

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 2.0

19 August 2020

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

1. Summary.....	3
2. Issue.....	3
3. Solution	4
4. Impacts	8
5. Costs	9
6. Implementation approach	10
7. Assessment of the proposal	11
Appendix 1: Progression timetable	23
Appendix 2: Glossary	23

This document also has nine annexes:

- **Annex A** contains the Service Request Traffic Management Mechanism Document.
- **Annex B** contains the business requirements for the proposed solution.
- **Annex C** contains the Reporting Wireframes.
- **Annex D** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the proposed solution.
- **Annex E** contains the full Data Communications Company (DCC) Impact Assessment response.
- **Annex F** contains the full first Refinement Consultation responses.
- **Annex G** contains a worked example of how the solution will work.
- **Annex H** contains the Business Case.
- **Annex I** contains the full second Refinement Consultation responses.

Contact

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

Harry Jones, 020 7081 3345; Harry.jones@gemserv.com

1. Summary

This proposal has been raised by Graeme Liggett on behalf of the DCC.

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 from the Data Service Provider (DSP). The DCC has recommended management of the System, in order to prevent an outage without the expense of expanding the DCC infrastructure.

The Proposed Solution is to introduce a mechanism to regulate the volume of Service Requests when the DCC System is experiencing heavy traffic. **This mechanism would be activated if the DSP system capacity threshold is breached and only take place in exceptional circumstances.**

Service Users will be allocated their own capacity thresholds, proportional to their portfolio; they can exceed this allocation where there is spare System capacity but will be forced to operate within that allocation if the System is near capacity and the mechanism is active.

The DCC will provide reporting on the frequency of how often the mechanism is used and its duration, as well as individual Users' allocation and monthly traffic. **It is noted that only Users who exceed their capacity threshold will have their Service Requests regulated if the solution's mechanism is in effect.** Any User who keeps within their capacity will not be regulated. Users can independently prioritise their Service Request traffic as part of their business processes.

This modification was submitted to Ofgem for Authority Decision in April 2020 but was sent back to industry for further work in May 2020. The Working Group was reconvened, and the business case was discussed again and the impacts of moving to a June 2021 implementation were assessed. Following the responses from the Second Refinement Consultation, the June 2021 SEC Release is recommended for the mechanism to be implemented with the current Http 503 re-try response. Improved functionality to enable use of the Http 429 response codes will be available from November 2021 following a DCC User Interface Specification (DUIS) uplift.

All SEC Parties are expected to be impacted by this Modification Proposal. The central costs of the solution will be approximately £1.6m. The proposed implementation date of the mechanism proposed under this Modification Proposal, if approved, is the June 2021 SEC Release. The updates to the DUIS for optional functionality will be implemented in the November 2021 SEC Release.

2. Issue

What happens currently in DCC Systems?

The DCC System has a finite capacity. Even when configured 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 sent by Users. In the current DCC System configuration, F5 Load Balancers provide the only protection for the DSP against overloading from the network. Once the system is overloaded the F5 Load Balancers will respond with 'Http 503 Service Unavailable' error messages to all the Users and will essentially stop the input so that no Users can send anything. There is no processing or prioritisation of any Service Requests, all Users are

impacted, and the DSP would not be able to respond to any further Service Requests sent by any User. This would include any high priority Service Requests such as prepayment top-ups.

What is the issue?

The DCC System has a finite capacity and is unable to meet accidental or unexpected large bursts of Service Requests. The causes of these bursts might include User System's sending excessive numbers of Service Requests or Denial of Service (DoS) attacks.

The current system penalises Service Users equally rather than those responsible for the overload.

What is the impact this is having?

This means that if the System is overloaded, all Service Requests will be rejected, and Users 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 System to control the Service Requests of only those Service Users whose use of the service exceeds their fair share.

3. Solution

Proposed Solution

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

The details of the solution's mechanism and the Capacity Allocation Formula can be found in the Service Request Traffic Management Mechanism Document in Annex A. Please note that the Service Request Traffic Management Mechanism Document introduced in this Modification Proposal is independent of the Traffic Management Mechanism Document that is created in [SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection'](#).

Capacity allocation formula

Service Users will be notified of the DSP System Capacity by the DCC. Under it, each Service User will be allocated a proportion of the available capacity based on an agreed formula. This formula can be found in the Service Request Traffic Management Mechanism Document and can only be amended by Panel (or a Sub Committee of their choosing, which the Smart Energy Code Administrator and Secretariat (SECAS) recommends should be the Operations Group).

The proposed capacity allocation formula will operate at a SEC Party ID level and is built on the weighted proportionality principle; that is, each allocation is scaled using one or more weighting factor(s). To ensure fairness, capacity will be allocated on a basis that is clear and does not disadvantage any one User. Two considerations will be applied here:

- Allocation will be based on installed Devices to which that User has an allocated role; and
- Allocation will be based on the financial contribution of that User to the DCC System, as measured by the User's charging group weight factor.

These two factors will be multiplied together. Thus, if either of the factors is zero the weight itself becomes zero. Consideration will also be given to the expected additional volume of Service Requests required to manage prepayment customers relative to non-prepayment customers. The proposed formula will also guarantee a minimum allocation for Other Users.

Users who pay most and those with the most customers and the most meters to serve will therefore receive larger allocations than smaller Service Users. These two principles, minimum allocations and weighted proportionality, form the base for a fair and equitable capacity allocation formula.

Notification of capacity allocations

The DCC will notify the DSP of the agreed DSP System Capacity and Service User Capacity settings via the upload of a configuration file in a similar fashion to that used for DCC System Wide Anomaly Detection Thresholds (ADT).

Service User Capacity settings will be expressed as a percentage of the total capacity, thus allowing the overall DSP System Capacity to be increased without the need for new Service User Capacity settings to be uploaded.

Capacity management process

The DCC will set amber and red threshold percentages for each of the DSP System Capacity and Service User Capacity setting, which will form the basis of the invocation of the traffic management mechanism.

The DSP will record two new sets of values as Service Requests are received or actioned:

- a count of all Service Requests processed in the last [1] seconds; and
- a count of all Service Requests processed for each Service User in the last [1] seconds.

It should be noted that this includes DSP Scheduled Service Requests, but these will be subject to existing DSP load management features to ensure they are processed at a controlled rate. This rate will be set to ensure that there is always DSP System Capacity available for On Demand requests.

The time period for counting Service Requests will be a configurable rolling interval managed in a similar fashion to the intervals used in anomaly detection, albeit that the interval used for traffic management is expected to be much shorter.

The count of Service Requests over the period shall determine a 'requests per second usage' value for the DSP System as a whole and for each Service User. These values will be compared against the DSP System Capacity and the Service User Capacity as follows:

- If the DSP System usage exceeds the amber threshold for DSP System Capacity, then a System Usage Warning event will be recorded and notified to the DSP monitoring solution.
- If any Service User usage exceeds the amber threshold for Service User Capacity, then a Service User Usage Warning event will be recorded for each Service User and notified to the DSP monitoring solution.

- If any Service User usage exceeds the red threshold for Service User Capacity but the DSP System usage remains below the red threshold for DSP System Capacity then a Service User Excess Usage event will be recorded for each Service User and notified to the DSP monitoring solution.
- If the DSP System usage exceeds the red threshold for DSP System Capacity, then a System Overload event will be recorded and notified to the DSP monitoring solution. This event may also be configured to create an Incident in the DCC Service Management System (DSMS) if required.
- The system will disable Schedule Activation, DSP Future Dated execution, Low Priority Execution and Certificate Replacement requests while there is a System Overload event in place.
- If the DSP System usage exceeds the red threshold for DSP System Capacity and any Service User usage exceeds the red threshold for Service User Capacity, then a Service User Overload event will be recorded for each Service User and notified to the DSP monitoring solution. Any Service User who has exceeded capacity will be marked as subject to Traffic Overload.

Once a Traffic Overload event occurs, the processing for each Service User will operate as illustrated below.

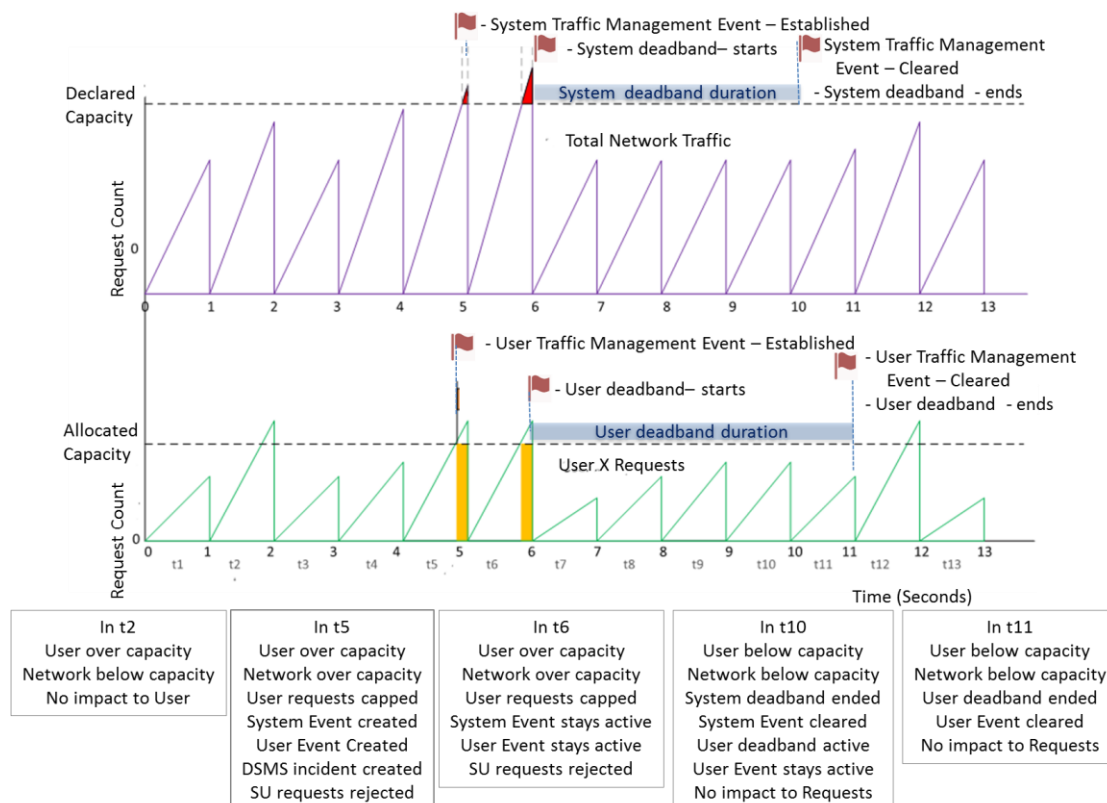


Figure 1 Southbound Traffic Management Processing

Within each [1] second window, the DSP will accept Service Requests up until the Service User reaches its Service User Capacity. At this point, the Service User will be marked as subject to Traffic Overload for the remainder of that window.

The processing at the DSP boundary within the Message Gateway will check whether a Service User is marked as subject to Traffic Overload and if so then the following action will be taken:

- Any Service Request with a Service Request Variant (SRV) which is identified as being subject to Traffic Management will be rejected using a configurable Http Status code.
- Any Service Request with an SRV that is identified as NOT being subject to Traffic Management will be processed as normal.

The list of which SRVs are subject to Traffic Management will be configurable and held within the DSP solution. Updates to this list will be managed by the SEC Panel (who may choose to delegate this responsibility to a Sub-Committee).

The processing under Traffic Management mode will continue until the DSP System usage returns below the red threshold for DSP System Capacity and stays there for a period greater than the system deadband duration. During the system deadband period, if the DSP System goes over capacity there will not be a new event created; instead this will be linked to the existing system traffic management event. Once the rate of messages falls within the system capacity then the deadband window will be restarted. This mechanism will help reduce the number of incidents. The deadband durations for both System and User will be configurable.

(Note: The deadband durations in Figure 1 are kept shorter for illustration purposes; these can be configured for longer durations).

If a Service User who is subject to Traffic Overload returns below the red threshold for Service User Capacity before the DSP System usage returns below the red threshold then that Service User will be cleared of being subject to Traffic Overload.

Otherwise, when the DSP System usage returns below the red threshold for DSP System Capacity then any Service User who is above the red threshold will be cleared of being subject to Traffic Overload.

Reporting

Events generated by the Traffic Management system and any Service Requests that are rejected will be recorded and made available to the reporting and monitoring systems.

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. The DCC confirmed its support for the Panel to delegate responsibility to the Operations Group to oversee management of the reporting as well as the management of the Priority Service Request list and the wider solution mechanism's configurable parameters. The Working Group agreed with this but wanted the Security Sub-Committee (SSC) and the Technical Architecture and Business Architecture Sub-Committee (TABASC) to provide input to the Operations Group meetings where this is discussed.

An example of the reporting that will be provided by the DCC can be found in Annex C.

Legal text

The changes to the SEC required to deliver the proposed solution can be found in Annex D and the Service Request Traffic Management Mechanism Document can be found in Annex A.

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 and Network Operators will be affected by this modification due to having to work to their capacity allocation in times of heavy Service Request traffic.

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

Some Users' systems may need to be amended to be able to interpret the new Http error code being introduced and to prioritise Service Requests when the mechanism is active. It was stated that 12 months at minimum would be required to facilitate these changes on an individual basis according to the majority of responses to the second Refinement Consultation.

DCC System

The DCC has developed a mechanism responsible for throttling Service Requests once the total capacity threshold is breached. The DCC has defined the formula for allocating capacity for Service Users and deliver reporting on a monthly basis. These will be implemented within the DCC Systems.

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

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section H 'DCC Services'
- Appendix AB 'Service Request Processing Document'
- Appendix AD 'DCC User Interface Specification'

The redlined changes to these documents can be found in Annex D

The Service Request Traffic Management Mechanism Document will also be created to account for traffic management changes being introduced. This can be found in Annex A.

Consumers

Consumers are less likely to suffer an outage of service (such as not being able to top-up prepayment meters) as the actions of one User will not impact other Service Users.

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

The estimated DCC implementation cost to implement this modification is £1,629,167. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Cost
Design	£65,095
Build and Pre-Integration Testing (PIT)	£1,406,345
Systems Integration Testing (SIT)	£36,768
User Integration Testing (UIT)	£55,738
Implement to Live	£0
Application Support	£65,221

More information can be found in the DCC Impact Assessment response in Annex E.

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

As part of the first Refinement Consultation, respondents were asked about the costs that they face individually as SEC Parties outside of the central costs above. All Parties said there would be implementation costs, but no monetary values were given nor any idea of the magnitude of these costs.

The first Refinement Consultation Responses can be found in Annex F.

The second Refinement Consultation Responses can be found in Annex I.

6. Implementation approach

Agreed implementation approach

The Panel agreed an implementation date of:

- **24 June 2021** (June 2021 SEC Release) for implementation of the traffic management mechanism and **4 November 2021** (November 2021 SEC Release) for the DUIS change if a decision to approve is received on or before 30 September 2020; or
- **4 November 2021** (November 2021 SEC Release) for all changes if a decision to approve is received after 30 September 2020 but on or before 4 November 2020.

The Proposer wants to deliver this Modification Proposal as soon as possible, if approved. The DCC requires nine months lead time to deliver the mechanism.

From the First Refinement Consultation responses, two SEC Parties stated they would take longer than six months from the point of approval to prepare themselves for the planned changes. They stated their lead time required would be closer to 12 months. Other SEC Parties stated that they could either meet this within six months, couldn't gauge it or didn't comment in the consultation. The full First Refinement Consultation responses can be found in Annex F.

When the Modification Proposal was taken to the Change Board on 22 April 2020, several members stated that they would require between six and 12 months to change their internal processes and systems to accommodate these changes. The Authority subsequently sent the Modification Report back to the Panel to assess the impact of moving the implementation date from the November 2020 SEC Release to the June 2021 SEC Release.

A Second Refinement Consultation was issued following the send back. Of the eight responses, six claimed that they would require 12 months or longer to change their system to accommodate Service Request prioritisation. This informed the decision to implement the DUIS changes in the November 2021 SEC Release in line with what was provided in the responses. The full Second Refinement Consultation responses can be found in Annex I.

The TABASC supported implementation of the mechanism in June 2021, with improvements to the DUIS, and thereby the re-try message, implemented in November 2021. It considered the DCC System capacity was sufficient and therefore the likelihood of the mechanism being used in the next 12 months was small, giving Parties time to make the necessary system changes. However, the mechanism would be in place should an extreme event take place in this time.

SECAS is recommending this modification be included in the June 2021 SEC Release for the non-System impacting changes and the November 2021 SEC Release for the DUIS change if a decision to approve is received by 30 September 2020. If this cut-off date is missed, the modification's full solution would fall back to the November 2021 SEC Release and delivered as a single package.

7. Assessment of the proposal

How does the mechanism work?

Service Users will be given a capacity allocation based on their portfolio of operational Devices and weighted DCC Service Request usage (i.e. Suppliers need to send more Service Requests than Network Parties). Other SEC Parties will also be given a capacity allocation to ensure they are able to send Service Requests. If the DCC System is running under total capacity and a User breaches their capacity allocation they will not be regulated. If the DSP System usage exceeds the red threshold for DSP System Capacity and any Service User usage exceeds the red threshold for Service User Capacity, then a Service User Overload event will be recorded for each Service User and notified to the DSP monitoring solution. Any Service User who has exceeded capacity will be marked as subject to Traffic Overload. The processing at the DSP boundary within the Message Gateway will check whether a Service User is marked as subject to Traffic Overload and if so then the following action will be taken:

- Any Service Request with an SRV which is identified as being subject to Traffic Management will be rejected using a configurable Http Status code
- Any Service Request with an SRV that is identified as NOT being subject to Traffic Management will be processed as normal.

The list of which SRVs are subject to Traffic Management will be configurable and held within the DSP solution. Updates to this list will be under the governance of the Panel (or a Sub-Committee nominated by it).

The processing under Traffic Management mode will continue until the DSP System usage returns below the red threshold for DSP System Capacity and stays there for a period greater than the system deadband duration. During the System deadband period if the DSP System goes over capacity there will not be a new event created, instead this will be linked to the existing system traffic management event. Once the rate of messages falls within the System Capacity then the deadband window will be restarted. This mechanism will help reduce the number of incidents. The deadband durations for both System and User will be configurable.

This means Service Requests sent over and above a User's capacity allocation will get a Http 429 Response. In the initial stages of the modification the DCC suggested an Http 503 response would be used, but the Working Group questioned this. The Working Group thought that receiving an Http 503 would not differentiate anything regulated through the modification's mechanism as opposed to any business-as-usual reasons. Following the Impact Assessment, the DCC changed this to a Http 429 'too many requests'.

Within the header of the Http 429 will be a retry time delay. This is a minimum time that the User should delay sending a retry. The Working Group spent time debating whether the System Deadband period and User Deadband period should be different, but in the end concluded that keeping them the same was the simplest answer.

The Retry After attribute was also debated, and specifically whether this should be less than or greater than the System Deadband period. The Working Group concluded that this should be less than the System Deadband period, otherwise there would be a danger of constantly ending the System level Traffic Management event only to trip back over it a few seconds later when the User sends in another burst of requests from the retry processing. By keeping the 'Retry After' less than the

Deadband there will be just one Traffic Management event that continues until the overload situation has ended.

A retry strategy was discussed at the Working Group as well. This retry strategy has a 'short retry' and 'long retry', with the short sequence being retrying 45 seconds after an initial failed attempt, then a third attempt after waiting 60 seconds and ending with a fourth retry after 75 seconds. If this 'short retry' fails to submit the User's Service Request, the 'long retry' sequence should be used where the User waits an hour before retrying the 'short retry' sequence again. If that doesn't work, the User should wait two hours before retrying the 'short retry again', then wait four hours if unsuccessful and so on. The DCC recommended that the rate of Service Requests that are retried do not exceed the User's allocation so that this doesn't risk triggering the Modification Proposal's solution. Further details of the retry strategy can be found in the Impact Assessment in Annex E.

This was presented at the Working Group on 16 March 2020. The Working Group was keen to see an example of how this would work for an individual User. A worked example was provided by the DCC and can be found in Annex G.

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 where events only lasted a few seconds. The rationale was that 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 (see Annex H) that the DCC presented, it stated that DoS attacks and accidental (human error or technical error) or malicious surges of Service Requests were the situations this mechanism was designed to deal with. It stated that a scenario has occurred before in standard business operations where several Users had submitted large quantities of Service Requests around the same time of day causing a strain on the System. Severe weather events were also mentioned as causing large bursts of Service Request traffic; however, Network Parties pointed out that they need to send large numbers of SRs to check customers are on supply. Network Parties will be able to manage their SRs within their capacity allocation however they see fit, determining the prioritisation themselves.

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 provided information about historic outages to strengthen this area of the overall business case. 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 subsequently presented the modification business case and solution to the SSC. The SSC was supportive although pointed out this the mechanism would protect the System from DoS attacks but would not prevent them.

How will this be affected by Half Hourly Settlement changes?

One Working Group member asked how the System and mechanism would be affected by the new Half Hourly Settlement arrangements. The DCC has confirmed that as Service Users usage increases

due to Half Hourly Settlement or business as usual rollout, they will receive a higher Capacity Allocation and the DCC Systems will be scaled to deal with the increased traffic.

Were other solutions considered during the Refinement Process?

Consideration of other options

Three other solution options were considered during the Refinement Process. A summary of these options and the costs are presented below.

A Buffering system

A potential 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 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 to 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 the Alternative Solution was not progressed further.

Following the Preliminary Assessment, the Working Group expressed concern about the cost of the modification. They questioned why this was the best solution and asked the DCC to consider if:

- additional infrastructure would be a better solution at an equal (or lower) cost; and
- if these events are rare perhaps 'taking the hit' of a DCC System outage and subsequent Disaster Recovery (DR) plans would be cheaper over a period of time.

The DCC investigated both proposals and responded with the following comments:

Additional Infrastructure ('Motorway Lane')

One alternative option is to increase the capacity of the existing DCC System by building additional 'Motorway' lanes that could accommodate surges in Service Request volumes. This would not require any SEC changes so would not require a modification to implement.

