early triage of User issues and queries, including access to the anonymous resolution details of service management problems and I~~i~~ncidents. • FAQ information. • DCC User Manuals detailing the operation of DCC S~~s~~ervices. • Search capability, allowing Users to search for content provided by the SSI using tagged keywords, or textual content of page titles and descriptions.	Knowledge management UC_KnowledgeManagement_001	Full
			FAQs UC_FAQ_001	Full
			DCC user manuals UC_Manuals_001	Full
			UC_Search_001	Full

BFD ID	**Business Functional Domain Name**	**Service capability**	**Functional Component**	**DCC Defined Access**
BFD13	Forecasting and Ordering	Enable Users to access OMS in accordance with H8.16(e). In OMS Users can submit orders and forecasts of future orders for Communications Hubs and Communication Hu~~i~~b Auxiliary Equipment.	Forecasting and ordering of Communications Hubs and auxiliary equipment UC_CSPOMS_001	Full
BFD14	User Identity & Login Access Management	Manage the verification of U~~u~~ser identities requesting login access to SSI and DCC Platforms.	Log In UC_Login_001	Full
		Manage the functionality available to individual Users based on their U~~u~~ser R~~r~~ole. This includes the following capabilities: • Enable Users to use DCC Identity Provider Service to assign access to functionality to their User Personnel based on Job Type Role and manage the SSI accounts and associated settings (~~e.g~~e.g. password resets) for User Personnel accounts subsequently created by an Administration User. • Enable Administration Users to unlock, delete and manage the details of another account created within their organis~~z~~ation. • Enable an Administration User to create a new account for User Personnel~~create a new person's account~~ within their organiszation. • Enable User Personnel to view detailed information about the account they are accessing via SSI including the functionality they have access to.	User account management UC_OrgManager_001-, UC_OrgManager_002-, UC_OrgManager_003	Conditional. Access shall be granted to Administration Users.
			User profile information UC_Profile_001	Full
		Ensure secure communications between DCC systems and Users.		

~~The DCC shall provide full access for the following Interface Transactions for any User:~~

- ~~UC_Login_001 - Log In as set out in clause 1.10.2~~
- ~~UC_Inventory_001 - Smart Metering Inventory as set out in Section H8.16(a)~~
- ~~UC_MeterRead_001 – Meter Read Transactions as set out in Section H8.16(c)~~
- ~~UC_CSPCoverage_001 - SM WAN network coverage as set out in Section H8.16(f)~~
- ~~UC_CSPOMS_001 - Access to the Order Management System as set out in Section H8.16(e)~~
- ~~UC_KnowledgeManagement_001 - Knowledge Management in accordance with Section H8.16(g)~~
- ~~UC_Schedule_001 - Forward schedule of change in accordance with Section H8.16(g)~~
- ~~UC_ServiceDashboard_001 - DCC Service Status in accordance with Section H8.16(g)~~
- ~~UC_ServiceAlerts_001 - DCC Service Alerts in accordance with Section H8.16(g)~~
- ~~UC_FAQ_001 - FAQs in accordance with Section H8.16(g)~~
- ~~UC_Manuals_001 - DCC User Manuals in accordance with Section H8.16(g)~~
- ~~UC_ServiceCatalogue_001 - Service Catalogue Publication and Call Off~~
- ~~UC_RaiseSMI_001 - Raise Incidents in accordance with the Incident Management Policy~~
- ~~UC_Search_001- Search as set out in clause 1.10.22~~
- ~~UC_Profile_001 - User profile information as set out in clause 1.10.21~~

~~The DCC shall provide conditional access on the following basis in relation to the following Interface Transactions and shall not provide access other than on the basis set out below:~~

- ~~UC_ServiceAudit_001 - Service audit trails for which access shall be granted as set out in Section H8.16(b).~~

DRAFT

- ~~UC_HubStatus_001 - Communications Hub availability and diagnostics, for which access shall be granted to the Responsible Supplier, the Network Party or Registered Supplier Agent for any Smart Metering System of which the Communications Hub Function in question forms a part.~~
- ~~UC_Reports_001 – Access to the following reports, available to any User and pertaining to that User:~~
  - ~~Installation Status Smart Meter Report~~
  - ~~Smart Metering Devices Status and Firmware Report~~
  - ~~Smart Metering Devices Status and Model Report~~
  - ~~Communications Hub with No Attached Devices Report~~
  - ~~Scheduled Service Requests Report~~
  - ~~Quarantined Requests Report~~
  - ~~Monthly Transaction Report~~
  - ~~Smart Metering Device Transaction Report~~
  - ~~Firmware Activations Service Request Report~~
  - ~~Load Balance Report~~

  ~~The DCC shall ensure that documentation relating to the format and content of such reports shall be provided to Users via secured electronic means, as and when produced or updated.~~
- ~~UC_ViewSMI_001., UC_UpdateSMI_001 - View and Update Service Management Incidents for which access shall be granted as set out in Section H9.~~
- ~~UC_OrgManager_001 – User Account management for User Personnel of Users using the DCC Identity Provider Service, for which access shall be granted to Administration Users.~~
- ~~UC_ProblemManagement_001 - Problem Management for which access shall be granted in accordance with Section H9.~~

DRAFT

Where a User is entitled to conditional access to more than one ~~Interface Transaction~~Functional Component, the DCC shall apply permissions such that any User Personnel can access any of those ~~Interface Transaction~~Functional Components that the User is eligible to access, subject to such User Personnel being entitled to such access on the basis of the Job Type Role(s) as further set out in 1.5.2.

~~1.9.2~~1.5.2 Administration User defined access

In addition to the full and conditional access restrictions applied by the DCC in 1.5.1, Administration Users, appointed in accordance with the process set out in the DCCKI RAPP, may further define access restrictions for User Personnel to individual ~~Interface Transaction~~Functional Components by assigning one or more Job Type Roles to User Personnel in relation to one or more User IDs. Where a User is using the DCC Identity Provider Service, the DCC shall enable an Administration User to do this through the use of the Functional Component~~Interface Transaction UC_OrgManager_001~~User Account Management~~, as set out in clause 1.10.20~~.

The DCC shall ensure that access to ~~Interface Transaction~~Functional Components is only provided to the Job Type Role(s) presented to the DCC by the User in the SAML assertion accompanying the request for access to the ~~Interface Transaction~~Functional Component, on the basis of the ~~Interface Transaction~~Functional Components that the Job Type Role is entitled to access as set out in the table below.

The table below shows which ~~Interface Transaction~~Functional Components that User Personnel with a given Job Type Role are only permitted to access (User Personnel with a given Job Type Role may only access those ~~Interface Transaction~~Functional Components where there is a 'Y' in the corresponding box).

Where the SAML assertion presented to the DCC when seeking to access the ~~Interface Transaction~~Functional Component(s) contains multiple Job Type Roles, the DCC shall grant access to that User Personnel to all of the ~~Interface Transaction~~Functional Components that it is entitled to access in all of those Job Type Roles.

DRAFT

Functional Component	Job Type Role										
	All Access	Organisational Administrator	Security User	Lead Agent	Call Centre User	MI User	Service Management User	Smart Meter Operations User	Asset Management Ordering	SEC Contract Manager	Logistics
BFD01 Service Management											
Raise service management incidents UC_RaiseSMI_001 UC_RaiseSMI_002 UC_RaiseSMI_003 UC_RaiseSMI_004	Y	Y	Y	N	N	N	Y	N	N	N	Y
Update service management incidents UC_UpdateSMI_001	Y	Y	Y	N	N	N	Y	N	N	N	Y
View service management incidents UC_ViewSMI_001 UC_ViewSMI_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y
Problem management UC_ProblemManagement_001-, UC_ProblemManagement_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y

DRAFT

BFD02 Smart Metering Inventory											
Smart metering inventory UC_Inventory_001-, UC_Inventory_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BRD03 DCC Service Status											
DCC service status UC_ServiceDashboard_001	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
BDF04 Service Audit Trails											
Service audit trails UC_ServiceAudit_001-, UC_ServiceAudit_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
BFD05 Forward Schedule Of Change											
Forward schedule of change UC_Schedule_001-, UC_Schedule_002-, UC_Schedule_003	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD06 Meter Read Transactions											
Meter Read Transactions UC_Inventory_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
BFD07 CSP SMWAN Network Coverage											
SM WAN network coverage UC_CSPCoverage_001 UC_CSPCoverage_002	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
BFD08 DCC Service Alerts											
DCC service alerts UC_ServiceAlerts_001, UC_ServiceAlerts_002	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD09 Service Requests											

DRAFT

Service catalogue publication and call off UC_ServiceCatalogue_001-, UC_ServiceCatalogue_002-, UC_ServiceCatalogue_003	Y	Y	N	Y	N	N	N	N	Y	N	Y
BFD10 Communications Hub Availability & Diagnostics											
Communications Hub availability and diagnostics UC_HubStatus_001 UC_HubStatus_002	Y	Y	N	Y	Y	N	Y	Y	N	N	Y
BFD11 Reporting											
Reporting UC_Reports_001	Y	Y	N	Y	N	Y	N	N	N	Y	Y
BFD12 Knowledge Management, Search and FAQ											
Knowledge management UC_KnowledgeManagement_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
FAQs UC_FAQ_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DCC user manuals UC_Manuals_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
UC_Search_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BFD13 Forecasting and Ordering											
Forecasting and ordering of Communications Hubs and auxiliary equipment UC_CSPOMS_001	Y	Y	N	N	N	Y	N	N	Y	N	Y
BFD14 User Identity & Access Management											

DRAFT

Log In UC_Login_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
User account management UC_OrgManager_001 , UC_OrgManager_002 , UC_OrgManager_003	N	Y	N	N	N	N	N	N	N	N	N
User profile information UC_Profile_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

DRAFT

~~1.9.3~~1.5.3 Users granting access to other Users

Information available through the Self-Service Interface that relates to one or more User IDs of a User may be shared with another User where that other User is also willing to share information relating to one or more of its User IDs with the first User.

Where two Users wish to grant access to each other's information accessible through the Self-Service Interface, each of those Users shall submit, via secured electronic means, a notification to the DCC which includes:

- that the notification relates to granting to another User access to its data which is available via the Self-Service Interface;
- the list of User IDs of both of the relevant Users, for which mutual access for the two Users is being granted; and
- details of the DCCKI SRO responsible for the relevant User IDs that is authorising such access on behalf of the User submitting the notification, which shall comprise:
    - the name of the authorising DCCKI SRO;
    - telephone and email contact details for the DCCKI SRO; and
    - signature of the DCCKI SRO.

Upon receipt of such notifications, the DCC shall confirm if each request is authentic, by:

- verification of the DCCKI SRO; and
- by confirming that the User IDs provided by each User granting access are User IDs that have been assigned to each such User by the Panel in accordance with H1.6.

Where both of the notifications are confirmed to be authentic, the DCC shall:

- configure the Self-Service Interface to enable any Administration User acting on behalf of either of the two Users to grant access to its User Personnel to information available via the Self-Service Interface relating to any of such User IDs; and
- confirm in writing, to each DCCKI SRO submitting a notification that such access has been granted.

Where either or both of the notifications are not confirmed to be authentic, the DCC shall confirm in writing, to each of the DCCKI SRO submitting a notification, that such access has been rejected and giving the reasons for rejection.

~~1.9.4~~1.5.4 Users rescinding access permission to other Users

Where a User wishes to rescind permission to allow another User to access its information available through the Self-Service Interface for a defined set of User IDs, having previously granted such access, the User wishing to remove access shall submit, in writing via secured electronic means, a notification to the DCC which includes:

- that the User wishes to rescind access to its information on the Self-Service Interface by another User;
- the list of User IDs pertaining to the User submitting the notification, for which it wishes to rescind access to another User (each a "Rescinding User ID");
- the list of User IDs pertaining to the other User for which access is to be rescinded (each a "Rescinded User ID"); and
- details of a DCCKI SRO that is authorising such rescinding of access on behalf of the User submitting the notification, which shall comprise:
  - the name of the authorising DCCKI SRO;
  - telephone and email contact details for the DCCKI SRO; and
  - signature of the DCCKI SRO.

Upon receipt of such a notification, the DCC shall confirm if the request is authentic, by:

- verification of the DCCKI SRO; and
- by confirming that the User IDs provided by the User notifying that access should be rescinded, are User IDs that have been assigned to that User by the Panel in accordance with H1.6.

Where the notification is confirmed to be authentic, the DCC shall:

- configure the Self-Service Interface to remove access to information relating to Rescinding User IDs by any User Personnel of the second User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinded User ID;
- configure the Self-Service Interface to remove access to information relating to Rescinded User IDs by any User Personnel of the first User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinding User ID; and

- confirm in writing, to the DCCKI SROs of both affected Users that such access has been rescinded.

Where the notification is not confirmed to be authentic, the DCC shall confirm in writing, to the DCCKI SRO, that the notification of permission to be rescinded has been rejected.

~~1.10 Freshness of Data SourcesInterface Transactions~~

~~Freshness of Data Sources~~

~~The DCC shall update data available to Users via the Self-Service Interface to reflect the most recent information held by the DCC as soon as reasonably practicable, but in any event within 24 hours of receipt or generation of that data by the DCC.~~

~~1.10.1 Log In~~

~~Interface transaction name~~	~~UC_Login_001~~
~~Definition~~	~~Enables User Personnel to login and access Self-Service Interface functionality~~
~~Preconditions~~	~~The User must exist within either the DCC Identity Provider Service, or a User Identity Provider Service~~
~~Inputs~~	~~Username, password and the certificate which is automatically presented by the User's browser~~ ~~additionally, upon first login:~~ ~~• First name~~ ~~• Last name~~ ~~• Email address~~ ~~• Contact telephone number~~
~~Outputs~~	~~Login confirmation~~

~~1.10.2 Smart Metering Inventory~~

~~**Interface transaction name**~~	~~UC_Inventory_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to query details of the Smart Metering Inventory~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~One or more of the following:~~ ~~- MPxN~~ ~~- Device ID~~ ~~- full postcode and property filter (inclusive of property name / number)~~ ~~- UPRN~~ ~~- include Devices that have an SMI Status that is not 'commissioned' (checkbox)~~
~~**Outputs**~~	~~If matches are found, a table of results is displayed, showing the following fields for each matching Device:~~ ~~- Device ID~~ ~~- Device Type~~ ~~- For installed Smart Meters, the related MPxN~~ ~~- For all Devices that are not Type 2 Devices, SMI Status~~ ~~- first line of address~~ ~~- UPRN~~ ~~- full postcode~~

DRAFT

~~**Interface transaction name**~~	~~UC_Inventory_002 (Ext. 1 – Specific Device Details View)~~
~~**Definition**~~	~~Enables User Personnel to query details of the Smart Metering Inventory~~
~~**Preconditions**~~	~~The User has used the Smart Metering Inventory search to find a specific Device, and followed the Device ID link, to request the details view for the selected Device (and associated Devices).~~
~~**Access Control**~~	~~The button that allows the user to jump across to UC_ServiceAudit_002 for this Device~~
~~**Inputs**~~	~~One of the following:~~ ~~– For installed Smart Meters, the related MPxN~~ ~~– Device ID~~ ~~– full postcode and property filter~~ ~~– UPRN~~ ~~– include Devices that have an SMI Status that is not 'commissioned' (checkbox)~~
~~**Outputs**~~	~~If matches are found, a table of results is displayed, showing the following fields for each matching Device and associated Devices, where applicable to the Device Type:~~ ~~– Device ID~~ ~~– Manufacturer~~ ~~– Device Model~~ ~~– Device Type~~ ~~– For Electricity Smart Meters, the applicable ESME Variant~~ ~~– SMETS Version~~ ~~– For Communications Hubs, the WAN Technology Type~~ ~~– Firmware Version~~ ~~– For Communications Hubs, the CSP region in which the Device is or has been installed~~ ~~– MPxN~~ ~~– For all Devices that are not Type 2 Devices, SMI Status (including Status history)~~ ~~– first line of address~~ ~~– UPRN~~ ~~– full postcode~~ ~~Associated Devices and Devices with which that Device is Associated~~ ~~– Device ID~~ ~~– SMI Status~~ ~~– Description of Device~~

DRAFT

~~1.10.3 Service Audit Trails~~

~~**Interface transaction name**~~	~~UC_ServiceAudit_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to query the service audit trail data held within the DCC Data Systems to show a record of all service activity~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Access Control**~~	~~Only the records pertaining to that User will be shown in search and individual message view, where the records pertaining to a User are those for:~~ ~~• the User IDs for that User; and~~ ~~• any User IDs for which that User has been granted permission to access the information in accordance with clause 1.9.3 and such permission has not been rescinded in accordance with clause 1.9.4.~~
~~**Inputs**~~	~~One of the following:~~ ~~MPxN~~ ~~Device GUID~~ ~~UPRN~~ ~~Service Reference Variant~~ ~~From date~~ ~~To date~~
~~**Outputs**~~	~~If matches are found, a table of results is displayed, showing the following Service audit trail details for each matching Device:~~ ~~**Field Name:**~~ ~~DCC Service User Organisation ID~~ ~~Device ID~~ ~~GBCS Transaction Sequence Number, where required by GBCS~~ ~~MPxN~~ ~~Service Request Received Date/Time~~ ~~Service Response Sent Date/Time~~ ~~Service Reference~~ ~~Simplified transaction status, which shall be one of the following:~~ ~~• Success~~ ~~• Failure~~ ~~• In Progress~~ ~~**Full Details**:~~ ~~Field Name~~

DRAFT

	~~Request ID~~ ~~Response ID~~ ~~DCC Service User Organisation ID~~ ~~Device ID~~ ~~CSP Region~~ ~~Mode of operation, which shall be one of the following:~~ • ~~On Demand~~ • ~~Future Date~~ • ~~DSP Scheduled~~ • ~~DCC Only~~ • ~~Device Alert~~ • ~~DCC Alert~~ • ~~Meter Scheduled~~ ~~Preceding Request ID (where applicable)~~ ~~MPxN~~ ~~Service Reference~~ ~~Service Reference Variant~~ ~~Command Variant~~ ~~Response Code~~ ~~Current Status~~ ~~Anomaly Detection Flag~~ ~~Status Change History~~

~~**Interface transaction name**~~	~~UC_ServiceAudit_002 (Ext. 1 – Direct Linked Search)~~
~~**Definition**~~	~~This is UC_ServiceAudit_001 (Main Flow) pre populated as the result of following a link on a previous page.~~
~~**Preconditions**~~	~~User Personnel followed a Device link on another Self-Service Interface page which has directed them to the Service audit trails search page with a value indicating that a search for a specific Device ID should be carried out immediately~~
~~**Inputs**~~	~~Service audit trail (selected from output of UC_ServiceAudit_001)~~
~~**Outputs**~~	~~Service audit trail details for the Device:~~ ~~**Field Name:**~~ ~~DCC Service User Organisation ID~~ ~~Device ID~~ ~~Sequence Number~~ ~~MPxN~~

DRAFT

	~~Service Request Received Date/Time~~ ~~Service Response Sent Date/Time~~ ~~Service Reference~~ ~~Simplified Transaction Status~~ ~~**Full Details:**~~ ~~Field Name~~ ~~Request ID~~ ~~Response ID~~ ~~DCC Service User Organisation ID~~ ~~Device ID~~ ~~CSP Region~~ ~~Mode of Operation~~ ~~Preceding Request ID (where applicable)~~ ~~MPxN~~ ~~Service Reference~~ ~~Service Reference Variant~~ ~~Command Variant~~ ~~Response Code~~ ~~Current Status~~ ~~Anomaly Detection Flag~~ ~~Status Change History~~

DRAFT

~~1.10.4 Meter Read Transactions~~

~~Interface transaction name~~	~~UC_MeterRead_001 (Main Flow)~~
~~Definition~~	~~Enables User Personnel to query the service audit trail data held within the DCC Data Systems to show records of meter read transaction activity for all Users. This differs from the main service audit trail use case [UC_ServiceAudit_001 (Main Flow)] in that all service audit trail entries for meter read transaction activity through this use case are available to all Users.~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Access Control~~	~~In the case of service audit records relating to 'Read Profile Data' and 'Retrieve Daily Consumption Log' Service Requests, any User may access the service audit records in accordance with H8.16(c).~~
~~Inputs~~	~~One of the following:~~ ~~Device GUID~~ ~~UPRN~~ ~~MPxN~~ ~~Service Reference Variant~~ ~~Checkboxes allowing the selection of any of the following Service Reference Variants ; 4.8.1, 4.8.2, 4.8.3 or 4.17~~ ~~From date~~ ~~To date~~
~~Outputs~~	~~If matches are found, a table of results is displayed, showing the following Service audit trail details for each matching Device:~~ ~~**Field Name:**~~ ~~DCC Service User Organisation ID Device ID~~ ~~GBCS Transaction Sequence Number, where required by GBCS~~ ~~MPxN~~ ~~Service Request Received Date/Time~~ ~~Service Response Sent Date/Time~~ ~~Service Reference Variant~~ ~~Service Reference~~ ~~Simplified transaction status, which shall be one of the following:~~ ~~• Success~~ ~~• Failure~~ ~~• In Progress~~

DRAFT

	~~**Full Details**~~~~:~~ ~~Field Name~~ ~~Request ID~~ ~~Response ID~~ ~~DCC Service User Organisation ID~~ ~~Device ID~~ ~~CSP Region, which shall be one of the following:~~ • ~~North~~ • ~~Central~~ • ~~South~~ • ~~Unknown~~ ~~Mode of operation, which shall be one of the following:~~ • ~~On Demand~~ • ~~Future Date~~ • ~~DSP Scheduled~~ • ~~DCC Only~~ • ~~Device Alert~~ • ~~DCC Alert~~ • ~~Meter Scheduled~~ ~~Preceding Request ID (where applicable)~~ ~~MPxN~~ ~~Service Reference Variant~~ ~~Command Variant~~ ~~Response Code~~ ~~Current Status~~ ~~Anomaly Detection Flag~~ ~~Status Change History~~

DRAFT

~~1.10.5 SM WAN Network Coverage~~

~~Interface transaction name~~	~~UC_CSPCoverage_001 (Main Flow)~~
~~Definition~~	~~Enables User Personnel to check SM WAN coverage data at a postcode level across GB in each of the three Regions~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~One of the following:~~ ~~• full postcode~~ ~~• full postcode and property name/number~~ ~~• a postcode outcode (all but the last three characters of a full postcode)~~
~~Outputs~~	~~CSP (the CSP responsible for this location/area)~~ ~~Postcode~~ ~~Property name/number (where appropriate)~~ ~~WAN coverage availability (Yes or No)~~ ~~Anticipated coverage date (if coverage availability was No), or "No Coverage Intended"~~ ~~Likelihood of connectivity to the SM WAN at the location~~ ~~Communications Hub WAN Variant to be used~~ ~~Auxiliary equipment required~~ ~~Additional information, which shall (where applicable) contain details of:~~ ~~• whether the location is included within an area that is the subject of a Service Exemption Category 2 and if so, where applicable, the date from which the location will cease to be included; and~~ ~~• issues giving rise to poor connectivity at the location and any information regarding likely resolution to such connectivity issues.~~ ~~A button to initiate the download of a comma separated variable file using the above list of outputs.~~

DRAFT

~~Interface transaction name~~	~~UC_CSPCoverage_002 (Ext. 1 – Direct Linked Search)~~
~~Definition~~	~~Enables User Personnel to view details of WAN coverage where returned as a result of a search other than that defined in UC_CSPCoverage_001 (Main Flow).~~
~~Preconditions~~	~~User Personnel followed a Device link on another Self-Service Interface page which has directed them to the WAN Coverage search page with an argument indicating that a search for a specific postcode or premises should be carried out immediately~~
~~Inputs~~	~~None~~
~~Outputs~~	~~CSP (the CSP responsible for this location/area)~~ ~~Postcode~~ ~~Property name/number (where appropriate)~~ ~~Coverage availability (Yes or No)~~ ~~Anticipated coverage date (if coverage availability was No), or "No Coverage Intended"~~ ~~Likelihood of connectivity (Low/Medium/High)~~ ~~Communications Hub WAN Variant to be used~~ ~~Auxiliary equipment required~~ ~~Additional information~~

~~1.10.6 Communications Hub Availability and Diagnostics~~

~~Interface transaction name~~	~~UC_HubStatus_001 (Main Flow)~~
~~Definition~~	~~Enables User Personnel to attempt to diagnose and resolve incidents using the DCC's remote diagnostic tools~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Access Control~~	~~The initial Communications Hub availability and diagnostics search form has full access to all User Roles~~ ~~The button "Communicate With Device" is only accessible to the Responsible Supplier, The Network Party or Registered Supplier Agent, for a Smart Metering System of which a Communications Hub Function forms a part.~~ ~~In order to be able to carry out a full diagnostics request, the User must be the Responsible Supplier, The Network Party or Registered Supply Agent for a Smart Metering system of which a Communications Hub Function forms a part.~~ ~~Roles apply (see clause 1.9)~~

DRAFT

~~**Inputs**~~	~~Communications Hub Function Device ID~~
~~**Outputs**~~	~~Anonymised table of Service Requests giving rise to up to the last 5 Commands transacted through the Communications Hub, showing time and success status in relation to the Command being issued to the Device.~~ ~~A table showing data provided by the CSP responsible for this Communications Hub (data resident on the Communications Hub displays "Requires device communication"), and providing the following fields:~~ ~~Aerial Installed~~ ~~Aerial Type~~ ~~Birth Event~~ ~~Network Status~~ ~~Deactivation Date/Time (if network status is deactivated)~~ ~~SMWAN Connectivity Status~~ ~~HAN Status~~ ~~Last Connection~~ ~~Last Tamper~~ ~~Last Outage~~ ~~Last Restore~~

~~**Interface transaction name**~~	~~UC_HubStatus_002 (Ext. 1 – Direct Linked Search)~~
~~**Definition**~~	~~Enables User Personnel to view details of selected Communications Hub availability information where returned as a result of a search other than that defined in UC_HubStatus_001 (Main Flow).~~
~~**Preconditions**~~	~~User Personnel followed a Device link on another Self-Service Interface page which has directed them to the Communications Hub availability and diagnostics search page with an argument indicating that a search for a specific Communications Hub should be carried out immediately~~
~~**Inputs**~~	~~None (Device ID selected on UC_HubStatus_001)~~
~~**Outputs**~~	~~Anonymised table of Service Requests giving rise to up to the last five Commands transacted through the Communications Hub, showing time and success status in relation to the Command being issued to the Device.~~ ~~A table showing data provided by the CSP responsible for this Communications Hub (data resident on the Communications Hub displays "Requires Device Communication")~~

DRAFT

~~1.10.7 Forecasting and ordering of Communications Hubs and auxiliary equipment~~

~~Interface transaction name~~	~~UC_CSPOMS_001 (Main Flow)~~
~~Definition~~	~~Redirects User Personnel to the OMS (which enables User Personnel to submit forecasts of future orders and actual orders for Communications Hubs and Communications Hub Auxiliary Equipment requirement)~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Access Control~~	~~Any User has access~~
~~Inputs~~	~~Region selection (buttons)~~
~~Outputs~~	~~None (CSP web based OMS page opens in a new window)~~

~~1.10.8 Reporting~~

~~Interface transaction name~~	~~UC_Reports_001~~
~~Definition~~	~~Enables User Personnel to run a set of standard pre-defined and parameterised reports against DCC data as listed in clause 1.9.1. Such reports are specified in the SSI reporting specification as published on the DCC Website.~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Access Control~~	~~Reports will only display data pertaining to the User.~~ ~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~Report specific input parameters~~
~~Outputs~~	~~Report output data~~

DRAFT

~~1.10.9 Raise Incident~~

~~Interface transaction name~~	~~UC_RaiseSMI_001 (Main Flow)~~
~~Definition~~	~~Enables User Personnel to raise service management Incidents within the DCC service management systems~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Access Control~~	~~User Personnel can only raise Incidents in accordance with H9~~
~~Inputs~~	~~Incident category-specific parameters~~ ~~User Personnel contact details:~~ ~~- first name, last name, telephone number (mandatory fields)~~ ~~- email address (optional)~~
~~Outputs~~	~~Incident reference~~

~~Interface transaction name~~	~~UC_RaiseSMI_002 (Ext. 1 – Direct Linked Pre Selection)~~
~~Definition~~	~~This is a special case of UC_RaiseSMI_001 (Main Flow), where User Personnel navigated from another screen, and the category of the Incident and some input fields are pre-populated~~
~~Preconditions~~	~~User Personnel followed a link on another page, indicating that they would like to raise an Incident related to the content that they are viewing, including the Communications Hub status and Communications Hub Availability and Diagnostics page to raise an incident for that Communications Hub, or a knowledge article to provide feedback on that article.~~
~~Inputs~~	~~Incident category-specific parameters~~
~~Outputs~~	~~Incident reference~~

~~Interface transaction name~~	~~UC_RaiseSMI_003 (Ext. 2 – Premises Related Incident)~~
~~Definition~~	~~This is a special case of UC_RaiseSMI_001 (Main Flow), where User Personnel chose to raise a premises related Incident, which has a more complex and specific workflow than other Incident categories~~
~~Preconditions~~	~~User Personnel chose "Premises Related Incident" in the second step of UC-RaiseSMI_001~~
~~Access Control~~	~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~DeviceID or MPxN~~

DRAFT

	~~User ID (where a User has been granted access to the Self-Service Interface on behalf of another User, in accordance with clause 1.9.3)~~ ~~Incident-specific information (optional)~~ ~~Incident summary~~ ~~Your reference~~ ~~Incident notes (optional)~~ ~~User Personnel contact details:~~ ~~- first name, last name, telephone number (mandatory fields)~~ ~~- email address (optional)~~
~~**Outputs**~~	~~Incident reference~~

~~**Interface transaction name**~~	~~UC_RaiseSMI_004 (Ext. 3 – Direct Linked Pre Selection For Premises Related Incident)~~
~~**Definition**~~	~~This is a special case of UC_RaiseSMI_003, where User Personnel navigated from the Communications Hub availability and diagnostics screen, and the category of the incident and input/verification of the Communications Hub have been pre-verified and pre-populated~~
~~**Preconditions**~~	~~User Personnel followed a link from the Communications Hub Availability and Diagnostics page, indicating that they would like to raise a premise related Incident against the Communications Hub that they are viewing.~~
~~**Inputs**~~	~~Incident-specific information (optional)~~ ~~Incident summary~~ ~~Business impact~~ ~~Incident notes (optional)~~ ~~User Personnel contact details:~~ ~~- first name, last name, telephone number (mandatory fields)~~ ~~- email address (optional)~~
~~**Outputs**~~	~~Incident reference~~

~~1.10.10 Update Service Management Incident~~

~~**Interface transaction name**~~	~~UC_UpdateSMI_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to make updates to an existing Incident~~
~~**Preconditions**~~	~~- Roles apply (see clause 1.9)~~ ~~- User Personnel must be appropriately privileged to update the Incident in question (according to section H9).~~

DRAFT

	~~User Personnel will have navigated from UC_ViewSMI_002~~
~~**Access Control**~~	~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~Incident reference~~ ~~Type of update~~ ~~Update text~~
~~**Outputs**~~	~~Update confirmation~~

~~1.10.11 View Service Management Incident~~

~~**Interface transaction name**~~	~~UC_ViewSMI_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to view details of previously raised Incidents within the DCC Service Management System~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Access Control**~~	~~The Incidents shown will be limited in accordance with H9~~ ~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~Incident (selected from prepopulated list of incidents)~~
~~**Outputs**~~	~~None (UC_ViewSMI_002 presents incident details)~~

~~**Interface transaction name**~~	~~UC_ViewSMI_002 (Ext. 1 – View Specific Incident)~~
~~**Definition**~~	~~This is a sub screen of the main UC_ViewSMI_001 (Main Flow) showing more detailed information relating to selected service management Incident information~~
~~**Preconditions**~~	~~User Personnel followed a link from another Interface Transaction indicating that they would like to see the details of a specific service management incident, and is appropriately privileged to view details of the incident (in accordance with H9)~~
~~**Access Control**~~	~~The Incidents shown will be limited in accordance with H9.~~ ~~Where the User did not raise the Incident, the Interface Transaction withholds from the User certain personal information about the raising individual, contact details and incident update description~~ ~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~None (incident prepopulated from UC_ViewSMI_001)~~
~~**Outputs**~~	~~Summary text~~ ~~Incident notes~~

	~~Raising individual - first and last name (only visible to the User that raised the Incident)~~ ~~Raising organisation (User)~~ ~~Device (where appropriate)~~ ~~Communications Hub model and version (where appropriate)~~ ~~MPxNs associated with Smart Meter(s) related to incident - comma-separated list~~ ~~CSP Diagnostic output (where appropriate)~~ ~~Postcode (where appropriate)~~ ~~Your reference~~ ~~Current status~~ ~~Target resolution date/time~~ ~~Requester contact details - first and last name, telephone number and email (not visible to interested persons)~~ ~~Additional contact details - first and last name, telephone number and email (not visible to interested persons)~~ ~~Incident priority~~

