

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.



SECMP0067 'Service Request Traffic Management'

Modification Report Version 0.1

About this document

This document is the Modification Report for [SECMP0067 'Service Request Traffic Management'](#). It provides detailed information on the background, issue, solutions, 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	5
4. Impacts	6
5. Costs	7
6. Implementation approach	8
7. Discussions and development	9
8. Conclusions	11
Appendix 1: Glossary	13

This document also has four annexes:

- **Annex A** contains the business requirements for the proposed solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the proposed solution.
- **Annex C** contains the Traffic Management Mechanism Document.
- **Annex D** contains the full Data and Communications Company (DCC) Preliminary Assessment response.

1. Summary

The DCC Systems are limited by a finite capacity. As numbers of Smart Meters and Devices increase in the Smart Metering Implementation Programme (SMIP), this will increase the traffic of Service Requests in the DCC Systems. In exceptional instances this traffic, if left unchecked, could result in an overload of the DCC Systems and cause an outage, resulting in no Service Requests being sent. Management of the DCC System has been recommended, in order to prevent this outcome without the expense of expanding the DCC infrastructure.

The Proposed Solution is therefore to introduce a mechanism to throttle Service Requests when the DCC System are experiencing heavy traffic. This mechanism will only be active once the capacity threshold in the DCC Systems is in danger of being breached. This way, the Service Request throttling will only take place in exceptional circumstances and not be day to day activity. Service Users will be allocated their own capacity thresholds, proportional to their portfolio and be forced to operate within that allocation once the mechanism is active. The DCC will provide reporting on the frequency of how often the mechanism is used and its duration. It is noted that only Users who exceed their capacity threshold will be throttled if the solution's mechanism is in effect. Any User who keeps within their capacity will not be throttled.

All SEC Parties are expected to be impacted by this Modification Proposal. The solution will cost approximately £1,6m up to Pre-Integration Testing (PIT). The proposed implementation date of this Modification Proposal if approved is the November 2020 Release.

2. Background

What happens currently in DCC Systems?

The DCC System has a finite capacity. Even with communication with Service Users to meet forecasted demand and making the most efficient use of the System's current capacity, it may be unable to cover accidental or unanticipated large bursts of Service Requests. This current system penalises Service Users equally rather than those responsible for the overload.

What is the issue?

The DCC's Data Service Provider (DSP) currently lacks protection from the danger of an overload, which could threaten to deteriorate the service provided or in an extreme situation lead to the failure of the system. These outcomes can occur in cases of heavy Service Request traffic, caused either by accident or with malicious intent.

The DCC works with Service Users to meet forecast demand and to make effective and efficient use of System capacity. However, the System has a finite capacity and is unable to scale dynamically to meet accidental or unexpected bursts of Service Requests. The causes of these bursts range from the anticipation of extreme weather to a Denial of Service (DoS) attack.

The network infrastructure already has a mechanism in place to protect the System under load, whereby the System responds with an HTTP 503 if it is unable to forward a request to the Message Gateways. This applies to all Service Users and Service Requests irrespective of the importance of the Service Request or which Service User(s) are responsible for the excess load. This means that crucial Service Requests can be rejected and must request retries. Additionally, this results in Service Users who have operated responsibly not being able to use the DCC System at its expected performance whilst it deals with this traffic.

This proposal is designed to provide reliable and predictable System behaviour under extreme conditions. It will enable the service to deliver Service Requests identified as priority even under extreme load and control the Service Requests of only those Service Users whose use of the service exceeds their fair share, potentially crowding out other Service Users use of the service.

3. Solution

Proposed Solution

The proposed solution is to implement a maximum system capacity, operating threshold and appropriate Service User allocations. When the DCC System reaches this operating threshold, a traffic management mechanism for the Service Requests will become active. Service Users who are exceeding their allocation will then have their requests throttled down to either their stated allocation or the operating threshold (whichever is greater). This should prevent Service Users crowding out others who are using the System by adhering to the allocations. The details of the solution's mechanism, its formula and a worked example can be found in Annex C.

The proposed solution will deliver a defined formula for determining the Service User allocations, according to the number of Service Requests they would expect to process, including those affecting Pre-Payment requests and measuring against their portfolio size of smart meters and devices. A list of priority Service Requests will also be created and managed by the Panel (or a nominated Sub-Committee) that will not be throttled under these conditions. This list will be kept outside of the SEC so that any amendment to the list can be made without having to raise and process a modification to deliver this. Additionally, this solution will include a monthly update of these factors so that they remain accurate over time. A reporting process will be introduced so that Service Users will be notified of any Service Request throttling that takes place and to keep Service Users informed of the frequency and duration that these occur in.