Each additional Motorway is equivalent to the processing of 450 transactions per second. The total set up costs for one Motorway lane is £280,000, with annual operational charges of £50,000 per lane. These are estimated DSP costs only. There will be further Communications Service Provider (CSP) costs that will be associated with the set-up and operation of additional Motorways, though these

have not been included. The table below shows the total costs for implementing up to five Motorway lanes:

Breakdown of DCC costs for new Motorways				
Number of additional Motorway lanes	Cost (£280k per lane)	Operational costs (£50k per lane)	Total cost	Additional transactions per second
1	£280,000	£50,000	£330,000	450
2	£560,000	£100,000	£660,000	900
3	£840,000	£150,000	£990,000	1,350
4	£1,120,000	£200,000	£1,320,000	1,800
5	£1,400,000	£250,000	£1,650,000	2,250

To increase the DSP Motorway to Profile 2¹, equivalent to 2,250 transactions per second, would require five more Motorway lanes at a cost of £1.4m with £250,000 of operational charges (although there could be some economies of scale here). However, other DSP infrastructure is likely to be needed to accommodate the accelerated rate of transactions such as change of Supplier (CoS), data management, databases etc, which will drive costs up further. This capability would then have to be replicated in the CSP costs, but if they're required to cope with surge volumes rather than actual usage, then they may need to scale to three or four times actual traffic volumes; this cost has not been included and would be additional to the costs set out above.

Current Gamma connections, which Users use to connect to the DCC Systems via the DSP, are capable of transmitting the equivalent of 30,000 Service Requests per second. Profile 5 caters for up to 6,000 transactions per second for the DSP. This will require 15 more motorway lanes. There would also be significant DSP Infrastructure increases when traffic levels reach 5,000 transactions per second which have not been included in the table above.

To provide the same protection as the Proposed Solution, this alternative option should be scaled for a worst-case instance to accommodate all 30,000 transactions per second. This is equivalent to an additional 67 Motorway lanes and would require a total investment in the region of £19m with an on-going maintenance cost of £3.4m. Again, this is the DSP cost only and does not provide protection to the CSP. The cost to the CSP is likely to be more than to the DSP.

Allowing DCC outages and using Disaster Recovery

It takes up to a maximum of four hours to switch over to the DR infrastructure, and if the same number of requests are then directed at the DR system, then it will also fall over when traffic reaches the level, as the DR system is sized the same.

The DCC Business Case found in Annex G estimates that for every hour the DCC System is down approximately £1m of costs would be incurred by the industry. Since it is not possible to estimate how frequently these events will occur and for how long, this leaves the DCC and the industry extremely exposed if they were to rely on DR only.

¹ Profiles are a stepped series of infrastructure allocations and configurations which will support increasing levels of traffic.

Other considerations

A Working Group member also suggested ADTs could be used instead as a solution. The DCC stated that ADTs were not granular enough to protect against a systematic error or DoS attack. It added that Service Requests subject to ADTs are still received by the DSP. Because of this, the ADT mechanism would not prevent a DSP outage and therefore would not provide protection against the Service Request traffic leading to a DCC System failure. Finally, even if ADT thresholds were breached, it results in the messages being placed in quarantine rather than being rejected, which means they must still be fully processed by the DSP in order to place them in quarantine. The Working Group agreed not to pursue this option further.

A Working Group member commented that they had been limited on Service Requests by the DCC since early 2020. Upon investigation this was identified as an issue relating only to that DCC User and not relating to this modification or the Proposed Solution.

Conclusions and summary of the business case

The indicative costs of the different options considered are summaries in the table below:

Indicative costs of all options considered		
Option	Description	Potential cost
1	Proposed Solution	£1,600,000
2	Input buffer to absorb peak demand	£2,350,000
3	Increased Capacity	£19,140,000 ²
4	Disaster Recovery	£4,000,000 ³

The Proposer believes the best option is the implementation of the traffic management mechanism. The Proposed Solution costs the least of all the solutions investigated. Furthermore, it provides enduring protection for the DSP System in the event of a spike in traffic.

The addition of five Motorway lanes will cost £1.4m with an additional estimated £250k of operational costs plus the ongoing costs of maintaining these. This would be large enough to cope with an additional 2,250 Service Requests per second. Each DCC User currently has the ability to submit 30,000 transactions per second.

Regardless of how many additional 'Motorways' could be added, a spike in Service Requests could still result in DSP failure or Service Users being 'crowded out' if the spike was large enough. Implementing the proposed traffic management mechanism at a cost of £1.6m would prevent this regardless of total capacity.

The Disaster Recovery choice was also discounted by the Proposer as in the event that the DSP fails there could be an outage of up to four hours (at an estimated cost to industry of £1m per hour, as detailed in Annex H). Furthermore, if the source of the influx of Service Requests had not been removed or restricted, the Disaster Recovery system would then also fail.

² This cost assumes the worst-case scenario of providing enough Motorway lanes to meet the maximum possible demand and thus provide the same level of protection as the Proposed Solution

³ This cost assumes one use of the DR system lasting four hours

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

The Working Group initially proposed an exemption list for priority Service Requests which would not be regulated even when the mechanism was in operation. 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 prepayment, as it was one 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.

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. However, the Working Group felt that all decisions relating to the traffic management under both [SECMP0062 'Northbound Application Traffic Management Alert Storm Protection'](#) and SECMP0067 should be delegated to the Operations Group. 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 were asked for any additional Service Requests they wanted to see on the list with accompanying rationale. Subsequent discussions with the Working Group highlighted that even if the mechanism was active the DSP would still be vulnerable to large bursts of these priority Service Requests. The DCC therefore agreed to take the advice of the TABASC and not to have a priority Service Request list. Service Users will know by receiving the Http 429 that they have reached their capacity allocation and are being regulated and can then use their own business processes to prioritise their Service Requests as they see fit. This means that the Modification Proposal will move away from the objective of [SECMP0028 'Prioritising Service Requests'](#) which proposed introducing a DCC controlled prioritisation system for Service Requests. Instead, it will allow individual Users to submit their Service Requests in their preferred order within their Capacity Allocation, rather than it being a design of the DCC System to allocate a priority.

Please note that the prioritisation list will still be built into the Proposed Solution as a configurable list but will be left empty upon go-live. If the industry was to later determine that any SRs should be prioritised, the relevant system changes would already be in place to accommodate this. The Working Group agreed that the ownership of the Priority Service Request List will be given to the Operations Group. It will be the responsibility of the Operations Group to agree the process for carrying out amendments to the list in due course. Any process that the Operations Group forms should include consultation with wider industry to agree on any changes to the Priority Service Request List before the Operations Group approves any said changes.

What percentage of total traffic did the proposed Priority Service Request list account for?

The Working Group questioned how much of the current Service Request traffic is made up of the SRs proposed to be on the priority Service Request list. The DCC has confirmed that overall, the proportion of total SRVs fluctuates from 0.5% to 5% depending on User activity and the day of the

week. However, it should be noted that the DCC is recommending no SRs be on the priority Service Request list. This view was supported by the TABASC.

Why is User Integration Testing not six weeks?

The Working Group was concerned that only four weeks had been allocated for User Integration Testing (UIT). The DCC provided the following response:

In terms of this Modification alone, plans for UIT are for two short testing windows to be scheduled in the UIT-B environment. All Service Users will be notified well in advance of when these testing windows will be in operation. The functionality will be enabled through a reconfiguration of parameters. The participating Service User(s) will be invited to send Service Requests and, being subject to traffic overload, will receive a 'system busy' response from the DSP.

The two testing windows will be spaced sufficiently apart to allow any remedial actions to be undertaken by the Service User between the first and second test window.

Proposals for UIT testing of the whole November 2020 SEC Release will be gathered and published as part of the DCC Testing Advisory Document, which is shared with, and approved by, the Testing Advisory Group.

For the November 2019 SEC Release there were 15 days of UIT testing, consisting of five days pre-UIT and 10 days UIT for Test Participants.

The DCC explained that the UIT figures previously presented were only a part of that testing. The testing would be considered as part of the wider November 2020 SEC Release. The Working Group members agreed that this made sense. The Working Group were concerned that if the Final Operating Capability (FOC) release slipped there would be a conflict with the November 2020 SEC Release Testing. It agreed that this was outside the scope of this modification but asked that the potential conflict should be highlighted as a risk.

Following the send back by Ofgem in May 2020 the proposed implementation date has been moved to June 2021. The DCC has allocated six weeks of UIT to ensure Users get the requested amount of time for testing.

What reporting will there be?

The Working Group wanted to know what reporting would be provided and where it would be sourced from. It requested to see a mock report. The DCC has provided wireframes of the proposed reports and this can be found in Annex C.

Additionally, the Working Group questioned how this would be reviewed and how the DCC would deal with Users who were 'persistent offenders' regarding capacity allocation breaches.

The DCC responded that Service Users in breach of their threshold will receive a report each month documenting when and how they breached their threshold and the impact on their SRVs and others. The SEC Panel (or a Sub-Committee nominated by it) will receive a report stating who had breached their threshold and the impact on the overall service. It will then be responsible for holding Service Users to account.

The DCC presented its wireframe reporting documents and asked for comments. One Working Group member questioned if the DSP scheduled activity would always be reduced in a traffic management

event. The DCC replied that the DSP would be aware of the scheduled activity and if a traffic management event were to take place, it would be able to manage the activity to ensure it was processed. One Working Group member suggested that it would be useful to have reporting on the DSP scheduled activity included in the reports presented. They further requested that this should include if the DSP scheduled activity was then carried out and received within or outside the SLA. Another Working Group member suggested that since most of the SLAs for scheduled activity were 24 hours it was highly unlikely they would be delivered outside the SLA, but the Working Group agreed that it would be good to have this information anyway.

The DCC said it would discuss this with its Service Provider to confirm if it was possible to get these figures. If it was, it would include them in the reporting.

Views against the General SEC Objectives

Proposer's views

*Objective (a)*⁴

The Proposer believes that SECMP0067 will better facilitate General SEC Objective (a) by improving the efficiency and protecting the DCC System in times of high demand therefore by reducing the likelihood of a DCC System outage leading to delays in installation and commissioning and prepayment meter top ups.

*Objective (e)*⁵

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.

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 protecting the business as usual process, offering innovation in managing the System and providing a securer energy supply.

First Refinement Consultation respondents' views

The responses from the first Refinement Consultation were mixed towards whether the Modification Proposal should be approved. At the time of the consultation, one of the most common reasons for not supporting the Modification Proposal was the question as to whether this was the best solution for the available funding and that this business case should be explored in more detail. All respondents acknowledged that they would be impacted and that they would incur some cost outside the SEC process in rearranging their business process to accommodate the solution, although not giving definitive figures to these. Only one respondent believed that the Modification Proposal should be

⁴ (a) Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

⁵ (e) Facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy.

accepted, the other respondents citing that further analysis was needed post-consultation before the Modification Proposal should be accepted.

The first Refinement Consultation respondents differed as to whether the SEC objectives were better facilitated, with Objective (a) being agreed with by those who said the objectives were better facilitated, but all respondents believing Objective (e) is left unaffected.

The full set of the first Refinement Consultation responses can be found in Annex F.

Sub-Committee views on the modification

The TABASC reviewed the Modification Proposal's business requirements before a Preliminary Assessment was sought from the 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, however the priority Service Request list has been removed from the solution.

The SSC was consulted in parallel with the Refinement Consultation. It agreed with the rationale that it could help prevent a DoS attack. However, it also noted that the Proposed Solution alone would only make it harder to inflict a DoS attack, not prevent one outright.

The Operations Group was supportive of the modification but was concerned about the priority Service Request list. As mentioned, the functionality for the priority Service Request list remains but currently no Service Requests are listed.

Panel's conclusions

The Panel raised concerns over the wider governance associated with including the Modification Proposal's solution into the Traffic Management Mechanism Document introduced in [SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection'](#). This was due to the Traffic Management Mechanism Document not being live at the time of the Modification Proposal going to Panel, and therefore making a change to that document was called into question. The Panel requested that the mechanism and accompanying details about the capacity allocation formula be moved to a new SEC referenced document. SECAS agreed to this.

One member of the Panel queried if this Modification Proposal could create unintended consequences if it goes live, given the number of other changes being introduced in the November 2020 SEC Release. The DCC stated it would share its testing strategy to ensure confidence that the Modification Proposal wouldn't create any adverse or unintended effects.

Following the Ofgem send back in May 2020 this modification is now targeted for June 2021. Fewer modifications are targeted for implementation in June 2021 and therefore the risk should be reduced.

Authority decision to send back

The Authority determined to send back the Modification Report on 14 May 2020. In its direction, the Authority requested the Modification Report include a clear succinct and complete assessment of the costs and benefits of the three options (the Proposed Solution, the additional 'motorways' and doing nothing). It also requested an assessment of the impacts of moving the modification from the November 2020 SEC Release to the June 2021 SEC Release.

Views on the modification after send back

Changing the implementation date

The DCC identified that one consequence of moving the implementation date to June 2021 was that the changes to DUIS to introduce the Http 429 would not be able to be implemented in June 2021 as there were no plans for a DUIS uplift. In order to ensure the mechanism could be implemented in June 2021 the DCC therefore suggested that the Http503 messages would be sent until the next DUIS uplift took place.

This was reviewed by the TABASC. It was concerned that the appropriate testing should take place and therefore expressed an opinion that the DUIS changes should take place in November 2021. It requested its opinions be shared with the Working Group.

The Working Group was reconvened and updated on the changes, namely the additional clarity to the business case and the change of implementation date to the June 2021 Release. The DCC's proposed approach, which was supported by the TABASC, was that the Http 429 response code would be linked to the DUIS version published in the November 2021 Release. If a User uplifts to that version, it can use the response code. Prior to then, if implemented in June 2021, the solution will use Http 503 responses. The Working Group supported this approach but remained unconvinced by the business case and unconvinced that the Proposed Solution to the Modification Proposal will provide adequate traffic management.

A further question was raised in the Working Group about what happens if the CSP is down. A Working Group member was concerned that the DSP would still 'fill up' to capacity with messages that could not be passed onto the DSP. The DCC subsequently responded that in the situation where there is a CSP outage, the DSP will try to send messages to the CSP for a defined retry period. If the CSP cannot accept them then the DSP will 'time out' fairly quickly and for any On Demand Service Request (with a 30 second Service Level Agreement (SLA)) will return a "Failed to send to CSP" message (Alert N12/error code E20) to the User. Only if the Service Request is Future Dated or DSP Scheduled (with a 24 hour SLA) will the DSP put the Service Request on a "long retry" queue and try again two hours later (for up to 24 hours). The DSP can manage the rate of handling retry messages to ensure it remains within capacity. In all cases, the number of requests sitting in retry queues (long or short) does not impact SECMP0067 or Traffic Management. The solution to this modification is all about managing the rate of receipt of new messages.

Second Refinement Consultation

Of the eight respondents to the consultation, one agreed with the Proposed Solution put forward and seven disagreed. The one respondent who agreed with the solution was a Large Supplier, the seven who disagreed were composed of five Electricity Network Parties and two Large Suppliers. Common reasons put forward by those not in favour were:

- concerns about the DCC System total capacity;
- uncertainty over the cost benefit analysis used for the business case;
- the Priority Service Request list not being populated (even though the functionality for this remained in the solution); and
- that there was no way of knowing how many or how few incidents would be avoided with this solution.

Of the respondents not in favour of the Proposed Solution, they stated that it was difficult for them to provide estimates of costs that would be saved or incurred by this change. Many said that irrespective of cost, it would take significant time and effort to make changes to their systems in order to enable prioritisation of Service Requests. The estimated time taken varied from these respondents anywhere between nine months to 15 months, with 'at least 12 months' being the most common answer. The one SEC Party who approved of the solution stated they would only incur minor implementation costs associated with accommodating the new Http 429 response code, which would be part of a DUIS release they would plan to uplift to. They also stated they would expect any individual User changes to take less than a month if the Modification Proposal were to be implemented as recommended where they were able to use the existing Http 503 response code.

The full responses can be found in Annex I.

TABASC's views

Following the Working Group meeting and the Second Refinement Consultation, the Modification Proposal was brought back to the TABASC for comment. The TABASC was happy that the Working Group had agreed with its earlier verdict of linking a new version of DUIS to the Http 429 response code. SECAS provided the Second Refinement Consultation responses which indicated the majority of respondents wanted a lead time of 12 months. The TABASC noted these views but supported implementation of the mechanism in June 2021, with improvements to the DCC User Interface Specification (DUIS), and thereby the re-try message, implemented in November 2021. Its view was that the DCC System capacity was sufficient and therefore the likelihood of the mechanism being used in the next 12 months was small, giving Parties time to make the necessary system changes. However, the mechanism would be in place should an extreme event take place in this time.

The full set of responses to the Second Refinement Consultation can be found in Annex I.

Panel views

Following the Authority decision to send the modification back to refinement, the updated Modification Report was returned to Panel on 14 August 2020. A Panel member questioned the solution again. Concerns were mainly around prepayment meter commands not being made a priority and Users being capped and not able to send 'enough' Service Requests in an event such as a severe weather event.

SECAS explained that there was the functionality for a Priority Service Request list on which prepayment meter requests could be placed. SECAS further explained that it was currently empty as the Working group, Proposer and TABASC had agreed that if any Service Requests were exempt a situation could arise whereby the DCC system could be overwhelmed by those Service Requests and the traffic management mechanism would not prevent that. These discussions and the decision are detailed above.

SECAS also explained that the capacity allocations included an extra allocation for Suppliers with prepayment meter customers calculated using data from the 'Beast from the East' weather event. The Panel member pointed out that the DCC did not have any significant number of SMETS2 prepayment meters installed at that time. The DCC Panel member confirmed that the data came from Suppliers with prepayment meters installed during that particular weather event and therefore accurately reflected the increase in prepayment meter activity likely to be seen from such an event.

SECAS re-iterated that the business case was clear in the report and the solution was clear, complete

and could be implemented and was ready to be presented to Change Board for the vote. It acknowledged that Parties may not agree with the solution or the business case, but that Parties were able to vote at Change Board to recommend the Authority reject the modification if they so wished.

The Panel agreed the implementation approach of introducing the Proposed Solution's mechanism in the June 2021 SEC Release and the DUIS change in the November 2021 SEC Release, and that it was ready to progress to the Change Board for a second vote and Authority decision.

Appendix 1: Progression timetable

Following the send back by the Authority, this Modification Report will be presented to the Panel on 14 August 2020 with the recommendation it proceeds directly to the Change Board vote.

Timetable	
Event/Action	Date
Modification raised	30 Nov 2018
Initial Modification Report presented to Panel	14 Dec 2018
Modification discussed with Working Group	14 Apr 2020
Modification Report approved by Panel	17 Apr 2020
Modification Report Consultation	20 Apr – 24 Apr 2020
Change Board Vote	w/c 27 Apr 2020
Authority decision to send back	14 May 2020
Modification discussed with TABASC	2 Jul 2020
Modification discussed with Working Group	9 Jul 2020
Second Refinement Consultation	20 Jul 2020 – 3 Aug 2020
Modification discussed with TABASC	6 Aug 2020
Updated Modification Report approved by Panel	14 Aug 2020
Change Board Vote	26 Aug 2020
Authority decision (anticipated date)	30 Sep 2020

Appendix 2: Glossary

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

Glossary	
Acronym	Full term
ADT	Anomaly Detection Threshold
DCC	Data and Communications Company
DoS	Denial of Service
DSMS	DCC Service Management System
DSP	Data Service Provider
DUIS	DCC User Interface Specification
FOC	Final Operating Capability
PIT	Pre-Integration Testing
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SLA	Service Level Agreement
SMIP	Smart Meter Implementation Programme

Glossary	
Acronym	Full term
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TOC	Technical Operations Centre
UIT	User Integration Testing

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’

Annex A

Service Request Traffic Management Mechanism Document version 1.0

Purpose of this Document

This document has been prepared in accordance with SEC Appendix AB ‘Service Request Processing Document’ Section 15.4 where the Service Request Management Mechanism implemented by the DCC has its allocation formula, mechanism parameters and Service User capacity allocation formula clearly defined.

Service Request Management Mechanism Parameter Values

The following table summarises the configuration parameters that will be required in support of this change. Note that while these are as accurate as possible at this stage, the final list is dependent upon the detailed solution design.

Parameter	Summary	Example Value
DSP Capacity	Declared DSP capacity in Requests/Second	1000
Traffic Management Window	The period used for service request counting and management in seconds	1
System capacity Amber threshold	An amber threshold for system usage, expressed in terms of service requests per second	800
System capacity Red threshold	A red threshold for system usage, expressed in terms of service requests per second	900
System deadband period	The period for which system usage must remain below the red threshold value before	10

Managed by

Parameter	Summary	Example Value
	the system traffic management event is cleared, expressed in seconds	
User deadband period	The period for which a user must remain below their red threshold value before the traffic management event for that user is cleared, expressed in seconds	10
Service User Amber Threshold	An amber threshold for User usage rate, expressed as a percentage of their allocation	75%
Service User Red Threshold	The red threshold for User usage rate, expressed as a percentage of their allocation	100%
Service User Allocation	An allocation value for each Service User, expressed as a percentage of total system declared capacity	7.84%
List of Priority Service Requests	A list of service request variants that will be regarded as 'priority' and not subject to traffic management measures	-
System Amber threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the system amber threshold is exceeded	Disable
System Red threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the system red threshold is exceeded	Disable
User Amber threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the amber threshold is exceeded for a User	Disable
User Red threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the system red threshold is exceeded for a User	Disable
HTTP Busy Response Code	The HTTP response code to be returned if a Service Request is rejected due to Traffic Management	429
Retry-After Delay	The static delay value returned as part of the HTTP busy response, expressed in seconds	5

Service Request Management Mechanism Service Capacity Allocation Formula

$$RTHR_u = \frac{ASC}{TMe} * \sum euTMu$$

Parameter	Value
THR_u	Total Throughput Allocation for each User.
R	Throughput Allocation value to the next highest integer number once rounded down.
ASC	Available Service Capacity. Calculated by Total System Capacity (TSCw) minus the System Buffer (BSCw).
TMe	Total number of Weighted Meters by User Role (e).
$\sum_{eu} TMu$	The sum of meters over all User Roles (e) for that User (u). This is calculated by ($\alpha e \times NSMeu \times PPMu$) with αe being the Charging Group Weighting Factor, $NSMeu$ being for each User (u) and their User Role (e), the number of Enrolled Smart Meters for which Users act in that Role and $PPMu$ is a Pre-Payment Multiplier to give additional weighting to Users that manage Pre-Payment meters.