~~1.10.12 Knowledge Management~~

~~**Interface transaction name**~~	~~UC_KnowledgeManagement_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to view relevant help and support information (provided by DCC and its Service Providers), for early triage of User issues and queries, including access to the anonymous resolution details of service management problems and Incidents~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~List of all stored Articles, from which the User Personnel will select an article~~
~~**Outputs**~~	~~Article details~~ ~~- Title~~ ~~- Creation Date/Time~~ ~~- Creator~~ ~~- Last Modifier~~ ~~- Tags~~ ~~- Article text~~ ~~- Attachments (optional)~~

DRAFT

~~1.10.13 Forward Schedule of Change~~

~~**Interface transaction name**~~	~~UC_Schedule_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to view details of any planned maintenance, changes scheduled or change freezes affecting any of the following elements of the DCC Total System:~~ ~~- Communications Hub firmware~~ ~~- Parse & Correlate Software~~ ~~- SMKI software~~ ~~- SEC releases~~ ~~- other major DCC releases~~ ~~- meter firmware events~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Access Control**~~	~~Meter firmware events will only be visible to Users for Devices for which they are the Responsible Supplier.~~ ~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~None~~
~~**Outputs**~~	~~Planned start date/time~~ ~~Planned end date/time~~ ~~Event type~~ ~~System component (or release/change type)~~ ~~Impact severity~~ ~~Geographic impact~~ ~~Notes~~ ~~Full details – button linking to UC_Schedule_003~~

DRAFT

~~Interface transaction name~~	~~UC_Schedule_002 (Ext. 1 – Calendar View)~~
~~Definition~~	~~Enables User Personnel to view details of planned events within the DCC Systems or relating to the SM WAN in a calendar format~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Access Control~~	~~Meter firmware events will only be visible to Users for Devices for which they are the Responsible Supplier.~~
~~Inputs~~	~~None~~
~~Outputs~~	~~Calendar day cells containing items representing event types relevant to that day~~

~~Interface transaction name~~	~~UC_Schedule_003 (Ext. 2 – View Specific Event)~~
~~Definition~~	~~Allows User Personnel, having chosen to view a specific event from UC_Schedule_001 or UC_Schedule_002, to view the full details held about the event in question~~
~~Preconditions~~	~~User Personnel followed a link from UC_Schedule_001 or UC_Schedule_002, choosing to view the full details held about a specific event~~
~~Access Control~~	~~Meter firmware events will only be visible to Users for Devices for which they are the Responsible Supplier.~~ ~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~Event (selected on UC_Schedule_001 or UC_Schedule_002)~~
~~Outputs~~	~~Event details:~~ ~~- event reference~~ ~~- planned start date/time~~ ~~- planned end date/time~~ ~~- event notes~~ ~~For maintenance and change freeze events:~~ ~~- event type~~ ~~- DCC System component or Region~~ ~~- impact severity~~ ~~- geographic impact~~ ~~For release, meter firmware and change events:~~ ~~- release/change type~~ ~~- manufacturer's reference~~

DRAFT

	~~- manufacturer's notes~~ ~~- Device type and Device Model~~ ~~- firmware version~~

~~1.10.14 DCC Service Status~~

~~Interface transaction name~~	~~UC_ServiceDashboard_001 (Main Flow)~~
~~Definition~~	~~Enables User Personnel to view a one page dashboard of DCC component availability for the DCC Service~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~None~~
~~Outputs~~	~~List of system components comprising:~~ ~~- DCC System component name~~ ~~- high level status of component~~ ~~- count of the number of underlying service alerts for the component~~ ~~Link to service alerts relating to Major Incidents~~

~~1.10.15 DCC Service Alerts~~

~~Interface transaction name~~	~~UC_ServiceAlerts_001~~
~~Definition~~	~~Enables User Personnel to view any service affecting news / alerts and other useful text (in terms of quality of service delivery and service management) to the User~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~None~~
~~Outputs~~	~~List of currently active Alerts:~~ ~~- Service Alert ID (link to UC_ServiceAlerts_002)~~ ~~- System component/s – listed in UC_Servicedashboard_001~~ ~~- geographic impact~~ ~~- alert creation~~ ~~- expected resolution~~ ~~- alert closure~~ ~~- latest update~~

DRAFT

~~Interface transaction name~~	~~UC_ServiceAlerts_002 (Ext. 1 – View Specific Alert)~~
~~Definition~~	~~This Interface Transaction allows User Personnel, having chosen to view a specific DCC Service Alert from UC_ServiceAlerts_001, to view the full details held about the alert in question.~~
~~Preconditions~~	~~User Personnel followed a link from UC_ServiceAlerts_001, choosing to view the full details held about a specific alert.~~
~~Inputs~~	~~Alert ID (specified in UC_ServiceAlerts_001)~~
~~Outputs~~	~~List of currently active Alerts:~~ ~~- Service Alert ID (link to UC_ServiceAlerts_002)~~ ~~- DCC System Component/s – listed in UC_Servicedashboard_001~~ ~~- geographic impact~~ ~~- alert creation~~ ~~- expected resolution~~ ~~- alert closure~~ ~~- latest update~~ ~~Reverse chronological list of updates for the alert, each comprising:~~ ~~- date/time of update~~ ~~- person/entity providing update~~ ~~- update text~~

~~1.10.16 FAQs~~

~~Interface transaction name~~	~~UC_FAQ_001 (Main Flow)~~
~~Definition~~	~~Enables User Personnel to access helpful DCC Service Frequently Asked Questions~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~Text filter string (optional)~~ ~~Tag selection from list of all tags (optional)~~
~~Outputs~~	~~FAQ question and answer~~ ~~Attached documents (optional)~~

~~1.10.17 DCC User Manuals~~

~~Interface transaction name~~	~~UC_Manuals_001 (Main Flow)~~
~~Definition~~	~~Enables User Personnel to access a set of DCC user manuals which help Users understand how the DCC Service operates~~

DRAFT

~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~Article reference~~ ~~Article usefulness rating selector~~
~~**Outputs**~~	~~Article page:~~ ~~- title of the article~~ ~~- creation date/time~~ ~~- creator~~ ~~- last modification~~ ~~- last modifier~~ ~~- tags~~ ~~- textual description of the user manual, other document, or content~~

~~1.10.18 Service Catalogue Publication/Call Off~~

~~**Interface transaction name**~~	~~UC_ServiceCatalogue_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to raise service management service requests with the DCC and track and update the status of such Requests within the DCC service management systems~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Access Control**~~	~~User Personnel will only be able to see requests raised by the User with which they are associated~~
~~**Inputs**~~	~~By accessing this page User Personnel will see the information listed in outputs section.~~ ~~Raise new request option (button) – redirects User Personnel to UC_ServiceCatalogue_003~~
~~**Outputs**~~	~~The Self-Service Interface will display all open service catalogue requests raised by their organisation with the following fields:~~ ~~Service request ID (hyperlink to UC_ServiceCatalogue_002) – Work order reference~~ ~~Request type~~ ~~Raised date/time~~ ~~Current delivery status~~

DRAFT

~~**Interface transaction name**~~	~~UC_ServiceCatalogue_002 (Ext. 1 – View Specific Request)~~
~~**Definition**~~	~~This Interface Transaction allows User Personnel, having chosen to view a specific service catalogue request from UC_ServiceCatalogue_001, to view the full details held about the request in question.~~
~~**Preconditions**~~	~~User Personnel followed a link from UC_ServiceCatalogue_001, choosing to view the full details held about a specific request.~~
~~**Access Control**~~	~~User Personnel will only be able to see requests raised by the User with which they are associated~~
~~**Inputs**~~	~~From selection in UC_Service_Catalogue_001~~
~~**Outputs**~~	~~Service Request ID (hyperlink to UC_ServiceCatalogue_002) – Work order reference~~ ~~Your reference~~ ~~Request type~~ ~~Raised date/time~~ ~~Current delivery status~~ ~~Raising user~~ ~~Raising Organisation – User ID~~ ~~Requester contact details – first and last name, telephone number and email.~~ ~~Additional contact details – first and last name, telephone number and email~~

DRAFT

~~**Interface transaction name**~~	~~UC_ServiceCatalogue_003 (Ext. 2 – Browse Catalogue / Raise Request)~~
~~**Definition**~~	~~Allows User Personnel to browse the service catalogue and raise a new service catalogue request~~
~~**Preconditions**~~	~~User Personnel followed a link from UC_ServiceCatalogue_001, choosing to browse the service catalogue and/or raise a new service catalogue request.~~
~~**Access Control**~~	~~User Personnel will only be able to raise requests on behalf of the User with which they are associated~~
~~**Inputs**~~	~~Business service category (selection list)~~ ~~Business service category services (selection list)~~ ~~Service request types (selection list)~~ ~~Raise request button~~ ~~First name – mandatory string~~ ~~Last name - mandatory string~~ ~~Telephone number – mandatory string~~ ~~Email address – a valid email address~~ ~~"Update contact details" button~~
~~**Outputs**~~	~~Final confirmation screen, showing the categories, inputs and contact details that have been provided, with a "Raise Request" button~~

DRAFT

~~1.10.19 User Account Management~~

~~Interface transaction name~~	~~UC_OrgManager_001 (Main Flow)~~
~~Definition~~	~~Enable Users electing to use the DCC Identity Provider Service to assign access to Interface Transactions to their User Personnel based on Job Type Roles and manage the SSI accounts and associated settings (e.g. password resets) for all subsequently created User Personnel accounts created by an Administration User.~~
~~Preconditions~~	~~- Roles apply (see clause 1.9)~~ ~~- User Personnel must be an Administration User for their organisation(s), where the process for becoming an Administration User is set out in the DCCKI Registration Authority Policies and Procedures (DCCKI RAPP).~~ ~~- The Administration User has pressed the "Manage My Users" button on their profile page (UC_Profile_001)~~
~~Access Control~~	~~User Personnel access is specific to the User~~
~~Inputs~~	~~User search page – This shows a sortable, pageable table of User Personnel accounts, with the following details in each row:~~ ~~- username (hyperlink to UC_OrgManager_002)~~ ~~- display name~~ ~~- Account Status (Active/Deleted/Locked)~~ ~~- last login date~~ ~~"Create New User" button - Pressing this button redirects the user to UC_OrgManager_003~~
~~Outputs~~	~~Displayed on SSI~~

DRAFT

~~**Interface transaction name**~~	~~UC_OrgManager_002 (Ext. 1 – Manage User)~~
~~**Definition**~~	~~Enable Administration Users to unlock, delete or manage the details of another account created within their corporation.~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~ ~~An Administration User has selected an individual's account to amend or reset in UC_OrgManager_001~~
~~**Access Control**~~	~~Only available to Administration Users of their organisation(s)~~
~~**Inputs**~~	~~Username - not editable~~ ~~Account status – not editable~~ ~~First name~~ ~~Last name~~ ~~Organisations – a list of User ID(s) in relation to which the User Personnel may access the Self-Service Interface, which shall comprise:~~ ~~one or more of the User IDs of the User ; and~~ ~~User IDs of any second User that has granted permission for the first User to access its information held on the Self-Service Interface in relation to one or more User IDs in accordance with clause 1.9.3.~~ ~~Roles – a list of Job Type Roles which may be assigned to this person (as defined in clause 1.9.2).~~ ~~Update User button – allows changes made to these fields to be saved. If any fields are found to be invalid, the form is re-displayed with validation errors messages and suggestions for resolution provided.~~ ~~Delete User button – allows the account to be deleted. A confirmation dialog is displayed, which must be accepted before deleting the account.~~ ~~Reset – a checkbox allowing the account to be unlocked, in which case a new single-use password is generated for the account being amended~~
~~**Outputs**~~	~~User Personnel account changes assigned, stored or deleted.~~

DRAFT

~~**Interface transaction name**~~	~~UC_OrgManager_003 (Ext. 1 – Create User)~~
~~**Definition**~~	~~Enable an Administration User to create a new person's account within their organisation.~~
~~**Preconditions**~~	~~- Roles apply (see clause 1.9)~~ ~~- The Administration User has pressed the "Create New User" button in UC_OrgManager_001~~
~~**Access Control**~~	~~Only available to Administration Users of their organisation(s)~~
~~**Inputs**~~	~~Username - Desired username (globally unique within the DCC Identity Provider Service). If the username is not unique, the DCC will reject the username and request submission of a new username.~~ ~~First name~~ ~~Last name~~ ~~Organisations – a list of User ID(s) in relation to which the User Personnel may access the Self-Service Interface, which shall comprise:~~ ~~- the User ID of the User ; and~~ ~~- User IDs of any second User that has granted permission for the first User to access its information held on the Self-Service Interface in relation to one or more User IDs in accordance with clause 1.9.3.~~ ~~Roles – a list of Job Type Roles which may be assigned to this person (as defined in clause 1.9.2.~~
~~**Outputs**~~	~~New User Personnel account created.~~

DRAFT

~~1.10.20 User Profile Information~~

~~Interface transaction name~~	~~UC_Profile_001~~
~~Definition~~	~~Enables User Personnel to view information about the account details with which they are accessing the Self-Service Interface, and details of the Interface Transactions that they are currently entitled to access.~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~By accessing this page User Personnel are shown the items listed in the outputs section.~~
~~Outputs~~	~~Unique user identification – changes depending on the nature and type of the Identity Provider Service~~ ~~Organisations – A list of User IDs that the User is assigned to~~ ~~Roles – A list of roles (as defined in clause 1.9.2) assigned to the person.~~ ~~Use cases – A list of Interface Transactions, with a "Yes" or "No" indication of whether the person has access as a result of their Job Type Role(s) (see clause 1.9.2)~~ ~~Bookmarks – A list of links to content that the person has bookmarked.~~

~~1.10.21 Search~~

~~Interface transaction name~~	~~UC_Search_001~~
~~Definition~~	~~Enables User Personnel to search for content provided by the Self-Service Interface by use of tagged keywords, or textual content of page titles and descriptions~~
~~Preconditions~~	~~Roles apply (see clause 1.9)~~
~~Inputs~~	~~A text box for entering search terms, a control allowing the User Personnel to select whether to match the terms using OR logic (any search term) or AND logic (all search terms), and a search button~~
~~Outputs~~	~~Search results.~~ ~~Each search result consists of:~~ ~~The title of the located item of content (which is also a link to that piece of content).~~ ~~A short summary description of the content.~~ ~~Reasons that the content was found (i.e. matches found in title, description, tags or attached filenames).~~

DRAFT

	~~If no results are found matching the search criteria, a message is displayed to this effect.~~

~~1.10.22 Problem Management~~

~~**Interface transaction name**~~	~~UC_ProblemManagement_001 (Main Flow)~~
~~**Definition**~~	~~Enables User Personnel to view details of open Problems related to incidents in accordance with H9~~
~~**Preconditions**~~	~~Roles apply (see clause 1.9)~~
~~**Access Control**~~	~~The Problems shown will be limited in accordance with H9.~~ ~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~User Personnel are presented with a page which shows a list of the Problems visible to them in accordance with H9~~
~~**Outputs**~~	~~For each Problem the following items are displayed:~~ ~~Problem Reference~~ ~~Current Problem Status~~ ~~Problem Summary~~

~~**Interface transaction name**~~	~~UC_ProblemManagement_002 (Ext. 1 – View Specific Problem)~~
~~**Definition**~~	~~This is a sub-screen of the main UC_ProblemManagement_001 (Main Flow) Interface Transaction showing more detailed information relating to a selected Problem.~~
~~**Preconditions**~~	~~User Personnel followed a link indicating that they would like to see the details of a specific Problem, and is appropriately privileged to view details of the Problem.~~
~~**Access Control**~~	~~The Problems shown will be limited in accordance with H9~~ ~~Roles apply (see clause 1.9)~~
~~**Inputs**~~	~~User Personnel follows link from UC_ProblemManagement_001~~
~~**Outputs**~~	~~User Personnel shown a page listing the details of the Problem:~~ ~~Field Name~~ ~~Problem Reference~~ ~~Current Problem Status~~ ~~Problem Summary~~ ~~Problem Notes~~ ~~Problem priority~~ ~~Date Raised~~

DRAFT

Data Communications Company

DCC

SSI Baseline Requirements Document

Version:	**V1.0.9**
Date:	**2 Nov 2018**
Classification:	**DCC Public**

Document Control

BRD Revision History

Revision Date	Summary of Changes	Changes Marked	Version Number
4/7/18	Initial version for internal review	N/A	0.1
16/07/2018	Internally reviewed	N/A	0.2
16/07/2018	Issued for external review	N/A	1.0
01/10/2018	Under review	N/A	1.0.3
12/10/2018	Traceability Matrix Req Included	N/A	1.0.4
16/10/2018	Included Robin Healy changes	N/A	1.0.5
19/10/2018	Include Business Functional Domains within Role – Access matrix	N/A	1.0.6
23/10/2018	Align with proposed SEC(AH)	N/A	1.0.7
23/10/2018	Working group review version	N/A	1.0.8
2/11/2018	Applied working group recommendations	N/A	1.0.9

Reviewers

Name	Title / Responsibility	Release Date	Version Number
Michael Boothby	DCC Systems Integration Design Authority	4/7/18	0.1
Robin Healy	DCC Regulation	16/07/2018	0.2

BRD RACI

Name	Title / Responsibility	Sign Off Role (RACI)	Sign Off Method and Date

Table of Contents

1 Introduction....4

1.1 Executive summary....4

1.2 Business drivers....4

1.3 Scope of this document....4

1.4 SSI documentation hierarchy....5

2 Business capabilities and business functional domains....6

2.1 Business functional domains overview....6

2.2 SSI business capabilities....9

3 Baseline business requirements....11

3.1 Baseline Epics, Process Maps to Business Functional Domain....11

3.2 Epic - Process Map....14

4 Baseline SSI platform requirements....41

4.1 Baseline functional components and requirements....41

4.2 Baseline non-functional requirements....71

5 References....83

Appendix A –Role, Interface Matrix....85

Appendix B –Definitions/Glossary....88

Appendix C –Document Reference....90

Appendix D –Delta Reference....91

1 Introduction

1.1 Executive summary

The purpose of this document is to define the baseline requirements for the Self-Service Interface capability defined in SEC H8.15, H8.16, H8.17 H8.18 and H8.19. The Self-Service Interface (SSI) is the entry point for Users to access DCC systems to retrieve information and data. It is the first point of contact for general DCC queries, and is intended to reduce the volume of queries raised directly with the DCC Service Desk.

There is a hierarchy of documents that together define the Self-Service Interface – see section 1.4 for more details. Section H8 of the SEC sits at the top of this hierarchy and specifies that the SSI must comply with the Self-Service Interface Access Control Specification and the SSI Baseline Requirements Document. Section H8 also permits DCC to make amendments to the SSI Baseline Requirements Document with the agreement of the Panel and following consultation with Parties. The governance process for making amendments to the BRD is set out in the SSI Change Governance Process.

The Self-Service Interface Access Control Specification, along with the SSI Change Governance Process form the next layer down in the hierarchy. The Self-Service Interface Access Control Specification specifies how the access rights permitted by the SEC are applied in practice and defines the information available to Users, whilst the SSI Change Governance Process contains the change governance which shall apply to the SSI Baseline Requirements Document.

This Baseline Requirements Document is the lowest layer in the hierarchy and specifies the Epics, high level Process Maps and associated business requirements that define the platform used to deliver the required business capability, along with the document control process for making amendments to this document.

1.2 Business drivers

The business drivers behind the SSI are:

Ref	Description
BD1	Support DCC Users to independently retrieve information and data to help them plan and manage the service they offer to their customers.
BD2	Support DCC Users independently inform DCC of information they deem DCC needs to know.
BD3	Enable DCC to provide current information to DCC Users enabling them to make informed decisions.
BD4	Support DCC Users provide business benefit to their customers.

1.3 Scope of this document

1.3.1 In scope of this document

The following items are in the scope of this document:

- Definition of the Business Functional Domains which will be used to deliver specific functionality.

- Description of the Epics and Process Maps that specify the decomposition of the Business Functional Domains.
- Baseline functional and non-functional requirements associated to Business Functional Domains on the Self-Service Interface.

1.3.2 Out of scope of this document

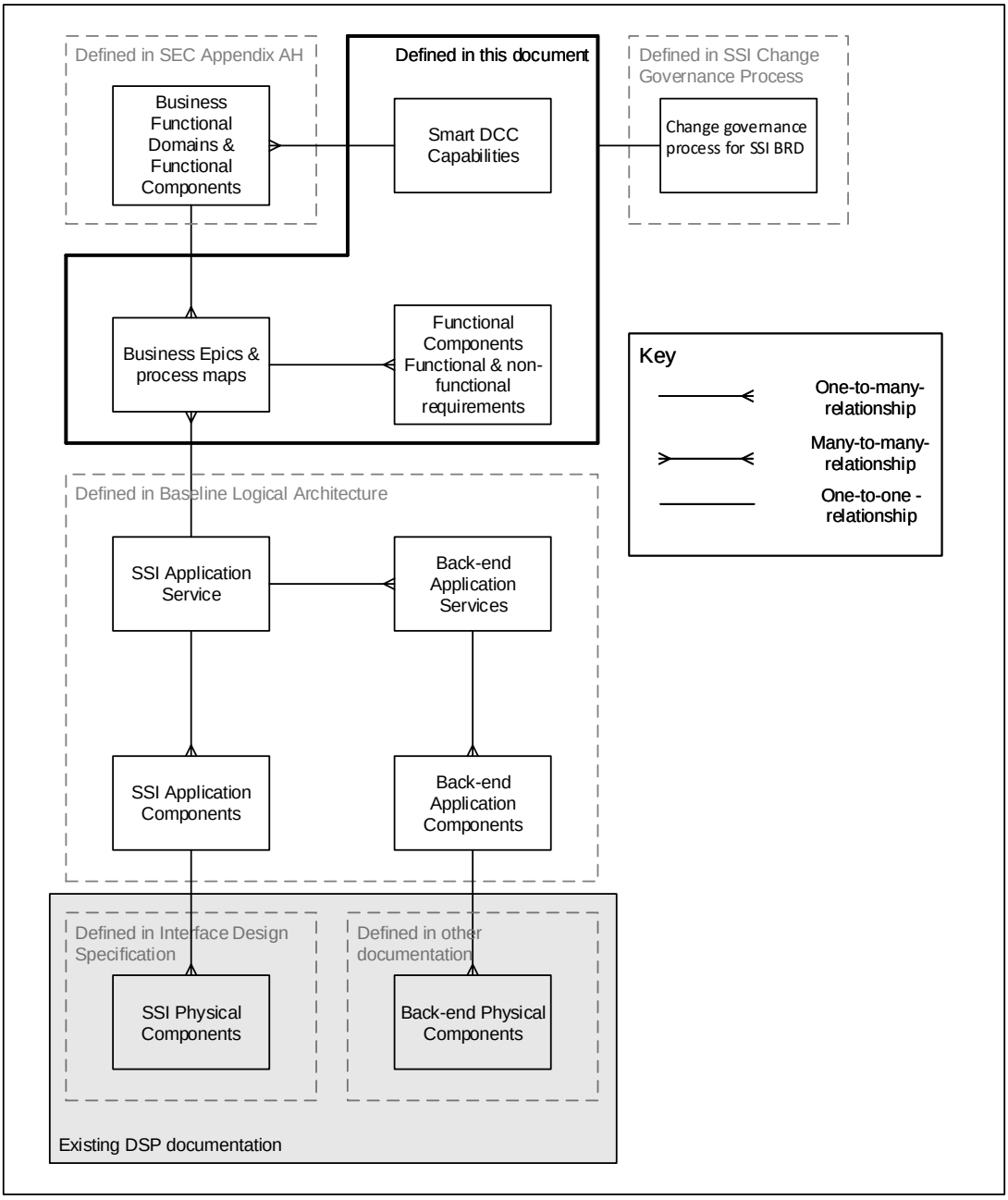
The following items are out of the scope of this document:

- The description of any services or application components that deliver the functionality of the Self-Service Interface. This information is contained in the Self-Service Interface Baseline Logical Architecture Document (reference 1)
- Functional and non-functional requirements of any of the back-end platforms. This information is contained in other business requirements specifications

1.4 SSI documentation hierarchy

The Self-Service Interface is a portal that is the entry point for Service Users to access and retrieve data from DCC Data Systems. The functionality of the SSI is broken down as follows:

- SEC H8.15, H8.16, H8.17 and H8.18 establish the information which Users are entitled to access via the SSI.
- The Self-Service Interface Access Control Specification (SEC Appendix AH) defines Business Functional Domains (BFD), Functional Components and their user access rules establishing the functionality which will be used to deliver SSI.
- The SSI Change Governance Process contains the change governance which shall apply to the SSI Baseline Requirements Document.
- Baseline Requirements Document (this document) provides traceability back to the Self-Service Interface Access Control Specification via Baseline Functional Domains and Functional Components. See sections 2 and 4.1 respectively. This document further describes:
    - DCC capability areas. As defined in section 2 of this document
    - User activity, described as Epics and is associated to a Process Map. As defined in section 3 of this document
    - Functional components and their requirements. As defined in section 4.1 of this document.
- Baseline Logical Architecture (BLA) document provides traceability back to the BRD (This Document) via BRD's Process Maps linked to BLA Service and component process map decomposition. As described in section 4.6 of that document. The BLA further describes:
    - SSI logical service.
    - SSI's back-end application services.
    - SSI's components. This is defined in the SSI Baseline Logical Architecture.
    - SSI interface relationships.



2 Business capabilities and business functional domains

This section summarises the business functional domains of the Self-Service Interface and maps these business functional domains to DCC business capabilities

2.1 Business functional domains overview

Below are the business functional domains of the Self-Service Interface.

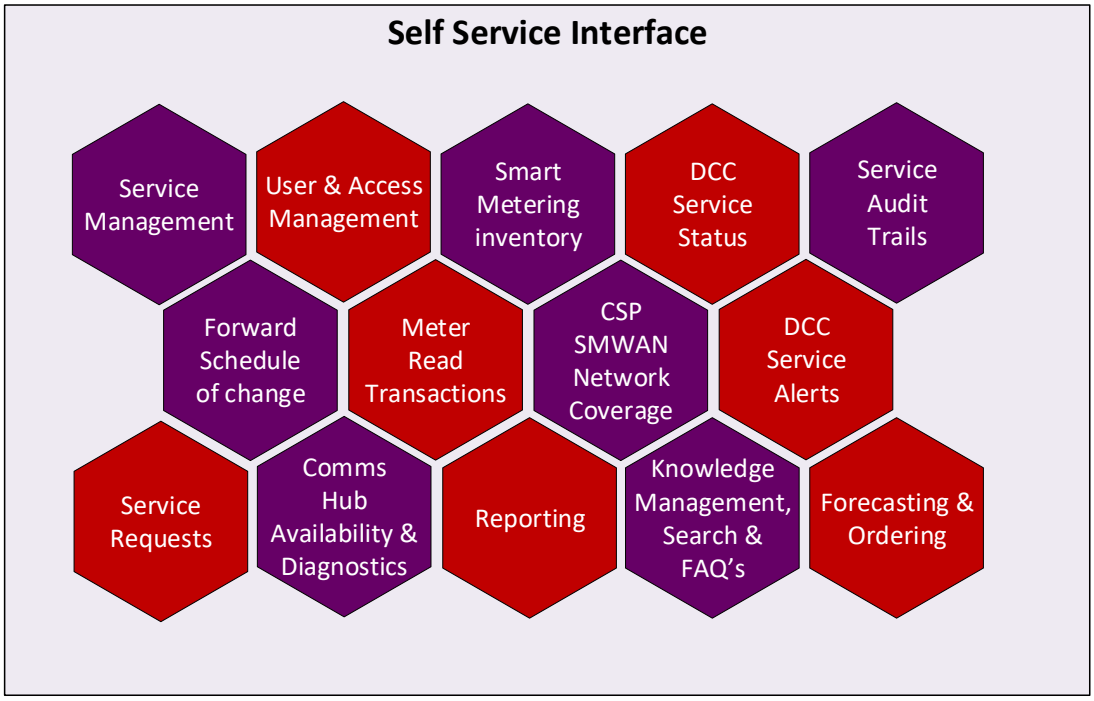


Figure 1 - SSI Business Function Domains

The descriptions of each of these business functional domains are as follows:

BFD ID	Business Functional Domain Name	Capability
BFD01	Service Management	Provide service management capabilities in accordance with H9.4, enabling Users to: • Raise, update, view and track incidents. • Track and view detailed problem information related to incidents.
BFD02	Smart Metering inventory	Enable Users to search and query current information on Smart Meter Inventory down to individual devices in accordance with H8.17(a). Provide detailed information on device and associated devices.
BFD03	DCC Service Status	Provide Users with a dashboard of component availability for the DCC Service in accordance with H8.17(g).
BFD04	Service Audit Trails	Enable Users to query information on Service audit trails, showing a record of service activity in accordance with H8.17(b).
BFD05	Forward Schedule of change	Enable Users to query and view detailed information on Planned Maintenance, changes scheduled or change freezes affecting any of the following elements of DCC Smart Metering ecosystem in accordance with H8.17(g): • Communications Hub firmware. • Parse & Correlate software. • SMIKI software. • SEC release. • Other major DCC releases.

BFD ID	Business Functional Domain Name	Capability
		• Meter firmware.
BFD06	Meter Read Transactions	Enable Users to query information on Meter Read Transactions for all users in accordance with H8.17(c).
BFD07	CSP SMWAN Network Coverage	Enable Users to query information on SM WAN network coverage down to premises level across each of the three GB regions in accordance with H8.17(f).
BFD08	DCC Service Alerts	Enable Users to view details of any service affecting news / alerts and other useful text relating to the quality of service delivery and service management in accordance with H8.17(g).
BFD09	Service Requests	Enable Users to: • Browse a catalogue of available DCC service requests. • Raise, update service management service requests with DCC from their service catalogue. Enabling Users to track and update the status of raised requests within DCC service management system. • View full details of the details of the raised service request
BFD10	Communications Hub Availability & Diagnostics	Enable Users to query information on Communication Hub availability and diagnostics down individual Communications Hub. Allows Users to attempt to diagnose and resolve Incidents relating to any Communications Hubs for which they are the Responsible Supplier, the Network Party or Registered Supplier Agent, using DCC's remote diagnostic tools.
BFD11	Reporting	Enable users to access on demand a standard set of pre-defined reports. Allow Users to view and download individual reports from a defined set of published reports.
BFD12	Knowledge Management, Search and FAQ's	Enable Users to access the following functionality in accordance with H8.17(g) where applicable: • Knowledge management. This allows Users to view help and support information enabling early triage of User issues and queries, including access to the anonymous resolution details of service management problems and incidents. • FAQ information. • DCC User Manuals detailing operation of DCC services. • Search capability, allowing Users to search for content provided by the SSI using tagged keywords, or textual content of page titles and descriptions.
BFD13	Forecasting and Ordering	Enable Users to access OMS in accordance with H8.17(e). In OMS Users can submit orders and forecasts of future orders for Communications Hubs and Communication Hib Auxiliary Equipment.

BFD ID	Business Functional Domain Name	Capability
BFD14	User Identity & Login Access Management	Manage the verification of user identities requesting login access to SSI and DCC Platforms. Manage the functionality available to individual Users based on their user role. This includes the following capabilities: • Enable Users to use DCC Identity Provider Service to assign access to functionality to their User Personnel based on Job Type Role and manage the SSI accounts and associated settings (e.g password resets) for User Personnel accounts subsequently created by an Administration User. • Enable Administration Users to unlock, delete and manage the details of another account created within their organization. • Enable an Administration User to create a new person's account within their organization. • Enable User Personnel to view detailed information about the account they are accessing via SSI including the functionality they have access to. Ensure secure communications between DCC systems and Users.

2.2 SSI business capabilities

2.2.1 Mapping between business functional domains and business capabilities

The table below defines the mapping between the Business Functional Domain as defined in section 2.1 of this document, and the DCC business capabilities. This mapping is informational only – per the hierarchy given in section 1.4 above, Epics and Process Maps will be related to business functional domains, not to DCC business capabilities.

BFD Id	Business Functional Domain Name	Business Capability
BFD01	Service Management	Management for Service Operations
BFD02	Smart Metering inventory	Asset Management
BFD03	DCC Service Status	Service Delivery and Logistics
BFD04	Service Audit Trails	Asset Management
BFD05	Forward Schedule of change	Service Forecasting and Capacity
BFD06	Meter Read Transactions	Service Delivery and Logistics
BFD07	CSP SMWAN Network Coverage	Service Forecasting and Capacity
BFD08	DCC Service Alerts	Service Delivery and Logistics
BFD09	Service Requests	Service Delivery and Logistics

BFD Id	Business Functional Domain Name	Business Capability
BFD10	Comms Hub Availability & Diagnostics	Service Delivery and Logistics
BFD11	Reporting	Service Delivery and Logistics
BFD12	Knowledge Management and FAQs	Service Delivery and Logistics
BFD13	Forecasting and Ordering	Forecasting Customer Demand
BFD14	User & Login Access Management	Service Delivery and Logistics

3 Baseline business requirements

This section describes the baseline business requirements for the Self-Service Interface. These are defined as Epics and associated Process Maps. The functional and non-functional requirements for these Epics are defined in section 4.