The business requirements for this solution can be found in Annex A.

The reporting in this solution will be undertaken by logging events in the DCC's Technical Operations Centre. This will form the basis for monthly reporting which will include details considering System Configuration, System Capacity, Users and any Trends. These reports will be issued to the Panel, or the nominated Sub-Committee – SECAS is recommending the Operations Group for this role.

Legal text

The changes to the SEC required to deliver the proposed solution can be found in Annex B.

The legal text introduces a new document, the 'Traffic Management Mechanism Document'; a draft copy can be found in Annex C. Supporting documentation that explains the service capacity allocation formula is included in this Annex.

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

Supplier Parties will be affected by this modification due to having to work to their capacity allocation in times of heavy Service Request traffic and may have to change their business processes in line with these allocations.

Network Operators will be affected by this modification where heavy Service Request traffic will require less active activity when the solution's mechanism is in effect.

Other SEC Parties will be affected by this modification for the reasons above, but will be guaranteed some capacity during heavy traffic to ensure that they can still send requests during this time.

DCC System

The DCC has developed a mechanism responsible for throttling Service Requests (excluding those that do not appear on the modification's priority Service Request list) once the capacity threshold is breached. The DCC has defined the formula for allocating capacity and consequently update the Service User allocations as well as deliver reporting on a monthly basis. This formula, a summary of its values and parameters can be found in Annex C.

The full impacts on DCC Systems and the DCC's proposed testing approach can be found in the DCC Preliminary Assessment response in Annex D.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section H 'DCC Services'
- Appendix AB 'Service Request Processing Document'

Other industry Codes

There is no impact on any other industry codes.

Greenhouse gas emissions

There are no impacts on greenhouse gas emissions.

5. Costs

DCC costs – Proposed Solution

The estimated DCC implementation costs to implement this modification up to PIT is £1,646,355. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Cost
Design, Build & Pre-Integration Testing	£1,646,355

More information can be found in the DCC Preliminary Assessment response in Annex D.

The full standalone implementation costs will be determined as part of the DCC Impact Assessment.

SECAS costs

The estimated Smart Energy Code Administrator and Secretariat (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

As part of the Refinement Consultation, respondents will be asked about the costs that they face individually as SEC Parties outside of the central costs above.

6. Implementation approach

Recommended implementation approach

The Working Group is recommending an implementation date of:

- **5 November 2020** (November 2020 SEC Release) if a decision to approve is received on or before 31 March 2020; or
- **24 June 2021** (June 2021 SEC Release) if a decision to approve is received after 31 March 2020 but on or before 5 November 2020.

The Working Group and the DCC want to deliver this Modification Proposal as soon as possible. Although the DCC have stated in the Preliminary Assessment the estimated lead time is 12 months, it has indicated it will be able to deliver the solution for the November 2020 SEC Release if a decision to approve is received before 31 March 2020.

7. Discussions and development

Which Service Requests need to be placed onto the Prioritised Service Request List?

The Working Group considered which Service Requests must have priority in the event of the DCC System approaching an overload. Early on, Working Group members wanted to include Service Requests relating to Pre-Payment, as it was a driving factor for why the Modification Proposal had been raised. Calls were also made by Network Party members to include Service Request 7.4 'Read Supply Status' to give information on outages.

When the first draft of the Priority Service Request List was created, the Working Group agreed to remove the requests related to installing, commissioning and de-commissioning. The rationale was that these choices were not time-critical and advised that only Service Requests with target response times with 30 seconds should be considered.

As part of the solution's refinement, the business requirements and subsequent Priority Service Request List were taken to the Technical Architecture and Business Architecture Sub-Committee (TABASC). The TABASC requested that it be the Sub-Committee that the Panel elects to manage and amend the list if the Modification Proposal is approved. Although some members felt the list included too many requests for a priority list, they agreed to it on the condition that it could be amended in future as stated in the business requirements.

As part of the Modification Proposal's Refinement Consultation, industry members will be asked for any additional Service Requests they want to see on the list with accompanying rationale. These submissions will be taken into consideration going forward and subject to the approval of the Panel (or a nominated Sub-Committee).

Which circumstances will trigger the solution's management mechanism?

The Working Group questioned the DCC on how often it would expect this management mechanism to be activated and whether this was specifically for situations outside the normal business processes or for everyday use. Working Group members felt the obligations of the DCC to provide an efficient system meant this solution should only be used in exceptional circumstances. If this was an everyday occurrence, then it should not be industry members that fund this change.