Service User Capacity Allocation Formula

The Service User Capacity Allocation formula detailed below has been provided by the DCC to explain how it functions and its rationale.

The proposed capacity allocation formula operates at a SEC Party ID level and is built on the weighted proportionality principle, that is, each allocation is scaled using one or more weighting factor. To ensure fairness, capacity will be allocated on a basis that is clear and does not disadvantage any one user. Two considerations are applied here:

- Allocation based on installed devices to which that user has an allocated role, and
- Allocation based on the financial contribution of that user to the DCC system, as measured by the Users' charging group weight factor.

These two factors are combined multiplicatively. Thus, if either of the factors is zero the weight itself becomes zero. Consideration is also given to the expected additional volume of service requests required to manage pre-payment customers relative to non-prepayment customers.

The proposed formula also guarantees a minimum allocation that Other Users receive. This will guarantee that even Other Users are given some allocation. The two factors (meter estate and charging group) incorporate aspects of fairness, in the sense that Users who pay most and those with the most customers and the most meters to serve will receive larger allocations than smaller Service Users. These two principles, minimum allocations and weighted proportionality, form the base for a fair and equitable capacity allocation formula.

The two weighting factors are calculated by the following methodologies below.

The first weighting factor is the number of smart meters that the Service User is responsible for, sourced from the Smart Metering Inventory. A growth factor taken from the previous month's growth for that Service Users is applied to the number of smart meters to calculate monthly meter volumes for the month to which the allocation formula applies (t+1).

The second factor is a Service Users' charging group weight factor, taken from the annual charging statement. As Gas Transporters, RSA's and OU's are omitted from the charging group weighting factors, a proportion of the active charging groups weighting factors are reallocated to them, as shown in Tables 1 to 3 below.

Table 1 – Key Weighting Factors

SEC Party Details	SEC Party ID	SEC Role	Group Weighting	Total Meters at time t+1
Service User A	A001	Electricity Supplier – Import	0.490	5,000
Service User A	A002	Gas Supplier	0.370	3,500
Service User B	A003	Electricity Supplier – Export	0.080	1,200
Service User C	A004	DNO	0.060	7,200
Service User D	A005	Gas Transporter	0.000	7,250
Service User E	A006	RSA	0.000	3,000
Service User F	A007	Other User	0.000	10,000

Note: The values provided in the table are for illustrative purposes only.

Table 2 – Charging Group Weight Adjustment

Group	Share
Share of Capacity Allocated to Service Users With a Charging Group ID	95%
Share of Capacity Allocated to Service Users Without a Charging Group ID	5%

Note: The values provided in the table are for illustrative purposes only.

Each charging group weighting is multiplied by 95%, with the balance of 5% allocated to those Service Users without a charging group weighting. This weighting will be calculated based on the proportion of actual SRV's originating from those Service Users without a charging group weight. This methodology and the resulting calculation will be agreed and regularly reviewed by the Panel.

Table 3 – Charging Group Weight Adjusted

SEC Party Details	SEC Party ID	SEC Role	Charging Group ID	Adjusted Charging Group Weighting
Service User A	A001	Electricity Supplier – Import	g1	0.4655
Service User A	A002	Gas Supplier	g3	0.3515

Managed by

Service User B	A003	Electricity Supplier – Export	g2	0.0760
Service User C	A004	DNO	g4	0.0570
Service User D	A005	Gas Transporter	g5	0.0400
Service User E	A006	RSA		0.0099
Service User F	A007	Other User		0.0001

Note: The values provided in the table are for illustrative purposes only

The next step is to adjust the Smart Meter Volumes by the Pre-Payment Multiplier to reflect the higher expected traffic volume of Pre-Payment customers. This is done by multiplying the percentage of a Service Users customers that are pre-payment customers by the pre-payment multiplier (which represents the increased volume of service requests from pre-payment customers) by the number of meters that a Service User is responsible for. The output is in the final column in Table 4 below.

Table 4 – Adjust Smart Meter Volumes by Pre-Payment Multiplier

SEC Party Details	SEC Party ID	SEC Role	Percentage Pre-Pay Customers	Pre-Pay Multiplier	Adjusted Number of Installed Meters at time t+1
Service User A	A001	Electricity Supplier – Import	16%	1.2	5,960
Service User A	A002	Gas Supplier	16%	1.2	4,172
Service User B	A003	Electricity Supplier – Export	0%	1.2	1,200
Service User C	A004	DNO	0%	1.2	7,200
Service User D	A005	Gas Transporter	0%	1.2	7,250
Service User E	A006	RSA	0%	1.2	3,000
Service User F	A007	Other User	16%	1.2	11,920
Total	-				40,702.0

Note: The values provided in the table are for illustrative purposes only.

The next step is to define the system's capacity and the proportion that will not be allocated (the buffer) to ensure capacity is provided for priority service requests during periods when the solution is active.

Table 5 – Key Weighting Factors

Capacity	Available Capacity	Buffer Zone
Transactions Per Second	270	30

Note: The values provided in the table are for illustrative purposes only.

The next step is to calculate the Weighted Number of Smart Meters Associated With a User Role, by multiplying the weighted charging group value for the role (e.g. 0.466) from Table 6, by the adjusted number of meters that Service User is responsible for in that role (e.g. 5,960), from Table 6. For Example, Service User A's weighted smart meter volumes for its role as an Electricity Import Supplier is calculated as below;

Table 6 – Weighted Number of Smart Meters Associated With a User Role

SEC Party Details	SEC Party ID	User Role	Charging Group Weighting	Adjusted Number of Installed Meters at time t+1	Weighted Smart Meter Volumes at time t+1
Service User A	A001	Electricity Supplier - Import	0.466	5,960	2,774
Service User A	A002	Gas Supplier	0.352	4,172	1,466
Service User B	A003	Electricity Supplier - Export	0.076	1,200	91
Service User C	A004	DNO	0.057	7,200	410
Service User D	A005	Gas Transporter	0.0400	7,250	290
Service User E	A006	RSA	0.0099	3,000	30
Service User F	A007	Other User	0.0001	11,920	1
Sum					5,063

The final step is then to divide the sum of weighted Smart Meters from Table 7 (e.g. **5,063**) by the total available capacity from table 6 (e.g. **270**) to calculate the allocated capacity per smart meter. This number is then multiplied by the total number of weighted smart meters for each service user from Table 6. For example, Service User A's allocated capacity would be:

$$\left(\frac{5,063}{270}\right) \times (2,774 + 1,466) = 226 \text{ tps or } 84\%$$

Each Service User is allocated a percentage share of capacity, ensuring that the DSP can transparently reallocate capacity in the event that capacity increases are introduced after a Service Users allocation share has been calculated.

Each Service User will have their transactions per second allocation rounded down with the exception of those service users who have an allocation of below 1 transaction per second, who will see their allocation rounded up. By rounding down, this ensures that allocated capacity cannot exceed available capacity. See Table 7 below for an illustrated example with Service User A's capacity.

Table 7 – Capacity Allocation

SEC Party Details	SEC Party ID	Capacity Allocation (Transactions Per Second)	Percentage Allocation for time t+1
Service User A	A001 + A002	226	84.33%
Service User B	A003	4	1.49%
Service User C	A004	21	7.84%
Service User D	A005	15	5.60%
Service User E	A006	1	0.37%
Service User F	A007	1	0.37%
Total		268	100%

Note: The values provided in the table are for illustrative purposes only.

For the purposes of the calculations, the DCC shall determine the number of Enrolled Smart Meters for which a User acts in a User Role based on the DCC's reasonable estimate of the number of Enrolled Smart Meters that there will be at the end of the 15th day of the month in respect of which the calculation applies.

Priority Service Requests

DUIS Reference	Service Request	Service Request Variant	Service Request Name

This table is currently not in use.

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’

Annex B

Business Requirements – version 2.0

About this document

This document contains the detailed context and business requirements to deliver SECMP0067.

Context

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. Currently all Service Users are impacted whether they are responsible for the overload or not, and this may result in critical messages to their customers, such as prepayment top-ups, being delayed with potentially serious consequences.

This proposal is designed to:

- provide reliable and predictable System behaviour under extreme load conditions;
- ensure Service Requests identified as priority are delivered in a timely fashion even under extreme load; and
- control the Service Requests of only those Service Users whose use of the service exceeds their allotted capacity.

As part of the DCC's Impact Assessment, they will be asked to define key elements of the proposed solution's operating model, which will include but not be limited to:

- The expected duration of how long the solution will be active when triggered;
- Provide a "layman's terms" version of the solution's allocation formula and explain every variable element; and
- How frequently they expect the solution to be triggered (how many times in a month).

Business Requirements

SECMP0067 business requirements

The following business requirements have been agreed for SECMP0067:

Requirement 1: The DCC will clearly define a formula/calculation and operating model that will be used to allocate individual Service User capacity in the event of the DSP capacity threshold being breached.

The DCC Systems will use a clearly stated formula/calculation and operating model to allocate Service User capacity to each Data Service Provider (DSP) Service User in the event of the DSP capacity threshold being exceeded. The result of this formula/calculation will be a percentage of the total capacity allocated to each Service User. This formula will be measured against a Service User's current portfolio rather than number of initial installations, unless a Service User has no current portfolio.

Requirement 2: The DCC System will include a clearly defined and configurable list of Priority Service Requests for when the solution's mechanism is operational.

The DCC Systems will contain a fully configurable list (see Appendix A) which explicitly states the Service Request Variants which are listed as Priority requests when the capacity allocation mechanism is operational. These Service Requests will not be throttled by the mechanism, therefore all submitted Service Requests will be counted but all Priority requests will not be subjected to capping.

The Priority Service Requests to be included on this list upon SECMP0067's implementation are recorded in Appendix A. This list may be revised from time-to-time by TABASC.

Requirement 3: Service user capacity allocations will be updated monthly.

The DCC will update the individual DSP Service User allocations on a timely basis agreed by industry (initially one month but may be revised if industry agrees) in order to keep an updated and accurate account of Service User capacity that aligns to their portfolio size. This list will only show the individual capacity allocation to that specific User and the DCC will ensure this updated list is made available to all Service Users in advance of the revised allocations taking effect.

Any reallocation of capacity between Suppliers as a result of a Supplier of Last Resort event is to take effect as soon as the process would allow.

Requirement 4: The solution will consider the effects of outages of the DSP systems, including (but not limited to) system maintenance and unexpected circumstances, on any subsequent traffic through the DCC Systems.

The DCC will provide clear analysis and state the courses of action that will be taken when outages of the DSP systems take place due to maintenance and or other unanticipated circumstances. In particular, this should assess the impact on traffic immediately following the end of the outage period.

This will include a process for what Service Users should do between the DSP's outage and it being fully operational.

Requirement 5: The DCC will provide a transparent reporting process to update Service Users on when throttling has taken place.

The DCC will provide reports on a monthly basis (subject to being revised if another timescale is preferred) to inform Service Users on when throttling has been used by DCC Systems and which Service Users have regularly exceeded their determined capacity allocation. This report including Service Users will not be made public, instead being brought to Panel and/or subcommittee confidentially and will be subject to independent audit, if necessary. This report should also specify how many seconds in a day is throttling is required, along with an explanation for any trends or particular events. The report will include the service allocation formula, what the variable elements are set to and state what changes have been made if any. As part of the Impact Assessment, the DCC will provide a copy of what they expect the reporting to look like so the Sub-Committee of the SEC Panel's choosing can agree what they will provide governance on.

The DCC will also provide a means of notifying Service Users when they are having any Service Requests being throttled in the event of the DSP capacity threshold being breached. This will be done via HTTP 503 response to the inbound request.

The DCC will investigate whether it can provide an early warning system to notify Service Users before capacity allocations are breached so that a User can't exceed their defined capacity unknowingly.

Appendix A – Priority Service Request List

DUIS Reference	Service Reference	Service Ref Variant	Service Request Name
3.8.5	1.5		Update meter balance
3.8.9	2.2		Top up device
3.8.10	2.3		Update debt
3.8.11	2.5		Activate emergency credit
3.8.78	6.25		Set electricity supply tamper state
3.8.86	7.1		Enable supply
3.8.87	7.2		Disable supply
3.8.88	7.3		Arm supply
3.8.81	7.4		Read supply status
3.8.98	8.1		Commission device
3.8.104	8.7		Join service (critical)
3.8.106	8.8		Unjoin service (critical)
3.8.113	8.14	8.14.1	Comms hub status update - install success
3.8.114	8.14	8.14.2	Comms hub status update - Install no sm wan
3.8.120	11.3		Activate firmware

SEC Modification Proposal, SECMP0067, DCC CR355

Service Request Traffic Management

Working Group 16th March, Reporting

Version:	0.53
Date:	6th April, 2020
Author:	DCC
Classification:	DCC PUBLIC

1 Reporting

1.1 Report Wireframes with TOC Resource

Report based on Incident Reports, for an event where the SECMP0067 mechanism might be invoked

1.1.1 SEC Panel Sample Report

The first set of reports are for the SEC Panel, with an overall summary of usage against capacity, and tracking individual users.

Service Request Traffic Management

Volumetrics for SEC Panel

Period Start 01/07/2020
Period End 31/07/2020

Number of Events	Total Duration	Number of SEC Parties
8	00:06:20	3

Figure 1: Sample SEC Panel Report, Front Cover, Volumetrics

Event Details for - SEC Party A									
Event ID	Event Start Time	Event End Time	Event Duration	DCC System Capacity	User Allocation %	User Allocation Request/Second	Maximum Request Submission Rate	Total Service Requests Rejected	Total Priority Requests Accepted
Event001	12/07/2020 13:40:13	12/07/2020 13:40:23	00:00:10	1000	7.14%	72	166	514	26
Event002	13/07/2020 14:57:03	13/07/2020 14:58:03	00:01:00	1000	7.14%	72	176	416	21
Event003	18/07/2020 12:15:40	18/07/2020 12:15:45	00:00:05	1000	7.14%	72	210	550	27
Event004	22/07/2020 14:05:45	22/07/2020 14:07:05	00:01:20	1000	7.14%	72	185	609	30
Event005	31/07/2020 20:48:35	31/07/2020 20:49:45	00:01:10	1000	7.14%	72	195	566	28
			00:03:45						
Event Details for - SEC Party B									
Event ID	Event Start Time	Event End Time	Event Duration	DCC System Capacity	User Allocation %	User Allocation Request/Second	Maximum Request Submission Rate	Total Service Requests Rejected	Total Priority Requests Accepted
Event006	10/07/2020 13:40:13	10/07/2020 13:40:23	00:00:10	1000	3.00%	30	47	90	4
Event007	24/07/2020 14:57:03	24/07/2020 14:58:03	00:01:00	1000	3.00%	30	44	137	7
			00:01:10						
Event Details for - SEC Party C									
Event ID	Event Start Time	Event End Time	Event Duration	DCC System Capacity	User Allocation %	User Allocation Request/Second	Maximum Request Submission Rate	Total Service Requests Rejected	Total Priority Requests Accepted
Event001	12/07/2020 13:40:13	12/07/2020 13:40:23	00:00:10	1000	4.50%	45	130	374	19
Event005	31/07/2020 20:48:35	31/07/2020 20:49:45	00:01:10	1000	4.50%	45	118	126	6
Event008	31/07/2020 23:15:40	31/07/2020 23:15:45	00:00:05	1000	4.50%	45	114	144	7
			00:01:25						

Figure 2: Event Details

Traffic Management Event ID	Log Event Time	Request ID	Service User ID	Device ID	SRV	Rejected
Event001	12/07/2020 13:40.001	req001	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	8.4	T
Event001	12/07/2020 13:40.002	req002	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	8.9	T
Event001	12/07/2020 13:40.003	req003	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	6.11	T
Event001	12/07/2020 13:40.004	req004	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	7.4	F
Event001	12/07/2020 13:40.005	req005	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	6.2.1	T
Event001	12/07/2020 13:40.006	req006	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	12.1	T
Event001	12/07/2020 13:40.007	req007	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	11.1	T
Event001	12/07/2020 13:40.008	req008	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	12.2	T
Event001	12/07/2020 13:40.009	req009	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	6.2.7	T
Event001	12/07/2020 13:40.010	req010	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	5.2	T

Figure 3: Overall Service Request Details

1.1.2 User Sample Report

These reports give a general status to each user, indicating how much each user used in the previous month.

Service Request Traffic Management

Volumetrics for - A SEC Party

Period Start 01/07/2020

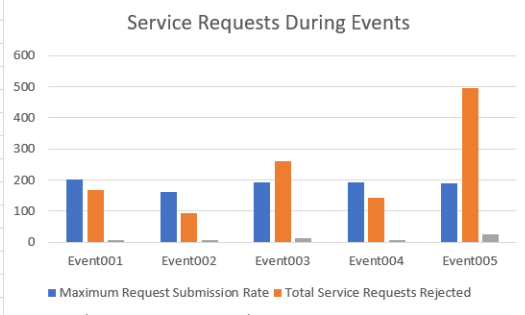
Period End 31/07/2020

Number of Events	Total Duration
5	00:03:10

Figure 4: Sample User Report, Front Cover, Volumetrics

Event Details for - A SEC Party									
Event ID	Event Start Time	Event End Time	Event Duration	DCC System Capacity	User Allocation %	User Allocation Request/Second	Maximum Request Submission Rate	Total Service Requests Rejected	Total Priority Requests Accepted
Event001	12/07/2020 13:40:13	12/07/2020 13:40:23	00:00:10	1000	7.14%	72	201	167	8
Event002	13/07/2020 14:57:03	13/07/2020 14:58:03	00:01:00	1000	7.14%	72	161	93	5
Event003	18/07/2020 12:15:40	18/07/2020 12:15:45	00:00:05	1000	7.14%	72	191	260	13
Event004	22/07/2020 14:05:45	22/07/2020 14:07:05	00:01:20	1000	7.14%	72	191	142	7
Event005	31/07/2020 20:48:35	31/07/2020 20:49:10	00:00:35	1000	7.14%	72	188	495	25
			00:03:10						

Service Requests During Events



■ Maximum Request Submission Rate ■ Total Service Requests Rejected ■ Total Priority Requests Accepted

Figure 5: Event Details

Traffic Management	Log Event Time	Request ID	Service User ID	Device ID	SRV	Rejected
Event001	12/07/2020 13:40.001	req001	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	8.4	T
Event001	12/07/2020 13:40.002	req002	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	8.9	T
Event001	12/07/2020 13:40.003	req003	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	6.11	T
Event001	12/07/2020 13:40.004	req004	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	7.4	F
Event001	12/07/2020 13:40.005	req005	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	6.2.1	T
Event001	12/07/2020 13:40.006	req006	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	12.1	T
Event001	12/07/2020 13:40.007	req007	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	11.1	T
Event001	12/07/2020 13:40.008	req008	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	12.2	T
Event001	12/07/2020 13:40.009	req009	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	6.2.7	T
Event001	12/07/2020 13:40.010	req010	00-11-22-33-44-55-66-77	xx-xx-xx-xx-xx-xx-xx-xx	5.2	T
Notes						
Rejected Column	T = Request was rejected due to Traffic Management Event					
	F = Request was processed as normal during TM Event as the SRV is on the Priority Request List					

Figure 6: User Service Request Details

Potential SRVs for Inclusion as Priority Service Requests

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’

Annex D

Legal text – version 1.0

About this document

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

Section H ‘DCC Services’

These changes have been drafted against version 8.0 of Section H.

Add Section H3.29 as follows:

H3.29 The DCC shall implement a Service Request Management Mechanism that will throttle Service Requests in the event of the DCC Systems’ capacity threshold being breached.

Appendix AB 'Service Request Processing Document'

These changes have been drafted against version 2.0 of Appendix AB.

Add new Sections 15.4 to 15.6 as follows:

15.4 The DCC shall ensure processed Service Requests are subject to the Service Request Management Mechanism defined in the Service Request Traffic Management Mechanism Document. Any changes to this document shall be prepared and consulted upon by the DCC and approved by the Panel.

15.5 The DCC shall ensure that the Service Request Management Mechanism adheres to the following parameters:

- a) Each Service User has potentially multiple (up to 7) User Roles [e].
- b) The number of Weighted smart meters [TM] by User Role [e]. To reflect the varying range of Service Requests available to each User Role, each User Role is weighted by the Charging Group Weighting Factor, as defined in Section K (Charging Methodology), for the Charging Group that corresponds to each User Role.

15.6 The following elements used in the Service Request Management Mechanism are specified in the Service Request Traffic Management Mechanism Document:

- a) The Service User Capacity Allocation [THRu] formula;
- b) The Parameters [TMe] for determining the Service User Total Throughput Allocation [THRu] formula;
- c) Available Service Capacity [ASC]. Calculated by Total System Capacity (TSCw) minus the System Buffer (BSCw);
- d) Smart Meter volumes weighted by User Role used in the Service Request Management Mechanism; and
- e) A worded explanation of the Service User Capacity Allocation formula, its

rationale and how it functions.

Appendix AD ‘DCC User Interface Specification’

These changes have been drafted against version 3.1 of Appendix AD.

Add to Section 2.7 as follows:

Only the following HTTP Response Codes shall be used by the DCC for each of their Web Services:

- 200 The message has been accepted by the DCC Systems. An XML response object is returned to the User, this contains a Response Code that indicates whether the request has passed or failed the business rules for the Service Request.

Note that it is possible for a request to be syntactically correct, but fail subsequent validation. Successful Service Requests will return a Response Code with the prefix “I” (Information) or “W” (Warning). Failed Service Requests will return a Response Code with the prefix “E” (Error).

- 300 The recipient requires that the client redirect its request to the alternative URL provided in the location header field.

- 400 Bad Request – Indicates that the syntax of the request is invalid and the DCC Systems are unable to parse the request.

- 429 Too Many Requests – Indicates that Service Request Traffic Management is in operation, the User has sent too many requests and this request is being rejected.

- 500 Internal Server Error – Indicates that the DCC Systems are malfunctioning.

The User shall send to DCC standard HTTP Response Codes in response to each Service Response, Device Alert and DCC Alert that it receives on its Receive Response Web Service.