3.1 Baseline Epics, Process Maps to Business Functional Domain

The following Epics and Process Maps are implemented through the Self-Service Interface. Each is mapped to a business functional domain as defined in section 2.1.

Epic Name	Description	Process Map	Business Functional Domain
Login	As a DCC Service User I want to be able to log into the Self-service interface, so that I will be able submit further requests through the Self-Service Interface	PM1	BFD14 User & Login Access Management
View Inventory	As a DCC Service User I want to be able to see high level information about the devices at a given property, or one specific device, so that I can use this information to help me manage these devices	PM2	BFD02 Smart Metering Inventory
View Service Audit Trail	As a DCC Service User I want to be able to see the history of service requests sent to devices at a given property, or one specific device, so that I can use this information to help me manage these devices	PM3	BFD04 Service Audit Trails
View Meter Reads	As a DCC Service User I want to be able to see the history of meter reads for devices at a given property, or one specific device, so that I can use this information to help me manage these devices	PM4	BFD06 Meter Read Transactions
View SMWAN Coverage	As a DCC Service User I want to be able to see if a given postcode has SM WAN coverage or when it will get it, so that I can plan my Smart Metering rollout	PM5	BFD07 CSP SMWAN Network Coverage
Run Comms Hub Diagnostics	As a DCC Service User I want to be able to run diagnostics on a Communications Hub, so that I can troubleshoot any problems with the Hub	PM6	BFD10 Comms Hub Availability & Diagnostics
Access OMS	As a DCC Service User I want to be able to access OMS from the Self-Service Interface, so that I can plan and execute my orders for Communications Hubs and auxiliary equipment	PM7	BFD13 Forecasting and Ordering
Run Reports	As a DCC Service User I want to be able to run pre-defined reports, so that I can use this information to help me manage the service I provide customers	PM8	BFD11 Reporting

Epic Name	Description	Process Map	Business Functional Domain
Raise Incident	As a DCC Service User I want to be able to raise an Incident so that my issue with the DCC service can be resolved	PM9	BFD01 Service Management
Update Incident	As a DCC Service User I want to be able to update an existing incident, so that the DCC has visibility of the latest status	PM10	BFD01 Service Management
View Incident	As a DCC Service User I want to be able to view an existing incident, so that I have visibility of the latest status	PM11	BFD01 Service Management
View Support Documents	As a DCC Service User I want to be able to view DCC support documents, so that I can try to answer questions and solve issues independently	PM12	BFD12 Knowledge Management and FAQs
View Planned Changes	As a DCC Service User I want to be able to view details of planned maintenance and upgrades to the DCC service, so that I can plan my operations to be aligned to the schedule	PM13	BFD05 Forward Schedule of change
View Service Status	As a DCC Service User I want to be able to see details of the DCC service status, so that I can understand if any outages are affecting my operations or the service I provide to customers	PM14	BFD03 DCC Service Status
View Service Alerts	As a DCC Service User I want to be able to see details of any DCC service alerts, so that I can understand if any outages are affecting my operations or the service I provide to customers, and if so when they will be resolved	PM15	BFD08 DCC Service Alerts
View FAQs	As a DCC Service User I want to be able to view DCC FAQs, so that I can try to answer questions and solve issues independently	PM16	BFD12 Knowledge Management and FAQs
View User Manuals	As a DCC Service User I want to be able to view DCC user manuals, so that I can try to answer questions and solve issues independently	PM17	BFD12 Knowledge Management and FAQs
Raise Service Request	As a DCC Service User I want to be able to raise service management service requests, so that I can deliver the best service to my customers and run my operations effectively	PM18	BFD09 Service Requests
Update Service Request	As a DCC Service User I want to be able to update service management service requests, so that I can deliver the best service to my customers and run my operations effectively	PM19	BFD09 Service Requests
View Service Request	As a DCC Service User I want to be able to view service management service requests, so that I can deliver the best service to my customers and run my operations effectively	PM20	BFD09 Service Requests

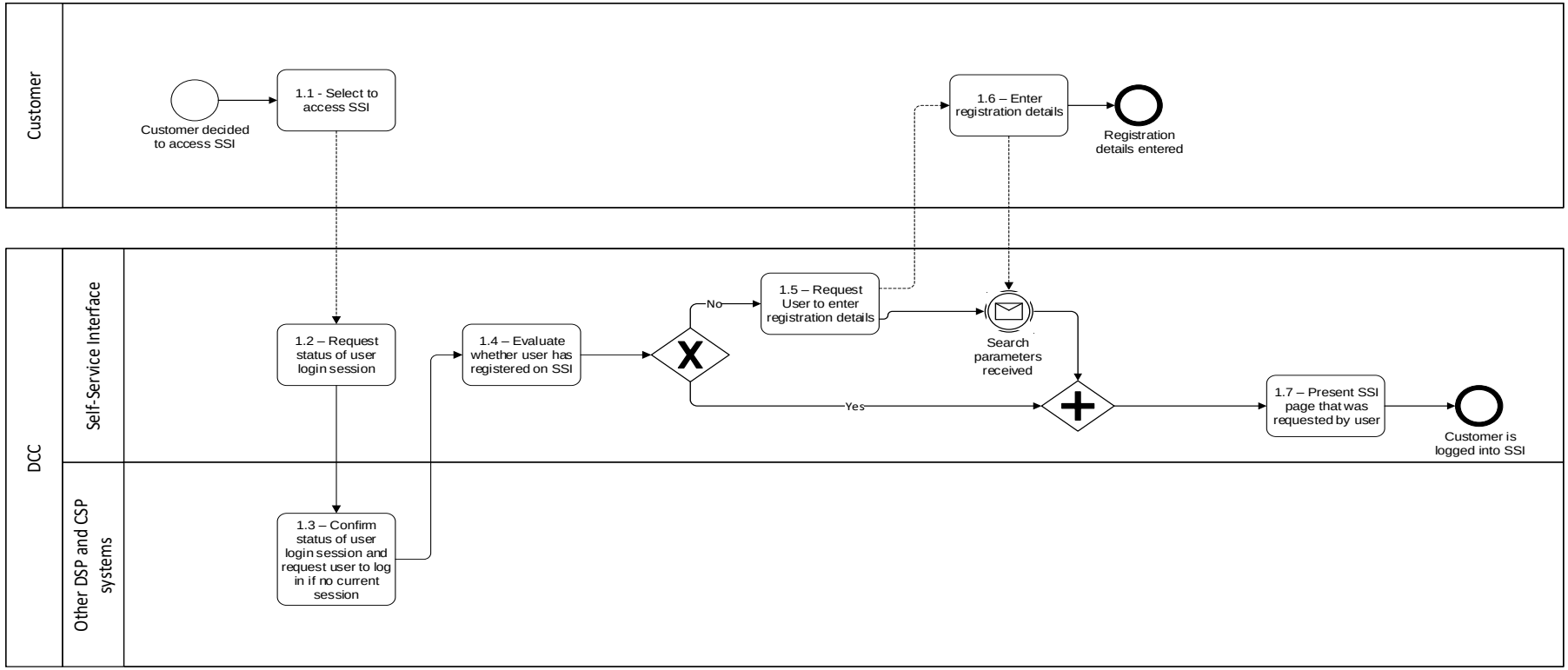
Epic Name	Description	Process Map	Business Functional Domain
Create SSI User	As a DCC Administration Service User I want to be able to create SSI accounts for my users, so that my users can use the SSI effectively	PM21	BDF14 User Management
Update SSI User	As a DCC Administration Service User I want to be able to update SSI accounts for my users, including resetting passwords, so that my users can use the SSI effectively	PM22	BFD14 User Management
View SSI User	As a DCC Administration Service User I want to be able to view SSI accounts for my users, so that my users can use the SSI effectively	PM23	BFD14 User Management
Delete SSI User	As a DCC Administration Service User I want to be able to delete SSI accounts for my users, so that people do not erroneously have access to the SSI	PM24	BFD14 User Management
View My User Profile	As a DCC Service User I want to be able to view my profile, so that I can confirm what I can do on the SSI and view items I have bookmarked	PM25	BFD14 User Management
Search SSI Content	As a DCC Service User I want to be able to search for all content published on the SSI, so that I can try to answer questions and solve issues independently	PM26	BFD12 Knowledge Management and FAQs
View Problem	As a DCC Service User I want to be able to view an existing problem, so that I have visibility of the latest status	PM27	BFD01 Service Management

3.2 Epic - Process Map

This section depicts the process maps for the defined Epics. Note that except for PM1 Login, the process maps assume the Service User is in a logged-in state prior to commencing the journey.

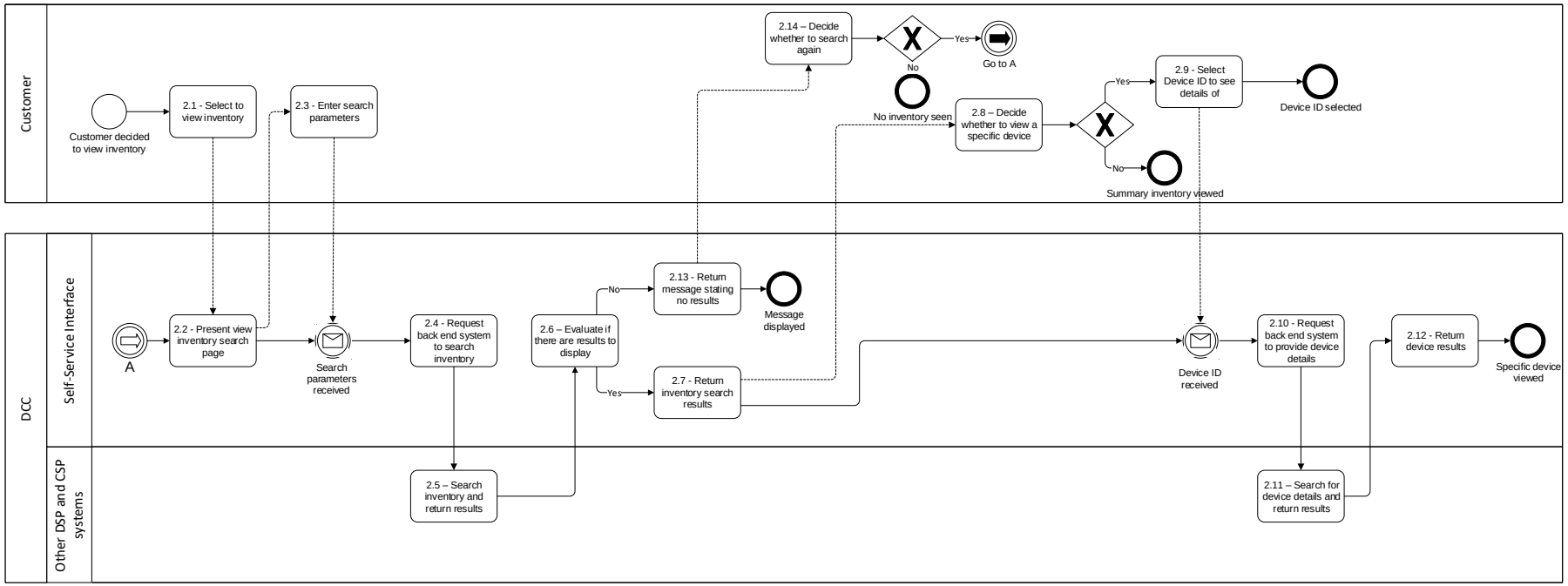
3.2.1 Login – PM1

The diagram below shows the baseline process map for PM1 (Login).



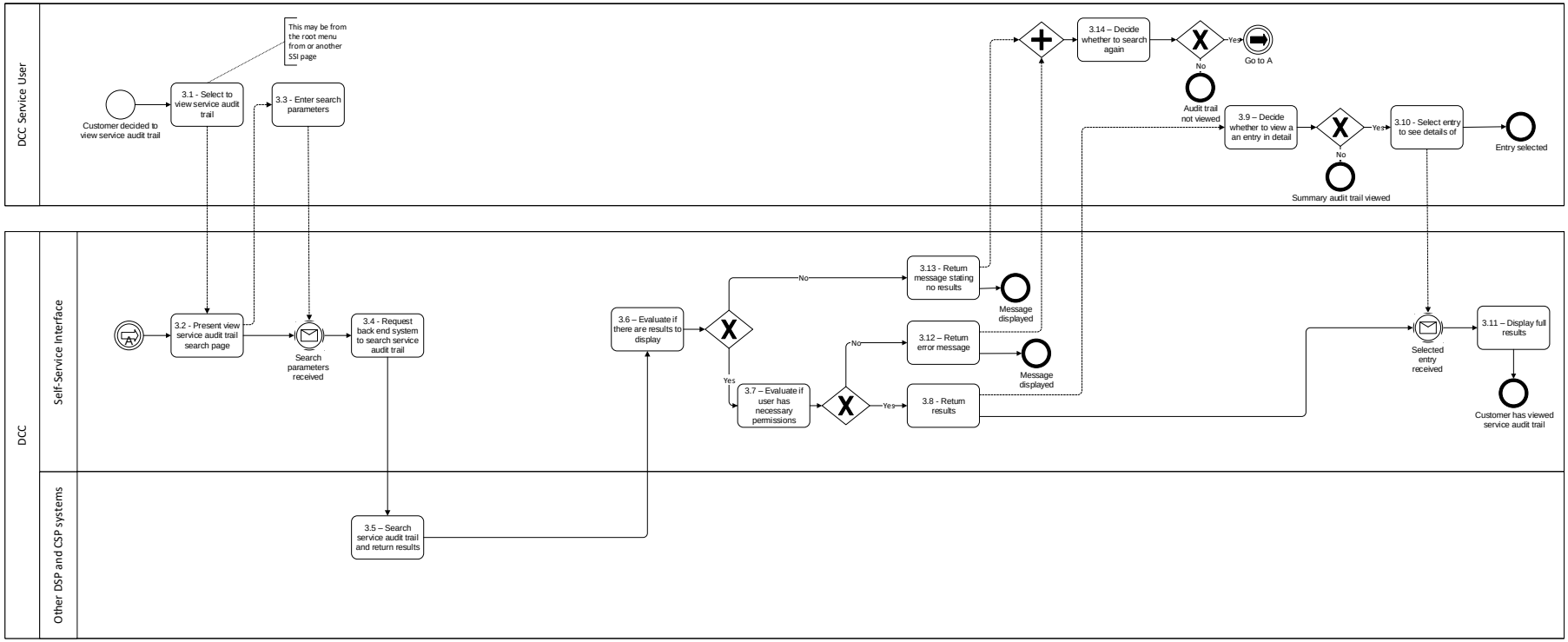
3.2.2 View Inventory - PM2

The diagram below shows the baseline process map for PM2 (View Inventory).



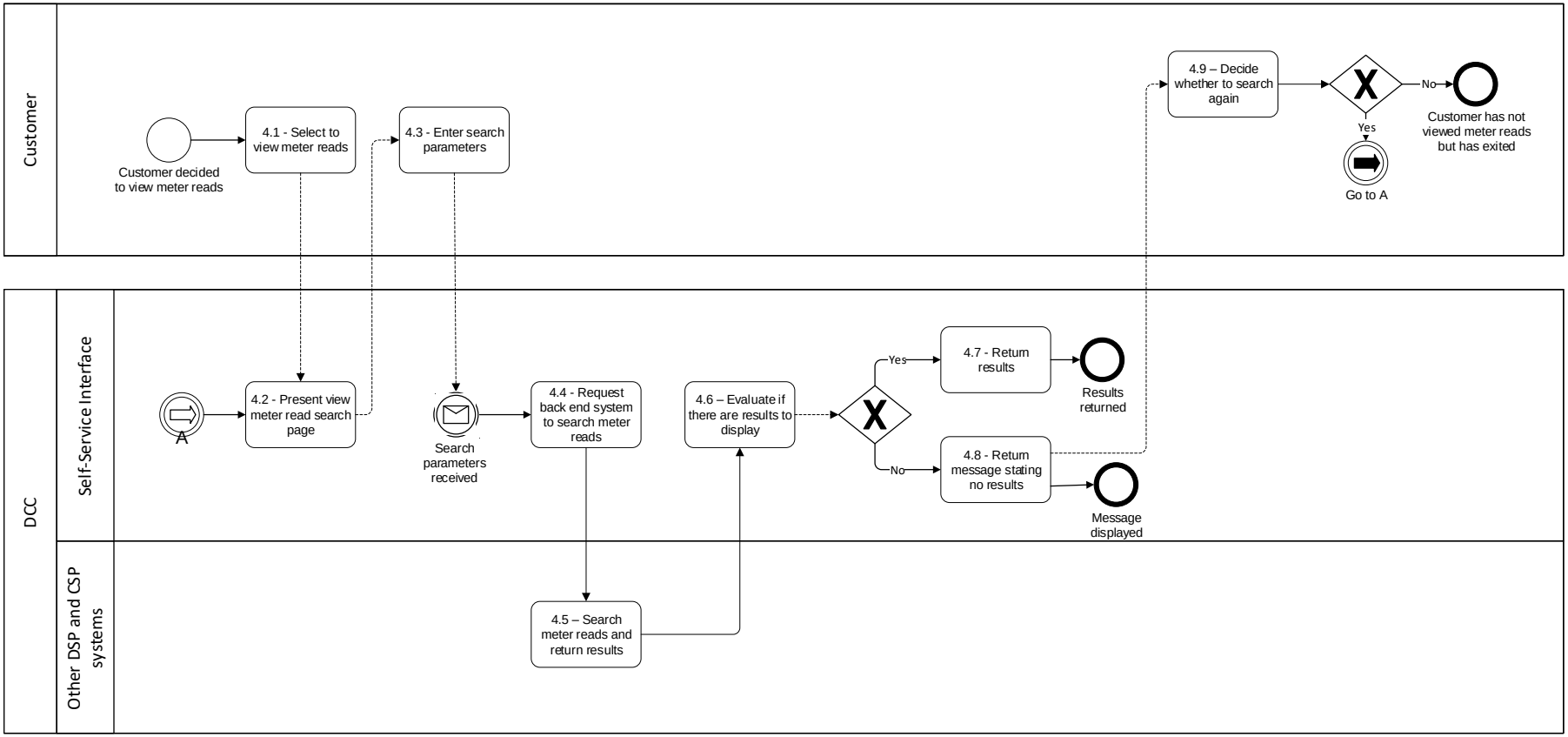
3.2.3 View Service Audit Trail – PM3

The diagram below shows the baseline process map for PM3 View Service Audit Trail.



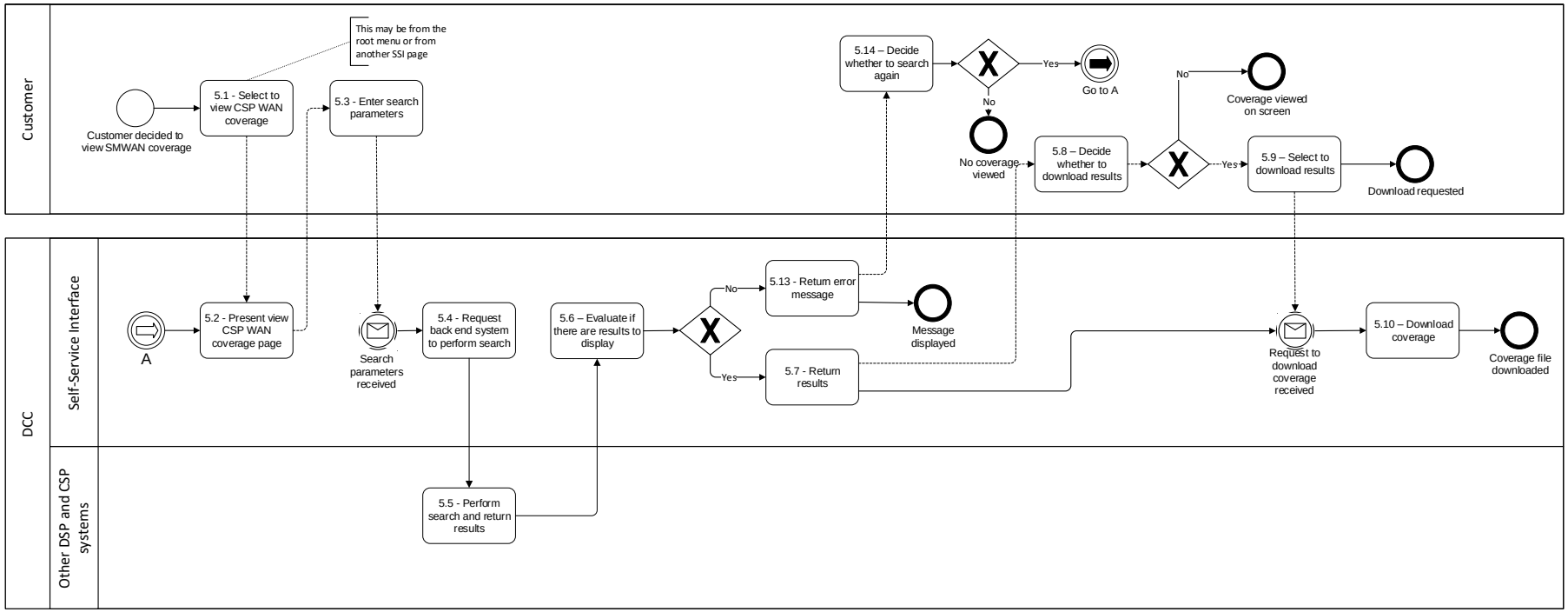
3.2.4 View Meter Reads – PM4

The diagram below shows the baseline process map for PM4 (View Meter Reads).



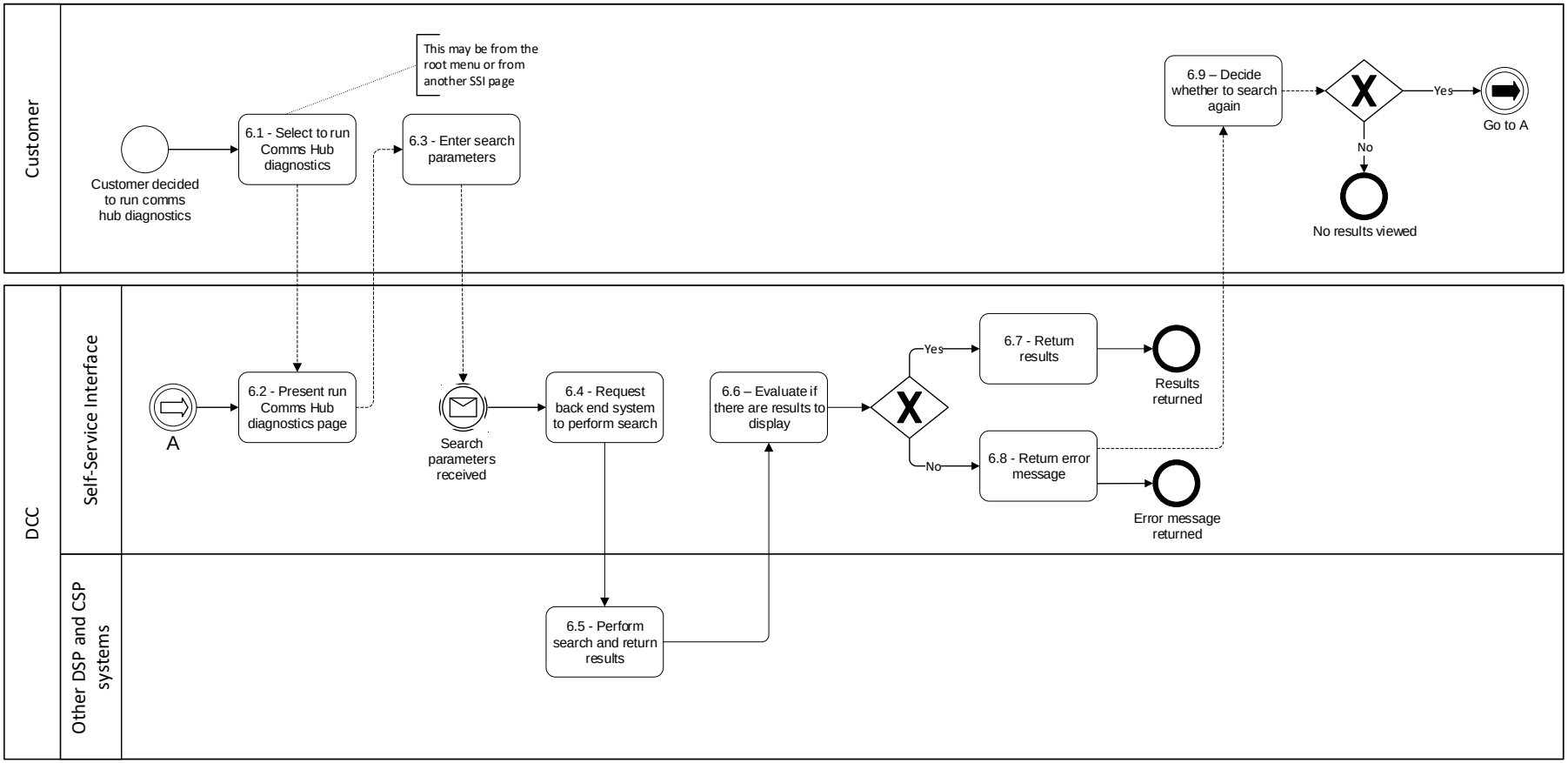
3.2.5 SMWAN Coverage – PM5

The diagram below shows the baseline process map for PM5 (View SMWAN Coverage).



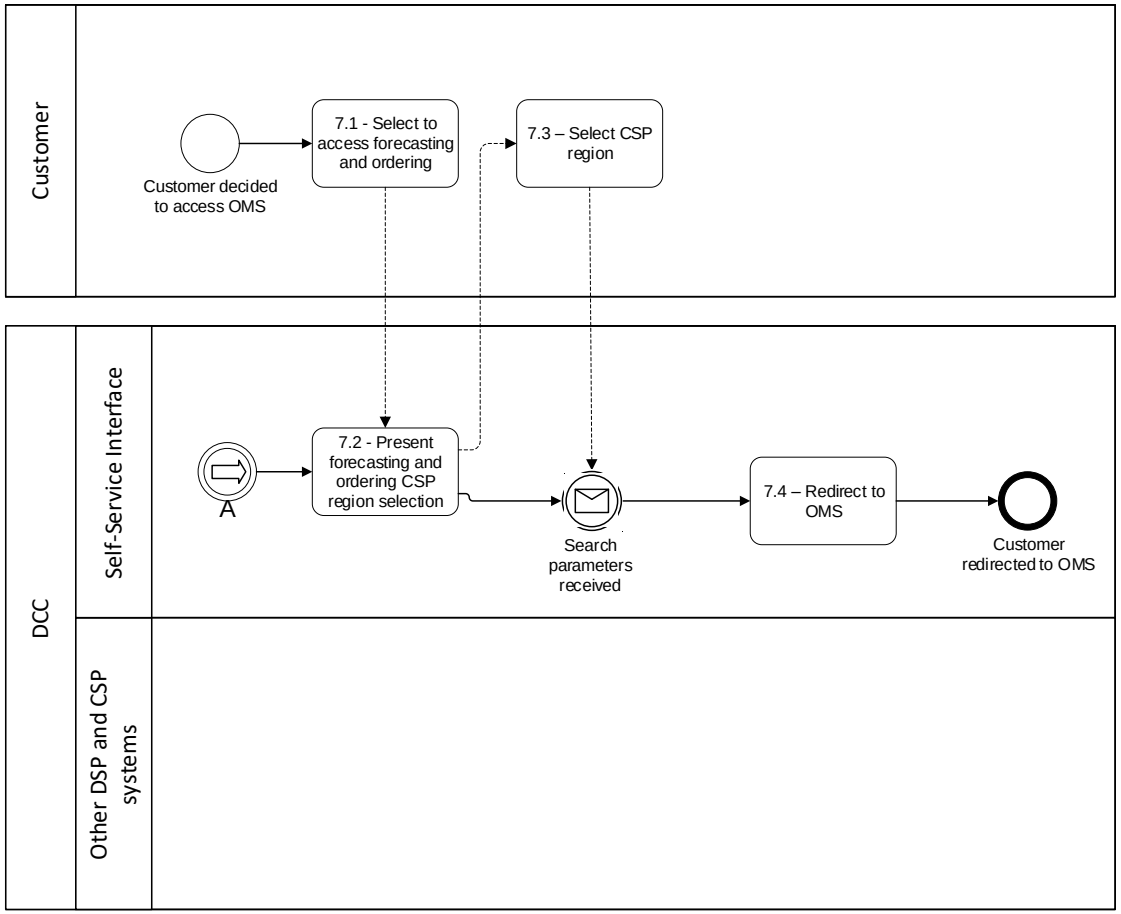
3.2.6 Run Comms Hub Diagnostics - PM6

The diagram below shows the baseline process map for PM6 (Run Comms Hub Diagnostics).



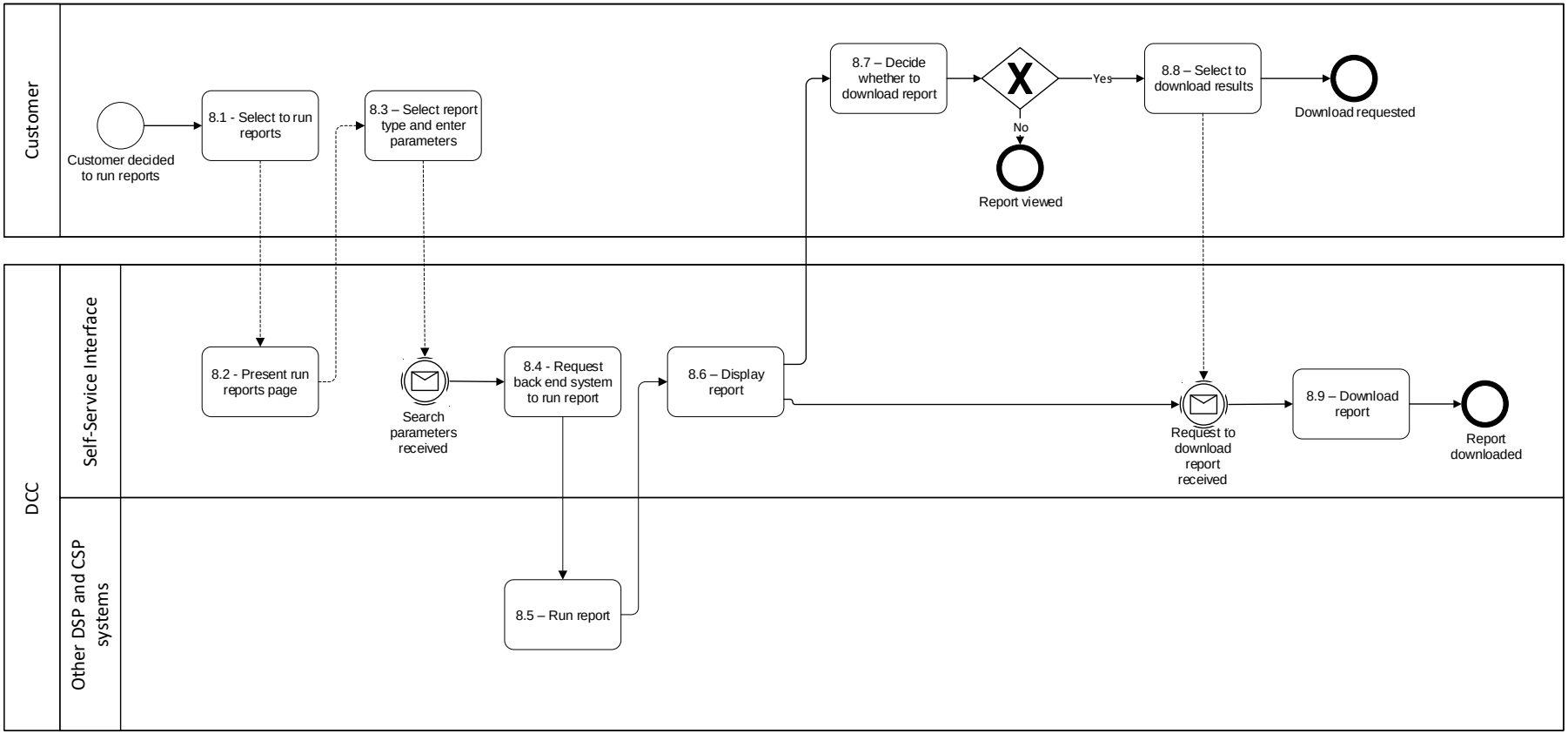
3.2.7 Access OMS - PM7

The diagram below shows the baseline process map for PM7 Access OMS.