The DCC stated that this solution was designed for exceptional circumstances, not for standard business operations. In a business case that the DCC presented, it stated that freak weather events such as 'The Beast from the East' and DoS attacks were the situations this mechanism was designed to deal with. The DCC also mentioned that if one or more Service Users were to submit too many Service Requests in a short period of time, this mechanism could be activated to manage the situation. It stated that scenario has occurred before in standard business operations where several Users have submitted large quantities of Service Requests around the same time of day.

The Working Group queried the business case and asked whether the DCC could provide any estimated quantities and frequencies of events this mechanism could mitigate. The DCC took note of this and will investigate historic outages to strengthen this area of the business case before the Modification Report is submitted to the Panel. One Working Group member also asked whether this business case had gone through review by the Security Sub-Committee (SSC), particularly concerning the potential DoS attack. SECAS agreed that the modification would be taken to the next available SSC meeting for input.

Were other solutions considered during the Refinement Process?

An Alternative Solution was considered by the Working Group. This differed from the Proposed Solution by introducing a buffering system to the mechanism that has been detailed in the Proposed Solution as a sixth business requirement. Instead of returning a HTTP 503 response requesting the User try again and re-sending the Request, it would instead queue the Request until the next applicable time window opens where the Request could be accepted. A notification response would be sent to the User through a variant of the HTTP 503 to inform them that their Request has been queued rather than rejected and needing a retry attempt. Otherwise, the Alternative Solution was identical to the Proposed Solution.

Following Preliminary Assessment by the DCC the Alternative Solution was presented to the Working Group. One Working Group member stated in a meeting that they would prefer the notification to attempt a retry rather than having a Service Request queued. This was because with a retry a response would be given back in a timely manner, whereas they feared through queuing the response would be slower to return. The additional business requirement for the Alternative Solution was estimated to cost between £350,000-£750,000. That would take the cost of solution up to PIT between approximately £2,000,000-£2,400,000. Other Working Group members felt this was too expensive to justify its inclusion into the solution, especially where it wasn't delivering a significant improvement. Both the Working Group and the Proposer expressed a clear preference for the Proposed Solution over the Alternative Solution, and so this Alternative Solution is not being progressed further.

8. Conclusions

Benefits and drawbacks

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

Benefits

- It provides assurance that when the maximum DCC System capacity is reached in an unanticipated event, it can throttle Service Requests to prevent an outage. The cost of an outage is significant to every User, so mitigating this risk could over time provide a substantial economic benefit.
- DCC have stated that the Proposed Solution's mechanism can prevent outages in standard business practise. Previously where multiple Service Users have almost caused an outage, the mechanism could assist in ensuring day to day operations aren't negatively impacted through lack of communication
- The Proposed Solution can also protect against outages caused by accidental or unintended triggering of large amounts of Service Requests or deliberate DDoS attack.

Drawbacks

- The Preliminary Assessment returned a lead time of 12 months from the point of approval to implement the modification. Some Working Group members felt this this was a long time to wait for protection, which is needed as soon as possible.

Proposer's rationale against the General SEC Objectives

Objective (a)¹

The Proposer believes that SECMP0067 will better facilitate General SEC Objective (a) by improving the conditions under which Smart Meters and Devices can be installed. Additionally, the testing required onsite will be less likely be to be postponed by reducing the likelihood of a DCC System outage.

Objective (e)²

The Proposer believes that SECMP0067 will better facilitate General SEC Objective (e) by improving the design of the existing DCC Systems. The improvement and innovation are being able to provide protection to the DCC Systems from heavy Service Request traffic, rather than just identifying it. Preventing potential outages should also provide a securer supply of energy to consumers.

¹ (a) Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

² (e) Facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy.

Working Group members' views

Working Group members agreed that the Modification Proposal better facilitates General SEC Objectives (a) and (e). They agreed with the Proposer's rationale for both on improving the installation process, offering innovation and providing a securer energy supply.

Sub-Committee views

The TABASC reviewed the Modification Proposal's business requirements before a Preliminary Assessment was sought from DCC. It queried the Priority Service Request List, in particular the inclusion of some requests it thought weren't time critical. The TABASC asked to be kept informed of any major changes to the Modification Proposal and expressed an interest in managing and amending the list.

The SSC will be consulted in parallel with the Refinement Consultation.

Appendix 1: Glossary

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

Glossary	
Acronym	Full term
DCC	Data and Communications Company
DoS	Denial of Service
DSP	Data Service Provider
PIT	Pre-Integration Testing
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMIP	Smart Meter Implementation Programme
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TOC	Technical Operations Centre



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

Harry Jones

020 7081 3345

harry.jones@gemserv.com

Smart Energy Code Administrator and Secretariat (SECAS)

8 Fenchurch Place, London, EC3M 4AJ

020 7090 7755

sec.change@gemserv.com