Only the following HTTP Response Codes shall be used by the User for each of their Web Services:

- 200 The User has accepted the message.

- 300 The recipient requires that the client redirect its request to the alternative URL provided in the location header field.

- 400 Bad Request – Indicates that the syntax of the request is invalid and the User Systems are unable to parse the request.

- 429 Too Many Requests – Indicates that Service Request Traffic Management is in operation, the User has sent too many requests and this request is being rejected.

- 500 Internal Server Error – Indicates that a User’s Systems are malfunctioning.

Add to Section 2.10, Table 8 as follows:

Error Scenario	Behaviour
DCC Systems unavailable	<p>The DCC shall notify Users if the DCC Systems are unavailable using a HTTP Response Codes of 503 – Service Unavailable (as defined in clause 2.7). This notification may be before the User notices that this is the case.</p> <p>In the absence of any such notification, where a User is unable to access the DCC Services, the User shall check connectivity of their own systems, check for known issues, and for notifications on the Self Service Interface (SSI) before investigation into DCC Systems is performed.</p> <p>If DCC Systems are persistently unavailable, the User may raise an Incident with the DCC.</p>
Invalid Service Request or access control failure	<p>Under these circumstances, the DCC shall return a Service Response with the appropriate Response Code – See clause Error! Reference source not found..</p>
<u>Too Many Service Requests</u>	<p><u>When the volume of Service Requests into the DCC System exceeds the system capacity, then the Service Request Traffic Management system will reject non-Priority Service Requests from a User that is exceeding their capacity allocation.</u></p> <p><u>Under these circumstances the DCC System shall respond with an HTTP Response Code of 429 – Too Many Requests.</u></p> <p><u>The User system shall reduce their request submission rate and re-attempt the failed Service Requests after at least the delay period indicated in the RETRY-AFTER field of the HTTP response.</u></p>

Table 1 : General error handling

SEC Modification Proposal, SECMP0067

Service Request Traffic Management

DCC Full Impact Assessment



Version:

1.1

Date:

12th March 2020

Author:

DCC

Classification:

DCC CONTROLLED

Contents

1	Introduction	3
2	Impact on DCC's Systems, Processes and People	5
3	Impact on the SEC.....	19
4	Testing Considerations.....	20
5	Implementation Timescales and Releases.....	23
6	DCC Costs and Charges	24
7	RAID.....	26
8	Related Documents.....	27
Appendix A – Proposed Formula.....		28
Appendix B –Priority Service Requests		37

1 Introduction

1.1 Document Purpose

The purpose of this DCC Full Impact Assessment (FIA) is to provide the relevant Working Group with the information requested in accordance with SEC Section D6.9 and D6.10.

1.2 Previous information provided by DCC

The DCC Preliminary Assessment was provided on 18/06/2019.

1.3 DCC Contact Details

Please raise any queries regarding this DCC Impact Assessment using the contact details provided below.

Name	DCC - SEC Modification queries
Contact email	mods@smartdcc.co.uk

1.4 Modification Description

This modification proposes the implementation of a traffic management solution to protect the DCC (Data Communications Company) system against Service Request traffic overloads.

The DCC System will scale in line with forecast demand, but at any point in time will have a finite capacity in terms of the Service Requests that can be processed per second. There is therefore a risk that the DCC System could be subject to overload resulting in a failure or degradation that would impact all Users and all Service Requests.

This proposal is designed to:

- Provide reliable and predictable System behaviour under extreme load conditions;
- Ensure Service Requests identified as priority are delivered in a timely fashion even under extreme load; and
- Maximise usage of the DCC System only when the system is close to maximum utilisation by managing only the Service Requests of Users who are exceeding their capacity allocation.

1.5 Requirements

The requirements for this modification have been developed by the Working Group during the Refinement phase and are documented in the Business Requirements v1.0 document [Ref 1] and summarised below. The impact on DCC has been assessed against these Business Requirements.

BR #	Summary	Relevant Sections of this document
1	The DCC will clearly define a formula/calculation and operating model that will be used to allocate individual Service User capacity in the event of the DSP capacity threshold being breached	Section 2.1.1 Appendix A
2	The DCC System will include a clearly defined and configurable list of Priority Service Requests for when the solution's mechanism is operational	Section 2.1.1 Section 2.1.3 Section 2.7.1 Appendix B
3	Service User capacity allocations will be updated monthly	Section 2.7.2
4	The solution will consider the effect of outages of the DSP systems, including (but not limited to) system maintenance and unexpected circumstances, on any subsequent traffic through the DCC Systems	Section 2.1.5
5	The DCC will provide a transparent reporting process to update Service Users on when throttling has taken place	Section 2.1.4 Section 2.8

2 Impact on DCC's Systems, Processes and People

This section describes the impact of SECMP0067 on DCC's Services and Interfaces that impact Users and/or Parties.

2.1 Description of Solution

2.1.1 Overview

Congestion is a problem that can occur on shared networks when multiple users contend for access to the same resources (bandwidth, buffers, and queues). Congestion occurs when network traffic approaches the capabilities of the service, leading to potential delays in transmission and deterioration in the quality of the service. In extreme cases where network traffic exceeds the transmission capabilities of the service, the network can fail, preventing access to the service for all users.

DCC proposes a solution to protect network performance by minimising the intensity, spread and duration of congestion due to unexpected or sporadic shocks (for example severe weather events or Service User system failures). By setting upper bounds on each Service Users traffic, the DCC can better protect Service Users Quality of Service (QoS) and Quality of Experience (QoE). Service Users who commit to not exceed an agreed allocated peak rate, will find that capacity is available when traffic is sent. Above this, traffic will be delivered on a best effort basis (within the limits of available resource). The exception being, that Service Requests identified as high priority and should always be accepted at the gateway.

Service Users will be notified of the DSP System Capacity by the DCC and each Service User will be allocated a proportion of the available capacity based on an agreed formula.

The proposed capacity allocation formula operates at a SEC Party ID level and is built on the weighted proportionality principle, that is, each allocation is scaled using one or more weighting factor. To ensure fairness, capacity will be allocated on a basis that is clear and does not disadvantage any one user. Two considerations are applied here:

1. Allocation based on installed devices to which that user has an allocated role, and
2. Allocation based on the financial contribution of that user to the DCC system, as measured by the Users' charging group weight factor.

These two factors are combined multiplicatively. Thus, if either of the factors is zero the weight itself becomes zero. Consideration is also given to the expected additional volume of service requests required to manage pre-payment customers relative to non-prepayment customers.

The proposed formula also guarantees a minimum allocation that Other Users receive. This will guarantee that even Other Users are given some allocation. The two factors (meter estate and charging group) incorporate aspects of fairness, in the sense that Users who pay most and those with the most customers and the most meters to serve will receive larger allocations than smaller Service Users. These two principles, minimum allocations and weighted proportionality, form the base for a fair and equitable capacity allocation formula.

A full explanation and example of allocation formula is included in Appendix A.

The DCC will notify the DSP of the agreed DSP System Capacity and Service User Capacity settings via the upload of a configuration file in a similar fashion to that used for DCC System Wide Anomaly Detection Thresholds.

It is expected that Service User Capacity settings will be expressed as a percentage of the total capacity, thus allowing the overall DSP System Capacity to be increased without the need for new Service User Capacity settings to be uploaded.

In addition, the DCC will also set amber and red threshold percentages for each of the DSP System Capacity and Service User Capacity, which shall form the basis of the invocation of traffic management.

The DSP will record two new sets of values as Service Requests (SR) are received/ actioned:

1. a count of all SR processed in the last [1] seconds;
2. a count of all SR processed for each Service User in the last [1] seconds.

(Note that this includes DSP Scheduled Service Requests but these will be subject to existing DSP load management features to ensure they are processed at a controlled rate. This rate will be set to ensure that there is always DSP System Capacity available for On Demand requests).

The time period for counting SR will be a configurable rolling interval managed in a similar fashion to the intervals used in anomaly detection, albeit that the interval used for traffic management is expected to be much shorter.

The count of SR over the period shall determine a requests/sec usage value for the DSP System as a whole and for each Service User. These requests/sec usage values will be compared against the DSP System Capacity and the Service User Capacity as follows:

- If the DSP System usage exceeds the amber threshold for DSP System Capacity then a System Usage Warning event will be recorded and notified to the DSP monitoring solution;
- If any Service User usage exceeds the amber threshold for Service User Capacity then a Service User Usage Warning event will be recorded for each Service User and notified to the DSP monitoring solution;
- If any Service User usage exceeds the red threshold for Service User Capacity but the DSP System usage remains below the red threshold for DSP System Capacity then a Service User Excess Usage event will be recorded for each Service User and notified to the DSP monitoring solution;
- If the DSP System usage exceeds the red threshold for DSP System Capacity then a System Overload event will be recorded and notified to the DSP monitoring solution. This event may also be configured to create an Incident in the DSMS if required;
- The system will disable Schedule Activation, DSP Future Dated execution, Low Priority Execution, Certificate Replacement while there is a System Overload event in place;
- If the DSP System usage exceeds the red threshold for DSP System Capacity and any Service User usage exceeds the red threshold for Service User Capacity, then a Service User Overload event will be recorded for each Service User and notified to the DSP monitoring solution. Any Service User who has exceeded capacity will be marked as subject to Traffic Overload.

Once a Traffic Overload event occurs, the processing for each Service User shall operate as illustrated below.

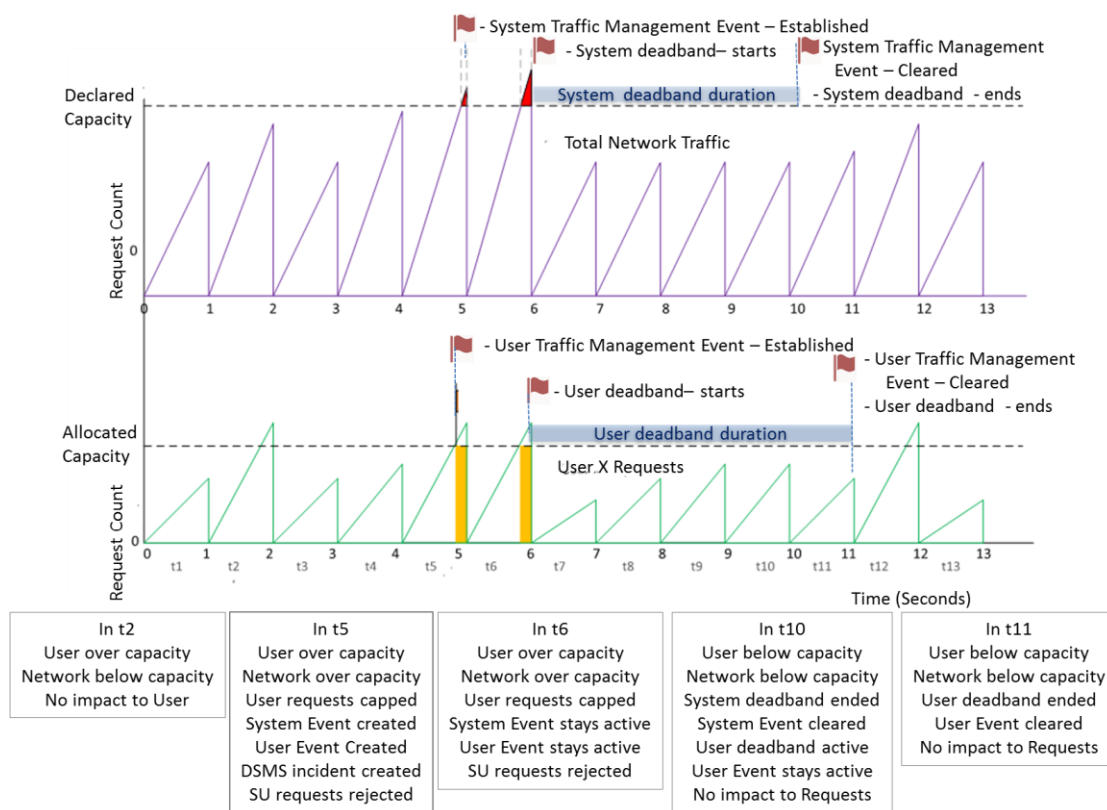


Figure 1 Southbound Traffic Management Processing

Within each [1] second window, the DSP will accept Service Requests up until the Service User reaches their Service User Capacity. At this point, the Service User will be marked as subject to Traffic Overload for the remainder of that window.

The processing at the DSP boundary within the Message Gateway will check whether a Service User is marked as subject to Traffic Overload and if so then the following action will be taken:

- Any Service Request with an SRV which is identified as being subject to Traffic Management will be rejected using a configurable HTTP Status code
- Any Service Request with an SRV that is identified as NOT being subject to Traffic Management will be processed as normal.

The list of which SRVs are subject to Traffic Management will be configurable and held within the DSP solution, updates to this list will be under the governance of a panel to be agreed by the Working Group.

The processing under Traffic Management mode will continue until the DSP System usage returns below the red threshold for DSP System Capacity and stays there for a period greater than the system dead band duration. During the system dead band period if the DSP system goes over capacity there will not be a new event created, instead this will be linked to the existing system traffic management event. Once the rate of messages falls within the system capacity then the dead band window will be restarted. This mechanism will help reduce the number of incidents. The dead band durations for both system and user will be configurable.

(Note: The deadband durations in Figure 1 are kept shorter for illustration purposes; these can be configured for longer durations).

If a Service User who is subject to Traffic Overload returns below the red threshold for Service User Capacity before the DSP System usage returns below the red threshold then that Service User will be cleared of being subject to Traffic Overload.

Otherwise, when the DSP System usage returns below the red threshold for DSP System Capacity then any Service User who is above the red threshold will be cleared of being subject to Traffic Overload.

Events generated by the Traffic Management system, and any Service Requests that are rejected will be recorded and made available to the reporting and monitoring systems.

2.1.2 The Busy Response

When the solution determines that a Service Request will be subject to traffic management and rejected, then the User will receive back a 'Busy' response, this would be an HTTP response with a status code in accordance with RFC7231. Our original proposal was to use a status code of 503 'Service Unavailable' as already defined in DUIS.

Feedback from the Working Group was that the response must indicate clearly the cause of the 'Busy' response, i.e. that it was caused by traffic management action.

We have looked at a number of different options around the HTTP response:

Status Code	Meaning	Observation
429	Too Many Requests	Closely applicable to this use case. Not currently in use by DCC Defined in RFC 6585
503	Service Unavailable	Defined in DUIS. Can be returned by User Gateway F5 loadbalancers if resources unavailable
509	Bandwidth Limit Exceeded	Not currently in use by DCC Unofficial code
529	Site is overloaded	Not currently in use by DCC Unofficial code

Table 1 - HTTP Busy Response Codes

Although the original proposition was to use a 503, this has the disadvantage that it can already be returned for other reasons. The use of 429 provides a response that is accurate in meaning, not

currently used for any other purpose, and correctly indicates that the cause of the issue is too many requests being submitted by the client.

DCC recommends that the HTTP 429 response is used as the 'Busy' response due to traffic management action.

We have also looked at the potential for supplying additional data as part of the response.

Data Item	Carried Via	Comment
Retry-After	HTTP Header field	Returned value indicates the time that should elapse before the message is resent
Specific message	Custom HTTP Header field	A custom header field could be defined, carrying a message that indicates the busy response is due to traffic management action
Specific message/data	Custom JSON object	A custom JSON object could be defined and returned in the HTTP response message

Table 2 - Additional Busy Response data

The 'Retry-After' header field can be used to indicate how long a User system should wait before re-submitting the request. As the traffic management solution will operate on per second time windows re-submissions should be at least one second delayed (to ensure they occur in the next time window).

To provide further clarification that the cause of the 'busy' response is traffic management action, a custom header field could be used, or a data object returned containing a suitable message/data. However if we use a dedicated response code (the 429 as recommended above) then there is no net gain.

We therefore recommend the use of the HTTP 429 response code, this will only be returned as a result of traffic management action, this will include a Retry-After header field with a static (configurable) delay of a few seconds.

2.1.3 Configuration Settings

The following table summarises the configuration parameters that will be required in support of this change. Note that this is illustrative only, the final list is dependent upon the detailed solution design.

Parameter	Summary	Example Value
DSP Capacity	Declared DSP capacity in Requests/Second	1000
Traffic Management Window	The period used for service request counting and management in seconds	1
System capacity Amber threshold	An amber threshold for system usage, expressed in terms of service requests per second	800
System capacity Red threshold	A red threshold for system usage, expressed in terms of service requests per second	900
System deadband period	The period for which system usage must remain below the red threshold value before the system traffic management event is cleared, expressed in seconds	10
User deadband period	The period for which a user must remain below their red threshold value before the traffic management event for that user is cleared, expressed in seconds	10
Service User Amber Threshold	An amber threshold for User usage rate, expressed as a percentage of their allocation	75%
Service User Red Threshold	The red threshold for User usage rate, expressed as a percentage of their allocation	100%
Service User Allocation	An allocation value for each Service User, expressed as a percentage of total system declared capacity	7.84%
List of Priority Service Requests	A list of service request variants that will be regarded as 'priority' and not subject to traffic management measures	See Appendix B
System Amber threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the system amber threshold is exceeded	Disable

Parameter	Summary	Example Value
System Red threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the system red threshold is exceeded	Disable
User Amber threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the amber threshold is exceeded for a User	Disable
User Red threshold incident creation	Enable/Disable the auto creation of DSMS incidents when the system red threshold is exceeded for a User	Disable
HTTP Busy Response Code	The HTTP response code to be returned if a Service Request is rejected due to Traffic Management	429
Retry-After Delay	The static delay value returned as part of the HTTP busy response, expressed in seconds	5

Table 3 - Configuration Parameters

2.1.4 Reporting

The proposed solution will generate event records whenever it operates which will be forwarded to DCC for analysis and reporting.

Monthly reports will be created and made available to both Users and the SEC Panel. User reports will only include data relating to that User, SEC Panel reports will include data relating to all Users.

Reports will identify:

- All events where the traffic management solution took action, including:
 - The SEC Party
 - The capacity allocation of the SEC Party
 - Date, time, duration of the event
- A summary over the reporting period, including:
 - The SEC Party
 - The total number of events
 - The total duration of the events
- The current configuration parameters of the traffic management solution

2.1.5 Handling DSP System Outages

The impact of system outages has previously been raised and considered as part of the SEC Operations Working Group activities. This FIA will not attempt to duplicate that work, but will aim to provide additional information pertinent to the objectives of SECMP0067.

Planned Outages

Planned outages are notified to Users in advance, with the expectation that Users will manage their activities and systems to avoid submitting Service Requests during the outage period. As part of the outage, it is normal for the DCC to close the User Gateway.

When the outage is complete and the User Gateway opened again, Users can begin to submit Service Requests. We can assume that at this point that from each User there is both the normal Service Request traffic rate, plus a backlog of requests waiting to be submitted. Users will also be aware of both the declared DCC system capacity and their own allocation. Request submission rates at this point could be higher than normal in order to clear any backlog, but they should be paced to remain at or below the User allocation rate in order to avoid triggering the Traffic Management mechanism.

Unplanned Outages

Unplanned outages are, by definition, unlikely to provide an opportunity for Users to suspend request submissions therefore exception and error handling will need to be relied upon.

Depending upon the cause of the outage and the effect that it has, User service request submissions may receive no response, a delayed response, or an error response (by error response we are referring to a HTTP Status code response of anything other than 200).

For no response or a delayed response that exceeds the SLA, the initial action should be to initiate a 'short retry' sequence. The request should be re-submitted a number of times, typically two further attempts, with increasing delays between them. For example the second attempt could be after a delay of 45 seconds, then wait for 60 seconds before trying a third attempt, waiting 75 seconds for a response before failing if there is no response.

Failure of a short retry sequence could, if considered appropriate based on the Service Request, context, and business scenario then initiate a 'long retry' sequence.

The 'long retry' sequence should consist of a number of 'short retry' sequence attempts, with increasing delays between each attempt. For example:

- Short Retry sequence 1
- Long retry delay of **1 hour**
- Short Retry sequence 2
- Long Retry delay of **2 hours**
- Short Retry sequence 3
- Long Retry delay of **4 hours**

- etc....

This would continue up to a maximum retry time of for example 24 hours.

If an HTTP status error code (other than 200) is received, then the User system should take action based upon the error code.

HTTP Code	Meaning	Action
300	Re-direct	Re-direct the request to the URL provided in the location header field
400	Bad Request	Syntax of request is invalid – do not attempt to re-submit
429	Too many requests	Reduce the rate of service requests. Re-submit this request after the delay specified in the Retry-After header field
500	Internal server error	Re-submit this request after a short delay
503	Service unavailable	Re-submit this request after a short delay

Table 4 - DUIS HTTP Status Codes

When the issue causing the unplanned outage is resolved, the User is likely to be submitting normal request load plus requests that are being re-submitted as a result of retry attempts (long or short). There is therefore a risk that the Traffic Management system could be triggered. The best mitigation action for this would be for the User system to ensure that requests be retried do not cause the overall request submission rate to exceed the User allocation.

2.2 Affected Components

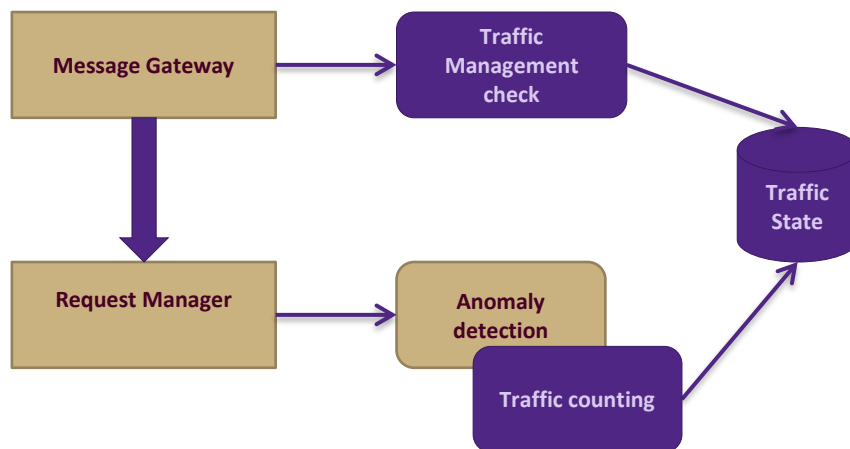


Figure 2 Southbound Traffic Management within DCC Systems

2.2.1 Message Gateway

The Message Gateway component will require changes to determine whether a Service User is subject to traffic overload and if so reject the applicable Service Requests from that Service User with the configured HTTP status code. The Message Gateway will use the new Traffic Management component to determine the traffic overload status.