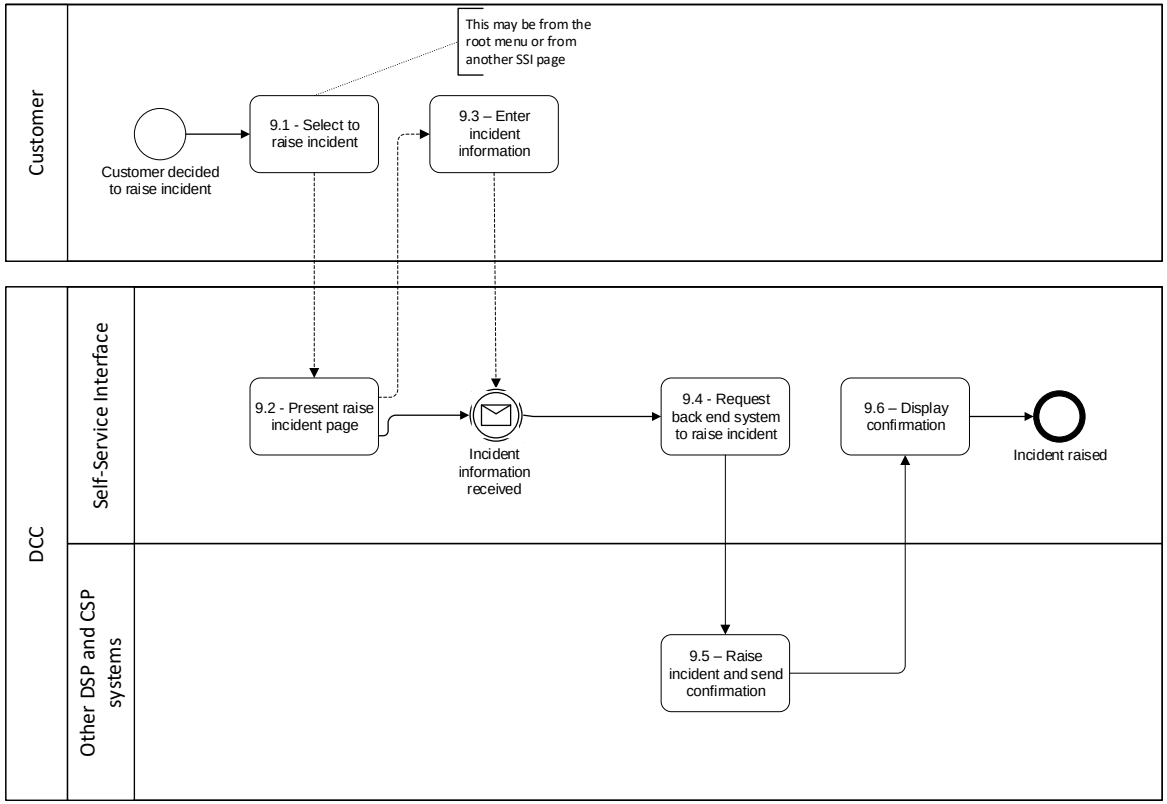
3.2.8 Run Reports – PM8

The diagram below shows the baseline process map for PM8 (Run Reports).



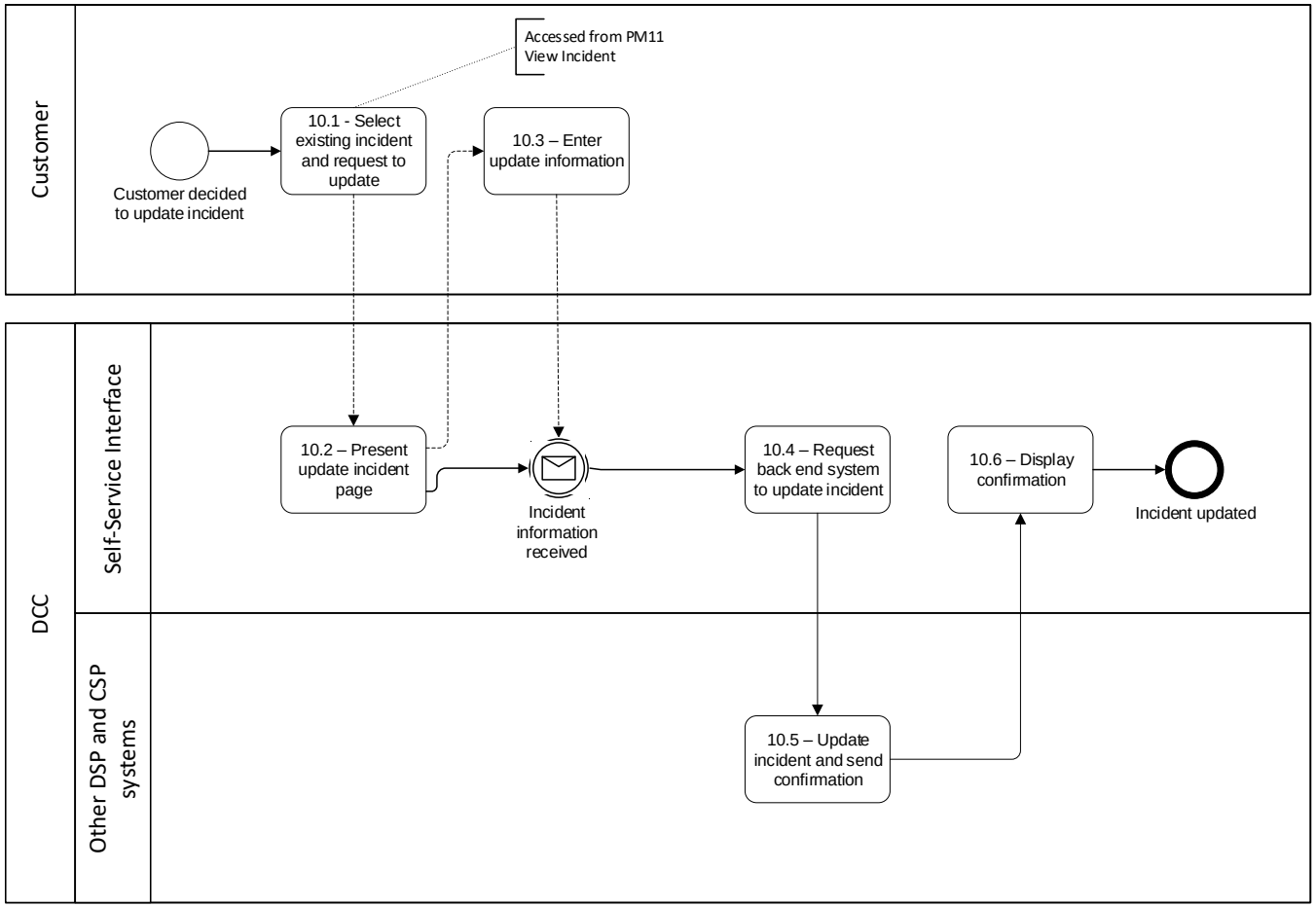
3.2.9 Raise Incident - PM9

The diagram below shows the baseline process map for PM9 (Raise Incident).



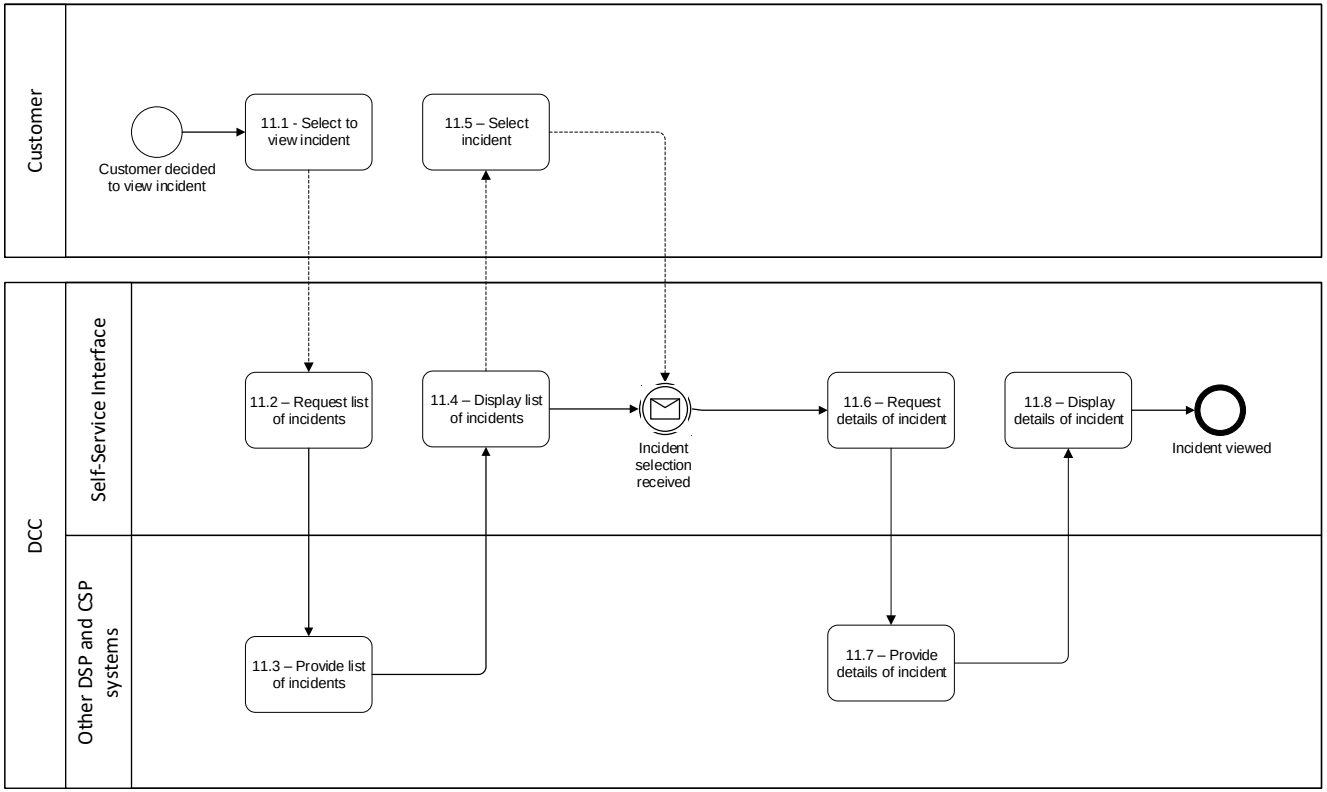
3.2.10 Update Incident - PM10

The diagram below shows the baseline process map for PM10 (Update incident).



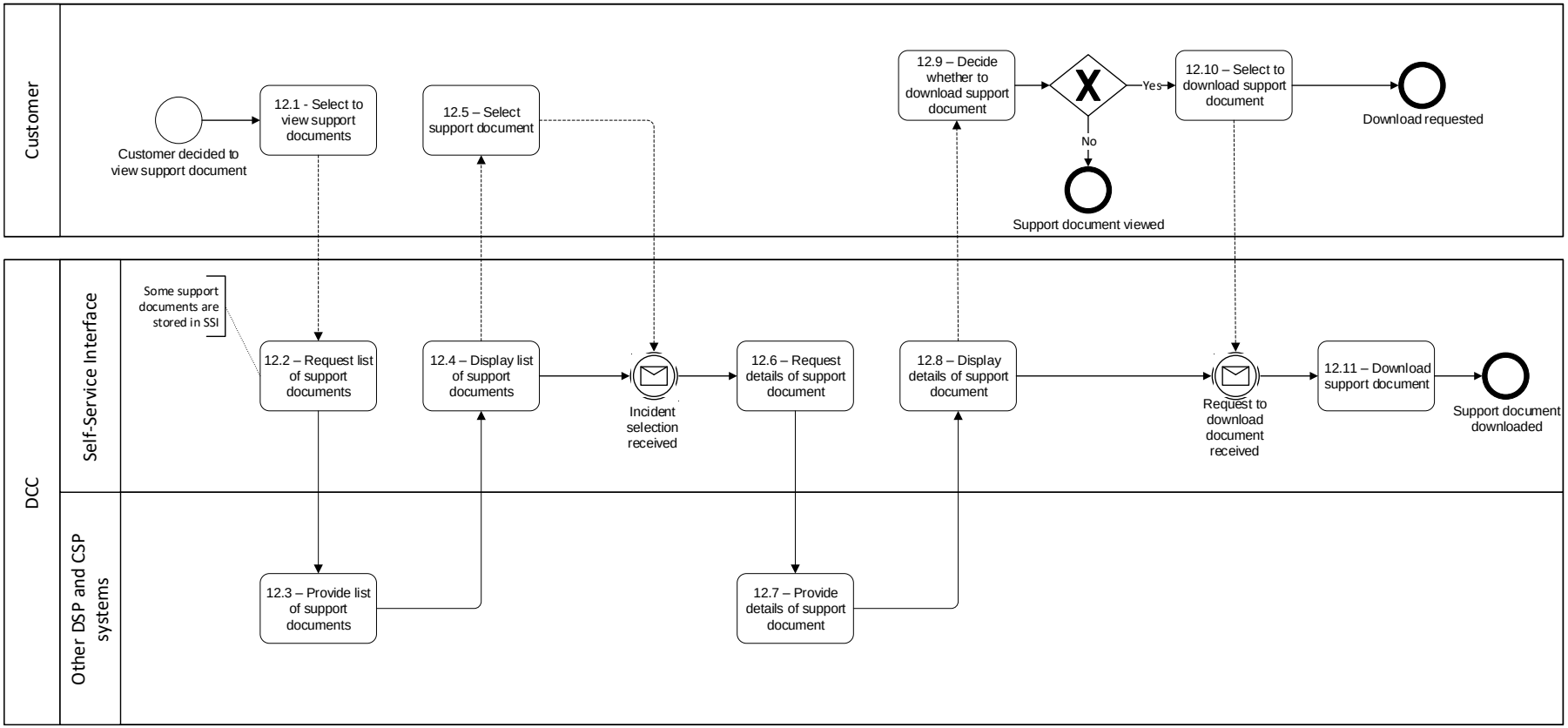
3.2.11 View Incident - PM11

The diagram below shows the baseline process map for PM11 (View Incident).



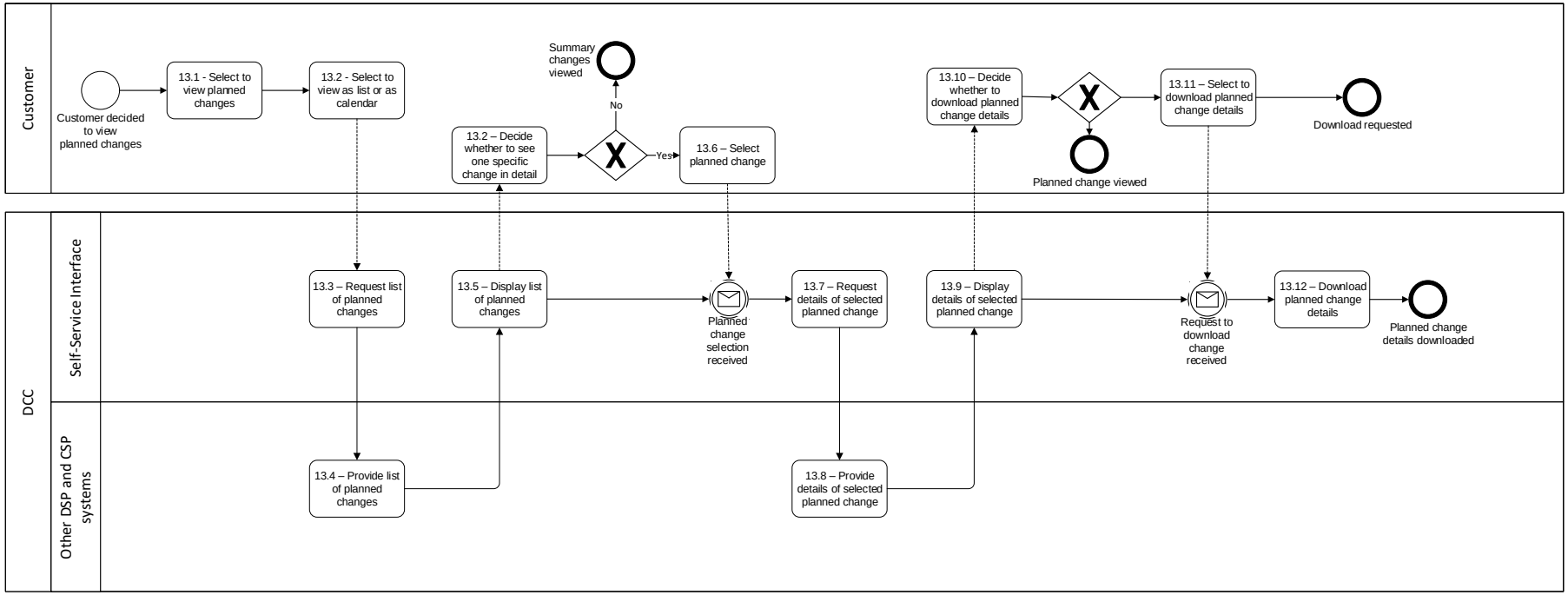
3.2.12 View Support Documents - PM12

The diagram below shows the baseline process map for PM12 (View Support Documents).



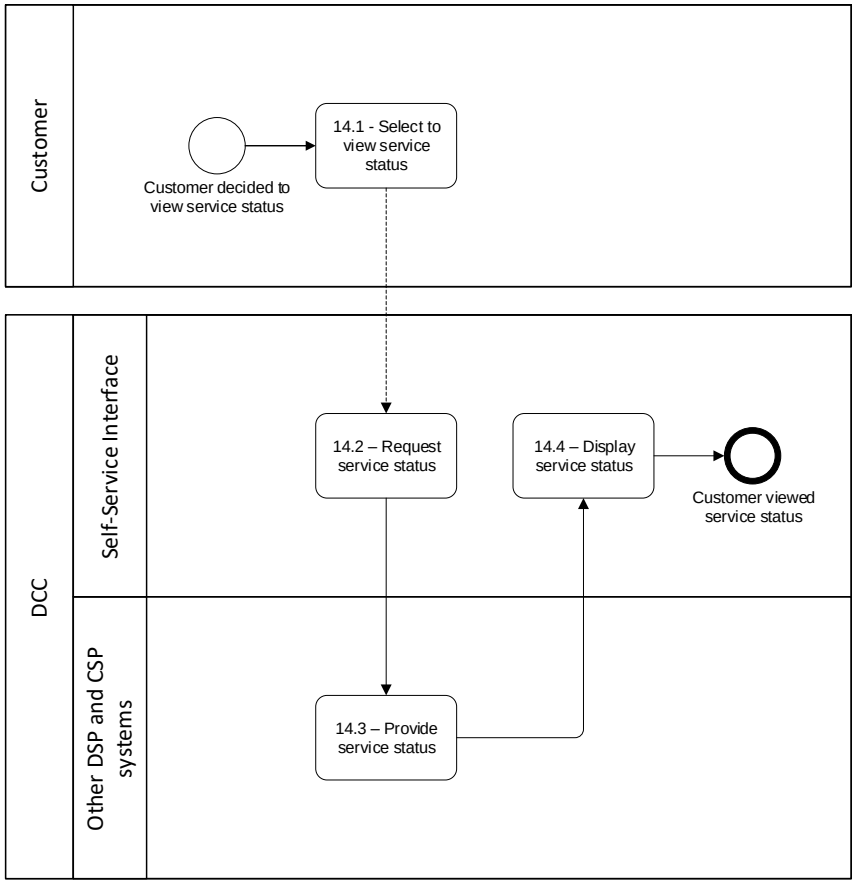
3.2.13 View Planned Changes - PM13

The diagram below shows the baseline process map for PM13 (View Planned Changes).



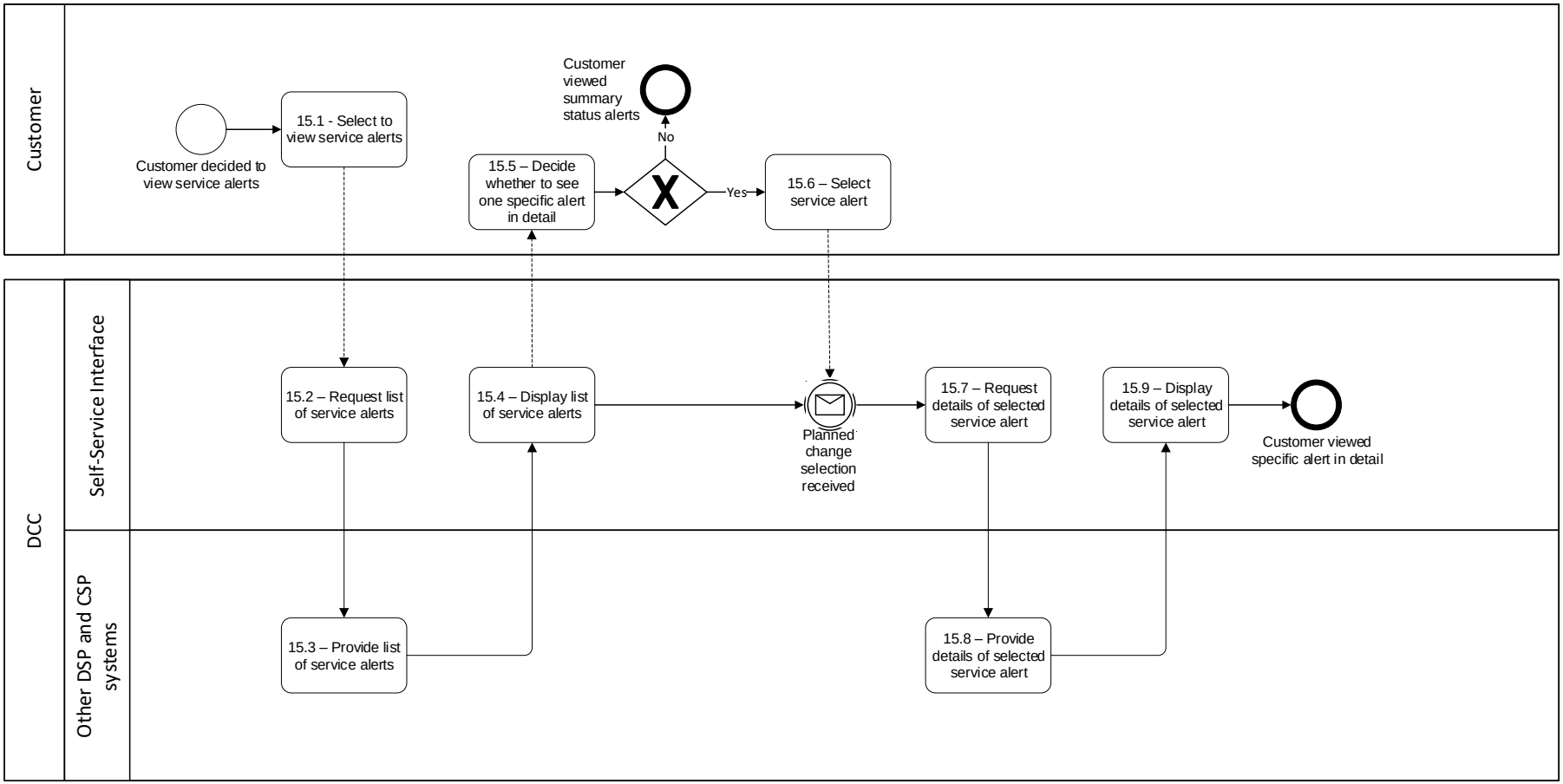
3.2.14 View Service Status - PM14

The diagram below shows the baseline process map for PM14 (View Service Status).



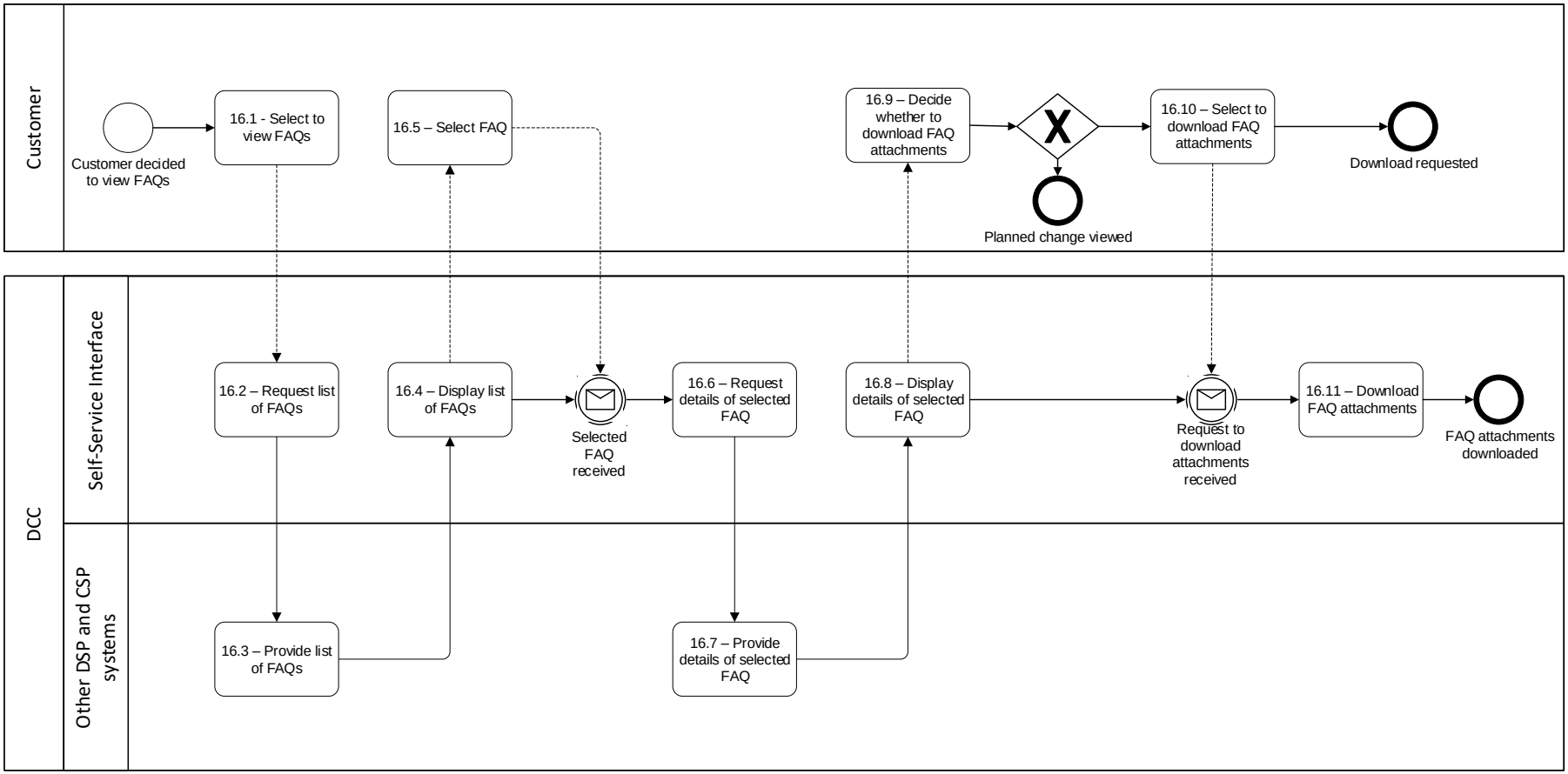
3.2.15 View Service Alerts - PM15

The diagram below shows the baseline process map for PM15 View Service Alerts.



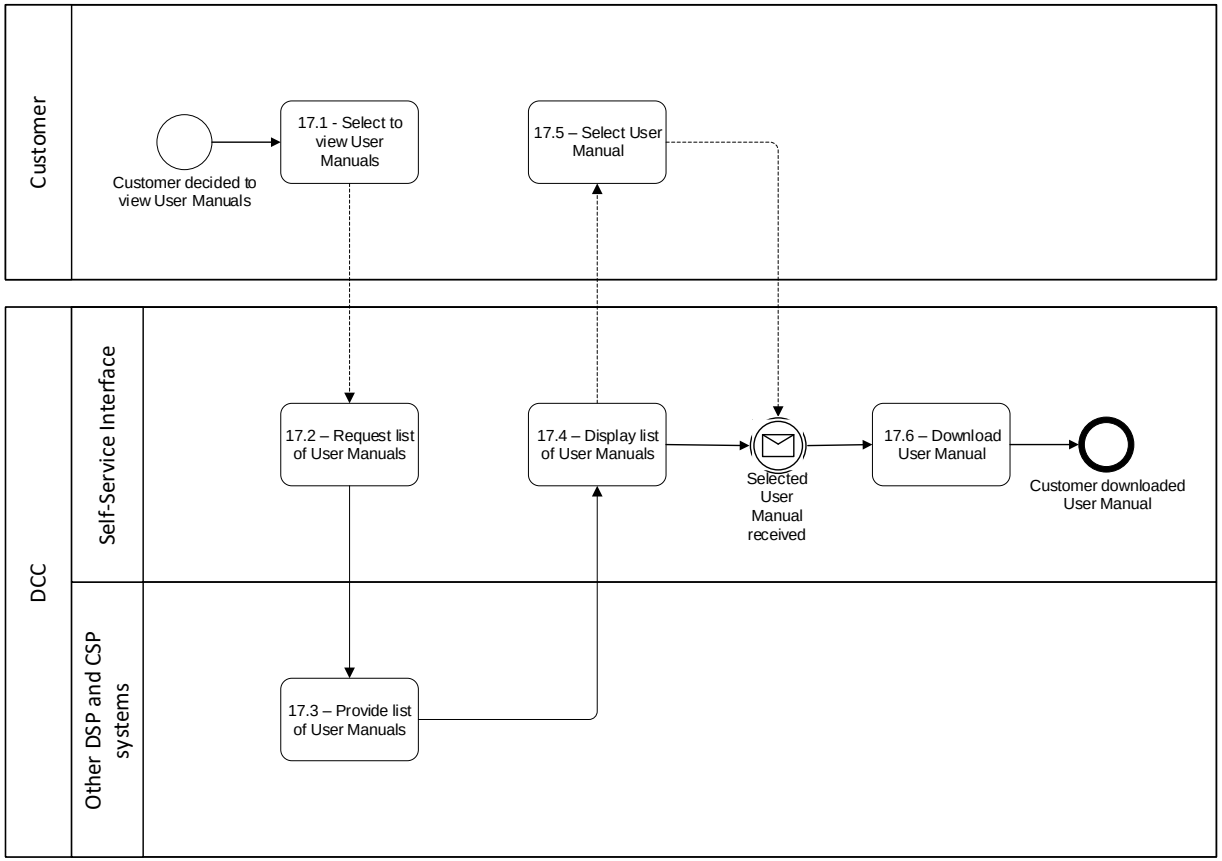
3.2.16 View FAQs - PM16

The diagram below shows the baseline process map for PM16 (View FAQs).



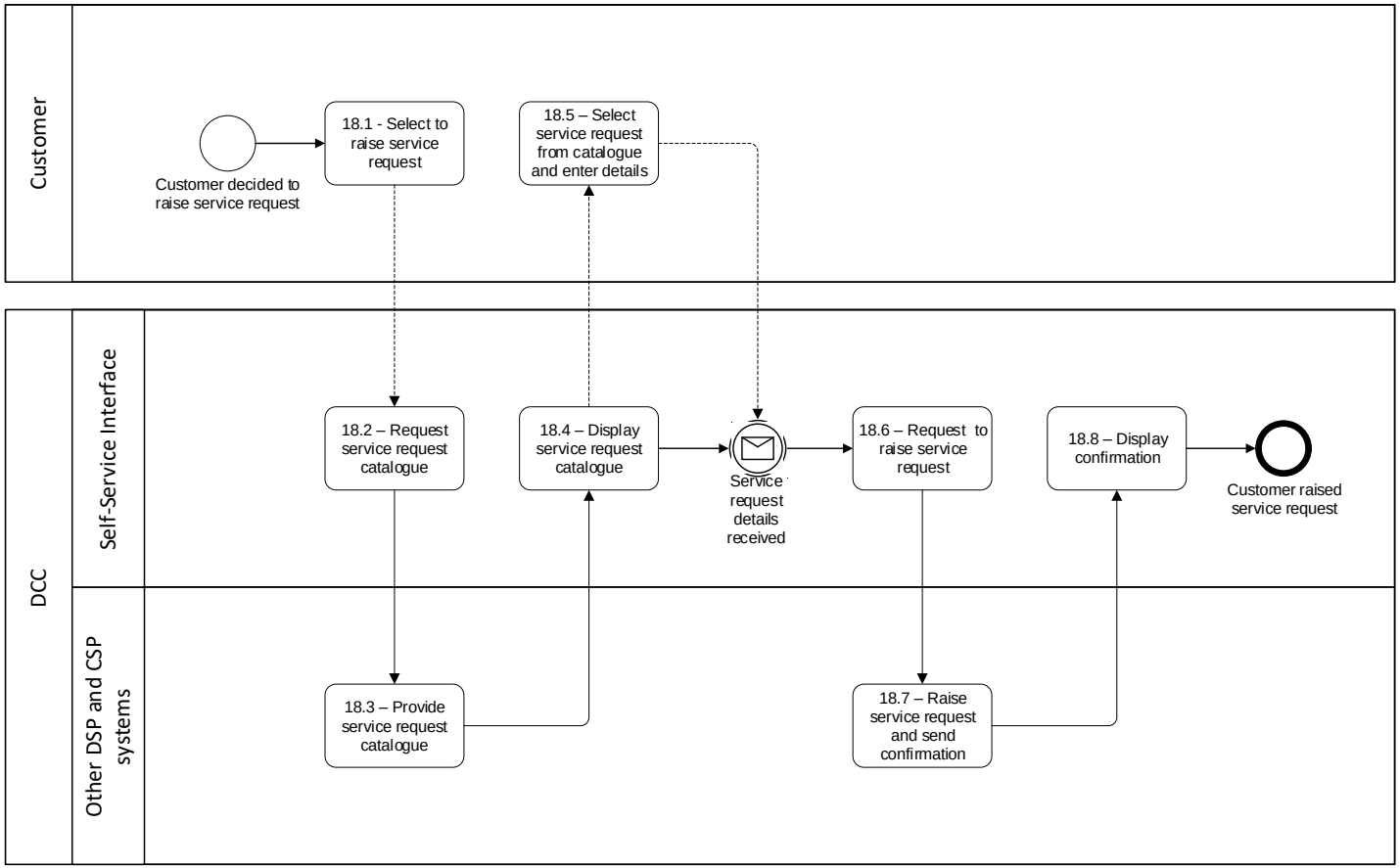
3.2.17 View User Manuals - PM17

The diagram below shows the baseline process map for PM17 (View User Manuals).



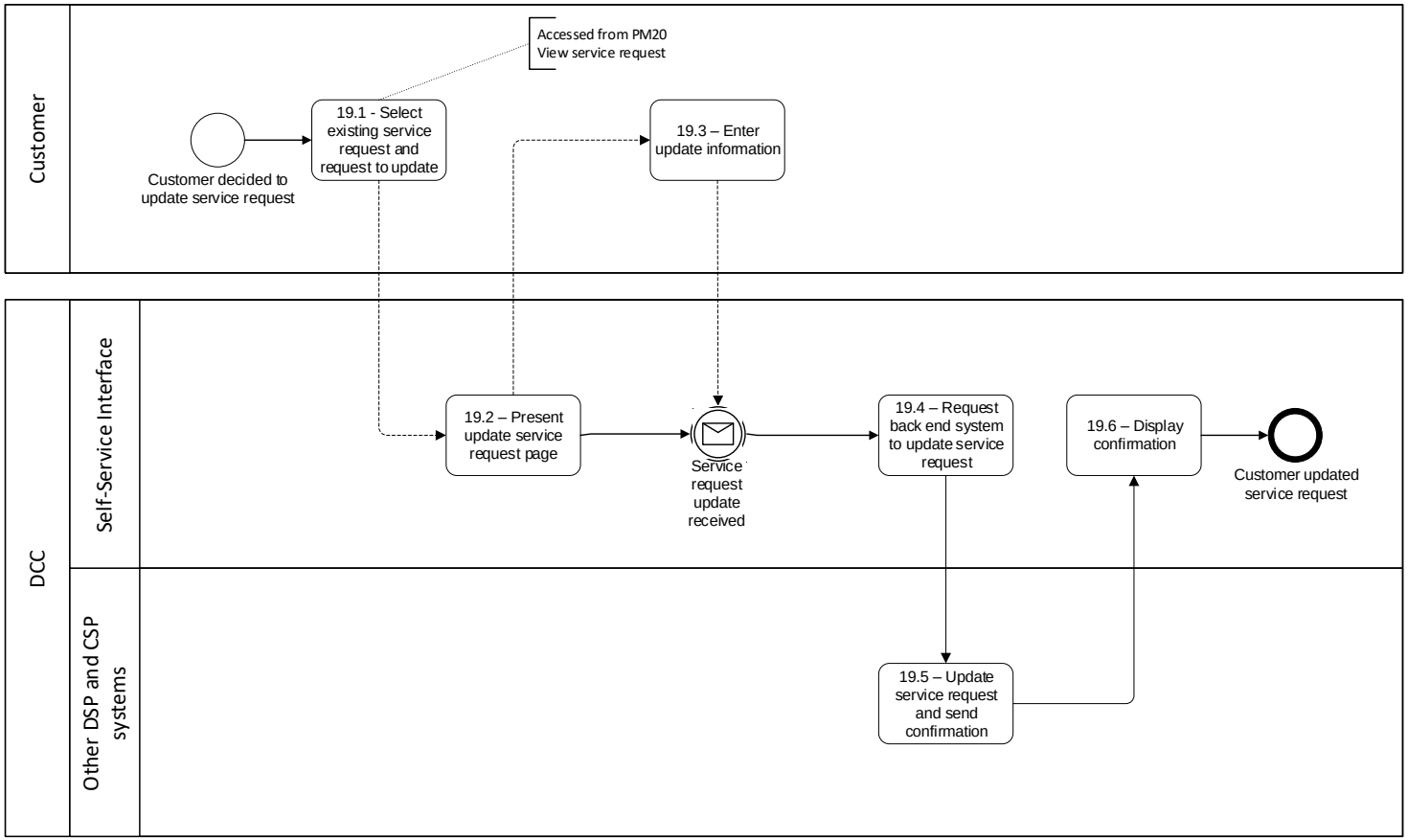
3.2.18 Raise Service Request - PM18

The diagram below shows the baseline process map for PM18 (Raise Service Request).



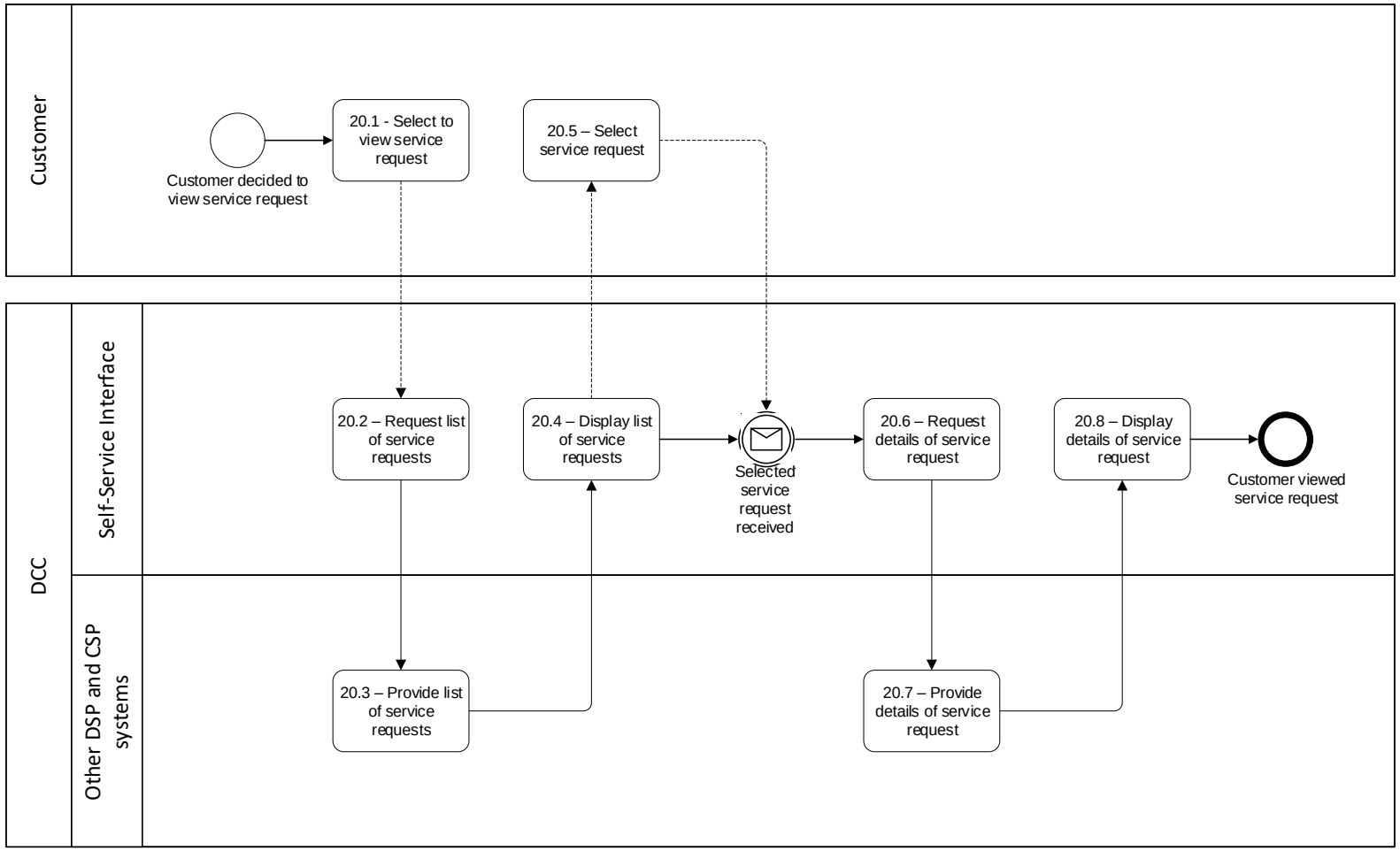
3.2.19 Update Service Request - PM19

The diagram below shows the baseline process map for PM19 (Update Service Request).



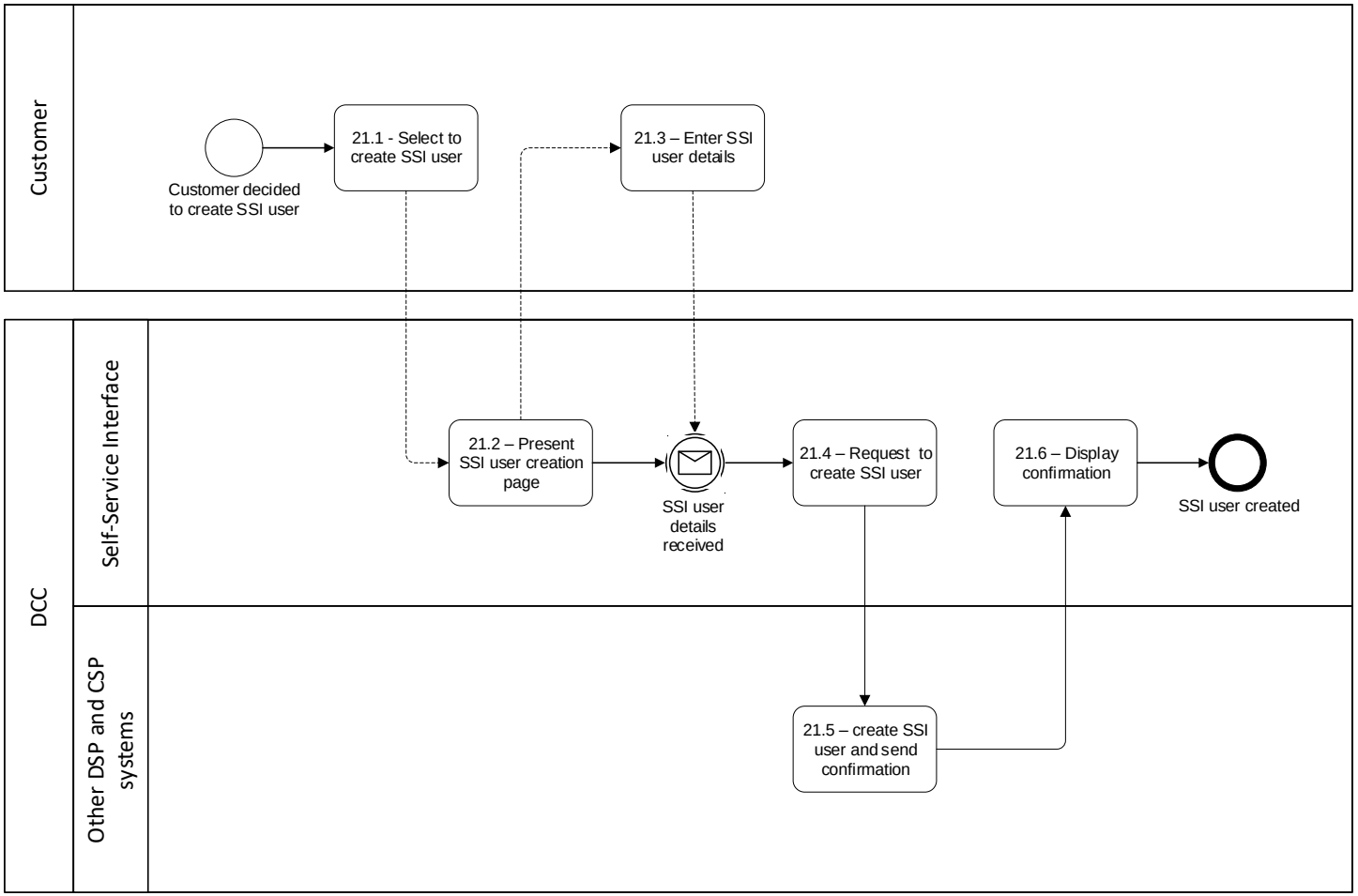
3.2.20 View Service Request - PM20

The diagram below shows the baseline process map for PM20 (View Service Request).



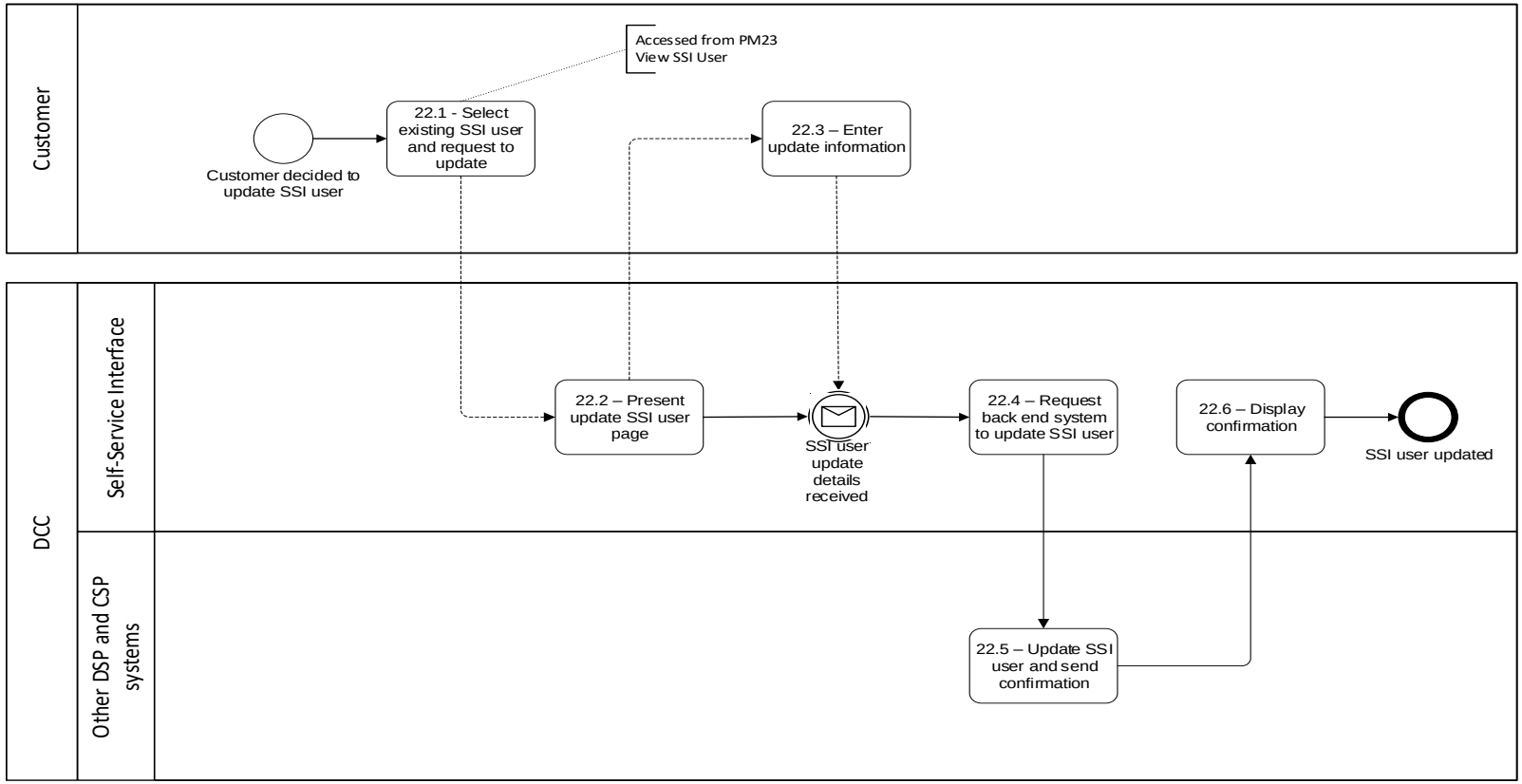
3.2.21 Create SSI User - PM21

The diagram below shows the baseline process map for PM21 (Create SSI User).



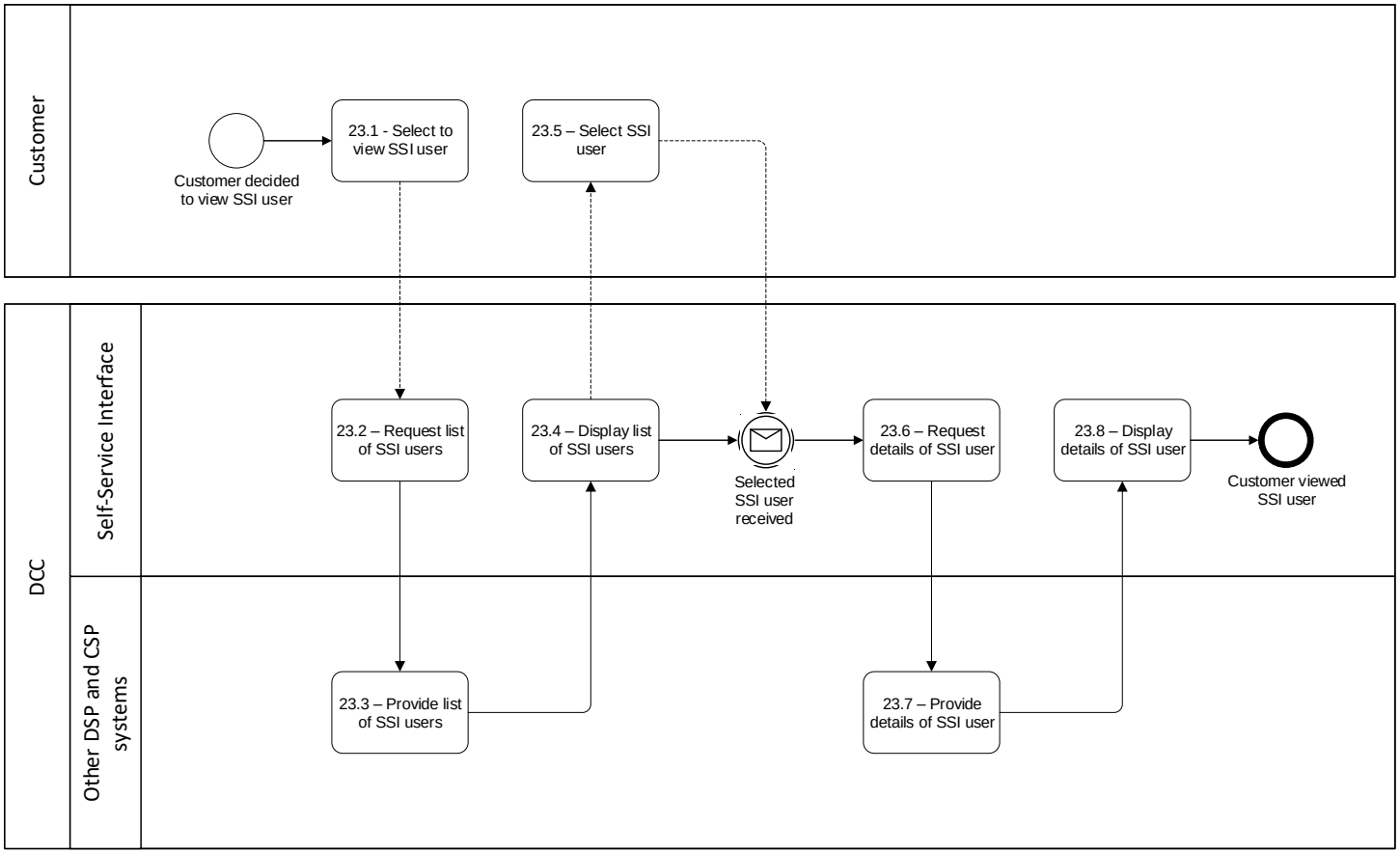
3.2.22 Update SSI User - PM22

The diagram below shows the baseline process map for PM22 (Update SSI User).



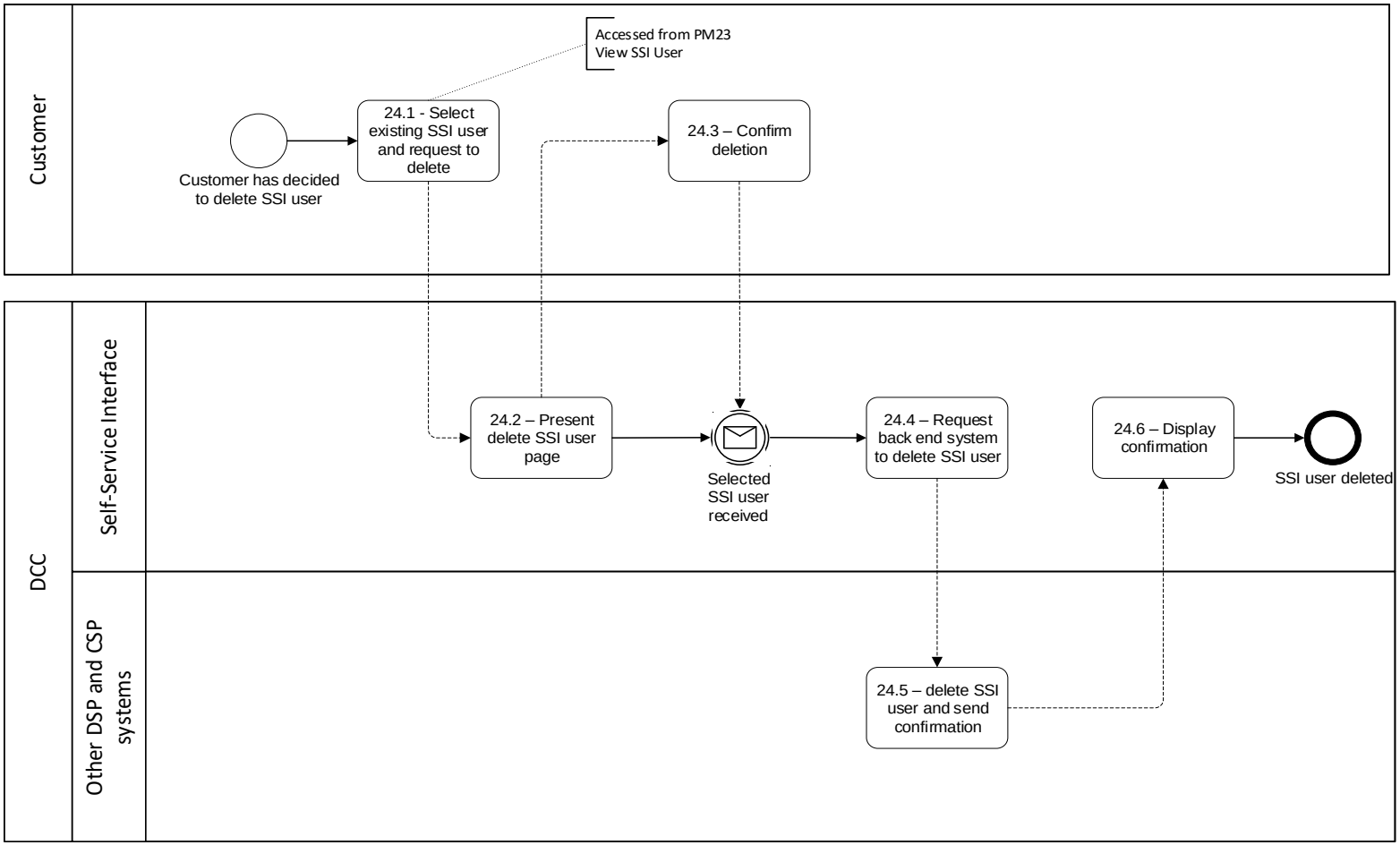
3.2.23 View SSI User - PM23

The diagram below shows the baseline process map for PM23 (View SSI User).



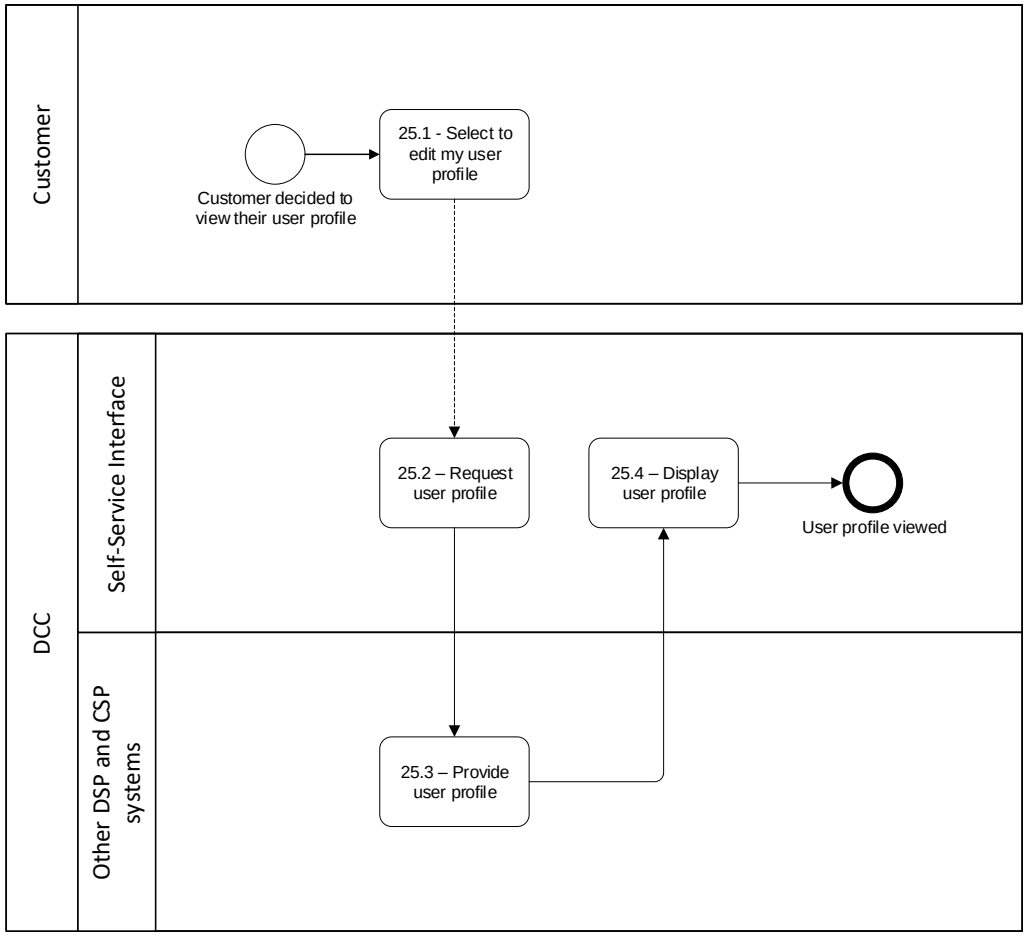
3.2.24 Delete SSI User - PM24

The diagram below shows the baseline process map for PM24 Delete SSI User.



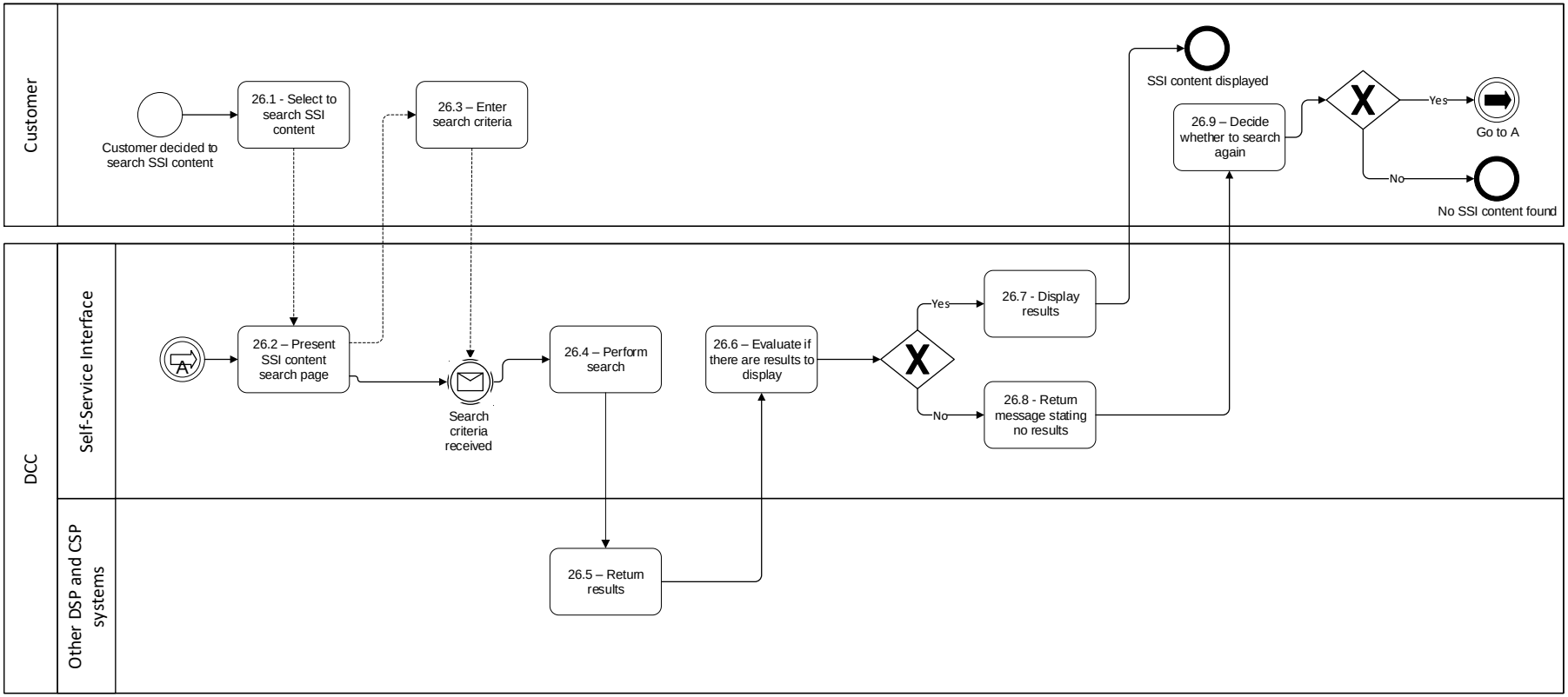
3.2.25 View My User Profile - PM25

The diagram below shows the baseline process map for PM25 (View My User Profile).