The Retry-After response-header field will be used with HTTP Status code to indicate how long the requesting Service User should wait before resending the request. This will be populated with an integer that denotes the duration in seconds, provided by a static configuration parameter.

Service Requests which are rejected by the Message Gateway will be recorded in a Rejected Service Requests Log. Each Message Gateway will maintain its own log and these logs will be forwarded to the Reporting Server and the Enterprise Systems Interface in a similar fashion to SAT log files.

2.2.2 Anomaly Detection

The Anomaly Detection service will be amended to count the southbound Service Requests and to manage traffic events. This will introduce new counters for Service Requests at the system level and for each Service User. Anomaly Detection will share the traffic information with the new Traffic Management component.

Anomaly Detection shall add support for creating traffic events that will be recorded in the event logs and reported to the DSP monitoring solution. These traffic events will also be recorded in a Southbound Traffic Management Log which will be forwarded to the Reporting Server and the Enterprise Systems Interface in a similar fashion to the Northbound Traffic Management Log created under CR1066. The traffic rate will be shared with the DSP monitoring solution.

2.2.3 Traffic Management

Traffic Management is a new logical component dedicated to handling the traffic management state. Anomaly Detection will share the traffic counts with Traffic Management. Traffic Management will maintain the traffic state data and will provide an interface for Message Gateway to check if a given Service User is in the Traffic Overload state.

2.2.4 Data Management/Data Model

Data Management will be modified to manage the configuration related to DSP System Capacity and Service User Capacity allocation percentages, from which Service User thresholds are calculated.

Data Model updates are required to support the traffic management processing and the associated configurations.

2.2.5 Request Management

Request Management will be changed to support the changes to southbound Service Request processing due to traffic management. For each new event type, an associated alarm identifier will be introduced in order to allow the DCC Service Management System to identify the incidents.

2.2.6 Transform

The Transform component will not require any changes.

2.2.7 Incident Client

The Incident Client will not require any changes.

2.2.8 Reporting Services

The Reporting Application Server will need a new upload process to load the traffic counts for operational monitoring.

2.2.9 Enterprise Services Interface (ESI)

The new Southbound Traffic Management Logs and the Rejected Service Requests Logs will need to be added to the ESI Reporting interface and delivered to the DCC on a regular basis.

2.2.10 SSI/SSMI

SSMI will need to introduce a mechanism for DCC to upload the configuration file that contains the DSP System Capacity and Service User Capacity settings. This will be similar to the mechanism used for the existing DCC System Wide Anomaly Detection Thresholds.

2.2.11 DCC Service Management System

DSMS will need to support two new incident types corresponding to the System Traffic Management Event and the User Traffic Management Event.

2.2.12 Data Migration

Since this is new functionality there is no need to migrate any existing data, however some database upgrade activity will be required due to changes needed on the existing database tables.

2.2.13 Feature Switches

DSP will implement this Modification with the 'Feature Switch' mechanism in order to allow flexibility in enabling the traffic management functionality during Integration Testing and in Production.

2.2.14 Operational Monitoring

The changes made under this Modification will need to be integrated with the DSP's operational monitoring facilities.

Events created for specific thresholds being breached or cleared will be recorded and made available to the reporting and monitoring systems.

2.3 Non Functional Impacts

Impact on Performance

This change provides the DSP system with the ability to be configured with various parameters and, when certain conditions/parameters are breached, to take appropriate action i.e. to reject certain Southbound Service Requests for identified Service Users.

Functional testing will exercise the various functional scenarios but there needs to be a validation of the design and implementation of the system while under load. For the avoidance of doubt, the rates and thresholds used will be appropriate for the non-functional, performance Test environment and not necessarily the applicable rates/values for Production.

Tests will be devised that show the system processing Service Requests and particular Service User(s) exceeding their limits. Testing will also demonstrate the overall system limit threshold

being exceeded, and the Service User having their Service Requests rejected until the system utilisation returns to within configured capacity. Testing will show the DSP System processing Service Requests normally from other Service Users who remain within their own limits.

It is assumed that no performance testing will take place in any environments apart from DSP's internal PIT environment i.e. no performance testing will take place in SIT or UIT environments.

Impact on Resilience

There is no impact on the underlying resilience of the DSP solution.

Impact on Disaster Recovery

There is no change to the Disaster Recovery solution or BCDR procedures.

Impact on Security

This change includes the implementation of a traffic management solution in the southbound message motorway. There is no impact on the Protective Monitoring because there is no new infrastructure.

Once the traffic management solution is designed there may be a need to include it within scope of a future penetration test to ensure it is configured correctly.

Security Assurance will be provided to:

- Support to the PIT Team during implementation
- Review of design document where there is a potential security consideration
- Review of changes to the security audit trail logging
- Review of test artefacts and outcomes where there is a potential security consideration
- Attendance at meetings where required by the PIT Team
-

2.4 Impact on processing, storage and/or transmission of the DCC Data

The objective of this Modification is to protect the DCC system from high volumes of Southbound Service Requests at the Message Gateway boundary. DCC assumes that the Traffic Overload events will be low in volume and when these occur, they not stay active for very long.

If the Traffic Overload happens for an average duration of 30 minutes a day, with a retention period of 21 days for these log files, the additional storage required is under 2GB of space. This calculation is based on an assumed average of 400 blocked SRs per second with a log record size of 100 bytes. Based on these volumetric assumptions, this change in itself does not warrant the procurement of additional infrastructure.

In the event that the assumptions prove to be invalid then the procurement of additional infrastructure, configuration and ongoing maintenance may be required.

2.5 Impact on Interfaces

The DCC User Interface Specification (DUIS) will require amendment to include the new HTTP Busy response code.

2.6 Impact on Infrastructure

Refer to Section 2.4.

2.7 Impact on Business Processes

2.7.1 Amendments to the list of Priority Service Request Variants

DCC will develop appropriate Business Processes in support of Business Requirement 2, for the amendment of the Priority Service Request list in conjunction with TABASC.

2.7.2 Updates to User Allocations

The DCC will determine the value of each User's allocation on a monthly basis. For these purposes, the DCC shall:

- a) develop, in consultation with Users and the Panel, a methodology for determining allocation and the values used to determine allocation;
- b) periodically (including where directed to do so by the Panel) review such methodology and the list of exempt priority services requests, in consultation with Users and the Panel;
- c) publish on the DCC Website the up-to-date version of such methodology from time to time, together with the outcome of the most recent consultation undertaken in respect of such methodology; and
- d) determine, in accordance with such methodology, the allocation (for each User to apply to each month prior to the beginning of that month; and
- e) notify each User via SSI, prior to the beginning of each month, of that User's allocation to apply during that month.

2.8 Impact on Reporting

The DCC will:

- a) produce a report detailing the circumstances that arose and provide that report to the Panel and the Authority;
- b) send to each User that was affected the section of the report that is relevant to that User (but without revealing the allocations of other Users that were affected); and

- c) respond to any queries raised by the Panel concerning the circumstances that led to the DCC engaging the solution.

3 Impact on the SEC

3.1 Impact on DUIS

Users submit Service Requests in accordance with the DCC User Interface Specification (SEC Appendix AD) where requests are submitted to a DSP hosted web service using an HTTP Post. Each Post will receive a response code from the DSP as described in DUIS Section 2.7. This modification will introduce an additional response code that will be returned when a request is rejected due to the action of the Traffic Management solution.

4 Testing Considerations

This section outlines the testing required to complete the Design, Build and Test phases for this SEC Modification.

4.1 Pre-integration Testing

During Pre-Integration Testing (PIT), each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. Specifically, the development team will carry out unit testing and the build will be subject to continuous build and automated testing to identify build issues at the earliest opportunity.

PIT will operate as a single phase of activity with a single drop. It will consist of a defined subset of system tests being observed by DCC.

4.2 Systems Integration Testing

The SMETS1 and SMETS2 Test Phases will be affected, with testing being conducted in the SIT-B Environment.

Updates to the following SIT Test Artefacts will be required:

- SIT Test Scenarios;
- SIT Test Scripts;
- SIT Test Traceability Matrix;

There will be a new Solution Test Plan and a new Heat map for testing of this Modification, reflecting the test scope defined in a Depth and Breadth document. There are no specific SIT dependencies in addition to those outlined in **Error! Reference source not found.**

It is assumed that Regression and EOC testing will be covered by wider release testing.

Testing Impact:

1. Create a new scenario for ESI for Rejected Services Log for Service Requests rejected by the Message Gateway. The logs are sent to the Reporting Server and Enterprise System Interface and DCC.
2. Create a new ESI test scenario for Southbound Traffic Management Logs for logging of Traffic Events. The logs are sent to the Reporting Server and Enterprise System Interface and DCC.
3. Create a new SSMI scenario to test the ability to upload a configuration file that contains the DSP System Capacity and Service User Capacity settings.
4. Update the existing scenario for the Operational Dashboard that Southbound Traffic Management will be displayed on the operational dashboard. This will be based on the Southbound Traffic Management Logs therefore verify what is being displayed on the operational dashboard against the logs.

Test Approach to verify the correct information is displayed on the logs:

Over time, a “requests per second” usage value for the DSP System as a whole and for each Service User will be determined. Validation of the traffic management functionality in relation to these configurations will generally only be verified during the PIT test stages. However, DSP SIT will develop and execute at least two scenarios within SIT-B to verify that the correct events are recorded within the logs. The scenarios are summarised below:

1. New scenario to execute SRs against two SUs (one SMETS1 & one SMETS2) where one SU the SRs are processed but for the other SU (SMETS1) the SRs are processed where the one SU SRs exceeds the amber threshold. Note the target device is not relevant to this test just chosen to demonstrate this
2. New scenario to process SRs against two Service Users (one SMETS1 and one SMETS2) where the DSP System Capacity and Service User capacity are set where System Usage and for one SU(SMETS2) usage exceeds the red thresholds. (Capacity will require careful consideration to achieve the required behaviour)

Note the target device is not relevant to this test, but has been chosen for demonstrative purposes.

Test Execution:

1. Execute a number of SRs against two SUs. For one SU the number of SRs processed exceeds the amber threshold.
2. Execute a number of SRs against two SUs. The number of SRs executed results in DSP System Capacity and SU capacity are set where System Usage and for one SU usage exceeds the red thresholds.
3. Execute new ESI scenario to verify Rejected Services Log records the correct rejected SRs and is received by DCC and successfully uploaded by DCC
4. Execute new ESI scenario for Southbound Traffic Management Logs and verify the correct Traffic Events have been logged.
5. Execute new scenario for SSML for the ability to upload configuration file that contains the DSP System Capacity and Service User Capacity settings.
6. Execute scenario to view the operational dashboard that the correct traffic events are displayed.

The following functional testing will be undertaken, resulting in the region of 50 tests:

1. Execute new scenario for SSML for the ability to upload configuration file that contains the DSP System Capacity and Service User Capacity settings.
2. Execute a number of SRs against two SUs. For one SU the number of SRs processed exceeds the amber threshold.
 - a. Expected to be between 5 and 10 SRs per SU against one CHF & device set for SMETS1 & SMETS2
3. Execute a number of SRs against two SUs. The number of SRs executed results in DSP System Capacity and SU capacity are set where System Usage and for one SU usage exceeds the red thresholds.
 - a. Expected to be between 5 and 10 SRs per SU against one CHF & device set for SMETS1 & SMETS2
4. Execute new ESI scenario to verify Rejected Services Log records the correct rejected SRs and is received by DCC and successfully uploaded by DCC
5. Execute new ESI scenario for Southbound Traffic Management Logs and verify the correct Traffic Events have been logged.
6. Execute scenario to view the operational dashboard that the correct traffic events are displayed.

4.3 User Integration Testing

The DSP UIT Projects Team anticipates that Test Participants (TPs) may wish to do specific testing of the new features in a UIT environment. This will require additional support effort from the DSP UIT Projects Team. To give value for money, DSP has assumed only one TP will take up the offer of specific functional support, in one UIT environment only.

The Southbound Traffic Management change will be deployed to UIT-B as part of the formal UIT phase associated with the assumed release timetable in section **Error! Reference source not found..** By default, it will operate using the Production Service User settings. As such, the functionality introduced by this change is unlikely to be triggered given the relatively low volume throughput per service user within UIT.

Therefore, in order to perform functional UIT testing for this change, the system and service user parameters in the configuration file for the UIT-B environment will be set appropriately in order to enable the traffic management functionality to be exercised.

Due to the disruptive nature of this change on normal UIT testing activity, two short testing windows will be scheduled in the UIT-B environment. Service Users will be notified well in advance of when these testing windows will be in operation. The functionality will be enabled through a reconfiguration of parameters. The participating Service User will be invited to send service requests and, being subject to traffic overload, will receive a 'system busy' response from DSP.

The two testing windows will be spaced sufficiently apart to allow any remedial actions to be undertaken by the Service User between the first and second test window.

Note that the two testing windows apply to all Service Users, i.e. the testing windows are not scheduled on an individual Service User basis.

For clarity, the scope of supply under this change does not include any UIT based release regression testing. In the event that the Modification is not implemented as part of a major release, then it will be necessary to perform additional regression testing within both the UIT-A and UIT-B environments. The additional regression testing will require a revision to the scope of supply under this Modification and will attract additional charges.

No UIT support for Transition to Operations activities is included (e.g. Operational Acceptance Testing, Business Acceptance Testing or validation of release in the A stream environments). It is assumed that such activities will be covered through a separate Release CR. Performance testing is out of scope since the UIT environments are not performance test environments.

5 Implementation Timescales and Releases

5.1 Change Lead Times

From the date of approval, (in accordance with Section D9 of the SEC), in order to implement the changes proposed DCC requires a lead time of **6 months**.

DCC propose the following implementation plan:

Table: November 2020 Release Timescales

Phase	Start	End
Confirmation of required November 2020 scope	March 2020	
Design, Build, and PIT Test	April 2020	August 2020
SIT Phase	End August 2020	End September 2020
UIT Phase	October 2020	October 2020
Transition to Operations and Go Live	October 2020	November 2020

6 DCC Costs and Charges

6.1 Cost Impact

This section indicates the quote per application development stage for this Modification. Note these costs assume a standalone release of just this SEC Modification without any other Modifications or Change Requests in the release, which is not truly reflective of what the test costs or programme duration will look like. A calculation of those costs will be carried out when the contents of the future Release are finalised and the post-PIT costs determined through a "Grouping CR" also referred to as a "Release CR".

For this SEC Modification, Build and PIT costs are combined into figure, because Build activities will use the PIT environment.

Note that the costs do not include CGI System Integrator testing or SIT and UIT testing by the Communication Service Providers (CSP). Those costs will be included in the Release CR.

£	Design	Build and PIT	SIT	UIT	TTO	App. Support	SP Total
Phase Total	65,095	1,406,345	36,768	55,738	0	65,221	£1,629,167

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.
Systems Integration Testing (SIT)	All the Service Provider's PIT-complete solutions are brought together and tested as an integrated solution, ensuring all SP solutions align and operate as an end-to-end solution.
User Integration Testing (UIT)	Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.
Implementation to Live (TTO)	The solution is implemented into production environments and made ready for use by Users as part of a live service.
Application Support	Any costs associated with supporting the new functionality.

6.2 Impact on Charges

This section describes the potential impact on Charges levied by DCC in accordance with the SEC.

DCC notes that SECMP0067 does not propose any changes to the charging arrangements set out in SEC Section K. DCC has made the assumption that, in the absence of an agreed alternative arrangement by the Working Group, the costs associated with the implementation of SECMP0067 will be allocated to DCC's fixed cost based and passed through to Parties via Fixed Charges.

Subject to the commercial arrangements put in place to support the relevant Release, DCC expects the increase in Charges associated with the implementation of SECMP0067 to commence in the month following the modification's implementation.

7 RAID

There are no Issues at this time.

7.1 Risks

Ref.	Risk Description	Risk Impact
R-001	There is no contingency in the planned timelines	High
R-002	Service User testing could be impacted for short periods whilst the functionality is tested within the UIT-B environment. This will be mitigated through the communication of test plans to Users	Low

7.2 Assumptions

Ref.	Description	Impact
A-001	Reports to be published in support of Business Requirement 5 will be made available via DCC SharePoint	Low
A-002	The solution presented here includes the raising of DSMS Incidents. It is assumed that there is no requirement for the automatic closing of incidents after the related device falls below the device threshold.	Low
A-003	SEC Panel or delegated Sub Committee will provide governance for the list of Priority Service Requests and will notify DCC in advance when these are required to be updated	Low

7.3 Dependencies

Ref.	Description	Impact
D-001	SEC Panel or delegated Sub Committee to provide an agreed list Priority Service Request Variants	Medium

8 Related Documents

Ref:	Title
1	SECMP0067 Service Request Traffic Management Business Requirements – version 1.1
2	SECMP0067 – DCC Preliminary Impact Assessment v1.1
3	SECMP0067 Working Group Consultation Responses

Appendix A – Proposed Formula

The proposed capacity allocation formula operates at a SEC Party ID level and is built on the weighted proportionality principle, that is, each allocation is scaled using one or more weighting factor. To ensure fairness, capacity will be allocated on a basis that is clear and does not disadvantage any one user. Two considerations are applied here:

1. Allocation based on installed devices to which that user has an allocated role, and
2. Allocation based on the financial contribution of that user to the DCC system, as measured by the Users' charging group weight factor.

These two factors are combined multiplicatively. Thus, if either of the factors is zero the weight itself becomes zero. Consideration is also given to the expected additional volume of service requests required to manage pre-payment customers relative to non-prepayment customers.

The proposed formula also guarantees a minimum allocation that Other Users receive. This will guarantee that even Other Users are given some allocation. The two factors (meter estate and charging group) incorporate aspects of fairness, in the sense that Users who pay most and those with the most customers and the most meters to serve will receive larger allocations than smaller Service Users. These two principles, minimum allocations and weighted proportionality, form the base for a fair and equitable capacity allocation formula.

8.1 Process

The DCC will determine the value of each User's allocation on a monthly basis. For these purposes, the DCC shall:

- f) develop, in consultation with Users and the Panel, a methodology for determining allocation and the values used to determine allocation;
- g) periodically (including where directed to do so by the Panel) review such methodology and the list of exempt priority services requests, in consultation with Users and the Panel;
- h) publish on the DCC Website the up-to-date version of such methodology from time to time, together with the outcome of the most recent consultation undertaken in respect of such methodology; and
- i) determine, in accordance with such methodology, the allocation (for each User to apply to each month prior to the beginning of that month; and
- j) notify each User via SSI, prior to the beginning of each month, of that User's allocation to apply during that month.

Where the solution is engaged, the DCC shall:

- d) produce a report detailing the circumstances that arose and provide that report to the Panel and the Authority;

- e) send to each User that was affected the section of the report that is relevant to that User (but without revealing the allocations of other Users that were affected); and
- f) respond to any queries raised by the Panel concerning the circumstances that led to the DCC engaging the solution.

8.2 Allocation Calculation

For the purposes of the allocation throughput formula, the following shall apply:

- (a) Each User's "**Total Throughput Allocation**" (THR_u) shall be determined as follows;

$$RTHR_u = \frac{ASC}{TMe} * \sum euTM_u$$

Where:

- R represents the rounding down of the Throughput Allocation value to the next highest integer
- ASC is the Available System Capacity (described in paragraph b)
- TMe is the total number of weighted meters by user role (described in paragraph d)
- $\sum euTM_u$ is the sum of meters over all User Roles 'e' for that User 'u' (described in paragraph c)

- (b) The **Available System Capacity (ASC)** shall be determined as follows;

The "Available System Capacity" shall be the DCC's reasonable estimate of the maximum number of messages that can be received by the DCC during any one DM Period without materially and adversely affecting the performance of the DCC Systems in their processing of those messages, minus a share of Total Capacity (the 'buffer') held back to accommodate priority messages, when DM is active.

$$ASC = TSC_w - BSC_w$$

Where;

TSC_w is the Total System Capacity

BSC_w is the System buffer

- (c) The **Number of Weighted Meters by User and User Role (*euTMu*)** shall be determined in accordance with the following;

$$euTMu = (\alpha e * NSMeu * PPMu)$$

Where

euTMu is the total number of weighted meters allocated to that user role and user

αe is the Charging Group Weighting Factor (as defined in Section K (Charging Methodology)) for the Charging Group that corresponds to each User Role 'e'. The User charging statement values as they apply to the roles of Import Supplier, Export Supplier, Gas Supplier, and Electricity Distributor are recalculated to distribute a share of the total charging statement value to the User Roles of Gas Transporter, Registered Supplier Agent and Other User. This reallocation is to be agreed by the Panel.

NSMeu is for each User 'u' and their User Role 'e', the number of Enrolled Smart Meters for which Users act in that Role

PPMu is a pre-payment multiplier applied to the number of Enrolled Smart Meters for which a User is responsible to reflect the expected greater number of messages required to manage Pre-Payment Meters. This multiplier is calculated by that taking the average number of messages sent to a Pre-Payment meter and dividing it by the average number of messages sent to non-prepayment meter on the 10th working day of the month in which the allocation is calculated. This is then multiplied by the number of meters associated with Pre-Payment Customer for that Service User and User Role.

- (d) The **Total number of Weighted Meters by User Role (TMe)** is calculated as follows;

$$TMe = \sum e (\alpha e * NSMe)$$

Where;

$\sum e$ represents a sum of the value in brackets across all User Roles 'e'

αe is the Charging Group Weighting Factor (as defined in Section K (Charging Methodology)) for the Charging Group that corresponds to each User Role 'e'. The

User charging statement values as they apply to the roles of Import Supplier, Export Supplier, Gas Supplier, and Electricity Distributor are recalculated to distribute a share of the total charging statement value to the User Roles of Gas Transporter, Registered Supplier Agent and Other User. This reallocation is to be agreed by the Panel.