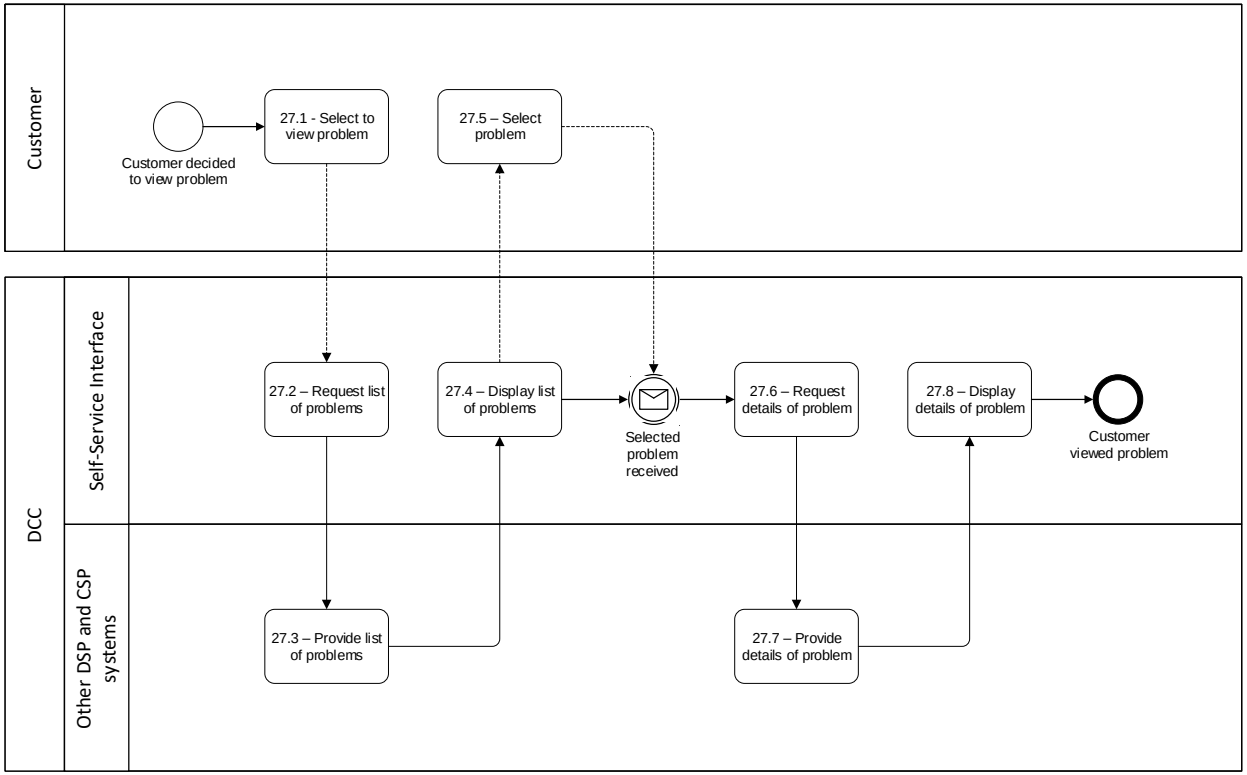
3.2.26 Search SSI Content - PM26

The diagram below shows the baseline process map for PM26 (Search SSI Content).



3.2.27 View Problem process - PM27

The diagram below shows the baseline process map for PM27 (View Problem).



4 Baseline SSI platform requirements

This section contains the baseline functional and non-functional requirements on the Self-Service Interface.

4.1 Baseline functional components and requirements

This section contains the baseline functional requirements on the Self-Service Interface.

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
Log In UC-Login-001: Enables User Personnel to login and access Self-Service Interface functionality.				
SSI-FR-1	The solution shall require a User to enter the following information on first login: • First name • Last name • Email address • Contact telephone number	BFD14	PM1	Must
SSI-FR-1a	Upon logging into SSI a confirmation shall be displayed	BFD14	PM1	Must
Smart Metering Inventory UC-Inventory-001: Enables User Personnel to query details of the Smart Metering Inventory.				
SSI-FR-2	The solution shall allow a User to search the Smart Metering Inventory by one or more of the following: MPxN Device ID full postcode and property filter (inclusive of property name / number) UPRN include Devices that have an SMI Status that is not ‘commissioned’ (checkbox)	BFD02	PM2	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-3	On a User searching the Smart Metering Inventory, if matches are found, a table of results shall be displayed, showing the following fields for each matching Device: - Device ID - Device Type - For installed Smart Meters, the related MPxN - For all Devices that are not Type 2 Devices, SMI Status - first line of address - UPRN - full postcode	BFD02	PM2	Must
UC-Inventory-002: Enables User Personnel to query details of the Smart Metering Inventory.				
SSI-FR-4	After a User has used the Smart Metering Inventory search to find a specific Device, and followed the Device ID link, to request the details view for the selected Device (and associated Devices), the solution shall allow a User to search the Smart Metering Inventory by one of the following: - For installed Smart Meters, the related MPxN - Device ID - full postcode and property filter - UPRN - include Devices that have an SMI Status that is not ‘commissioned’ (checkbox)	BFD02	PM2	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-5	On a User searching the Smart Metering Inventory, if matches are found, a table of results is displayed, showing the following fields for each matching Device and associated Devices, where applicable to the Device Type: - Device ID - Manufacturer - Device Model - Device Type - For Electricity Smart Meters, the applicable ESME Variant - SMETS Version - For Communications Hubs, the WAN Technology Type - Firmware Version - For Communications Hubs, the CSP region in which the Device is or has been installed - MPxN - For all Devices that are not Type 2 Devices, SMI Status (including Status history) - first line of address - UPRN - full postcode - Associated Devices and Devices with which that Device is Associated - Device ID - SMI Status - Description of Device	BFD02	PM2	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
Service Audit Trails UC-ServiceAudit-001: Enables User Personnel to query the service audit trail data held within the DCC Data Systems to show a record of all service activity.				

SSI-FR-6	The solution shall allow a Service User to retrieve service audit trail data by entering the following information:
	- One of the following:
	  o MPxN
	  o Device GUID
	  o UPRN
	- Service Reference Variant
	- From date
	- To date
		BFD04	PM3	Must

SSI-FR-6a	SSI service audit trail search shall only show records pertaining to a User where they are those for: • the User IDs for that User; and • any User IDs for which that User has been granted permission to access the information.	BFD04	PM3	Must

SSI-FR-7	On a User querying the service audit trail data, if matches are found, a table of results is displayed, showing the following Service audit trail details for each matching Device:
	
	Field Name:
	- DCC Service User Organisation ID
	- Device ID
	- GBCS Transaction Sequence Number, where required by GBCS
	- MPxN
	- Service Request Received Date/Time
	- Service Response Sent Date/Time
	- Service Reference
	- Simplified transaction status, which shall be one of the following:
	  o Success
	  o Failure
	  o In Progress
	
	Full Details:
	- Field Name
	- Request ID
	- Response ID
	- DCC Service User Organisation ID
	- Device ID
	- CSP Region
	- Mode of operation, which shall be one of the following:
	  o On Demand
	  o Future Date
	  o DSP Scheduled
	  o DCC Only
	  o Device Alert
	  o DCC Alert
	  o Meter Scheduled
	- Preceding Request ID (where applicable)
	- MPxN
	- Service Reference
	- Service Reference Variant
		BFD04	PM3	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
	- Command Variant - Response Code - Current Status - Anomaly Detection Flag - Status Change History			
UC-ServiceAudit-002 (Ext. 1 – Direct Linked Search): This is UC_ServiceAudit_001 (Main Flow) pre populated as the result of following a link on a previous page.				
SSI-FR-8	After a User has followed a Device link on another Self-Service Interface page which has directed them to the Service audit trails search page with a value indicating that a search for a specific Device ID should be carried out immediately, the solution shall allow the User to retrieve service audit trail details for the Device ID. The solution shall not require further User input but shall take as its input the Device ID that was followed.	BFD04	PM3	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-9	On a User querying the service audit trail details for a specific Device ID, the solution shall return the following information to the User: **Field Name:** - DCC Service User Organisation ID - Device ID - Sequence Number - MPxN - Service Request Received Date/Time - Service Response Sent Date/Time - Service Reference - Simplified Transaction Status **Full Details:** - Field Name - Request ID - Response ID - DCC Service User Organisation ID - Device ID - CSP Region - Mode of Operation - Preceding Request ID (where applicable) - MPxN - Service Reference - Service Reference Variant - Command Variant - Response Code - Current Status - Anomaly Detection Flag - Status Change History	BFD04	PM3	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
Meter Read Transactions UC-MeterRead-001: Enables User Personnel to query the service audit trail data held within the DCC Data Systems to show records of meter read transaction activity for all Users. This differs from the main service audit trail use case [UC_ServiceAudit_001 (Main Flow)] in that all service audit trail entries for meter read transaction activity through this use case are available to all Users.				

SSI-FR-10	The solution shall allow a User to query the service audit trail data to retrieve meter read transaction data, by entering the data below:
	- One of the following:
	  o Device GUID
	  o UPRN
	  o MPxN
	- Service Reference Variant
	- Checkboxes allowing the selection of any of the following Service Reference Variants ; 4.8.1, 4.8.2, 4.8.3 or 4.17
	- From date
	- To date
		BFD06	PM4	Must

SSI-FR-11	On a User querying the service audit trail data to retrieve meter read transaction data,
	if matches are found, a table of results is displayed, showing the following Service audit trail details for each matching Device:
	
	Field Name:
	- DCC Service User Organisation ID Device ID
	- GBCS Transaction Sequence Number, where required by GBCS
	- MPxN
	- Service Request Received Date/Time
	- Service Response Sent Date/Time
	- Service Reference Variant
	- Service Reference
	- Simplified transaction status, which shall be one of the following:
	  o Success
	  o Failure
	  o In Progress
	
	Full Details:
	- Field Name
	- Request ID
	- Response ID
	- DCC Service User Organisation ID
	- Device ID
	- CSP Region, which shall be one of the following:
	  o North
	  o Central
	  o South
	  o Unknown
	- Mode of operation, which shall be one of the following:
	  o On Demand
	  o Future Date
	  o DSP Scheduled
	  o DCC Only
	  o Device Alert
	  o DCC Alert
		BFD06	PM4	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
	○ Meter Scheduled - Preceding Request ID (where applicable) - MPxN - Service Reference Variant - Command Variant - Response Code - Current Status - Anomaly Detection Flag - Status Change History			
SM WAN Network Coverage UC-CSPCoverage-001: Enables User Personnel to check SM WAN coverage data at a postcode level across GB in each of the three Regions.				
SSI-FR-12	The solution shall allow a User to check SM WAN coverage data at a postcode level across GB in each of the three Regions, by entering the information below: - One of the following: ○ full postcode ○ full postcode and property name/number ○ a postcode outcode (all but the last three characters of a full postcode)	BFD07	PM5	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)

SSI-FR-13	On a User checking SM WAN coverage data at a postcode level across GB in each of the three Regions, the solution shall present back to the user the following information:
	
	- CSP (the CSP responsible for this location/area)
	- Postcode
	- Property name/number (where appropriate)
	- WAN coverage availability (Yes or No)
	- Anticipated coverage date (if coverage availability was No), or “No Coverage Intended”
	- Likelihood of connectivity to the SM WAN at the location
	- Communications Hub WAN Variant to be used
	- Auxiliary equipment required
	- Additional information, which shall (where applicable) contain details of:
	  ○ whether the location is included within an area that is the subject of a Service Exemption Category 2 and if so, where applicable, the date from which the location will cease to be included; and
	  ○ issues giving rise to poor connectivity at the location and any information regarding likely resolution to such connectivity issues.
		BFD07	PM5	Must

UC-CSPCoverage-002 Enables User Personnel to view details of WAN coverage where returned as a result of a search other than that defined in UC-CSP-Coverage-001 (Main Flow).				
SSI-FR-14	After a User followed a Device link on another Self-Service Interface page which has directed them to the WAN Coverage search page with an argument indicating that a search for a specific postcode or premises should be carried out immediately, the solution shall allow the user to retrieve SM WAN coverage at this postcode or premises.	BFD07	PM5	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-15	On a User checking SM WAN coverage data for a specific postcode or premises, the solution shall present back to the User the following information: - CSP (the CSP responsible for this location/area) - Postcode - Property name/number (where appropriate) - Coverage availability (Yes or No) - Anticipated coverage date (if coverage availability was No), or “No Coverage Intended” - Likelihood of connectivity (Low/Medium/High) - Communications Hub WAN Variant to be used - Auxiliary equipment required - Additional information	BFD07	PM5	Must
Communications Hub Availability and Diagnostics UC-HubStatus-001: Enables User Personnel to attempt to diagnose and resolve incidents using the DCC's remote diagnostic tools.				
SSI-FR-16	The solution shall allow the User to attempt to diagnose and resolve incidents using the DCC's remote diagnostic tools by entering a Communications Hub Function Device ID	BFD10	PM6	Must
SSI-FR-16a	Only the Responsible Supplier, The Network Party or Registered Supplier Agent, for a Smart Metering System of which a Communications Hub Function forms a part of shall be able to communicate with the device.	BFD10	PM6	Must
SSI-FR-16b	Only the Responsible Supplier, The Network Party or Registered Supply Agent for a Smart Metering system of which a Communications Hub Function forms a part of shall be able to carry out a full diagnostics request.	BFD10	PM5	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)

SSI-FR-17	On a User entering a Communications Hub Function Device ID to attempt to diagnose and resolve incidents, the solution shall present back to the User the information below:
	
	- Anonymised table of Service Requests giving rise to up to the last 5 Commands transacted through the Communications Hub, showing time and success status in relation to the Command being issued to the Device.
	- A table showing data provided by the CSP responsible for this Communications Hub (data resident on the Communications Hub displays "Requires device communication"), and providing the following fields:
	  o Aerial Installed
	  o Aerial Type
	  o Birth Event
	  o Network Status
	  o Deactivation Date/Time (if network status is deactivated)
	  o SMWAN Connectivity Status
	  o HAN Status
	  o Last Connection
	  o Last Tamper
	  o Last Outage
	  o Last Restore
		BFD10	PM6	Must

UC-HubStatus-002 (Ext. 1 – Direct Linked Search): Enables User Personnel to view details of selected Communications Hub availability information where returned as a result of a search other than that defined in UC-HubStatus-001 (Main Flow).				
SSI-FR-18	After a User followed a Device link on another Self-Service Interface page which has directed them to the Communications Hub availability and diagnostics search page with an argument indicating that a search for a specific Communications Hub should be carried out immediately. The Solution shall allow the User to attempt to diagnose and resolve incidents for this Communications Hub Function Device ID using the DCC's remote diagnostic tools	BFD10	PM6	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-19	On a User having attempted to diagnose and resolve incidents for this Communications Hub Function Device ID by following a Device link, the system shall present the information below back to the User: Anonymised table of Service Requests giving rise to up to the last five Commands transacted through the Communications Hub, showing time and success status in relation to the Command being issued to the Device. A table showing data provided by the CSP responsible for this Communications Hub (data resident on the Communications Hub displays "Requires Device Communication")	BFD10	PM6	Must
Interaction with Order Management Systems (OMS)				
SSI-FR-20	The DCC shall provide a link from the Self-Service Interface that enables Users to navigate to the OMS. Access to the OMS and capabilities of the OMS are defined in the Communications Hub Handover Support Materials.	BFD13	PM7	Must
Forecasting and ordering of Communications Hubs and auxiliary equipment UC-CSPOMS-001 (Main Flow): Redirects User Personnel to the OMS (which enables User Personnel to submit forecasts of future orders and actual orders for Communications Hubs and Communications Hub Auxiliary Equipment requirement).				
SSI-FR-20a	The solution shall allow a User to open the Order Management System by clicking a button	BFD13	PM7	Must
Reporting UC-Reports-001: Enable User Personnel to run a set of standard pre-defined and parameterised reports against DCC data. Such reports are specified in the SSI reporting specification as published on the DCC Website.				
SSI-FR-21	The solution will allow a User to run a set of standard pre-defined and parameterised reports against DCC data. Such reports are specified in the SSI reporting specification as published on the DCC Website.	BFD11	PM8	Must
SSI-FR-21a	SSI reports shall only show data pertaining to the user.	BFD11	PM8	Must
Raise Incident UC_RaiseSMI_001 (Main Flow): Enables User Personnel to raise service management Incidents within the DCC service management systems.				

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-22	The solution shall allow User Personnel to raise service management Incidents within the DCC service management systems by entering the following information: - Incident category-specific parameters - User Personnel contact details: o first name, last name, telephone number (mandatory fields) o email address (optional)	BFD01	PM9	Must
SSI-FR-22a	SSI shall only allow User Personnel to raise Incidents in accordance with H9	BFD01	PM9	Must
SSI-FR-23	On a User raising a service management incident, the solution shall present back the following information to the User: - Incident reference	BFD01	PM9	Must
UC-RaiseSMI-002 (Ext. 1 – Direct Linked Pre Selection): This is a special case of UC_RaiseSMI_001 (Main Flow), where User Personnel navigated from another screen, and the category of the Incident and some input fields are pre-populated.				
SSI-FR-24	After a User followed a link on another page, indicating that they would like to raise an Incident related to the content that they are viewing, including the Communications Hub status and Communications Hub Availability and Diagnostics page to raise an incident for that Communications Hub, or a knowledge article to provide feedback on that article, the solution shall allow the User to create an incident by entering the following information, with some information being pre-populated: - Incident category-specific parameters	BFD01	PM9	Must
SSI-FR-25	On a User raising a service management incident after following a link from another page, the solution shall present back the following information to the User: - Incident reference	BFD01	PM9	Must
UC-RaiseSMI-003 (Ext. 2 – Premises Related Incident): This is a special case of UC_RaiseSMI_001 (Main Flow), where User Personnel chose to raise a premise related Incident, which has a more complex and specific workflow than other Incident categories.				

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)

SSI-FR-26	The solution shall allow Users to raise a premises-related incident by entering the information:
	
	- DeviceID or MPxN
	- User ID (where a User has been granted access to the Self-Service Interface on behalf of another User)
	- Incident-specific information (optional)
	- Incident summary
	- Your reference
	- Incident notes (optional)
	- User Personnel contact details:
	  o first name, last name, telephone number (mandatory fields)
	  o email address (optional)
		BFD01	PM9	Must

SSI-FR-27	On a User raising a premises-related incident, the solution shall present back the following information to the User: - Incident reference	BFD01	PM9	Must
UC-RaiseSMI-004 (Ext. 3 – Direct Linked Pre Selection For Premises Related Incident): This is a special case of UC-RaiseSMI-003, where User Personnel navigated from the Communications Hub availability and diagnostics screen, and the category of the incident and input/verification of the Communications Hub have been pre-verified and pre-populated.				

SSI-FR-28	After a User followed a link from the Communications Hub Availability and Diagnostics page, indicating that they would like to raise a premise related Incident against the Communications Hub that they are viewing, the solution shall allow the User to raise a premise-related Incident by entering the information below:
	
	- Incident-specific information (optional)
	- Incident summary
	- Business impact
	- Incident notes (optional)
	- User Personnel contact details:
	  o first name, last name, telephone number (mandatory fields)
	  o email address (optional)
		BFD01	PM9	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-29	On a User raising a premises-related incident by following a link from the Communications Hub Availability and Diagnostics page, the solution shall present back the following information to the User: - Incident reference	BFD01	PM9	Must
Update Service Management Incident UC-UpdateSMI-001 (Main Flow): Enables User Personnel to make updates to an existing Incident.				
SSI-FR-30	After a User views a specific incident, the solution shall allow the User to make updates to the Incident by entering the information below: - Incident reference - Type of update - Update text	BFD01	PM10	Must
SSI-FR-30a	SSI shall only allow appropriately privileged User Personnel to view and update an incident in accordance with section H9.	BFD01	PM10	Must
SSI-FR-31	On a User making updates to an existing Incident, the solution shall present the information below back to the User: - Update confirmation	BFD01	PM10	Must
View Service Management Incident UC-ViewSMI-001 (Main Flow): Enables User Personnel to view details of previously raised Incidents within the DCC Service Management System.				
SSI-FR-32	The solution shall allow a User to select an incident from a pre-populated list of incidents and request to see details of this incident	BFD01	PM11	Must
SSI-FR-32a	SSI shall only allow appropriately privileged User Personnel to view and update an incident in accordance with section H9.	BFD01	PM11	Must
UC-ViewSMI-002 (Ext. 1 – View Specific Incident): This is a sub screen of the main UC_ViewSMI_001 (Main Flow) showing more detailed information relating to selected service management Incident information.				

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-33	After a User follows a link from another Interface Transaction indicating that they would like to see the details of a specific service management incident, the solution shall allow the User to see this incident. Where the User did not raise the Incident, solution shall withhold from the User certain personal information about the raising individual, contact details and incident update description	BFD01	PM11	Must
SSI-FR-34	On a User following a link from another Interface Transaction indicating that they would like to see the details of a specific service management incident, the solution shall return the information below to the User: - Summary text - Incident notes - Raising individual - first and last name (only visible to the User that raised the Incident) - Raising organisation (User) - Device (where appropriate) - Communications Hub model and version (where appropriate) - MPxNs associated with Smart Meter(s) related to incident - comma-separated list - CSP Diagnostic output (where appropriate) - Postcode (where appropriate) - Your reference - Current status - Target resolution date/time - Requester contact details - first and last name, telephone number and email (not visible to interested persons) - Additional contact details - first and last name, telephone number and email (not visible to interested persons) - Incident priority	BFD01	PM11	Must
Knowledge Management UC_KnowledgeManagement_001 (Main Flow): Enables User Personnel to view relevant help and support information (provided by DCC and its Service Providers), for early triage of User issues and queries, including access to the anonymous resolution details of service management problems and Incidents.				
SSI-FR-35	The solution shall allow Users to view relevant help and support information by selecting an article from a list of stored articles.	BFD12	PM12	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)

SSI-FR-36	On a User selecting an article to view, the solution shall present the information below back to the User:
	
	- Article details
	  ○ Title
	  ○ Creation Date/Time
	  ○ Creator
	  ○ Last Modifier
	  ○ Tags
	  ○ Article text
	  ○ Attachments (optional)
		BFD12	PM12	Must

Forward Schedule of Change UC-Schedule-001 (Main Flow): Enables User Personnel to view details of any planned maintenance, changes scheduled or change freezes affecting any of the following elements of the DCC Total System: • Communications Hub firmware • Parse & Correlate Software • SMKI software • SEC releases • other major DCC releases • meter firmware events				
SSI-FR-37	The solution shall allow Users to view details of any planned maintenance, changes scheduled or change freezes affecting any of the following elements of the DCC Total System: - Communications Hub firmware - Parse & Correlate Software - SMKI software - SEC releases - other major DCC releases - meter firmware events (only visible to Users for Devices for which they are the Responsible Supplier)	BFD05	PM13	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-37a	SSI shall only allow Meter firmware events to be visible to Users for Devices for which they are the Responsible Supplier.	BFD05	PM13	Must
SSI-FR-38	On a User selecting to view details of any planned maintenance, changes scheduled or change freezes, the solution shall present the information below back to the User: - Planned start date/time - Planned end date/time - Event type - System component (or release/change type) - Impact severity - Geographic impact - Notes - Button to click to obtain full details	BFD05	PM13	Must
UC-Schedule-002 (Ext. 1 – Calendar View): Enables User Personnel to view details of planned events within the DCC Systems or relating to the SM WAN in a calendar format.				
SSI-FR-39	The solution shall enable Users to view details of planned events within the DCC Systems or relating to the SM WAN in a calendar format. Calendar day cells shall contain items representing event types relevant to that day.	BFD05	PM13	Must
SSI-FR-39a	SSI shall only allow Meter firmware events to be visible to Users for Devices for which they are the Responsible Supplier.	BFD05	PM13	Must
UC-Schedule-003 (Ext. 2 – View Specific Event): Allows User Personnel, having chosen to view a specific event from UC-Schedule-001 or UC-Schedule-002, to view the full details held about the event in question.				
SSI-FR-40	After a User either a) views details of any planned maintenance, changes scheduled or change freezes or b) views details of planned events within the DCC Systems or relating to the SM WAN in a calendar format the solution shall allow the User to select a specific event to view details of.	BFD05	PM13	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)

SSI-FR-41	On a User selecting a specific event to view details of, the solution shall present the information below back to the User:
	
	For all events:
	- Event details:
	  ○ event reference
	  ○ planned start date/time
	  ○ planned end date/time
	  ○ event notes
	
	For maintenance and change freeze events:
	- event type
	- DCC System component or Region
	- impact severity
	- geographic impact
	
	For release, meter firmware and change events:
	- release/change type
	- manufacturer's reference
	- manufacturer's notes
	- Device type and Device Model
	- - firmware version
		BFD05	PM13	Must

DCC Service Status UC-ServiceDashboard-001 (Main Flow): Enables User Personnel to view a one page dashboard of DCC component availability for the DCC Service.				
SSI-FR-42	The solution shall enable Users to view a one page dashboard of DCC component availability for the DCC Service	BFD03	PM14	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-43	On a User selecting to view a one page dashboard of DCC component availability for the DCC Service, the solution shall present the information below back to the User: List of system components comprising: - DCC System component name - high level status of component - count of the number of underlying service alerts for the component - Link to service alerts relating to Major Incidents	BFD03	PM14	Must
DCC Service Alerts UC_ServiceAlerts_001: Enables User Personnel to view any service affecting news / alerts and other useful text (in terms of quality of service delivery and service management) to the User.				
SSI-FR-44	The solution shall enable User Personnel to view any service affecting news / alerts and other useful text (in terms of quality of service delivery and service management) to the User	BFD08	PM15	Must
SSI-FR-45	On a User selecting to view service affecting news / alerts and other useful text, the solution shall present the information below back to the User: List of currently active Alerts: - Service Alert ID (link to view in more detail) - System component/s (as listed in service dashboard) - geographic impact - alert creation - expected resolution - alert closure - latest update	BFD08	PM15	Must
UC-ServiceAlerts-002 (Ext. 1 – View Specific Alert): This Interface Transaction allows User Personnel, having chosen to view a specific DCC Service Alert from UC_ServiceAlerts_001, to view the full details held about the alert in question.				
SSI-FR-46	After a User selects to view service affecting news / alerts and other useful text, the solution shall allow the User to select a specific Alert and see full details.	BFD08	PM15	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)

SSI-FR-47	On a User selecting a specific Alert to see full details of, the solution shall present the information below back to the User:
	
	- Service Alert ID (link to view in more detail)
	- DCC System Component/s (as listed in service dashboard)
	- geographic impact
	- alert creation
	- expected resolution
	- alert closure
	- latest update
	- Reverse chronological list of updates for the alert, each comprising:
	  o date/time of update
	  o person/entity providing update
	  o update text
		BFD08	PM15	Must

FAQs UC-FAQ-001 (Main Flow): Enables User Personnel to access helpful DCC Service Frequently Asked Questions.				
SSI-FR-48	The solution shall enable User Personnel to access helpful DCC Service Frequently Asked Questions by entering the information below: - Text filter string (optional) - Tag selection from list of all tags (optional)	BFD12	PM16	Must
SSI-FR-49	On a User requesting to access helpful DCC Service Frequently Asked Questions, the solution shall present back the information below to the User: - FAQ question and answer - Attached documents (optional)	BFD12	PM16	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
DCC User Manuals UC-Manuals-001 (Main Flow): Enables User Personnel to access a set of DCC user manuals which help Users understand how the DCC Service operates.				
SSI-FR-50	The solution shall enable User Personnel to access a set of DCC user manuals which help Users understand how the DCC Service operates by entering the information below: - Article reference - Article usefulness rating selector	BFD12	PM17	Must

SSI-FR-51	On a User selecting to access a set of DCC user manuals which help Users understand how the DCC Service operates, the solution shall present back the information below to the User:
	
	- Article page:
	  ○ title of the article
	  ○ creation date/time
	  ○ creator
	  ○ last modification
	  ○ last modifier
	  ○ tags
	  ○ textual description of the user manual, other document, or content
		BFD12	PM17	Must

Service Catalogue Publication/Call Off UC-ServiceCatalogue-001 (Main Flow): Enables User Personnel to raise service management service requests with the DCC and track and update the status of such Requests within the DCC service management systems.				
SSI-FR-52	The solution shall enable Users to raise service management service requests with the DCC and track and update the status of such Requests within the DCC service management systems	BFD09	PM18	Must
SSI-FR-52a	SSI shall only allow User Personnel to see requests raised by the User with which they are associated.	BFD09	PM18	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-53	On a User selecting to raise service management service requests with the DCC or track and update the status of such Requests within the DCC service management systems, the solution will display all open service catalogue requests raised by their organisation with the following fields: - Service request ID - Work order reference - Request type - Raised date/time - Current delivery status	BFD09	PM19	Must
UC-ServiceCatalogue-002 (Ext. 1 – View Specific Request): This Interface Transaction allows User Personnel, having chosen to view a specific service catalogue request from UC-ServiceCatalogue-001, to view the full details held about the request in question.				
SSI-FR-54	After a User views all open service catalogue requests raised by their organisation, the solution shall allow the User to select one service catalogue request to view full details of.	BFD09	PM19	Must
SSI-FR-55	On a User selecting one service catalogue request to view full details of, the solution shall present the information below back to the User: - Service Request ID - Work order reference - Your reference - Request type - Raised date/time - Current delivery status - Raising user - Raising Organisation - User ID - Requester contact details - first and last name, telephone number and email. - Additional contact details - first and last name, telephone number and email	BFD09	PM20	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
UC-ServiceCatalogue-003 (Ext. 2 – Browse Catalogue / Raise Request): Allows User Personnel to browse the service catalogue and raise a new service catalogue request.				
SSI-FR-56	The solution shall enable Users to browse the service catalogue and raise a new service catalogue request, by entering the information below: - Business service category (selection list) - Business service category services (selection list) - Service request types (selection list) - Raise request button - First name - mandatory string - Last name - mandatory string - Telephone number - mandatory string - Email address - a valid email address - “Update contact details” button	BFD09	PM18	Must
SSI-FR-57	User Personnel shall only be able to raise requests on behalf of the User with which they are associated	BFD09	PM18	Must
User Account Management UC-OrgManager-001 (Main Flow): Enable Users electing to use the DCC Identity Provider Service to assign access to Interface Transactions to their User Personnel based on Job Type Roles and manage the SSI accounts and associated settings (e.g. password resets) for all subsequently created User Personnel accounts created by an Administration User.				
SSI-FR-58	The solution shall enable Administration Users electing to use the DCC Identity Provider Service to assign access to Interface Transactions to their User Personnel based on Job Type Roles and manage the SSI accounts and associated settings (e.g. password resets) for all subsequently created User Personnel accounts created by an Administration User.	BFD14	PM22	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)

SSI-FR-59	On an Administration User electing to use the DCC Identity Provider Service to assign access to Interface Transactions to their User Personnel based on Job Type Roles and manage the SSI accounts and associated settings (e.g. password resets) for all subsequently created User Personnel accounts created by an Administration User, the solution shall present the information below back to the User:
	
	- User search page - This shows a sortable, pageable table of User Personnel accounts, with the following details in each row:
	  o username (hyperlink to UC_OrgManager_002)
	  o display name
	  o Account Status (Active/Deleted/Locked)
	  o last login date
		BFD14	PM23	Must

UC-OrgManager-002 (Ext. 1 – Manage User): Enable Administration Users to unlock, delete or manage the details of another account created within their corporation.				

SSI-FR-60	The solution shall enable Administration Users to unlock, delete or manage the details of another account created within their corporation. The list below specifies how users may be edited:
	
	- Username - not editable
	- Account status – not editable
	- First name
	- Last name
	- Organisations - a list of User ID(s) in relation to which the User Personnel may access the Self-Service Interface, which shall comprise:
	  o one or more of the User IDs of the User; and
	  o User IDs of any second User that has granted permission for the first User to access its information held on the Self-Service Interface in relation to one or more User IDs.
	- Roles - a list of Job Type Roles which may be assigned to this person.
		BFD14	PM24	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
UC-OrgManager-003 (Ext. 1 – Create User): Enable an Administration User to create a new person's account within their organisation.				

SSI-FR-61	The solution shall enable an Administration User to create a new person's account within their organisation by entering the information below:
	
	- Username - Desired username (globally unique within the DCC Identity Provider Service). If the username is not unique, the DCC will reject the username and request submission of a new username.
	- First name
	- Last name
	- Organisations - a list of User ID(s) in relation to which the User Personnel may access the Self-Service Interface, which shall comprise:
	  o the User ID of the User ; and
	  o User IDs of any second User that has granted permission for the first User to access its information held on the Self-Service Interface in relation to one or more User IDs.
	- Roles - a list of Job Type Roles which may be assigned to this person
		BFD14	PM21	Must

User Profile Information UC-Profile-001: Enables User Personnel to view information about the account details with which they are accessing the Self-Service Interface, and details of the Interface Transactions that they are currently entitled to access.				
SSI-FR-62	The solution shall enable Users to view information about the account details with which they are accessing the Self-Service Interface, and details of the Interface Transactions that they are currently entitled to access.	BFD14	PM25	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
SSI-FR-63	On a User selecting to view information about the account details with which they are accessing the Self-Service Interface, and details of the Interface Transactions that they are currently entitled to access, the solution shall present the information below back to the User: - Unique user identification - changes depending on the nature and type of the Identity Provider Service - Organisations - A list of User IDs that the User is assigned to - Roles - A list of roles assigned to the person. - Use cases - A list of Interface Transactions, with a “Yes” or “No” indication of whether the person has access as a result of their Job Type Role(s) - Bookmarks - A list of links to content that the person has bookmarked.	BFD14	PM25	Must
Search UC-Search-001: Enables User Personnel to search for content provided by the Self-Service Interface by use of tagged keywords, or textual content of page titles and descriptions.				
SSI-FR-64	The solution shall enable Users to search for content provided by the Self-Service Interface by use of tagged keywords, or textual content of page titles and descriptions	BFD12	PM26	Must
SSI-FR-65	On a User searching for content provided by the Self-Service Interface by use of tagged keywords, or textual content of page titles and descriptions, the solution shall present the information below back to the User. The title of the located item of content (which is also a link to that piece of content). A short summary description of the content. Reasons that the content was found (i.e. matches found in title, description, tags or attached filenames). If no results are found matching the search criteria, a message is displayed to this effect.	BFD12	PM26	Must

ID	Functional Component / Requirement	Business Functional Domain	Process Map	(MoSCoW)
Problem Management UC-ProblemManagement-001 (Main Flow): Enables User Personnel to view details of open Problems related to incidents.				
SSI-FR-66	The solution shall enable Users to view details of open Problems related to incidents by presenting them with a list of the Problems visible to them in accordance with SEC H9	BFD01	PM27	Must
SSI-FR-67	On a User selecting to view details of open Problems related to incidents, the solution shall present back the information below to the User, for each Problem. - Problem Reference - Current Problem Status - Problem Summary	BFD01	PM27	Must
UC-ProblemManagement-002 (Ext. 1 – View Specific Problem): This is a sub screen of the main UC_ProblemManagement_001 (Main Flow) Interface Transaction showing more detailed information relating to a selected Problem.				
SSI-FR-68	After a User selects to view details of open Problems related to incidents, the solution shall allow them to select one Problem to see more detailed information about.	BFD01	PM27	Must
SSI-FR-69	On a User selecting one Problem to see more detailed information about, the solution shall present the information below back to the User: - Field Name - Problem Reference - Current Problem Status - Problem Summary - Problem Notes - Problem priority - Date Raised	BFD01	PM27	Must
File Download Interface The DCC shall ensure that the Self-Service Interface provides User Personnel who are downloading files with a prompt to save files.				
SSI-FR-70	The SSI shall provide the facility for Service Users to download files to save files, where the Process Map specifies it	BFD04	All	Must
Interactive Web Interface SSI Interface will provide an interactive web interface				
SSI-FR-71	Thee Self-Service Interface shall provide a web interface to Service Users.			