NSMe is for each User Role 'e', the number of Enrolled Smart Meters for which Users act in that Role;

- (e) The minimum value for a Users total allocated throughput shall be shall be 1 message per DM Period (this excludes the modes 'Device scheduled' and 'Device Future Dated')
- (f) For the purposes of the calculations, the DCC shall determine the number of Enrolled Smart Meters for which a User acts in a User Role based on the DCC's reasonable estimate of the number of Enrolled Smart Meters that there will be at the end of the 15th day of the month in respect of which the calculation applies.

8.3 Example Calculation

The first step is to populate the values of the two key weighting factors. The first weighting factor is the number of smart meters that the Service User is responsible for, sourced from the Smart Metering Inventory. A growth factor taken from the previous month's growth for that Service Users is applied to the number of smart meters to calculate monthly meter volumes for the month to which the allocation formula applies (t+1).

The second factor is a Service Users' charging group weight factor, taken from the annual charging statement. As Gas Transporters, RSA's and OU's are omitted from the charging group weighting factors, a proportion of the active charging groups weighting factors are reallocated to them, as shown in Tables 2 to 4 below.

Key Weighting Factors

SEC Party Details	SEC Party ID	SEC Role	Group Weighting	Total Meters at time t+1
Service User A	A001	Electricity Supplier – Import	0.490	5,000
Service User A	A002	Gas Supplier	0.370	3,500
Service User B	A003	Electricity Supplier – Export	0.080	1,200

SEC Party Details	SEC Party ID	SEC Role	Group Weighting	Total Meters at time t+1
Service User C	A004	DNO	0.060	7,200
Service User D	A005	Gas Transporter	0.000	7,250
Service User E	A006	RSA	0.000	3,000
Service User F	A007	Other User	0.000	10,000

Note: The values provided in the table are for illustrative purposes only.

Charging Group Weight Adjustment

Group	Share
Share of Capacity Allocated to Service Users With a Charging Group ID	95%
Share of Capacity Allocated to Service Users Without a Charging Group ID	5%

Note: The values provided in the table are for illustrative purposes only.

Each charging group weighting is multiplied by 95%, with the balance of 5% allocated to those Service Users without a charging group weighting. This weighting will be calculated based on the proportion of actual SRV's originating from those Service Users without a charging group weight. This methodology and the resulting calculation will be agreed and regularly reviewed by the Panel.

Charging Group Weight Adjusted

SEC Party Details	SEC Party ID	SEC Role	Charging Group ID	Adjusted Charging Group Weighting
Service User A	A001	Electricity Supplier – Import	g1	0.4655

SEC Party Details	SEC Party ID	SEC Role	Charging Group ID	Adjusted Charging Group Weighting
Service User A	A002	Gas Supplier	g3	0.3515
Service User B	A003	Electricity Supplier – Export	g2	0.0760
Service User C	A004	DNO	g4	0.0570
Service User D	A005	Gas Transporter	g5	0.0400
Service User E	A006	RSA		0.0099
Service User F	A007	Other User		0.0001

Note: The values provided in the table are for illustrative purposes only.

The next step is to adjust the Smart Meter Volumes by the Pre-Payment Multiplier to reflect the higher expected traffic volume of Pre-Payment customers. This is done by multiplying the percentage of a Service Users customers that are pre-payment customers by the pre-payment multiplier (which represents the increased volume of service requests from pre-payment customers) by the number of meters that a Service User is responsible for. The output is in the final column in Table 5, below.

Adjust Smart Meter Volumes by Pre-Payment Multiplier

SEC Party Details	SEC Party ID	SEC Role	Percentage Pre-Pay Customers	Pre-Pay Multiplier	Adjusted Number of Installed Meters at time t+1
Service User A	A001	Electricity Supplier – Import	16%	1.2	5,960
Service User A	A002	Gas Supplier	16%	1.2	4,172

Service User B	A003	Electricity Supplier – Export	0%	1.2	1,200
Service User C	A004	DNO	0%	1.2	7,200
Service User D	A005	Gas Transporter	0%	1.2	7,250
Service User E	A006	RSA	0%	1.2	3,000
Service User F	A007	Other User	16%	1.2	11,920
Total	-				40,702.0

Note: The values provided in the table are for illustrative purposes only.

The next step is to define the system's capacity and the proportion that will not be allocated (the buffer) to ensure capacity is provided for priority service requests during periods when the solution is active.

Key Weighting Factors

Capacity	Available Capacity	Buffer Zone
Transactions Per Second	270	30

Note: The values provided in the table are for illustrative purposes only.

The next step is to calculate the Weighted Number of Smart Meters Associated With a User Role, by multiplying the weighted charging group value for the role (*e.g.* **0.466**) from Table 7, by the adjusted number of meters that Service User is responsible for in that role (*e.g.* **5,960**), from Table 7. For Example, Service User A's weighted smart meter volumes for its role as an Electricity Import Supplier is calculated as below;

$$0.466 \times 5,960 = 2,774$$

Weighted Number of Smart Meters Associated with a User Role

SEC Party Details	SEC Party ID	User Role	Charging Group Weighting	Adjusted Number of Installed Meters at time t+1	Weighted Smart Meter Volumes at time t+1
Service User A	A001	Electricity Supplier - Import	0.466	5,960	2,774
Service User A	A002	Gas Supplier	0.352	4,172	1,466
Service User B	A003	Electricity Supplier - Export	0.076	1,200	91
Service User C	A004	DNO	0.057	7,200	410
Service User D	A005	Gas Transporter	0.0400	7,250	290
Service User E	A006	RSA	0.0099	3,000	30
Service User F	A007	Other User	0.0001	11,920	1
Sum					5,063

Note: The values provided in the table are for illustrative purposes only.

The final step is then to divide the sum of weighted Smart Meters from Table 7 (*e.g.* **5,063**) by the total available capacity from table 6 (*e.g.* **270**) to calculate the allocated capacity per smart meter. This number is then multiplied by the total

number of weighted smart meters for each service user from Table 7. For example, Service User A's allocated capacity would be:

$$\left(\frac{5,063}{270}\right) \times (2,774 + 1,466) = 226 \text{ tps or } 84\%$$

Each Service User is allocated a percentage share of capacity, ensuring that the DSP can transparently reallocate capacity in the event that capacity increases are introduced after a Service Users allocation share has been calculated.

Each Service User will have their transactions per second allocation rounded down with the exception of those service users who have an allocation of below 1 transaction per second, who will see their allocation rounded up. By rounding down, this ensures that allocated capacity cannot exceed available capacity.

Capacity Allocation

SEC Party Details	SEC Party ID	Capacity Allocation (Transactions Per Second)	Percentage Allocation for time t+1
Service User A	A001 + A002	22	84.33%
Service User B	A003	4	1.49%
Service User C	A004	21	7.84%
Service User D	A005	15	5.60%
Service User E	A006	1	0.37%
Service User F	A007	1	0.37%
Total		268	100%

Note: The values provided in the table are for illustrative purposes only.

Appendix B – Priority Service Requests

The following is an example of the Priority Service Request list.

DUIS Reference	Service Request	Service Request Variant	Service Request Name
3.8.5	1.5	1.5	Update Meter Balance
3.8.9	2.2	2.2	Top Up Device
3.8.10	2.3	2.3	Activate Debt
3.8.11	2.5	2.5	Activate Emergency Credit
3.8.78	6.25	6.25	Set Electricity Supply Tamper State
3.8.86	7.1	7.1	Enable Supply
3.8.87	7.2	7.2	Disable Supply
3.8.88	7.3	7.3	Arm Supply
3.8.81	7.4	7.4	Read Supply Status
3.8.98	8.1	8.1.1	Commission Device
3.8.104	8.7	8.7.1	Join Service (Critical)
3.8.106	8.8	8.8.1	Unjoin Service (Critical)
3.8.113	8.14	8.14.1	Comms Hub Status Update – Install Success
3.8.114	8.14	8.14.2	Comms Hub Status Update – Install No SMWAN
3.8.120	11.3	11.3	Activate Firmware

Table 5 - Priority Service Requests

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’

Annex F

Refinement Consultation responses

About this document

This document contains the full non-confidential collated responses received to the SECMP0067 Refinement Consultation.

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

Question 1			
Respondent	Category	Response	Rationale
SSE	Large Supplier	No	Given the impacts assessed, there is a potential detrimental effect on systems and processes.
E.ON	Large Supplier	Yes	<p>E.ON is broadly in favour of the proposed solution put forward but have concerns in the following areas:</p> <ol style="list-style-type: none"> 1. How this solution will work with individual/supplier specific retry strategies in the event of a HTTP503 response being received when commands are being throttled. E.ONs retry strategy is currently designed to be specific to SR types and associated DSP timeout values, which would require a high degree of rework to accommodate throttling of unknown duration that this change will introduce. 2. The absence of most installation and commissioning commands from the list of exempt SRs. Join and unjoin commands have been included in the list, but that might be academic if commands before and after unjoin are not included. For example, the orchestration may never make it to the join/unjoin activity causing higher volumes of manual intervention and/or much higher volumes of alerts being generated depending on where the orchestration was stalled due to throttling. 3. The lack of detail regarding backlog management following DSP outages.

Managed by



Question 1			
Respondent	Category	Response	Rationale
			<p>Planned maintenance activity often completes at around 2am, which coincides with other scheduled metering tasks such as checking for available OTA images as well as Supplier scheduled tasks. We don't currently have a high degree of confidence that this would not trigger throttling and much higher failure rates when the DSP comes back online.</p> <p>4. The impact on PAYG installs has not been fully considered if I&C commands are not included in the exempt list, particularly when SMETS2 installs are the only option available.</p>
SSEN	Electricity Network Party	Yes	The Modification proposed looks to provide a suitable solution for providing reliable and predictable system behaviour under extreme load conditions.
EDF Energy	Large Supplier	No	<p>We do not agree with the solution provided, as it does not seem to fully meet the business requirements.</p> <p>Specifically, requirement 5 requires that 'the DCC will provide a transparent reporting process to update Service Users on when throttling has taken place'. The solution to this within the DCC's Preliminary Assessment is that:</p> <p>"Users will receive synchronous responses to Service Requests, and if the request is subject to throttling an HTTP 503 response will be received."</p> <p>An HTTP 503 response only indicates that the service is unavailable, not why – it does not indicate that throttling has taken place. In this situation Service Users will not know why the Service Request are not being processed, or that they could take actions to remedy the situation. This is not transparent, or fit for purpose.</p>

Question 1			
Respondent	Category	Response	Rationale
			<p>The solution also doesn't provide an early warning system to notify Service Users before capacity allocations are breached, although it is noted that this will be investigated further. This would seem to be an important requirement as it would enable Users to take action to prevent the overload scenario for occurring in the first place. Given the potential impacts that throttling of Service Requests has on Users preventing the problem from occurring in the first place should be more prominent within the solution.</p> <p>The Mechanism Service Capacity Allocation Formula detailed in references Pre-Payment Multiplier to give additional weighting to Users that manage Pre-Payment meters. While this is broadly reasonable it is not clear how DCC will determine whether a meter is in prepayment mode or not and apply this to the allocation. As far as we are aware DCC does not hold the payment mode of each smart in the Inventory, so it is not clear how this calculation will be undertaken and relevant thresholds determined.</p>
Electricity North West Limited	Electricity Network Party	No	<p>We have a concern that this proposal results in a significant spend (£1.6m) without any clear volumetric / performance analysis and has the potential to restrict network operators use of the system during extreme weather events.</p> <p>Our understanding is that capacity issues are mostly associated with spurious alerts sent from non-compliant / defective devices. Focussing initially on the root cause around a perceived lack of compliance testing by manufacturers and suppliers may be more beneficial at this stage than progressing this proposed modification.</p> <p>The proposal references "the beast from the east" as an example of how traffic management would protect the DDC network – the implication clearly being that DCC would want to restrict network operators ability to check the Supply Status of customers. When</p>

Question 1			
Respondent	Category	Response	Rationale
			<p>extreme weather events do occur then it is exactly this functionality that network operators need to ensure that we can bring the networks back and ensure that we get customers back on supply. Is it worth considering whether such funds would be better spent by the DCC carrying out a study finding out whether refreshing hardware or adding additional capacity could mitigate any risks around traffic management?</p> <p>Additionally, the traffic management mechanism gives preference to Pre-payment commands but no preference to the ability of the DNO's to read the Supply Status. We already cannot rely on the Power Outage solution alone due to compromises made by the DCC and CSP's without consultation/agreement from network operators and therefore using the option to Read Supply Status is the only effective tool we have.</p>
Western Power Distribution	Electricity Network Party	No	<p>Whilst we agree that it is sensible to have some protection for the DSP in the event of extreme circumstances, we question if this is the best solution. We have concerns that this solution is potentially not addressing the root cause.</p> <p>We would expect this mechanism to be used rarely (if ever) due to the DCC being designed to cope with Users expected traffic and existing protection mechanisms that are in place.</p> <p>We are unsure if using the standard HTTP503 response is the best solution as from a User perspective it will be unclear whether the DCC System is down or if a breach has occurred, and each scenario could require different actions by the users.</p> <p>Also we seek clarification as to how the solution will protect the DSP if their capacity is breached and Users are sending Priority Service Requests?</p> <p>We have concerns as to whether the proposed solution is the most efficient and financially appropriate solution (see comments in Question 10).</p>

Question 1			
Respondent	Category	Response	Rationale
Npower	Large Supplier	No	<p>Whilst we understand the concerns, we feel that this proposed solution is a step too far. This is a near draconian resolution to a problem that could have adverse impacts to commissioning, and therefore the smart rollout. Prior to this step, npower would want to see alternatives that include process controls to prevent this, analysis of the key at risk periods, the points at which differences could be seen in future data SR's and immediate - etc. We feel until these alternatives and proactive approaches are thoroughly investigated, we would be unable to support this kind of throttling. DCC to explore better ways to organise the traffic</p> <p>We would like the DCC to explore other ways to organise the traffic.</p>

Question 2: Will there be any impact on your organisation to implement SECMP0067?

Question 2			
Respondent	Category	Response	Rationale
SSE	Large Supplier	Yes	Our operational teams have assessed the impacts and believe the throttling down of SRs would impact internal systems and processes as each SR has an associated time which would time-out and stop the activities. This would require a re-trigger the SR which impacts the threshold (System Capacity & Service User Capacity), with expenditure costs due to time and resources to resolve the SR issue.
E.ON	Large Supplier	Yes	A full review of automated retry actions would be required to determine the impact during a throttling event and any required changes developed/tested/implemented.
SSEN	Electricity Network Party	Yes	From the modification report, the repurpose of HTTP response code 503 will potentially require some internal system changes.
EDF Energy	Large Supplier	Yes	As a DCC User we would be subject to the Service Request Management Mechanism and so would need to implement business process changes to be able to manage the impact. Depending on the final technical solution we may also need to make changes to our User systems; for example if there is an 'early warning' mechanism and this is sent as a form of alert or other DUIS message.
Electricity North West Limited	Electricity Network Party	Yes	<p>We do feel that more information would help identify the potential impacts, for example:</p> <ul style="list-style-type: none"> • Has the DCC already established at what point a capacity breach may occur? • Have any breaches occurred to date, if yes when and under what circumstances. If no, then when does the DCC forecast reaching capacity given the next phase of the smart meter rollout is up to 2024? • At what point would the solution be expected to actually kick in, what would be the optimum time to implement such a change – if at all?

Managed by

Question 2			
Respondent	Category	Response	Rationale
Western Power Distribution	Electricity Network Party	Yes	Western Power Distribution will be impacted by this change should there be breaches in the DCC system capacity, as we will need to handle the HTTP503 error differently.
Npower	Large Supplier	Yes	This has the potential to disrupt our field and back office services.

Question 3: Will your organisation incur any costs in implementing SECMP0067?

Question 3			
Respondent	Category	Response	Rationale
SSE	Large Supplier	Yes	There will be costs associated with the potential changes to systems and processes however we are unable to ascertain the full extent at this time.
E.ON	Large Supplier	Yes	Analysis, design, development and delivery costs for any required changes to retry capability based on receipt of HTTP503 responses
SSEN	Electricity Network Party	Yes	The costs that would be incurred are currently unknown
EDF Energy	Large Supplier	Yes	Again this will depend on the exact nature of the final solution and whether any system/DUIS changes are required. As currently proposed the costs for implementing SECMP0067 would be relatively low, however as noted in our response to question 1 would do not believe that the current solution is fit for purpose.
Electricity North West Limited	Electricity Network Party	Yes	<p>The proposal mentions “fair share” and we would be interested in additional details of how this has been defined / calculated.</p> <p>Network Users are required to pay DCC charges based upon their respective share of MPANs – we are paying for 2.4m MPANs (smart and non-smart) but only 60k have been enrolled. Our customers would find it difficult to accept continuing to foot the bill while giving the DCC a licence to restrict our use of the system.</p>
Western Power Distribution	Electricity Network Party	Yes	In addition to the implementation costs we will incur if this modification is approved, we will need to update our systems to handle the HTTP503 differently. We don't believe that these costs will be significant.

Question 3			
Respondent	Category	Response	Rationale
Npower	Large Supplier	Yes	Potentially this would impact cost from a install perspective and a number of our teams. Costs tbc.

Question 4: Do you believe that SECMP0067 would better facilitate the General SEC Objectives?

Question 4			
Respondent	Category	Response	Rationale
SSE	Large Supplier	No	There may be merit to this improving the operation of Smart Meter services, objective (a). We disagree that this better facilitates SEC Objective (e) regarding security of supply for end consumers.
E.ON	Large Supplier	Yes	
SSEN	Electricity Network Party	Yes	SSEN agree that this modification would better facilitate General SEC Objective (a)
EDF Energy	Large Supplier	Yes	<p>We agree that SECMP0067 would better facilitate SEC Objective (a) as it should reduce the amount of DCC system downtime that Users that operate within their allocations experience.</p> <p>We do not agree that this change better facilitates SEC Objective (e). We would welcome clarification as to the intent of this SEC Objective as this is not the first time DCC has noted that a change to their systems would better facilitate this Objective. In our view the DCC systems are not an “energy network” as referenced in this SEC Objective.</p>
Electricity North West Limited	Electricity Network Party	No	While we understand the intent of this proposed modification we are not convinced that any General SEC Objectives will be better facilitated by its implementation.
Western Power Distribution	Electricity Network Party	No	We don't agree that this modification would better facilitate SEC Objective (a) by ensuring an efficient operation of Smart Metering Systems as we don't feel that it fully addresses the problem.

Question 4			
Respondent	Category	Response	Rationale
			We disagree that this modification better facilitates SEC Objective (e) as we do not feel that it facilitates Network Operators in innovating the design and operation of their networks to ensure a secure and sustainable supply of energy, especially as Network Operators cannot send SRVs that control the supply to a premise.
Npower	Large Supplier		

Question 5: Noting the costs and benefits of this modification, do you believe SECMP0067 should be approved?

Question 5			
Respondent	Category	Response	Rationale
SSE	Large Supplier	No	We believe that further analysis is required to understand the likelihood of these rare events occurring and whether this would justify the costs of the modification. At current assessment, we do not believe SECMP0067 should be approved.
E.ON	Large Supplier	No	Without additional details provided on the areas of concern outlined in response to Question 1, we would not recommend approval of this proposal.
SSEN	Electricity Network Party	Yes	SSEN agree that this modification should be approved. However, from the illustrative examples in the appendices, it is not clear how much impact this will have on SSEN. Noting the implementation costs, SSEN would also like to understand the current capacity levels and how often this new functionality would potentially be invoked. This would allow SSEN to understand if this is the best solution to address the issue, noting the costs and benefits.
EDF Energy	Large Supplier	No	As noted in our response to question 1 there are a number of issues that would need to be addressed before this Modification should be approved.
Electricity North West Limited	Electricity Network Party	No	Please see our response to Question 1.
Western Power Distribution	Electricity Network Party	No	We are currently unsure whether this modification should be approved. There is a significant cost to implement this modification and there is not a clear benefit case detailed. We can also see that the DCC were asked to advise how often they believe that this throttling would be used but that is unanswered.

Question 5			
Respondent	Category	Response	Rationale
			<p>We question if this is the best solution and whether all other options have been considered, i.e. User ADTs (which are designed to protect against a DoS), or gateway restrictions into the DSP.</p> <p>There have also been no details around the DCC capacity and how much of this is being used to provide any perspective.</p> <p>Finally, due to not knowing the DCC capacity, amongst other factors, (all the values in the legal text are for illustrative purposes only) it is difficult to understand exactly how this modification might impact us.</p>
Npower	Large Supplier	No	As per our comments to question 1.

Question 6: How long from the point of approval would your organisation need to implement SECMP0067?

Question 6			
Respondent	Category	Response	Rationale
SSE	Large Supplier	12 months	There will be lead time associated with systems and processes.
E.ON	Large Supplier	Unknown at this stage	
SSEN	Electricity Network Party	Minimal	The time needed to implement is currently unknown
EDF Energy	Large Supplier	Dependent on final solution	As noted previously this would depend on the exact nature of the final technical solution and whether any system/DUIS changes might be required, for example for 'early warning' alerts. If not then a minimum lead time of three months would be required.
Electricity North West Limited	Electricity Network Party	At least 6 months	Based on any final solution we would need to review our systems and processes and complete any relevant changes.
Western Power Distribution	Electricity Network Party	12 months	Due to potential system changes to handle the HTTP503 error code we require a 12 month lead time.
Npower	Large Supplier		

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

Question 7			
Respondent	Category	Response	Rationale
SSE	Large Supplier	No	Given the lead time required to undertake full impact assessment and delivery of any changes, eight months to implementation date will not be sufficient.
E.ON	Large Supplier	Yes	
SSEN	Electricity Network Party	Yes	Understanding the changes required, SSEN agree with the implementation approach
EDF Energy	Large Supplier	Yes	We agree that this change should be implemented as early as possible subject to a final technical solution being agreed.
Electricity North West Limited	Electricity Network Party	Yes	This does seem a reasonable approach to take.
Western Power Distribution	Electricity Network Party	No	See Question 6.
Npower	Large Supplier	No	We are not supportive of the solution

Question 8: Do you agree that the legal text will deliver SECMP0067?

Question 8			
Respondent	Category	Response	Rationale
SSE	Large Supplier	No	As we do not agree with the actual change being proposed, we are unable to agree that the legal text will deliver SECMP0067 as it currently stands.
E.ON	Large Supplier	Yes	
SSEN	Electricity Network Party	Yes	SSEN agree that the legal text changes are adequate in delivering SECMP067.
EDF Energy	Large Supplier	No	While we broadly agree with the content of the legal text, we note the following comments: <ul style="list-style-type: none"> • The use of the word 'throttle' seems out of place within this legal text – would it be more appropriate to use a term like 'manage' or 'control'. • The legal text does not place any of the obligations on the DCC that are noted in the business requirements – specifically the obligations on providing reporting as to when throttling has taken place. These should be included for completeness.
Electricity North West Limited	Electricity Network Party	Yes	We believe the legal text will deliver the modification as drafted.
Western Power Distribution	Electricity Network Party	No	We believe that there is a misprint on page five of the Traffic Management Mechanism Document, under Table 6 it states 'by the total available capacity from table 6 (e.g. 270)' and we believe that this should read 'by the total available capacity from Table 6-5 (e.g. 270)'.

Question 8			
Respondent	Category	Response	Rationale
			Also according to DUIS there is a Service Reference Variant for all Service Requests and therefore for consistency these should be included in all rows in the Prioritised Service Requests List.
Npower	Large Supplier		

Question 9: Do you have any Service Requests you want added or removed from the list of prioritised Service Requests?

Question 9			
Respondent	Category	Response	Rationale
SSE	Large Supplier	No	These seem reasonable and given that there should be a process by which this SR list can be modified in the future, we have no amendments at this time.
E.ON	Large Supplier	Yes	Additional SRs involved in HAN creation/device join completion as a minimum e.g. 8.11 8.1.1 Configuration can be completed later and would not require a further site visit
SSEN	Electricity Network Party	Potentially	Looking forward, with the uptake of EV, alongside SEC Mod's 25 and 46. It may be required that any SRV's relating to ALCS/HCALCS (7.6, 7.7 & 7.8) may need to be added to the prioritised Service Requests list.
EDF Energy	Large Supplier	Yes	It would have been useful to have the logic for why these prioritised Service Requests have been included on the list as in many cases it is not clear. Where something should be included on this priority list should be driven by the critical nature of sending the relevant command – for example to complete a meter installation while an installer is on site or to put a customer back on supply. It is not clear why the following Service Requests have been included as they do not seem to meet these criteria: <ul style="list-style-type: none">• SRV1.5 (Update meter balance) – we can understand why SRV 2.2 would be included but it is not clear why this one would be time critical.• SRV 6.25 (Set electricity supply tamper state) – it is not clear why this would be a priority or what the impacts of delaying sending this SRV would be.

Question 9			
Respondent	Category	Response	Rationale
			<ul style="list-style-type: none"> • SRVs 8.14.1 and 8.14.2 – We really don't understand the logic behind allocating these as a priority given that there is a time window in which they can be sent in the first place and a short delay will not have any material impact. <p>Consideration should be given to including SRVs 7.5 (Activate Auxiliary Load) and 7.6 (Deactivate Auxiliary Load) as the logic is the similar to enablement and disablement, these SRVs might also be used as part of a time critical demand control event.</p>
Electricity North West Limited	Electricity Network Party	Yes	<p>We would want Service Request SR7.4 Read Supply Status' adding as our requirement.</p> <p>We were concerned that without first agreeing what the likely candidate list is and analysing the impact of those service request volumes on the DCC that it would be difficult to go ahead and develop system changes.</p>
Western Power Distribution	Electricity Network Party	No	<p>We are happy with the SRVs that are currently included on the list.</p> <p>We would like to highlight that if SECMP0046 were to be approved then SRV 7.6 Deactivate Auxiliary Load should be added to the list as this SRV would be used by Network Operators in a situation where the networks are on the verge of being overloaded and would enable supplies to remain on.</p> <p>Please note that we have concerns about Prioritised Service Requests (as per Question 1).</p>
Npower	Large Supplier		

Question 10: Please provide any further comments you may have

Question 10		
Respondent	Category	Comments
SSE	Large Supplier	SSE has been actively involved in all stages of the development of this Mod and have repeatedly challenged both the requirements and the proposed solution as they do not seem to align to the actual problems being faced and place changes upon DCC Users to resolve problems within the DCC Total System. All the changes are toward protecting the DCC without achieving any such protections to those connected to them whilst placing additional obligations upon Users.
E.ON	Large Supplier	N/A
SSEN	Electricity Network Party	
EDF Energy	Large Supplier	There seems to be misalignment between the solution expressed in the Modification Report and that detailed in the DCC's Preliminary Impact Assessment which has made it difficult to understand the exact nature of the technical solution. For example the PIA notes that "The DCC will investigate whether it can provide an early warning system to notify Service Users before capacity allocations are breached so that a User can't exceed their defined capacity unknowingly" – this early warning system is not referenced at all in the Modification Report so it is not clear whether it will ever form part of the actual solution.
Electricity North West Limited	Electricity Network Party	
Western Power Distribution	Electricity Network Party	Western Power Distribution would like to understand if the reports that will be provided to the SEC Panel will only be in the event of a User and/or DCC capacity breach and if so question if there is a need for the SEC Panel to have a monthly report showing capacity compared to usage, even if there has not been a breach event. It would also help highlight if there are concerns regarding capacity prior to a breach event happening.

Managed by



Question 10		
Respondent	Category	Comments
		<p>As per our responses to Questions 1 and 5 we have some questions and concerns that we feel should be addressed.</p> <p>We would also like to understand the comment in the DCC PIA that states:</p> <p><i>Dependency Management/Feature Switch</i></p> <p><i>DSP will implement this CR with the 'Feature Switch' mechanism in order to allow flexibility in enabling the traffic management functionality during Integration Testing and in Production.</i></p> <p>Does this mean that the DCC are planning to release the code with the switch 'OFF', possibly prior to a modification approval in the same way that they have with SECMP0062? If not can this statement be explained?</p> <p>Finally, there is nothing in this proposal that explains the course of action taken to User(s) that constantly breach their capacity allowance. What is the process for addressing the issue at the root cause and not just acting when the situation arises?</p>
Npower	Large Supplier	

SEC Modification Proposal, SECMP0067, DCC CR355

Service Request Traffic Management Worked Example

Version:	0.54
Date:	8th April, 2020
Author:	DCC
Classification:	DCC PUBLIC

How Will the Mechanism Work for a User?

The following is a worked example of how Service Requests (SRs) would be throttled. User traffic rate is mapped over a period and compared to a resulting profile if SECMP0067 was active for a User with an allocation equating to 400 requests/second.

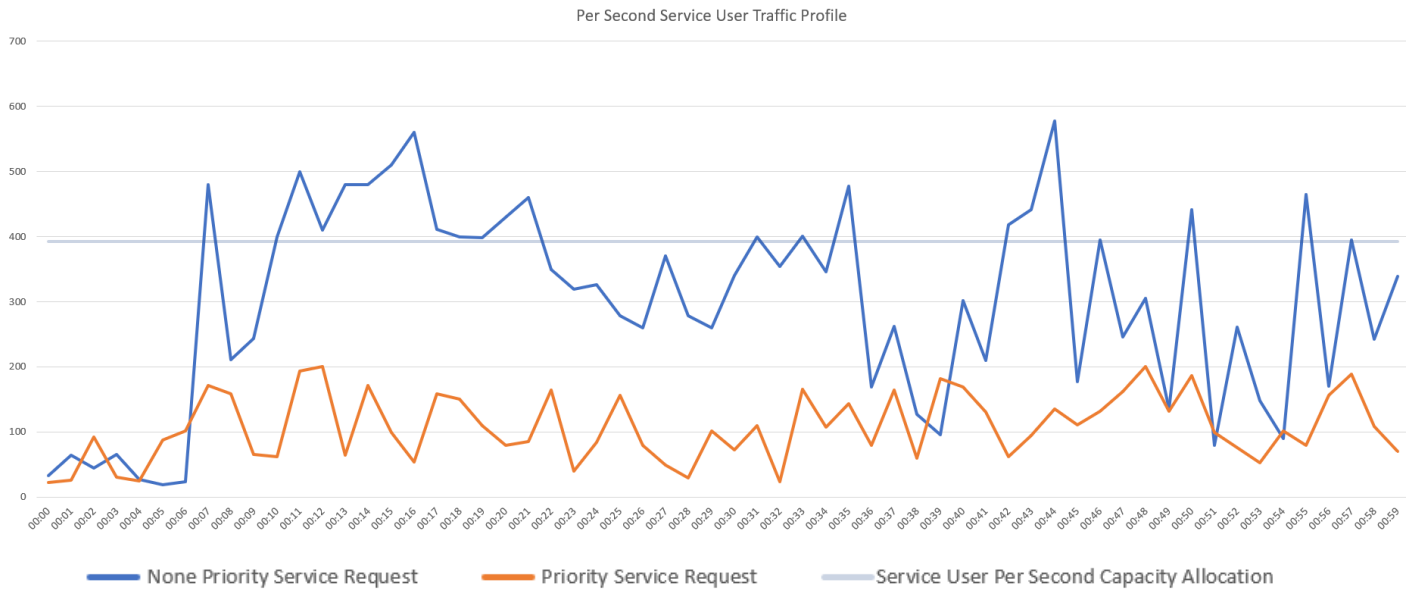


Figure 1: Traffic Management Inactive

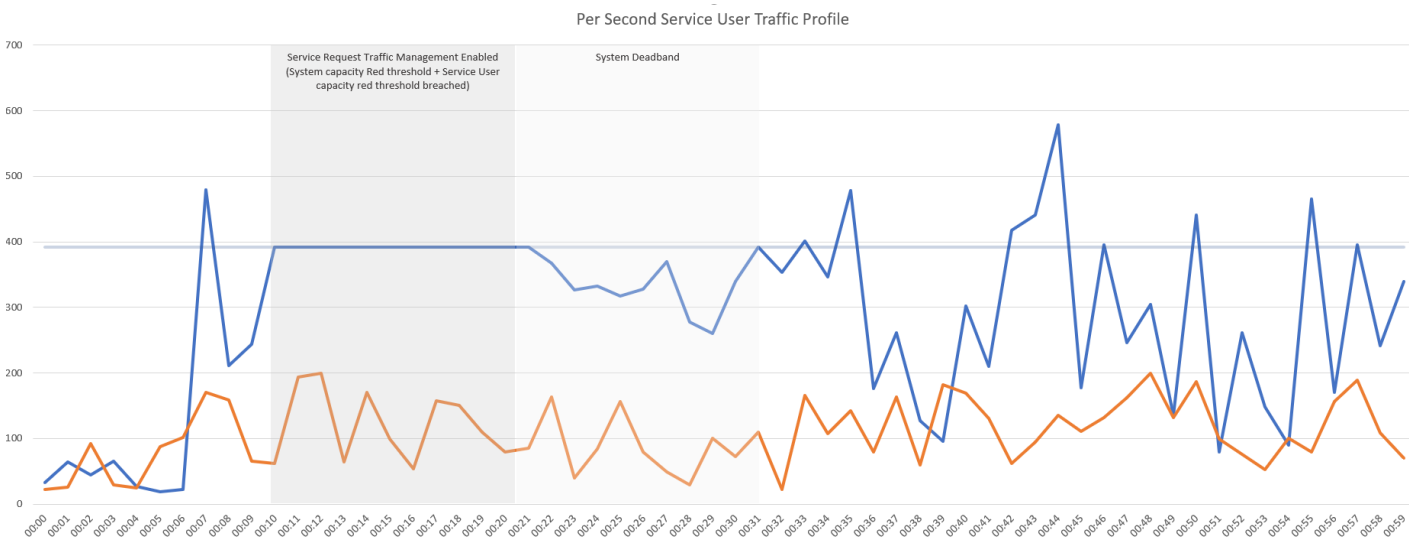


Figure 2: Traffic Management (SECMP0067) Active

Time	Req/Sec	Limit/Accepted	Rejected
00:10	400	400	0
00:11	500	400	100
00:12	410	400	10
00:13	470	400	70
00:14	470	400	70
00:15	500	400	100
00:16	560	400	160
00:17	410	400	10
00:18	405	400	5
00:19	405	400	5
00:20	420	400	20
00:21	460	400	60
Total	5410	4800	610

The impact of the Service Request Traffic Management Enabled (System capacity Red threshold + Service User capacity red threshold breached) is clear as the number of Service Requests are throttled. Also note that the "recovery period" during System Deadband shows that the number of SRs passed is increased towards, but not over, the Capacity Allocation value.

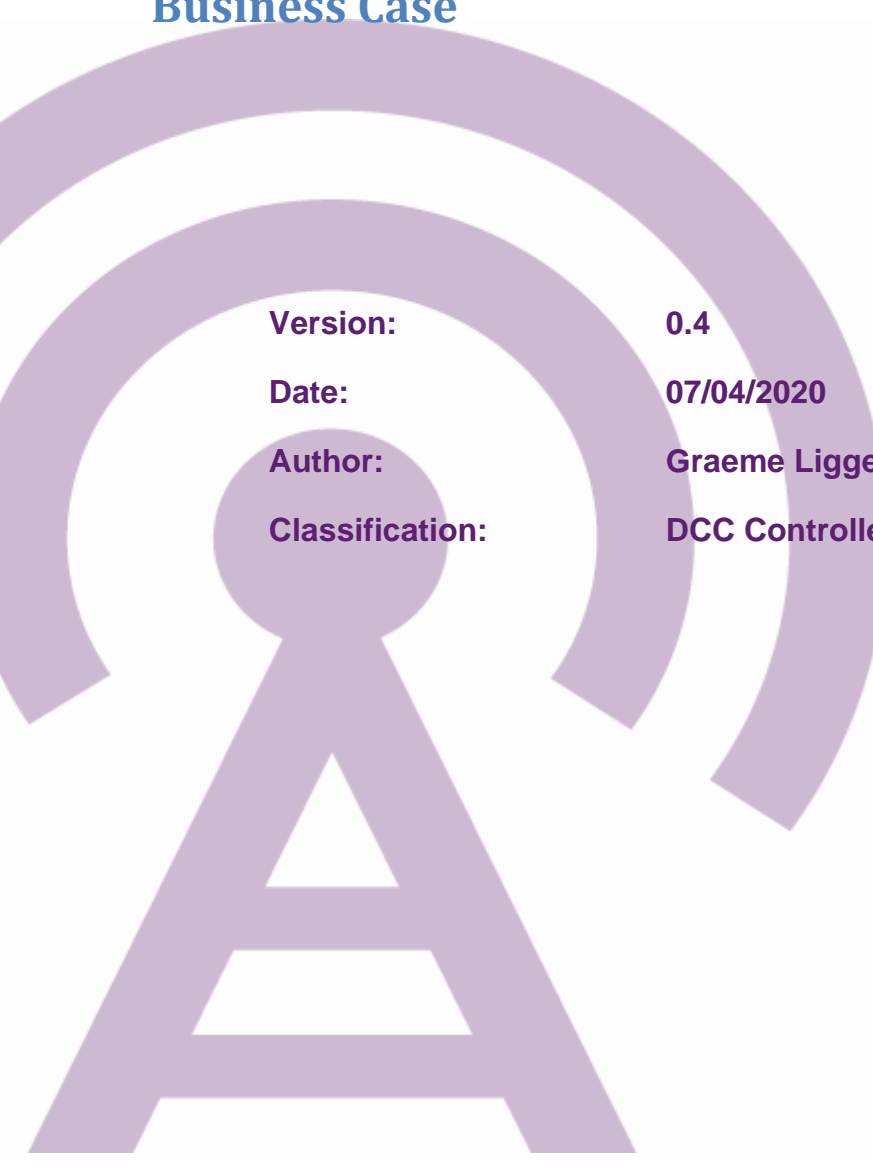
It should be noted that the HTTP Header field contains a RETRY-AFTER value which indicates the time that should elapse before the message is resent by the Service User.

In the example above, the Service User could resubmit the "Rejected" Service Requests 25 seconds after the initial threshold breach, and these would be processed as usual. It will be the responsibility of the Service User to amend their systems to retry the Service Requests, and guidance is provided in the FIA and the WG Consultation response. It will also be in the proposed amendment to DUIS in Annex G of the MRC. This says they should re-submit after a minimum delay as specified in the RETRY-AFTER header.

Service Request Traffic Management

SECMP0067

Business Case



Version:	0.4
Date:	07/04/2020
Author:	Graeme Liggett
Classification:	DCC Controlled

Document Control

Documentation Control

Version	Date	Description	Author
0.1	02/09/2018	Initial Draft	Graeme Liggett
0.2	23/09/2018	Data Updated	Graeme Liggett
0.3	07/04/2020	Update following SECAS review	DCC
0.3	07/04/2020	Updated Section 1.2	Graeme Liggett

Table of Contents

1

Introduction

4

1.1

Summary.....

4

1.2

System Usage.....

4

1.3

Traffic Scenarios.....

6

1.4

Business Case

6

1 Introduction

1.1 Summary

As there are currently no constraints placed on Service Users, the potential demand on the Data Communications Company (DCC) System is unbounded, placing considerable responsibility for cooperative behaviour on the part of Service Users.

Ofgem reports that there are currently 50 active domestic fuel Suppliers in the UK and growing, although not all of these currently have a Gamma connection. Gamma connections to the DCC System are capable of transmitting the equivalent of 30,000 Service Requests per second, based on an average Service Request payload of 2Kbytes. This is equivalent to some 80 billion Service Requests per month, which is 10 times the contracted capacity of the service at scale. Additionally, a single Service User with a 100Mb connection could theoretically introduce up to 5000 Service Requests per second into the DCC System, potentially consuming over half of DCC System resources at scale and a greater proportion of System resources prior to the DCC system reaching full scale over the coming years.

The risk of a single Service User experiencing issues with their back-end systems or human error triggering the transmission of concentrated bursts of large volumes of Service Requests, increases as rollout continues, traffic volumes increase and the number of active Service Users with a Gamma connection increases. The impact of such an incident could be a severe and sustained deterioration in performance or a failure in the service for all Service Users as a single Service User crowds out the activities of others.

It is not feasible, economically viable or efficient to provide a System with infinite capacity, therefore a mechanism is required by which the rate of Service Requests accepted at the Message Gateway can be controlled to prevent a severe and sustained deterioration in performance or a failure in the service.

The solution proposed in SECMP0067 provides a mechanism and mathematical formula to control and share system utilisation across Service Users overlapping traffic flows in a fair, stable and scalable manner. In doing so, this solution aims to smooth statistical fluctuations and reconcile the potentially conflicting notions of fairness and efficiency, across both the Smart Metering Equipment Technical Specifications (SMETS)1 and SMETS2 solutions.

This paper summarises the business case for the proposed SECMP00067 'Service Request Traffic Management'.

1.2 System Usage

Aggregate daily Service Request volumes were five times greater in March 2020 (168 million) compared to April 2019 (38 million). If current trends continue, in another twelve months aggregate monthly volumes could be close to 1 billion a month.

As Service Request volumes increase over time this limits the ability of the DCC system to absorb large volumes of concentrated bursts of traffic, as the rate of average system utilisation increases.

Figure 1-1. Daily Service Request Volumes by Mode of Operation (1st April 2019 to 31st March 2020)

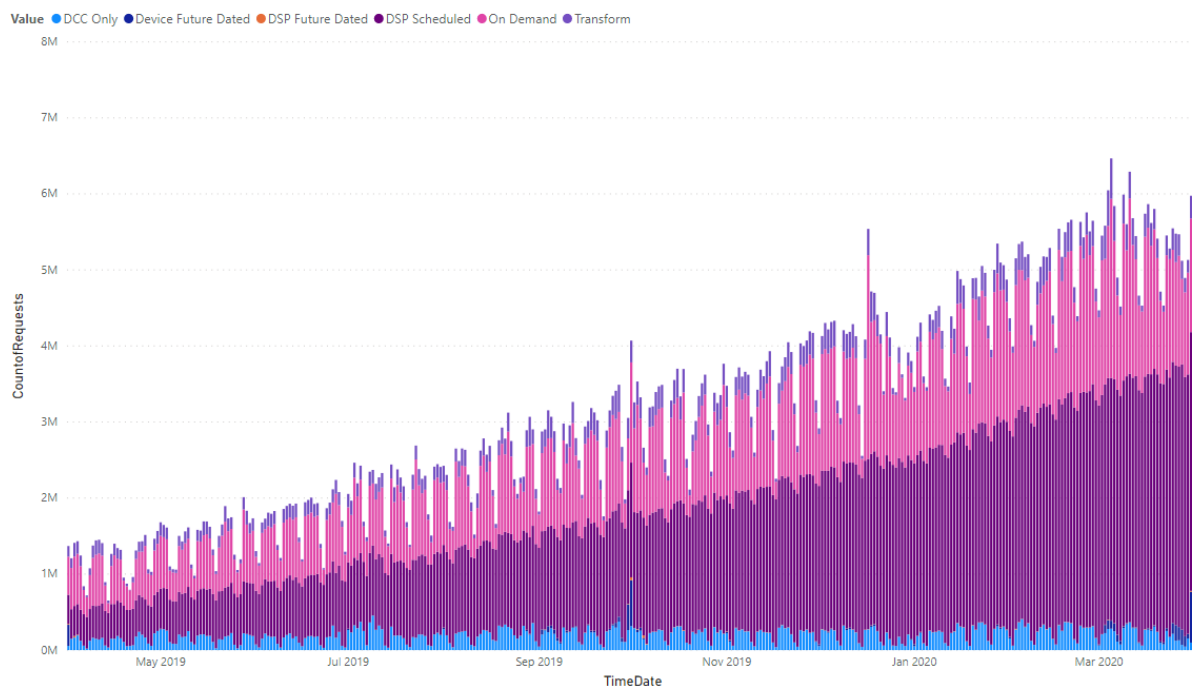
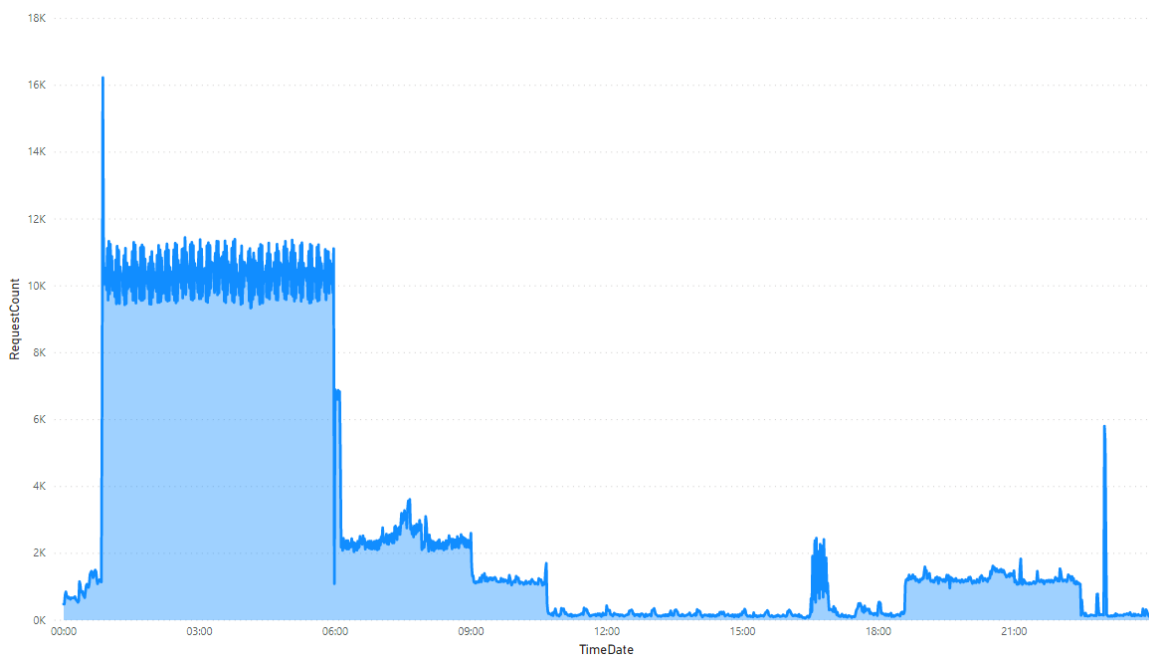


Figure 1-2, illustrates the per minute profile for the 1st March 2020. Approximately 70% of service request traffic is carried between midnight and 6am. This period of concentrated service traffic is when the System is most at risk from environmental shocks such as Service User incidents as utilisation will be at its highest, reducing the services ability to absorb or withstand these events. The DSP capacity as of the 1st March was 1,350 transactions per second or 81,000 transaction per minute. Service Request peak usage on that day, was the equivalent of 20% of DSP capacity.