4.2 Baseline non-functional requirements

This section contains the baseline non-functional requirements on the Self-Service Interface.

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SELF-SERVICE INTERFACE DESIGN SPECIFICATION				
SSI-NFR-1	Requests to access the Self-Service Interface shall be directed to the appropriate URL for dealing with that request, and such URL shall be implemented and maintained such that communications across it can be authenticated.	Security	All	Must
Authorisation				
SSI-NFR-2	Each user of the Self-Service Interface shall only be permitted to access an Interface Transaction if it is entitled to do so given the User ID(s) and Job Type Role(s) that are supplied as attributes of the SAML assertion.	Security	All	Must
SAML Authentication				
SSI-NFR-3	The DCC shall provide to Users a SAML-capable Identity Provider Service for the purpose of authentication of User Personnel to the Self-Service Interface (the “DCC Identity Provider Service”).	Security	PM1	Must
SSI-NFR-4	Each User may use an Identity Provider Service that is not the DCC Identity Provider Service for the purpose of authentication of its User Personnel to the Self- Service Interface. The solution shall support the use of such Identity Provider Services.	Security	PM1	Must
SSI-NFR-5	Each request from a User Personnel to access the Self-Service Interface shall be authenticated with either: - a) a SAML assertion provided by the DCC Identity Provider Service (as defined in SSI-NFR-10); or - b) a SAML assertion provided by an Identity Provider Service provided by the User.	Security	PM1	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SSI-NFR-6	After an Identity Provider Service provides the User Personnel's SAML assertion, a secure cookie shall be stored in the User Personnel's browser. Such secure cookie shall be set to expire 8.5 hours after initial authentication by: a) the DCC, for the DCC Identity Provider Service; or b) the User, where such User is using an Identity Provider Service that is not the DCC Identity Provider Service.	Security	PM1	Must
SSI-NFR-7	If a secure cookie exists during subsequent authentication for a User, the DCC shall bypass SAML authentication. Where using either the DCC Identity Provider Service or any other Identity Provider Service, if a User wishes to change the rights of that User Personnel to access the Self-Service Interface, the User shall delete the cookie from the User Personnel's browser cookie store.	Security	PM1	Must
SSI-NFR-8	The solution shall support the transfer of SAML via HTTP POST between its Identity Provider Service and the Self-Service Interface.	Security	PM1	Must
SSI-NFR-9	The solution shall support the inclusion in each SAML assertion of a Digital Signature produced by a DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate in accordance with the FIPS 186-4 Digital Signature Standard using SHA-256 hashing algorithm.	Security	PM1	Must
SSI-NFR-10	Where a User Personnel attempts to access the Self-Service Interface and a non-expired cookie is not stored in the User Personnel's browser cookie store: - 1. A SAML assertion request shall be sent to the DCC Identity Provider Service via the User Personnel's browser; - 2. When requested, the User shall provide the requested credentials (username, password, and certificate) to the DCC Identity Provider Service; - 3. The solution shall grant or deny that person's access to the Self-Service Interface by providing a cookie enabling such access to be stored in the User Personnel's browser cookie store. If access is denied, a browser message shall be provided which requests that the User Personnel resubmits their credentials.	Security	PM1	Must
SSI-NFR-11	Where a User is using the DCC Identity Provider Service, access to the Self-Service Interface shall only be provided once a User Personnel performs a login and generates a new password the first time that it uses that Identity Provider Service.	Security	PM1	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SAML Authentication via an Identity Provider Service that is not the DCC Identity Provider Service				
Authentication Requirements				
SSI-NFR-12	SSI shall support external Identity Provider Service SAML assertion where their User Personnel have provide their credentials (username, password, and certificate) and that their User Personnel's credentials have been successfully validated by their external Identity Provider Service prior to sending a SAML response including a SAML assertion to the Self-Service Interface.	Security	PM1	Must
SSI-NFR-13	SSI shall support SAML assertions connections via DCC Identity Provider Service that comply with the OASIS Standard – Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0.	Security	PM1	Must
SSI-NFR-14	SSI shall support Identity Provider Service authentication connections that use an appropriate SAML security assertion that conformance to UK Government Authentication Framework Level 2.	Security	PM1	Must
Enrolment of an Identity Provider Service that is not the DCC Identity Provider Service				
SSI-NFR-15	Where using an Identify Provider Service that is not the DCC Identify Provider Service, prior to seeking to access the Self-Service Interface for the first time, the User shall obtain at least one DCCKI Infrastructure Certificate in accordance with the DCCKI RAPP, and shall install such DCCKI Certificates on its Identity Provider Service. The User shall export and send a copy of the Identity Provider Service metadata to the DCC via secured electronic means, where such metadata shall include the URL of the Identify Provider Service and contact details in respect of the Identity Provider Service. Where the DCC reasonably requires the metadata to include additional information, the DCC shall inform the User of the information required and the User shall provide the information requested.	Security	PM1	Must
SAML Profiles, Bindings and Protocols				
SSI-NFR-16	The solution shall support a User Identity Provider Service using the following SAML profile, binding and protocol: **Profile**: Web Browser SSO (single sign-on) **Binding**: HTTP POST (HTTP/1.1) **Protocol**: Authentication Request Protocol	Security	PM1	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
Identity Provider Service SAML Configuration				
SSI-NFR-17	Where a User notifies the DCC that it wishes to use an Identity Provider Service that is not the DCC Identity Provider Service, the DCC shall upon request provide, to that User via secured electronic means, the following information to be included in each SAML assertion: - the service provider unique ID to be used by the Identity Provider Service; and - the URL formatted identifier of the Self-Service Interface	Security	PM1	Must
SSI-NFR-18	SSI shall support SAML connections from external parties where their Identity Provider Service: • shall not sign Authentication Requests (AuthnRequest); • shall sign SAML Assertions; • shall not sign Authentication responses; • shall not encrypt any part of the SAML assertion (other than the Digital Signature); • shall use persistent and unique nameIDs; • shall only include NotBefore, NotOnOrAfter or AudienceRestriction in the SAML Condition elements; and • shall set the SAML assertion nameID to be persistent and unique to the User Personnel.	Security	PM1	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SSI-NFR-19	The solution shall support the User Identity Provider Service setting the following SAML attributes shown in square brackets, making reference to the information shown after each colon: - [UNIQUE IDENTIFIER IDP]: a unique ID assigned to the SAML response by the Identity Provider Service. - [UNIQUE IDENTIFIER SP]: the service provider unique ID for the SAML request, as provided by the DCC. - [TIMESTAMP]: a timestamp in standard SAML format. - [DCC SP URL]: the URL formatted identifier for the Self-Service Interface, as provided by the DCC. - [IDP ISSUER URL]: a URL identifying the Identity Provider Service issuing the SAML assertion. - [SAML ASSERTION UNIQUE IDENTIFIER]: a unique identifier assigned to the SAML assertion by the Identity Provider Service. - [MESSAGE SIGNATURE]: a Digital Signature generated by the signing of the SAML assertion message using the DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate. - [USERNAME]: a unique username assigned to the User Personnel by the Identity Provider Service. - [SESSION EXPIRY]: a valid SAML date/time object describing the expiry time of the session associated with the user. - [ASSERTION START]: a valid SAML date/time object describing the start time of the validity of the SAML assertion. - [ASSERTION EXPIRY]: a valid SAML date/time object describing the expiry time of the validity of the SAML assertion. - [SAML AUTHENTICATION CONTEXT]: a valid SAML Authentication Context Class describing the authentication that the user has completed with the Identity Provider Service. - [Role name]: Job Type Role(s). Multiple roles should be specified by separating role names using commas (,). - [OrgID]: a list of User ID(s) in relation to which the User has been granted permission to access information held on the Self-Service Interface by the other User(s) to whom that information pertains. Such permission having been granted and not having been rescinded. Multiple User IDs should be specified by separating values with commas (,).	Security	PM1	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
Interactive Web Interface				
SSI-NFR-20	Any connection to the Self-Service Interface may time-out after a period of inactivity of 15 minutes.	Security	PM1	Must
File Download Interface				
SSI-NFR-21	The solution shall provide User Personnel who are downloading files with a prompt to save files.	Security	All	Must
Error Handling				
SSI-NFR-22	The solution shall present, when an error is detected when a User attempts to either access the Self-Service Interface or access any Interface Transaction, meaningful error messages containing codes as per HTTP/1.1 standard.	Security	All	
Roles				
SSI-NFR-23	The DCC shall provide to User Personnel of each User access to each Interface Transaction that the User is eligible to access as set out in Section H8.16 or, where not specified in Section H8.16. Such access shall either be full or conditional, where: - 'Full' means that the User can access data and use all functions associated with the specific Interface Transaction; and - 'Conditional' means that a User's entitlement to access data and use all functions associated with the specific Interface Transaction is based on the access rules for conditional access.	Security	All	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SSI-NFR-24	Full access shall be provided for the following Interface Transactions for any User: - UC_Login_001 - Log In - UC_Inventory_001 - Smart Metering Inventory as set out in Section H8.16(a) - UC_MeterRead_001 – Meter Read Transactions as set out in Section H8.16(c) - UC_CSPCoverage_001 - SM WAN network coverage as set out in Section H8.16(f) - UC_CSPOMS_001 - Access to the Order Management System as set out in Section H8.16(e) - UC_KnowledgeManagement_001 - Knowledge Management in accordance with Section H8.16(g) - UC_Schedule_001 - Forward schedule of change in accordance with Section H8.16(g) - UC_ServiceDashboard_001 - DCC Service Status in accordance with Section H8.16(g) - UC_ServiceAlerts_001 - DCC Service Alerts in accordance with Section H8.16(g) - UC_FAQ_001 - FAQs in accordance with Section H8.16(g) - UC_Manuals_001 - DCC User Manuals in accordance with Section H8.16(g) - UC_ServiceCatalogue_001 - Service Catalogue Publication and Call Off - UC_RaiseSMI_001 - Raise Incidents in accordance with the Incident Management Policy - UC_Search_001- Search • UC_Profile_001 - User profile information	Security	All	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SSI-NFR-25	Conditional access shall be provided on the following basis in relation to the following Interface Transactions and shall not be provided other than on the basis set out below: - UC_ServiceAudit_001 - Service audit trails for which access shall be granted as set out in SEC Section H8.16(b). - UC_HubStatus_001 - Communications Hub availability and diagnostics, for which access shall be granted to the Responsible Supplier, the Network Party or Registered Supplier Agent for any Smart Metering System of which the Communications Hub Function in question forms a part. - UC_Reports_001 – Access to the following reports, available to any User and pertaining to that User: o Installation Status Smart Meter Report o Smart Metering Devices Status and Firmware Report o Smart Metering Devices Status and Model Report o Communications Hub with No Attached Devices Report o Scheduled Service Requests Report o Quarantined Requests Report o Monthly Transaction Report o Smart Metering Device Transaction Report o Firmware Activations Service Request Report o Load Balance Report Note that documentation relating to the format and content of such reports shall be provided to Users via secured electronic means, as and when produced or updated. - UC_ViewSMI_001 , UC_UpdateSMI_001 - View and Update Service Management Incidents for which access shall be granted as set out in SEC Section H9. - UC_OrgManager_001 – User Account management for User Personnel of Users using the DCC Identity Provider Service, for which access shall be granted to Administration Users. - UC_ProblemManagement_001 - Problem Management for which access shall be granted in accordance with SEC Section H9.	Security	All	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SSI-NFR-26	Where a User is entitled to conditional access to more than one Interface Transaction, the solution shall apply permissions such that any User Personnel can access any of those Interface Transactions that the User is eligible to access, subject to such User Personnel being entitled to such access on the basis of the Job Type Role(s).	Security	All	Must
Administration User defined access				
SSI-NFR-27	In addition to the full and conditional access restrictions applied by the DCC, Administration Users, appointed in accordance with the process set out in the DCCKI RAPP, may further define access restrictions for User Personnel to individual Interface Transactions by assigning one or more Job Type Roles to User Personnel in relation to one or more User IDs. Where a User is using the DCC Identity Provider Service, the solution shall enable an Administration User to do this using the Interface Transaction UC_OrgManager_001. The solution shall ensure that access to Interface Transactions is only provided to the Job Type Role(s) presented to the DCC by the User in the SAML assertion accompanying the request for access to the Interface Transaction, based on the Interface Transactions that the Job Type Role is entitled to access as set out in Appendix A. Appendix A (Appendix A – Role, Interface Matrix) shows which Interface Transactions that User Personnel with a given Job Type Role are only permitted to access (User Personnel with a given Job Type Role may only access those Interface Transactions where there is a 'Y' in the corresponding box). Where the SAML assertion contains multiple Job Type Roles, the solution shall grant access to that User Personnel to all of the Interface Transactions that it is entitled to access in all of those Job Type Roles.	Security	All	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
Users granting access to other Users				

SSI-NFR-28	Information available through the Self-Service Interface that relates to one or more User IDs of a User may be shared with another User where that other User is also willing to share information relating to one or more of its User IDs with the first User. Where two Users wish to grant access to each other's information accessible through the Self-Service Interface, each of those Users shall submit, via secured electronic means, a notification to the DCC which includes:
	
	- that the notification relates to granting to another User access to its data which is available via the Self-Service Interface;
	- the list of User IDs of both of the relevant Users, for which mutual access for the two Users is being granted; and
	- details of the DCCKI SRO responsible for the relevant User IDs that is authorising such access on behalf of the User submitting the notification, which shall comprise:
	  o the name of the authorising DCCKI SRO;
	  o telephone and email contact details for the DCCKI SRO; and
	  o signature of the DCCKI SRO.
	
	Upon receipt of such notifications, the DCC shall confirm if each request is authentic, by:
	
	- verification of the DCCKI SRO; and
	- by confirming that the User IDs provided by each User granting access are User IDs that have been assigned to each such User by the Panel in accordance with SEC H1.6.
		Security	All	Must

SSI-NFR-29	Where both of the notifications are confirmed to be authentic, the DCC shall: - configure the Self-Service Interface to enable any Administration User acting on behalf of either of the two Users to grant access to its User Personnel to information available via the Self-Service Interface relating to any of such User IDs; and - confirm in writing, to each DCCKI SRO submitting a notification that such access has been granted.	Security	All	Must
SSI-NFR-30	Where either or both of the notifications are not confirmed to be authentic, the DCC shall confirm in writing, to each of the DCCKI SRO submitting a notification, that such access has been rejected and giving the reasons for rejection.	Security	All	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
Users rescinding access permission to other Users				

SSI-NFR-31	Where a User wishes to rescind permission to allow another User to access its information available through the Self-Service Interface for a defined set of User IDs, having previously granted such access, the User wishing to remove access shall submit, in writing via secured electronic means, a notification to the DCC which includes:
	
	- that the User wishes to rescind access to its information on the Self-Service Interface by another User;
	- the list of User IDs pertaining to the User submitting the notification, for which it wishes to rescind access to another User (each a “Rescinding User ID”);
	- the list of User IDs pertaining to the other User for which access is to be rescinded (each a “Rescinded User ID”); and
	- details of a DCCKI SRO that is authorising such rescinding of access on behalf of the User submitting the notification, which shall comprise:
	  o the name of the authorising DCCKI SRO;
	  o telephone and email contact details for the DCCKI SRO; and
	  o signature of the DCCKI SRO.
		Security	All	Must

SSI-NFR-32	Upon receipt of such a notification, the DCC shall confirm if the request is authentic, by: - verification of the DCCKI SRO; and - confirming that the User IDs provided by the User notifying that access should be rescinded, are User IDs that have been assigned to that User by the Panel in accordance with SEC H1.6.	Security	All	Must

ID	Non-functional Requirement	Category	Process Map	(MoSCoW)
SSI-NFR-33	Where the notification is confirmed to be authentic, the DCC shall: - configure the Self-Service Interface to remove access to information relating to Rescinding User IDs by any User Personnel of the second User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinded User ID; - configure the Self-Service Interface to remove access to information relating to Rescinded User IDs by any User Personnel of the first User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinding User ID; and - confirm in writing, to the DCCKI SROs of both affected Users that such access has been rescinded.	Security	All	Must
SSI-NFR-34	Where the notification is not confirmed to be authentic, the DCC shall confirm in writing, to the DCCKI SRO, that the notification of permission to be rescinded has been rejected.	Security	All	Must
Freshness of Data Sources				
SSI-NFR-35	The DCC shall update data available to Users via the Self-Service Interface to reflect the most recent information held by the DCC as soon as reasonably practicable, but in any event within 24 hours of receipt or generation of that data by the DCC.	Performance/Data	All	Must

5 References

	Reference	Description	Document Link
1	Self-Service Interface Baseline Logical Architecture	Defines application service architecture, application component architecture, data information architecture, component interfaces and information flow	TBC
2	SD4.2 SSI Interface Design Specification	Describes how the logical architecture is physically implemented	TBC
3	British Computer Society (BCS)	This requirements template is based on techniques taught on the BCS International Diploma in Business Analysis. This training maps to level 4 of the Skills Framework for the Information Age (SFIA) framework	https://www2.bcs.org/certifications/ba/
4	UML	Any use cases included in this document are based on UML 2.0 standards	http://uml.org/
5	BPMN	Any process maps included in this document are based on BPMN 2.0 standards	http://www.bpmn.org/
6	NFR framework	DCC NFR framework	DCC NFR framework

	Reference	Description	Document Link
7	SEC H8.8	H8.8 Where the DCC is proposing to make a change to DCC Internal Systems, the DCC shall: (a) undertake an assessment of the likely impact upon: (i) Parties in respect of any potential disruption to Services; and/or (ii) RDPs in relation to the sending or receipt of data pursuant to Section E (Registration Data), that may arise as a consequence of the Maintenance required to implement the contemplated change; (b) where such assessment identifies that there is a Material Risk of disruption to Parties and/or RDP's, consult with Parties and/or RDPs (as applicable) and with the Technical Architecture and Business Architecture Sub-Committee regarding such risk; (c) provide the Parties and RDPs the opportunity to be involved in any testing of the change to the DCC Internal Systems prior to its implementation; and (d) undertake an assessment of the likely impact of the contemplated change upon the security of the DCC Total System, Smart Metering Systems, and the Systems of Parties and/or RDPs.	n/a
8	DCC Business Scenario list	Business Scenario definitions are now being used by Service Providers and Test Assurance to link defects to a Business Scenario in HP ALM. These should be referenced in Appendix A to 'inform' test assurance focus.	Business Scenario list

Appendix A – Role, Interface Matrix

	Job Type Role										
Categories of Interface Transaction	**All Access**	**Organisational Administrator**	**Security User**	**Lead Agent**	**Call Centre User**	**MI User**	**Service Management User**	**Smart Meter Operations User**	**Asset Management Ordering**	**SEC Contract Manager**	**Logistics**
BFD01 Service Management											
Raise service management incidents UC_RaiseSMI_001 UC_RaiseSMI_002 UC_RaiseSMI_003 UC_RaiseSMI_004	Y	Y	Y	N	N	N	Y	N	N	N	Y
Update service management incidents UC_UpdateSMI_001	Y	Y	Y	N	N	N	Y	N	N	N	Y
View service management incidents UC_ViewSMI_001 UC_ViewSMI_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y
Problem management UC_ProblemManagement_001 , UC_ProblemManagement_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y
BFD02 Smart Metering Inventory											
Smart metering inventory UC_Inventory_001 , UC_Inventory_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BRD03 DCC Service Status											
DCC service status UC_ServiceDashboard_001	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
BDF04 Service Audit Trails											
Service audit trails UC_ServiceAudit_001 , UC_ServiceAudit_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N

BFD05 Forward Schedule Of Change											
Forward schedule of change UC_Schedule_001 , UC_Schedule_002 , UC_Schedule_003	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD06 Meter Read Transactions											
Meter Read Transactions UC_Inventory_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
BFD07 CSP SMWAN Network Coverage											
SM WAN network coverage UC_CSPCoverage_001 UC_CSPCoverage_002	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
BFD08 DCC Service Alerts											
DCC service alerts UC_ServiceAlerts_001, UC_ServiceAlerts_002	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD09 Service Requests											
Service catalogue publication and call off UC_ServiceCatalogue_001 , UC_ServiceCatalogue_002 , UC_ServiceCatalogue_003	Y	Y	N	Y	N	N	N	N	Y	N	Y
BFD10 Communications Hub Availability & Diagnostics											
Communications Hub availability and diagnostics UC_HubStatus_001 UC_HubStatus_002	Y	Y	N	Y	Y	N	Y	Y	N	N	Y
BFD11 Reporting											
Reporting UC_Reports_001	Y	Y	N	Y	N	Y	N	N	N	Y	Y
BFD12 Knowledge Management, Search and FAQ											
Knowledge management UC_KnowledgeManagement_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
FAQs UC_FAQ_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DCC user manuals UC_Manuals_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

UC_Search_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BFD13 Forecasting and Ordering											
Forecasting and ordering of Communications Hubs and auxiliary equipment UC_CSPOMS_001	Y	Y	N	N	N	Y	N	N	Y	N	Y
BFD14 User Identity & Access Management											
Log In UC_Login_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
User account management UC_OrgManager_001 , UC_OrgManager_002 , UC_OrgManager_003	N	Y	N	N	N	N	N	N	N	N	N
User profile information UC_Profile_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Appendix B – Definitions/Glossary

In this document, the following definitions are defined, except where the context otherwise requires:

- expressions defined in Section A1 of the Code (Definitions) have the same meaning as is set out in that Section;
- any expressions not defined here or in Section A1 of the Code have the meaning given to them either in this document or the Self-Service Interface Code of Connection.

Serial	Definition	Description
1	BFD	Business Functional Domain
2	BRD	Baseline Requirements Document
3	DCC Service User	Means a displayed field which will follow the following
4	DCC Service User Organisation ID	means a displayed field which will follow the following format: “<(<User ID>)>< Party >/<User Role Reference> <(< Service User Descriptor >)>”. NOTE: User Role Reference is as detailed in the DCC User Interface Specification.
5	Epics	High level story that encapsulate business requirements in a solution neutral manner.
6	Functional Component	Means a specific item or set of functionality provided by the Self-Service Interface which is subject to the access controls set out in Appendix AH.
7	Job Type Role	Means one of the functional roles as set out in the table contained in appendix A.
8	Order Management System (OMS)	As defined in the CH Handover Support Materials
9	Organisation ID	Format: “<(<User ID>)>< Party >/<User Role Reference> <(< Service User Descriptor >)>”. NOTE: User Role Reference is as detailed in the DCC User Interface Specification.
10	Process Map	Mapping of a user process (Epic)
11	Security Assertion Markup Language (SAML)	An open, published framework for exchanging security
12	Service User Descriptor	Means an optional free text field of up to 30 characters set by a User when a User ID is registered. Once this field is set it can only be changed via a request to the DCC Service Desk.
13	SSI	Self Service Interface

Table 1 - Definition of terms

Appendix C – Document Reference

Ref	Title	Description	Link
1	SSI BLAD	Self Service Interface Baseline Logical Architecture Document	
2			

Appendix D – Delta Reference

Serial	Doc Id	Title	Date	Status

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0058 'Changes to the governance of the Self-Service Interface'

Annex D

Proposed SSI Change Governance Process – version 0.6

Purpose

This document is the proposed Self-Service Interface (SSI) governance process produced in accordance with SECMP0058 'Changes to the governance of the Self-Service Interface'.

1. Proposing improvements to the SSI

SEC Parties may propose improvements to the SSI by submitting an SSI Improvement Proposal (SIP) form (Annex F) provided by the Data Communications Company (DCC), to SSIRemedyImprovements@smartdcc.co.uk. Within five Working Days of the proposer sending the SIP, the DCC will endeavour to respond to confirm receipt of the request and advise if there is any additional information it needs. If the DCC requires more time to assess if any additional information is needed, the DCC will inform the proposer and advise a reasonable timescale they can expect to receive the DCC's confirmation.

Where the proposer of a SIP believes it is required as a matter of urgency, the DCC shall validate the urgency of the request and the Panel or a delegated Sub-Committee will determine the timetable that the SIP should follow.

2. Validation and Prioritisation

The DCC will validate the SIP to ensure the requirements are clear and viable and as a minimum, each request will have to meet the capabilities of the SSI and comply with one of the Business Functional Domains contained in SEC Appendix AH. To achieve this the DCC will proactively provide support and guidance to all proposers. Once a SIP has been validated and accepted by the DCC, they will assign the request with a unique ID number and feed this back to the proposer.

DCC will then assess the impacts that the SIP will have on DCC Systems, SEC Parties and any other SIPs already under consideration. As well as the impacts, DCC will also consider the costs of each SIP and apply a category of Small (below £50k), Medium (£50k-£100k) and Large (exceeds £100k). Each SIP will then be prioritised against any other SIP currently under consideration.

Following the DCC's confirmation of receipt of the SIP and the receipt of any further information sought from the proposer, the DCC will complete its validation and prioritisation of each SIP within a reasonable timescale dependent on the scale of each SIP and shall endeavour to provide its findings to the proposer within 20 Working Days. Where this is not possible and the DCC cannot fulfil this

timescale, they will inform the proposer and advise a reasonable timescale they can expect to receive the DCC's findings.

3. SSI Improvement Consultation

To maintain efficiency, the Working Group and the DCC propose to issue SSI improvement consultations to the industry in quarterly intervals following the implementation of SECMP0058. A consultation will have the capacity to consult on several SIPs at once with a view to deploying them over a defined time period, rather than consulting on each SIP individually. Subject to the approval of SECMP0058, SSI improvement consultations could be issued by SECAS on behalf of DCC, with each consultation expected to last for a minimum of 15 Working Days allowing all SEC Parties the opportunity to provide their feedback to each SIP.

In the initial period following the approval of this modification and considering DCC's current approach relating to Planned Maintenance of the SSI, it is expected that the current backlog of SIPs will decrease and so it is proposed over the long term, possibly in 2020, that SEC Parties are consulted on a less frequent basis. In any event, the implementation window for a batch of SIPs in a given consultation would not straddle two Regulatory Years.

Each SSI improvement consultation will include the following:

- The proposer of each SIP;
- A description of each SIP;
- The benefits of each SIP;
- The SEC Parties impacted;
- Whether each SIP is seeking to add, amend or remove functionality;
- The anticipated cost range; and
- The anticipated timescales to develop and deploy.

The SSI improvement consultation responses will be collated and the DCC will refine improvements to each SIP where this is required.

4. Panel (or Sub-Committee) Impact Assessment sign-off

All feedback received shall be collated into a single document and referred to the SEC Panel or a delegated Sub-Committee for consideration, where they will consider the scope and cost of the SIPs and approve or reject their progression through to DCC Impact Assessment.

If the decision to approve the DCC Impact Assessment of SIPs following the SSI improvement consultation is delegated to a Sub-Committee and that Sub-Committee deems it cannot form a decision, the Sub-Committee may escalate the matter to the Panel to approve or reject, requesting the DCC Impact Assessment of SIPs, or alternatively advise DCC to refine the solution(s).

5. Panel (or Sub-Committee) Development sign-off

Once the DCC have carried out their Impact Assessment to each SIP, the Impact Assessment(s) shall be considered by the SEC Panel or a delegated Sub-Committee where they will consider any material

changes to the scope and cost of the SIPs and approve or reject their progression through to DCC development.

If the development of SIPs is approved, the DCC shall develop the SIPs and continuously assess whether there are any material changes to the scope and costs that were previously considered under the Impact Assessment. If changes have occurred to the agreed scope and costs, DCC shall advise the Panel (or any delegated Sub-Committee).

If the decision to approve the revised scope of SIPs is delegated to a Sub-Committee and that Sub-Committee deems it cannot form a decision, the Sub-Committee may escalate the matter to the Panel, who can approve or reject the revised scope, or alternatively request SECAS issue a second SSI improvement consultation to seek SEC Parties' feedback prior to making this decision.

6. Panel (or Sub-Committee) deployment sign-off

Once the DCC have developed the SIPs, accounting for any agreed revisions in scope, the Panel (or any delegated Sub-Committee) shall consider any changes to the previously agreed scope. If it is deemed that the scope has changed from what was previously agreed, the Panel (or any delegated Sub-Committee) could choose to approve or reject the deployment of the SIPs or advise the DCC to revise the solution(s).

The DCC will propose the implementation approach they would like to take to deploying the now developed SIPs. If the decision to approve the deployment of SIPs is delegated to a Sub-Committee and that Sub-Committee deems it cannot form a decision, the Sub-Committee may escalate the matter to the Panel, who can approve or reject the deployment of the SIPs, or advise DCC to revise the solution(s).

7. Sub-Committee Terms of Reference

It is expected that the review and sign-off for any programme of change to the SSI would be made by the Panel or any delegated Sub-Committee. If the Panel chooses to delegate any SSI improvement related sign-off requirements to a Sub-Committee, the Working Group recommend that the Operations Group is tasked with this role. The Operations Group currently consider SIPs under Planned Maintenance of the SSI and thus there is precedent under this approach. The Working Group considered the current Operations Group Terms of Reference and agreed that this should be amended to add conditions specifically for SSI impacting improvements in terms of quoracy and voting rights. The Working Group also considered the conditions should the Panel choose to form a new Sub-Committee and agreed that conditions in terms of quoracy and voting rights would be required in the terms of reference.

The terms of reference, membership and operation of the SSI improvement consultation process, may be reviewed by the Panel at any time, however at least annually, to ensure that they remain appropriate to reflect the duties and requirements of the SEC. Amendments to these terms of reference will be approved solely by the Panel.

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0058 'Changes to the governance of the Self-Service Interface'

Annex F

First Working Group Consultation responses

About this document

This document contains the full collated responses received to the first SECMP0058 Working Group Consultation.

Question 1: Do you agree that the SECMP0058 proposed solution better facilitates the SEC Objectives and should be approved?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	Yes	We note that the proposed changes to not alter Self-Service Interface (SSI) access and we do not therefore support the views expressed by the Working Group (WG). However, we believe a more efficient change process for the SSI will enable more effectual installation and operation of Smart Metering Systems in the short term, and thus that this Modification better facilitates SEC objective a.
Western Power Distribution	Network Party	Yes	We believe that this modification better facilitates SEC Objective (a) by improving the process for making changes to the SSI, and therefore aiding the efficient provision, installation and operation of Smart Metering Systems. We also believe that this modification better facilitates SEC Objective (b) as improving the process for making changes to the SSI will allow the DCC to efficiently comply with the General Objectives of the DCC.
Bryt Energy Limited	Small Supplier	Neutral	At present it is not clear on how agile in delivery DCC will be and imposes no detail on the release cycle for delivery of the change, only the timescales for authorisation up until the change is agreed. There are no timescales for each of the “Four Month” release consultations or imposes minimum/maximum delivery times for DCC for the agreed SSI changes or how much change DCC can cope with in each cycle. The reason for this MOD is stated that the current SSI does not meet the current requirements and is to slow to implement change. However, at present there appears to be no evidence in the MOD of how this will speed up delivery of SSI change. Secondly there appears to be no “SSI MODS” lined up awaiting delivery.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			We would expect to see a clear defined process as per diagram, each clearly defined with a total day allowance for each stage of the change process. The new process is unclear on if multiple changes are "bundled" together and can be accepted or rejected or can a single change be removed from scope and not agreed? Which sub-groups will be responsible? Which groups will resolve differences of opinion? How long should this take? While we agree in principle with the MOD as the SSI is the primary customer interface between SEC User and DCC and should be Agile in receiving, impact assessment, and delivering changes and the SEC parties in defining and signing off deliverables, this proposed process falls short and does not put enough ownership on key parts of the process for time and delivery and new financial burdens to SEC parties.
SSE	Large Supplier	Yes	We agree that the proposed solution better facilitates SEC Objectives: (b) though improved co-ordination of the activities, systems, and procedures of SEC Parties by providing a more efficient and agile route to improve how we access DCC Services. (a) we believe this will be positively impacted because of introducing this new governance approach and therefore implementing improvements more efficiently to increase the access to DCC Services via the SSI.
EDF Energy	Large Supplier	Yes	We agree that the proposed solution better facilitates SEC Objective (b) as it will enable DCC to provide services that meet the needs of its Users in the most efficient and economical manner, in line with the First Enduring General Objective in the DCC Licence. We also agree that the proposed solution better facilitates SEC Objective (g) as it will ensure that low level design detail that is not relevant to the objectives of the Smart Energy Code is not included in the SEC and therefore made subject to a disproportionately onerous change process.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			For the avoidance of doubt we believe that the proposed solution is neutral against the other SEC Objectives. There is no direct link between the change process for the SSI and the actual operation of smart meters; we do not believe that there is an evidence to substantiate that this change would directly impact the operation of smart meters. It will, however, enable changes that do have a beneficial impact to be made in a more agile, cost-effective way.
Npower	Large Supplier	Neutral	We feel that the SSI is not currently fit for purpose and requires updating. There are benefits of improving the change control process for the SSI, however, we would like to see the necessary governance arrangements that would need to be in place to ensure proper control and approval Our preference would be for the DCC to implement the alternative solution that they proposed i.e. to leave Appendix AH as detailed but to implement an alternate change process for this document (and also other documentation that may require quicker/cheaper turnaround) – such a process could perhaps be a monthly process along the lines of other code Change Pack processes

Question 2: Will your organisation be impacted due the implementation of this modification?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	Yes	We expect that with a robust governance process in place which cannot be misused (in place of Elective Services for example), we will experience positive operational impacts from changes to the SSI.
Western Power Distribution	Network Party	Yes	We will be required to review and potentially respond to additional consultations that will be issued as a result of this modification. Implementation of this modification will also provide a new process to follow should we wish to raise any changes to the SSI.
Bryt Energy Limited	Small Supplier	Yes	Yes, more industry change on a key Customer Service Element used to interact with the DCC.
SSE	Large Supplier	Yes	We believe the proposed modification would generally have a positive impact allowing changes to the DCC SSI to be raised, assessed and implemented in a more efficient and agile way.
EDF Energy	Large Supplier	Yes	We will need to ensure that we are properly resourced to be able to engage with the proposed change process for the SSI Baseline Requirements Document. However, we do not expect the demand on our resources to be more than we currently see for SSI related matters.
Npower	Large Supplier	Neutral	

Question 3: Will your organisation incur any costs due to the implementation of this modification?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	Yes	Our share of the implementation costs in the short-term, our share of the charges for approved SSI changes in the long-term.
Western Power Distribution	Network Party	No	
Bryt Energy Limited	Small Supplier	Yes	Yes, more work to impact assess changes on a more regular basis. Approx. 1 full FTE week per change release cycle to assess, IA & create new changes into business processes and training/rollout.
SSE	Large Supplier	Yes	In terms of the initial implementation, this would be minimal as a proportion of the SECAS costs. On an ongoing basis, these would be our involvement in the consultation impact assessment and responses, alongside the relevant DCC apportioned development costs associated with implementing changes to the SSI.
EDF Energy	Large Supplier	No	We do not expect to incur any direct costs as a result of the implementation of this Modification. We note, however, that the consultation document does make reference to any additional costs that might be incurred by DCC, or any changes to their existing costs that would result from making these changes. We would welcome confirmation from DCC on the expected impact of this Modification on the charges that they would seek to recover from their Users.
Npower	Large Supplier	Neutral	

Question 4: Having considered the potential impacts and costs to your organisation, as well as the cost to deliver the modification, do you agreed that SECMP0058 should be approved?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	No	We fully support the notion of a more flexible, more agile approach to SSI changes, and believe that such a change to be beneficial to Users. However, we believe that further work is required within the legal text and the consultation documentation. It is our understanding that the intent of this Modification is to introduce the following changes: SEC Appendix AH would be stripped of technical detail pertaining to the requirements of the Functional Components of each Business Functional Domain, and this technical detail would be moved into a DCC-owned document; SEC Appendix AH would be retained within the SEC to detail the access requirements and governance controls relating to the SSI; The SSI Baseline Requirements Document containing the technical specifications of the SSI will reflect the live functionality of the SSI at the time of its publication; The SSI Baseline Requirements Document (SSI BRD) would be published each time a revision was made to the requirements of the Functional Components of any Business Functional Domain; A 'delta' document would be published alongside each version of the DCC-owned specification document, detailing the changes that have been made to the specification since the last version was published; The process to manage changes to the SSI is three-fold:

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			Pre-design development of change: consultation with Industry to seek approval for an initial scope of SSI changes (including amongst other things, a forecast cost for said changes); Post-design development of change: engagement with Panel or a relevant sub-committee to seek approval of any scope changes that arise in development; Post-build development but pre-deployment of change: engagement with Panel or a relevant sub-committee to seek approval of deployment for the developed SSI changes; Consequential changes will be made to SEC to denote the impact of the SSI changes to Maintenance activities; Consequential changes will be made to SEC to extend the role of the Panel in accordance with the requirements of this change, and Consequential changes will be made to the ToR of any Panel Sub-Committee to facilitate the requirements of this change. We would appreciate some clarity on this though because there is not a complete and concise version of the full solution in a single space within the consultation documentation. We feel that the detail included within the consultation documentation either does not well reflect the discussions at the last Working Group (WG), or is inconsistent with other parts of the consultation documentation. We note these points for consideration below, but due to the scale of comments, we have separated these into major and minor: **Major:** No business-case has been provided within the consultation documents, thus we are unable to determine the value of this modification with regard to the potential costs (which as a minimum will include additional DCC resource over time, and a 9.5% Shared Service Charge).

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			The consultation documents do not cover the cost recovery mechanism for the SSI changes. We expect this to be made explicitly clear to SEC Parties such that they may make informed consultation responses with regard to the impact that this Modification will have on them. The consultation documents note that SEC Appendix AH will contain the key governance rules for the SSI change process, whereas the SSI BRD will contain the step-by-step rules which will apply to the process. It is our view that the governance of this process should be in one place only, to avoid any misunderstanding of governance arrangements; it is further our view that the governance arrangements must be within SEC to ensure that the arrangements are robust, transparent, visible and of course, binding. Where this is not the case we would request that the WG reconsider the Path of this Modification in accordance with SEC Section D2.6 (a), (c) and (d). – We note that the Draft Modification Report does not contain the Path of this Modification but is it recorded within the Initial Modification Report as a Path 3 Modification. The consultation documents do not cover the communications requirements that we believe were agreed upon at the last WG meeting. We believe it necessary that the communication of this process is fully captured and contained within the legal drafting due to the nature and potential consequences of the changes that may occur outside of the consultation process. The content of the initial consultation for SSI changes does not include the governance process; it is our view that the previous WG had noted that Industry would be required to endorse or at least be informed of, the governance process for changes to the scope of the SSI changes being consulted upon. There are currently no powers for either Panel or any of their relevant Sub-Committees to make financial decisions on behalf of Industry; we believe this is a valid omission and would request that where changes to scope result in an increase to the forecast spend, Industry

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			are re-consulted. We believe that this needs to be a requirement, rather than simply an option for individuals in attendance at a single meeting to decree. We would further request that this consultation process be made clear within the legal text (e.g. minimum number of WDs for consultation period etc). Consequential changes are missing from the Modification and we find that we cannot support the proposal without understanding and approving these changes: the planned maintenance arrangements contained within the SEC will apply once the Panel's current derogation expires. The arrangements do not permit the SSI amendments to be made unless DCC declares them as Unplanned Maintenance. The notification requirements for Unplanned Maintenance are not sufficient for operational mitigation and we therefore feel that until the implications for DCC outages are clear we cannot support the proposal: the improvements to SSI that may result from this process do not outweigh the risk to our live operations or consumers where outages lacking adequate notice periods become commonplace. In addition we would note here that the approval rights that Panel delegated to the Operations Group cease with the Panel 'derogation'; the SEC amendments required to permit/obligate Panel to perform the requirements outlined within this solution have not been included (i.e. Panel may need to manage and approve changes to the SSI changes consulted upon and certainly will in the case of escalation, Panel would have to review the consultation process relevant to SSI changes at least annually, and Panel would have to approve changes to the specification document for SSI following consultation with Users. We would like to see these updates contain a specific requirement that Panel are provided with all consultation responses, not amended in any way, in sufficient time ahead of being asked to provide approval for changes to the DCC-owned SSI specification document.

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			the ToR of any relevant Panel Sub-Committee would need to be amended much the same as above. **Minor:** The process diagram does not reflect: how the changes for SSI being proposed have been scoped (i.e. how Users may feed-in their change requests); the two sets of approval required from Panel or a relevant Sub-Committee: development and deployment; the second consultation that can be requested by Panel or a relevant Sub-Committee; escalations to Panel from the relevant Sub-Committee; the outcome of rejections from Panel or Sub-Committees; the consultation process for 'urgent' SSI changes that can be requested by Users, and the result of change approval or of change send-back. We would request that any diagram provided within the consultation documentation reflect the full process being proposed so as to avoid any misconception. The process diagram requires the Panel or a relevant Sub-Committee to be consider the scope of proposed SSI changes after the consultation but ahead of the consultation content sign-off. This seems to us to be an unnecessary inefficiency; we would have expected this to fall ahead of the consultation. The renaming proposed by DCC means that on an enduring basis there is no Specification for the SSI i.e. the DCC-owned document is titled 'SSI Baseline Requirements Document' and SEC Appendix AH is titled 'SSI Access Control'. We do not support this proposal because we feel that it introduces inconsistency and ambiguity rather than adding any value

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			when compared with today's arrangements. We would additionally highlight that the suggested change to Appendix AH would not adequately reflect the content of the subsidiary document if the solution were amended such that the governance process was retained under SEC-governance.
Western Power Distribution	Network Party	Yes	We believe that this modification should be approved as the benefits of having a more flexible, transparent modification process for changes to the SSI, will help to ensure that Users have an efficient system that provides benefits to their processes. This modification also provides a strict governance process that will ensure that any changes Parties or the DCC wish to make to the SSI are approved and signed off by appropriate groups.
Bryt Energy Limited	Small Supplier	No	No. At present, the MOD only contains a cost to remove the high-level requirements of SSI from SEC Appendix. It contains no monthly running costs to administer this new governance process. It contains no running costs for DCC to manage the new governance process. Can we assume that the running costs are only the IA & Development work undertaken by DCC? This is only identified partially, by a noted risk of wasted development: Drawbacks One drawback was identified in the Working Group in that to contain the level of detail required in the industry consultation, DCC would have to carry out more development prior to the consultation, which would increase the risk of cost wastage if the proposed SSI changes would not come to fruition, although this risk was not considered to increase significantly compared to the existing Section D Modification Process. This statement appears to suggest there is a risk the new SSI Governance process is not fit for purpose by that the gap DCC delivery of the IA and acceptance, means that

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			requirements have could result in wasted DDC change effort seems odd. Secondly, why would the effort required for an IA change to effort into more development? On email request to SECAS Bryt Energy requested the DCC operating costs for this mod (And to be clear not the cost for each proposed IA or change) and the reply was: "Unfortunately I don't have much detail to give you here but DCC have just advised that they will be looking to provide a view on timescale and cost at the consultation stage of SSI changes and then they would continue to maintain the current range of £50k - £75k per sprint, with approval sought at SEC Ops Group on a monthly basis." It is unclear if DCC means this to be a total yearly cost to maintain the governance approach of a maximum £225k per year. We are disappointed that costs are not being clearly transparent from the working group and DCC on this mod. In the absence of this, the MOD should not be approved until the question of running costs of the new governance regime are clearly identified. How can a new process be implemented by DCC without a clear cost to serve and the commitment SEC parties are to undertake? We are extremely concerned on this MOD and its approach due to the fact no costs have been provided by DCC and DCC itself is the proposer.
SSE	Large Supplier	Yes	As previously noted, we believe this change should introduce a more efficient and agile mechanism to make changes to the SSI and we are in general agreement to approve the modification.
EDF Energy	Large Supplier	Yes	We agree that implementing SECMP0058 will result in a more agile, timely, and therefore cost-effective change process for the self-service interface. It retains the key elements of the SEC Modifications process while enabling them to be achieved in a more efficient way, being that:

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			• Any SEC Party is able to raise a change to the SSI. • All Parties will be consulted for their views on proposed changes to the SSI, and the estimated costs of making those changes. • SEC Parties and not DCC will make the decision on whether the changes that are proposed should be implemented.
Npower	Large Supplier	Neutral	We would like consideration given to our comments above. In order to support this modification, further development is required

Question 5: Do you believe that the draft legal text changes deliver the intention of the modification?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	No	The legal text provided within the consultation documentation does not appear to cover the requirements for the consultation periods relevant to SSI or SSI BRD changes. The legal text provided within the consultation documentation does not appear to cover the requirements for the SSI changes consulted upon to be within a single financial/regulatory year. **SEC Appendix AH** Definitions – both DCC Service User Organisation ID and Service User Descriptor have been removed from the legal drafting, we would like to understand the rationale for this and check that these references have been removed from all other relevant text (i.e. the SSI BRD), where this removal is valid. 1.1 – we believe that the third paragraph ought to be reworded to denote that Panel's approval sequentially follows the consultation e.g. "The DCC may make amendments to the SSI Baseline Requirements Document with the agreement of the Panel (or a Sub-Committee to which the Panel has formally delegated the required decision-making power), following consultation with Parties." 1.1 – we believe that the sixth paragraph ought to detail the definition or criteria for 'urgent', as well as the content requirements of any such consultation. We further believe that where a consultation for an 'urgent' SSI change follows a successful consultation for SSI changes over a period of time, the consultation for the 'urgent' change ought to make the following explicitly clear:

Question 5			
Respondent	**Category**	**Response**	**Rationale**
			any consequential changes to the arrangements approved by Panel (or any delegated Sub-Committee) i.e. any amendments to timelines, any alteration to the costs involved etcetera, and any potential SSI changes that were in-scope of the original consultation that could be removed to ensure that the arrangements so approved do not alter (with a specific question as to whether this course of action ought to be taken). In addition, we believe that it ought to be clear within the legal text that no 'urgent' change to the SSI can be made where the delivery of such a change would bridge two financial/regulatory years. 1.6 - we believe that 'Self Service' ought to be written 'Self-Service'. 2.5.1 Table – the table within 2.5.1 contains instances of defined terms written in lower-case, we would ask that these be corrected. 2.5.1 Table – the table within 2.5.1 contains instances of 'organization', we would request that these are replaced with 'organisation'. 2.5.1 Table – the current legal drafting removes the User Catalogue references utilised throughout the table within the Functional Component column. We would request clarification as to whether these references are contained anywhere else, and if not whether a list of these references and their associated description ought to be retained within SEC Appendix AH for clarity. We believe it would be difficult for new SEC Parties to understand these references where they are no longer part of the legal text, or retrievable from any other source. 2.5.1 Table: BFD02 – we believe that the first instance of 'device' within the Service capability field ought to be written as 'devices', or as 'the device and'.

Question 5			
Respondent	**Category**	**Response**	**Rationale**
			2.5.1 Table: BFD04 – SEC Section H8.16(b) is not as clear with regard to the User access restrictions as was the legal text for UC_Service Audit_001. We would therefore request that the Access Controls relevant to this Interface Transaction be copied over into the 'Defined Access' field of the new legal text (i.e. the requirements of 1.10.4 from the original SEC Appendix AH are moved into the relevant field within 2.5.1 of the new legal drafting of SEC Appendix AH). 2.5.1 Table: BFD05 – we believe that 'SEC release' ought to be written as 'DCC-impacting SEC Releases', such that this meets the criteria of the list in which it falls (i.e. DCC Smart Metering ecosystem). 2.5.1 Table: BFD05 – the relevant access controls from the original legal text of SEC Appendix AH (1.10.14) are missing from this row. We would request that these be written into the table and retained as SEC requirements; we would not condone meter firmware events being visible to any User other than the Responsible Supplier. 2.5.1 Table: BFD09 – we believe that 'raise, update' we believe ought to be 'raise and update', that that 'Enabling Users to track' ought to simply be 'track', and that 'full details of the details of the raised', ought to be 'full details of the raised'. 2.5.1 Table: BFD09 – the relevant access controls from the original legal text of SEC Appendix AH (1.10.19) are missing from this row. We would request that these be written into the table and retained as SEC requirements; we would not condone service request activity being undertaken by or visible to any Party other than the relevant User. 2.5.1 Table: BFD10 – we believe that 'diagnostics down individual' ought to be written 'diagnostics down to individual'. 2.5.1 Table: BFD11 – we would ask for clarification as to whether the list of pre-defined reports that has been removed from the original SEC Appendix AH text is available from

Question 5			
Respondent	**Category**	**Response**	**Rationale**
			any other source. Where is not, we believe that the list of pre-defined reports original contained within 1.9.1 ought to be written into the Service capability field. 2.5.1 Table: BFD12 – we believe that 'detailing operation of DCC services' ought to be written 'detailing the operation of DCC Services'. 2.5.1 Table: BFD13 – we believe that 'Hib' ought to be written 'Hub'. 2.5.1 Table: BFD14 – for clarity, we believe it would make more sense for 'create a new person's account' to be written as 'create a new account for User Personnel', so as to permit accounts to be created for existing personnel (due to role changes etc). As a result of all of the other consultations requiring an address at present, we have not been able to review the re-numbering of the legal text for accuracy of cross-referencing, so we can make no further comment. In addition, we have been unable to review the SSI Baseline Requirement Document but we have included the previous feedback that we shared with the Proposer below in case that helps. SECMP0058_Proposer.docx
Western Power Distribution	Network Party	Neutral	Although we have not yet reviewed all the legal text in depth, we feel that in the SEC Appendix AH Section 1.1 there is wording that requires further clarification. We believe that the statement 'Any SEC Party may propose a change to the Self-Service Interface at any time' should be expanded to explain how a Party proposes a change, and to who this request should be sent. This clarification is also missing from the Proposed SSI Governance Process document.
Bryt Energy Limited	Small Supplier	No	No. See Q1.

Question 5			
Respondent	**Category**	**Response**	**Rationale**
SSE	Large Supplier	No	We are in general agreement that the draft legal text changes deliver the intention of this modification however, we believe there is still further clarity required on elements of the process and these need to be addressed in some form to ensure that Parties clearly understand the SSI Change Governance Process. We have noted these in our response to Q10) as dependent on the WG consultation responses and subsequent WG review, these could be addressed in: SEC Appendix AH SSI Baseline Requirements Document SSI Change Governance Process
EDF Energy	Large Supplier	Neutral	We have not identified any issues with the draft legal text changes but we have not been through the changes in a lot of detail.
Npower	Large Supplier	Neutral	

Question 6: Do you agree with the recommended implementation date?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	Neutral	Where we can support the solution proposed we agree with the recommended implementation date, at this time however we do not agree with the proposed solution.
Western Power Distribution	Network Party	Yes	
Bryt Energy Limited	Small Supplier	No	No, more work to define the change process is needed as per Q1.
SSE	Large Supplier	Neutral	We are supportive of implementation being prior to the next Regulatory Year 2019/20, to enable the new process to be implemented in line with that period.
EDF Energy	Large Supplier	Yes	We agree with the recommended implementation date. As part of the implementation of this change consideration will need to be given to whether/how changes to the SSI that are currently being discussed and progressed will be handled under the new change process.
Npower	Large Supplier	Yes	

Question 7: Do you agree with the proposed SSI Change Governance Process (Attachment E)?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	No	As above, we believe that further work is required on this process
Western Power Distribution	Network Party	Yes	As detailed in our answer to Q5, we believe that the statement 'SEC Parties may propose changes to the SSI at any time' should be expanded to explain how a Party proposes a change, and to who this request should be sent.
Bryt Energy Limited	Small Supplier	No	No, more work to define the change process is needed as per Q1.
SSE	Large Supplier	Yes	We are in general agreement with the proposed SSI Change Governance Process, however we believe further clarification is required for certain elements, as referenced in our responses to Q5) and Q10).
EDF Energy	Large Supplier	Yes	We agree with the high level process as set out in the documentation but we would welcome further detail on how each of the steps will be undertaken – and especially how the decision to implement a change is made, and by whom.
Npower	Large Supplier	Neutral	We would prefer the alternative solution provided that could be implemented with a change process for this document. This would provide assurance that parties have visibility and provide assurance of proper control and approval.

Question 8: Do you think the proposed SSI Change Governance Process (Attachment E) should be referenced to in the legal text?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	Yes	As aforementioned.
Western Power Distribution	Network Party	Yes	We believe that the SSI Change Governance Process should be referenced in the legal text to ensure that the correct process is followed by all Parties. It will also help Parties with ease of reference if this document is noted within the appropriate section of the legal text.
Bryt Energy Limited	Small Supplier	Yes	Yes, this then provides a clear link between the process and the regulation that overarches it.
SSE	Large Supplier	Neutral	We are supportive in principle as it would be useful to have an overarching document where all the relevant information regarding the SSI Change Governance Process can be referenced, and potentially has further explanatory text to aid SEC Parties understanding. We believe this could be managed via the Code Administrator, for example using a similar approach to information provided for the Issues Process.
EDF Energy	Large Supplier	Neutral	We do not believe that the detailed steps of the process would need to be set out in the legal text as that could require further Modifications to amend that process if required. It would be more appropriate for the legal text to refer to a governance process that is consulted on and managed by the Panel, but which sits outside of the SEC itself.
Npower	Large Supplier	Yes	

Question 9: Should clauses 1.2 to 1.6 in SEC Appendix AH be moved to the SSI Baseline Requirements Document (Attachment D)?

Question 9			
Respondent	**Category**	**Response**	**Rationale**
E.ON Energy Solutions	Large Supplier	Neutral	We do not understand this question: clauses 1.2 to 1.6 from the original text of SEC Appendix AH have been retained within the amended legal text of the Appendix (Attachment C); 1.2-1.4 have simply been renumbered, and 1.5-1.6 have been moved. – We agree with this retention, if that the is question? If the question refers to moving 1.2-1.6 of the amendment Appendix (Attachment C) into the SSI BRD via a further consultation, then no we do not agree with the move.
Western Power Distribution	Network Party	No	We believe that these are the security requirements surrounding access to the SSI and not the functionality of the SSI. Therefore, these specific requirements should remain within the SEC Appendix AH and should be subject to the Section D Modification process should a Party wish to amend them.
Bryt Energy Limited	Small Supplier	Yes	Yes
SSE	Large Supplier	Neutral	
EDF Energy	Large Supplier	No	Appendix AH should retain any obligations that are placed on DCC or its Users and which other Parties may be reliant on for their efficient operation. Some of the content in clause 1.2 to 1.6 should seem to fall under this definition: 1.2 (Freshness of Data Sources) – Users are reliant on the data presented via the SSI being as up to date as possible to this obligation on the DCC should be retained within the SEC.

Question 9			
Respondent	**Category**	**Response**	**Rationale**
			1.3 (Interactive Web Interface) – there are no clear obligations in this section, should the DCC be obliged to timeout any connection to the Self-Service Interface after a period of inactivity of 15 minutes for security purposes then this should be included in Appendix AH. 1.4 (File Download Interface) – this places obligations on DCC and should be retained. 1.5 (Interaction with Order Management Systems (OMS)) - this places obligations on DCC and should be retained. 1.6 (Error Handling) - this places obligations on DCC and should be retained.
Npower	Large Supplier	No	

Question 10: Do you have any other comments?

Question 10		
Respondent	**Category**	**Comments**
E.ON Energy Solutions	Large Supplier	The history of SSI changes aside, we would like to reiterate our thanks to the relevant members of the DCC for all of their time and effort in helping Users to achieve greater value from SSI via this body of work. – We would further like to thank those individuals for their efforts in making the SSI BRD an accessible and usable document for Users, it is very helpful and we are grateful to you.
Western Power Distribution	Network Party	No further comments.
Bryt Energy Limited	Small Supplier	No
SSE	Large Supplier	We would like clarification and further information provided around the proposed solution processes relating to: Mechanism by which SEC Parties can propose a change to the SSI – will this be via standard template, what will be the route to submit and how will these proposals be logged and visible to all Parties; Timescales for when DCC will respond to initial requests – both urgent and non-urgent; Timescales for when SSI Change Proposals need to be submitted to be considered within the standard consultation process; Timescales for when DCC will assess responses to the consultation and refer to the SEC Panel or a delegated Sub-Committee for consideration and subsequent approval or rejection; Point at which changes to SSI business requirements will be presented to the Customer Working Group – prior to live implementation.
EDF Energy	Large Supplier	We agree that a more agile approach to managing changes to the SSI would be of benefit, but as noted before any new process needs to retain the key features of the SEC Modifications process, which are that:

Question 10		
Respondent	**Category**	**Comments**
		• Any SEC Party is able to raise a change to the SSI. • All Parties will be consulted for their views on proposed changes to the SSI, and the estimated costs of making those changes. • SEC Parties will make the decision on whether the changes that are proposed should be made, based on an accurate view of the costs that will be incurred. We are especially concerned about the last point; it must be ensured that SEC Parties are in control of any costs that are incurred as a result of making changes to the SSI.
Npower	Large Supplier	No

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0058 'Changes to the governance of the Self-Service Interface'

Annex G

Working Group Consultation responses

About this document

This document contains the full collated responses received to the second SECMP0058 Working Group Consultation.

Question 1: Do you agree with the solution put forward?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	Yes	While we still have some concerns about the length of time that it might take to raise and implement a change using the proposed new process, we believe that this process would still be a better alternative than the current process that would require a SEC Modification to be raised for each SSI change. As the new SSI Change Governance Process sits outside of the SEC it should be easier to adjust and amend this process in light of real world experience to ensure that it enables changes to be raised and progressed on a timely and cost-effective basis.
Smartest Energy Ltd	Small Supplier	Yes	This solution will make the change modification process more efficient and will allow the DCC to make improvements to the SSI fast enough to meet the changing needs of the needs of SSI users.
SSE	Large Supplier	Yes	This seems to cover the governance process, development of new requirements and how changes to the requirements will be documented and made available to Parties. We would like clarification on the following points for implementing changes to the SSI, as we could not see these covered in the proposed legal text/documentation: SSI Governance process Will there be controls in place about who can submit a SSI SIP to the DCC email address? Similar to nominated contacts for each organisation. What will be the lead time for DCC notifying Parties of SSI changes in each sprint before they are implemented? Will these schedules be available on SSI? Will the implementation of the SSI changes be outside of Parties core business hours?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
Western Power Distribution	Network Party	Yes	We believe that the proposed solution will provide a more flexible, transparent modification process for changes to the SSI. It will allow users to raise requests and it will provide visibility of changes to industry via consultations.

Question 2: Will there be any impact on your organisation to implement SECMP0058?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	Yes	These will largely be business process impacts, in that we will need to have a mechanism for raising changes to the SSI via the new mechanisms, as well as responding to the consultations that will be issued in regards to proposed changes to the SSI.
Smartest Energy Ltd	Small Supplier	No	
SSE	Large Supplier	Yes	Minimal impact as this will relate to our internal communications to advise of the change in process to raise, impact assess proposed changes (SSI improvement consultation) and the subsequent development, approval and implementation.
Western Power Distribution	Network Party	Yes	Western Power Distribution will be required to review and potentially respond to additional consultations that will be issued as a result of this modification. Implementation of this modification will also provide a new process to follow should we wish to request any changes to the SSI.

Question 3: Will your organisation incur any costs in implementing SECMP0058?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	No	We do not expect that SECMP0058 will increase our costs; at the same time we do not expect this to present any cost reductions either.
Smartest Energy Ltd	Small Supplier	No	
SSE	Large Supplier	No	Minimal impact as this will relate to the communications required to advise of the change in process.
Western Power Distribution	Network Party	Unknown	The costs we will incur will include our share of the implementation costs as well as the ongoing costs to the review consultations. In addition we will incur costs that the DCC charge for additional work to produce and review the consultation documents as well as the changes that are designed, tested and implemented.

Question 4: Do you believe that SECMP0058 would better facilitate the General SEC Objectives?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	Yes	We agree that the proposed solution better facilitates SEC Objective (b) as it will enable DCC to provide services that meet the needs of its Users in the most efficient and economical manner, in line with the First Enduring General Objective in the DCC Licence. We also agree that the proposed solution better facilitates SEC Objective (g) as it will ensure that low level design detail that is not relevant to the objectives of the Smart Energy Code is not included in the SEC and therefore made subject to a disproportionately onerous change process. For the avoidance of doubt we believe that the proposed solution is neutral against the other SEC Objectives.
Smartest Energy Ltd	Small Supplier	Yes	This modification better facilitates SEC Objective (a) as this modification will provide Users with an improved means of accessing DCC Services directly, including information which could be critical to resolving issues related to the provision, installation and operation of Smart Metering Systems.
SSE	Large Supplier	Yes	We agree with the Modification Report for the reasons given, that this would better facilitate General SEC Objective (b). We think that implementing this new process would better facilitate SEC Objective (g) in that it would enhance the existing process to have greater transparency on how to request and deliver changes to the SSI, as well as being clearer on the requirements associated with SSI and the introduction of the SSI Baseline Requirements Document.

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			Utilising this new process, if this Modification is implemented, could lead to SSI improvements that would better facilitate SEC Objective (a).
Western Power Distribution	Network Party	Yes	We believe that this modification better facilitates SEC Objective (g) by facilitating the efficient administration and implementation of this Code. We also believe that this modification better facilitates SEC Objective (b) as improving the process for making changes to the SSI will allow the DCC to efficiently comply with the General Objectives of the DCC.

Question 5: Noting the costs and benefits of this modification, do you believe SECMP0058 should be approved?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	Yes	We believe that the proposed process represents an improvement, although not a significantly material one, over the current processes for making to the SSI.
Smartest Energy Ltd	Small Supplier	Yes	There are no costs to the DCC and the cost to SECAS is minimal
SSE	Large Supplier	Yes	This seems a reasonable approach to support greater flexibility, efficiency and agility to implement changes to the Self-Service Interface.
Western Power Distribution	Network Party	Yes	We believe that this modification should be approved as the benefits of having a more flexible, transparent modification process for changes to the SSI, will help to ensure that Users have an efficient system that provides benefits to their processes. This modification also provides a strict governance process that will ensure that any changes Parties or the DCC wish to make to the SSI are approved and signed off by appropriate groups.

Question 6: How long from the point of approval would your organisation need to implement SECMP0058?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	1 week	We would need a minimal amount of lead time to ensure that our operational processes, roles and responsibilities are aligned to the new process.
Smartest Energy Ltd	Small Supplier	N/A	
SSE	Large Supplier	As per consultation document.	This seems to provide sufficient time to support our internal communications on the changes to the process.
Western Power Distribution	Network Party	Flexible	We do not require a minimum time before this modification is implemented.

Question 7: Do you agree with the proposed implementation approach?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	Yes	We don't see any issues with the proposed implementation approach.
Smartest Energy Ltd	Small Supplier	Yes	June 2019 SEC release is the earliest SEC release that the modification can be implemented in
SSE	Large Supplier	Yes	
Western Power Distribution	Network Party	Yes	We believe that this modification should be implemented as soon as is practical.

Question 8: Do you agree that the legal text will deliver SECMP0058?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
EDF Energy	Large Supplier	Yes	We have not identified any issues with the legal text. We note, however, that while the original proposal was to remove Appendix AH from the SEC in its entirety, the current drafting retains a significant amount of content. We agree that obligations on SSI Users should remain in the SEC itself and not the new SSI Baseline Requirements Document, and assume that the sections that remain are less likely to need to change on an 'agile' basis and so would remain suitable to be changed through the SEC Modifications.
Smartest Energy Ltd	Small Supplier	Yes	The changes are minimal
SSE	Large Supplier	Yes	We would also expect to see references to the points we've raised for clarification, as per our response to Q1.
Western Power Distribution	Network Party	Neutral	We believe that there should be clarification around the DCC 'prioritising' SIPs. What will justify one SIP being prioritised over another?

Question 9: Please provide any further comments you may have

Question 9		
Respondent	**Category**	**Comments**
EDF Energy	Large Supplier	
Smartest Energy Ltd	Small Supplier	
SSE	Large Supplier	
Western Power Distribution	Network Party	