Figure 1-2. Aggregate Service Requests Per Minute (1st March 2020)



1.3 Traffic Scenarios

The table below summarises the key scenarios against which this Sec Modification is designed to protect Service User traffic against being crowded out by environmental shocks or the technical or human errors of other Service Users and the prioritisation of Service Requests during peak periods of traffic.

Table 1-1. Traffic Scenarios

Scenario	Description	Risk of Occurance
Service User Technical or Human Error	A technical or human error within a Service Users systems triggers a Service User to submit a days or a months volume of Service Requests in a matter of minutes or seconds.	Service User issues with their back-end systems are monthly events. New entrants to the market increase this risk as their back-end systems may not be as developed as existing Service Users. At least one event in the past 12 months led to a Service User triggering the submission of Service Request volumes many times their expected volume
Denial of Service Attack	Denial of service events in which the perpetrator seeks to make network resource unavailable by temporarily or indefinitely disrupting services may prevent service users from submitting priority service requests and responding to the needs of vulnerable customers	Denail of Service Attacks grow in frequency and impact each year, especially targeting critical infrastructure. A recent attack on a US energy company in March 2019 led to “ <i>interruptions of electrical system operations</i> ” for more than 10 hours. The risk to of such attacks only increase as the service scales, with at least one likely in the next two years
DCC System Failure	System failure over extended periods may create a backlog of priority service requests that under the current system would not be prioritised above other service requests	DCC’s target availability measure of 99.99% implies the equivalent of a service outage of 1 hour each year. Environmental factors creating physical damage to key components or critical events such as Telefonica’s network outage in December 2018 could see a service outage for an extended period of time

1.4 Business Case

Concentrated high volume bursts of traffic from one Service User could monopolise the capacity of the DCC System preventing other Service Users from running their business process, installing smart meters, vulnerable customers from topping up their pre-payment meters and Service Users from responding to consumer queries.

The impact and likelihood of these events occurring increases over time and as the volume of meters connected to the system scales. As an example, the financial impact of a one hour disruption to Service Users activities is considered below.

Table 1-2. Business Case

Business Case	Financial Impact
Delays to the Installation and Commission Process	A one hour delay to the installation and commission process across a workforce of 10,000 engineers would result in the loss of 10,000 workforce hours, which at a cost of £20 per hour per engineer, is equivalent to £200,000. This may result in additional costs in the form of missed appointments, which would need to be rebooked, to the frustration of customers and require engineers to work overtime to complete their target number of installations

Vulnerable Consumers May be Unable to Top-Up Their Pre-Payment Meters	A one hour delay to consumers being unable to top-up their meters could create thousands of additional calls to the affected Service Users call centre. With nearly 5 million pre-payment customers, if 1% of these are unable to top-up and call a Service Users call centre this could create an additional 50,000 calls to the call centre, at a typical cost of a call made to a call centre of £5, this would equate to £250,000. Additionally the call centre would be unable to assist these customers as they could not interact with the meter
Disruption to Business Processes	A one hour delay to business processes at critical times may push these outside of the operational windows of a Service User which may disrupt a Service Users internal data processing processes. Industry wide disruption to the timing of business process would likely be in excess of £250,000
Inability to Respond to and Address Customer Issues Efficiently	Service Users may not be able to respond to consumers who have directly contacted them due to issues or questions related to their smart meters which could lead to customer dissatisfaction. Across industry this could result in lost efficiency gains from Smart Meters in excess of £100,000
Negative Press coverage	Disruption to the service and any associated negative or harmful consumer experiences reported by the press could suppress customer interest in smart meters and slow the roll-out and delay consumers and Service Users sharing the benefits of the Smart Metering Programme. Smart Energy GB, reportedly spent £20m on advertising in 2016. If negative publicity around any events is only equivalent to 1% of this budget, its value would be £200,000

The combined cost of these impacts for a 1 hour disruption to the service could be in the region of £1 million. Disruption for periods in excess of an hour will obviously see these costs escalate.

This document is classified as **RED**. It contains non-disclosable information and is restricted to Panel Members (including alternates). Participants must not disseminate the information outside of the governance group. **RED** information may only be discussed during a meeting where all participants present have signed a declaration form, stating their acceptance to abide by these terms. **RED** information should not be discussed with anyone who is not a member of the governance group.

SECMP0067 ‘Service Request Traffic Management’

Annex I

Second Refinement Consultation responses

About this document

This document contains the full confidential collated responses received to the SECMP0067 Second Refinement Consultation.

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

Question 1			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	No	<p>Whilst the DCC have now provided a business case analysis by citing the cost to industry if the DCC systems were to be unavailable due to overload. In this respect the costs stand up to scrutiny although as ever DCC costs for change remain very high.</p> <p>However, we are rejecting this solution on the following grounds:</p> <ol style="list-style-type: none"> 1) with this change the DCC are seeking to flatten the traffic curve which is reasonable in itself but there needs to be a mechanism to cope with Service Requests which cannot be scheduled or flattened, SR 7.4 Read Supply Status is a case in point, DNO's will use this command to check supply status following network faults/storm events and as such we cannot predict when we will need to use this command. DNO's will also need to use SR7.4 Read Supply Status in far higher volumes than originally expected due to the high numbers of SMETS1 meters forecast to be enrolled by DCC as SMETS1 meters do not support Power Outage reporting. If the use of this command is restricted by DCC Traffic Management solution then it undermines the DNO's Power Outage management solutions and benefits case, this is on top of the Power Outage solution currently delivered by DCC to DNO's which significantly fails to meet the published SEC requirements. 2) The proposed DCC mechanism is predicated on calculations based upon the agreed DCC 'system capacity'. Whilst DCC has provided illustrations of capacity calculations it has not explicitly stated what the actual system capacity is. Before agreeing to this modification we need the DCC to publish a clear statement on its current system capacity and the expected capacity as installed meter volumes increase over time. The Traffic Management solution should not be used by DCC as a mechanism to suppress 'reasonable' User demand.

Question 1			
Respondent	Category	Response	Rationale
SSEN	Electricity Network Party	No	<p>As per our previous consultation response, SSEN fully support this SEC Mod, however we are rejecting this Modification for the reasons detailed below.</p> <p>As detailed in our previous response, we need to understand the current capacity levels and how often this new functionality would potentially be required/invoked. The documentation only references one previous scenario but does not mention traffic that was generated during the period to understand the impact this mechanism will have. This would allow us to understand if this is the best solution to address the issue noting the costs and benefits.</p> <p>In previous working groups the suggestion of extra motorways being introduced, among other ideas, as an alternative to the proposed solution had been highlighted. This has been noted in the documentation but with no reference made to the number of future incidents this should help avoid based on each additional motorway lane added. Noting the increase in system usage in the Service Request Traffic Management document, this is required to understand the impacts.</p> <p>As a DNO we are unable to forecast unplanned faults on the network, this can result in specific spikes in SRV demand. Alongside this, looking forward, other SRV's may need to be also added to the prioritised Service Requests list in the future. Without this list being implemented, we are unable to approve this modification.</p>
Northern Powergrid	Electricity Network Party	No	<p>Northern Powergrid accepts the principle that DCC's need to manage traffic on its network and that costs for unnecessary capacity or unavailability due to overload need to be avoided, however we are rejecting this Modification for the reasons detailed below.</p> <p>Details of the current system capacity threshold are not provided and therefore it is unclear how often a breach, which would result in the exceptional circumstances may occur. End to end capacity and response times need to be considered.</p>

Question 1			
Respondent	Category	Response	Rationale
			<p>We would expect that any associated costs of scalable traffic management to be included in the current DCC service charge. The amount of meters enrolled on the network is currently considerably lower than the enduring number anticipated, therefore sufficient technical headroom can be reasonably expected at this point in the rollout.</p> <p>We believe that existing processes and controls provide mechanisms to prevent or limit traffic peaks on the DCC network, such as the Service Request forecast process, Anomaly Detection Thresholds and quarantine controls. If more robust processes to manage user behaviour, or prevent abuse, are required, these should be considered first.</p>
Western Power Distribution	Electricity Network Party	No	<p>Whilst we agree that it is sensible to have some protection for the DSP in the event of extreme circumstances, we question if this is the best solution. We have concerns that this solution is potentially not addressing the root cause.</p> <p>We would expect this mechanism to be used rarely (if ever) due to the DCC being designed to cope with Users expected traffic and existing protection mechanisms that are in place.</p> <p>We are unsure of the cost benefit case for the proposed solution.</p>
E.ON	Large Supplier	No	<p>The revision has not addressed our principle objection from the previous iteration. It is unclear considering the imminent alert traffic management solution and recently delivered additional capacity whether the DCC is in imminent danger of exceeding capacity due to service request traffic.</p> <p>In addition, the split delivery of this change if approved by September 2020 will result in significant manual overhead to manage the resulting failures, in the event the traffic management measures are operationally triggered.</p>

Question 1			
Respondent	Category	Response	Rationale
UK Power Networks	Electricity Network Party	No	<p>UKPN do not agree with this proposal for the following reasons:</p> <ol style="list-style-type: none"> 1) UKPN are not aware of what the DCC current total system capacity is or at what point it becomes at risk. We would be grateful if this could be explained clearly to all parties. 2) DCC need to confirm to UKPN how their system capacity will flex to accommodate the increasing volumes of both SMETS1 and SMETS2 meters being installed by suppliers. UKPN would like assurance from the DCC that their system will be capable of managing this known increase in service requests from the new meter installations, instead of using mitigating actions, such as this SEC MOD change request, to throttle back the volume of service requests their system will be receiving. 3) Some Service Requests are vital to UKPN's customers such as the Service request 7.4 Read Supply Status, which are difficult to forecast due to the uncertain nature of supply disturbance events / Severe Weather events. During a Severe Weather event, there would be a larger than normal amount of Service Requests of this type. Should a Throttling scenario occur at this time, UKPN would be failing to deliver a service to our customers and this is not acceptable. 4) UKPN will soon be reading Smart Meters to collect consumption and voltage readings to provide the business with network related data for LV network modelling, which is one of the fundamental business benefits of Smart Metering. This will generate a large number of Service Requests and it is expected that all DNOs will be doing the same. The impact of unscheduled Throttling will be detrimental to this basic benefit to DNOs and their customers.
Utilita	Large Supplier	We do not support this	<p>Rationale: In order to mitigate the risk of prepayment customers going off supply this mod must have prioritisation across the industry for time critical Service Requests.</p>

Managed by

Question 1			
Respondent	Category	Response	Rationale
		<p>modification primarily because the prioritisation element is not fit for purpose. SECMP0028 sets out a solution we believe should be included as part of this mod.</p>	<p>The solution has two main elements to it, traffic management and service request prioritisation. These two elements must be considered together.</p> <p>Prioritisation: during the course of the refinement period a number of solutions have been discussed which included SECMP0028. The ultimate solution proposed in this SECMP0067 is not fit for purpose and is the reason for Utilita to reject this mod.</p> <p>SMETS2 and Enrolled SMETS1 meters produce UTRNs differently. Enrolled SMETS1 meters require access to the DCC systems in order to create UTRNs – without access to the DCC customers will not be able to top up their meters and remain on supply.</p> <p>Utilita is concerned that there is a high likelihood, based on experience, that SMETS2 vend traffic maybe throttled back leading to unmanageable call volumes and thus S2 customers going off supply, particularly as this could happen at any time with no prior warning or time for either the customer or Utilita to prepare.</p> <p>This risk is amplified for S1 meters under E&A where the vends are only supported by the DCC network and throttling will cause otherwise avoidable disconnections.</p> <p>Utilita has worked hard and invested heavily in SMART metering with approximately 1.4 million smart meters on supply with 90% of those operating in pre-payment mode. We work hard as an organisation to help customers avoid disconnections, however, we believe this Mod' (without market-wide prioritisation) will increase the risk of disconnections to the detriment of all pre-payment customers and that it is being considered without thought for the impacts on approximately 5 million pre-payment customers or the Suppliers that supply them.</p> <p>Utilita understand our own customer behaviour and we don't have the DCC analysis to be able to compare and contrast where the issues are likely to arise. Utilita would like to see the Impact Assessment undertaken by the DCC/BEIS to assess this impact and better understand how the DCC and BEIS have arrived at the conclusion that this Mod is in the</p>

Managed by

Question 1			
Respondent	Category	Response	Rationale
			<p>interests of pre-payment customers. The reason the prioritisation is not adequate is because it is done at a supplier level and not across the market as a whole. It is of paramount importance that this holistic approach is taken to prioritisation for commands relating to keeping prepay customers on supply and managed appropriately. Whilst a supplier may be able to prioritise within its' own SR load, prioritisation across portfolios must also be provided at time of system stress.</p> <p>Additionally, whilst the solution provides for 20% additional capacity for prepay customers, the analysis done is now years old and should be redone and shared with industry to verify it remains valid. There are now significantly more smart prepay customers than when the analysis was done originally and we must validate that the 20% provision will support the needs of the customers.</p> <p>As such, we see the need to either amend SECMP0067 or re-initiate SECMP0028 as an intrinsically linked modification.</p> <p><u>Traffic Management:</u> Utilita agrees a solution needs to be in place to maximise the efficient use of and prevent system outage of the DCC Systems. Currently, when system capacity is exceeded this means no Service Requests reach the Data Service Provider (DSP) until the issue is resolved. This results in a lack of protection for consumers (especially prepayment) leading to the potential of many consumers going off supply – SMETS1 enrolled meters will not be able to top up at all as DCC system access is required to create UTRNs.</p> <p>Utilita is concerned regarding the DCC capacity available. Capacity figures for the DCC system under various loads have not been made available. It is therefore unclear how the capacity modelling is done. In order to robustly assess this solution and whether this will</p>

Question 1			
Respondent	Category	Response	Rationale
			<p>provide sufficient protection for prepay customers, we request DCC share the full modelling undertaken to prove that the proposals set out in this modification are fit for purpose.</p> <p>Under the processes associated with the price caps, there is a high likelihood that suppliers will need to update tariffs and prices on their meters. These requirements will all be at a similar time and can be expected to exert pressure on the DCC systems. As there are now caps on all standard variable/default tariffs, the numbers of meters to be updated at the same time is much larger than before.</p> <p>This process and our understanding gained over the last few years underpins our conviction that traffic management alone is not sufficient and cross market prioritisation must be available at peak times.</p> <p>The main problems that cause most pressure on vend message volumes apart from price changes and reading are not related to predictable or supplier driven events. For example, the Beast from the East, caused outages due to heavy customer demand – network capacity is most likely to be breached during these periods and modelling must be done on these events and other high stress scenarios to fully understand the potential impacts and inform the solution proposed.</p>
British Gas	Large Supplier	Yes	<p>We agree with the issued identified and the principle of the modification. Based on the information provided by the DCC, the proposed solution appears proportionate. The proposed solution looks to only impact on those Users that are responsible for the issue. This appears to be more appropriate than a more general approach that would impact on all Users (e.g. general throttling of all Users) or a solution that builds additional capacity to accommodate increased levels of unintended / malicious network traffic.</p>

Question 2: Will there be any impact on your organisation to implement SECMP0067?

Question 2			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	Yes	We request that the DCC provide current system capacity details and also a forward plan for target system capacity which allows us to model what the restrictions will mean to our operations.
SSEN	Electricity Network Party	Yes	From the modification documentation, we are unable to fully understand the current capacity of the system and how this mod will scale with the roll out. Due to this, we are unsure on the full impact to SSEN.
Northern Powergrid	Electricity Network Party	Yes	<p>From the Modification documentation, we are unable to fully understand the current capacity of the system and how this Modification may be used. Therefore we are unsure on the full impact to Northern Powergrid.</p> <p>As a DNO we are unable to forecast unplanned faults on our electricity distribution network, which could result in operational peaks in Service Request demand whilst we use the smart metering infrastructure to assist our investigations. Should flattening be applied during a critical activity our customer service would be directly impacted and operational costs would increase. We would also incur costs to avoid any impact to our systems and processes.</p>
Western Power Distribution	Electricity Network Party	Yes	If this modification is implemented as proposed then as a minimum we will need to uplift to the relevant DUIS version in order to receive the new HTTP alert code. There is the potential that we would also need to amend our systems to automatically handle this code and prioritise Service Requests sent to the DCC during any period where the mechanism was active.
E.ON	Large Supplier	Yes	Significant effort will be required to amend auto-remedial actions for all failed commands where the reason code was http 429, as these would be required to trigger retries after the suggested time period. This work would not be completed for the interim solution when the

Managed by



Question 2			
Respondent	Category	Response	Rationale
			<p>http 503 message is returned, as this would effectively double the development effort and testing time having to change E.ONs solution twice in a short space of time.</p> <p>In the interim period, whilst the http 503 response was being used, E.ON will have to handle the command failures manually, which will require significant intervention to restart failure orchestrations.</p>
UK Power Networks	Electricity Network Party	Yes	<p>It is not clear how the DCC will inform UKPN of the fact that a Throttle scenario is active if throttling was implemented.</p> <p>UKPN need to understand the DCC Capacity levels being discussed for this change.</p> <p>Once informed of this, there will a need for system changes to remodel how and when we retry failed Service Requests, this will impact business processes in addition to systems.</p> <p>UKPN have spent significant sums of customers' money to ensure that Service Request 7.4 is fast tracked to DCC and that will need to be reviewed and adjusted in times of "Throttle".</p> <p>DCC Adaptor changes will be required to recognise this as different from a straight forward "time-out" which is something we experience now.</p>
Utilita	Large Supplier	Yes	<p>This is likely to result in prepay customers' critical commands being throttled due to a lack of a fit for purpose prioritisation solution.</p>
British Gas	Large Supplier	Yes	<p>Yes, there would be some minor effort to integrate the new http error code into our business processes. We would expect to see a DUIS change to accommodate this, but this would be part of a more significant scheduled DUIS uplift and therefore minimal incremental impact. If the modification were to be implemented in two parts (i.e. use existing http error codes initially) there will be some minor process effort required to implement.</p>

Question 3: Will your organisation incur any costs in implementing SECMP0067?

Question 3			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	Yes	<p>Whilst it is difficult for us to cost the impact in absence of the information we request in our response to Question 2, we estimate the cost to Electricity North West of implementing this modification to be in excess of £100k and will require 12 months to implement. The estimate is on the assumption that we will need to build complex routines to manage message re-tries where the original request has been rejected by this DCC Traffic Management solution.</p> <p>As per our response to the first refinement consultation the modification report mentions “fair share” and we would be interested in additional details of how this has been defined / calculated.</p> <p>Whilst you ask that our rationale exclude central costs we must mention that Electricity Network Users are required to pay DCC charges based upon their respective share of MPANs – our licence costs are calculated on a population of 2.4m MPANs (smart and non-smart). However, only 145k smart meters have been enrolled within our region of the CSP Northern network, a significant disparity when compared with DNOs served by the Southern and Central CSP regions.</p> <p>The net effect of the disparity between Northern and Central/Southern region installations is that the customers of Electricity North West are having to pay a higher premium than customers in other regions for our access to the DCC.</p>
SSEN	Electricity Network Party	Yes	<p>As we are unsure of how often this functionality will be invoked, we are unable to an estimate the potential costs. Based on the solution, this will require substantial system changes to handle and manage the different retry delay periods upon rejection from the DCC.</p>

Question 3			
Respondent	Category	Response	Rationale
Northern Powergrid	Electricity Network Party	Yes	As we are unsure of how often this functionality will be invoked, we are unable to an estimate the potential costs. Based on the solution, this will require substantial system changes to handle and manage the different retry delay periods upon rejection from the DCC.
Western Power Distribution	Electricity Network Party	Yes	It is difficult at this time to provide an estimate of costs for this change. A DUIS uplift is a simple enough value to calculate (and we can advise this if necessary), but in order to change the systems to be enable prioritisation of service requests will involve considerable time, effort, resource and costs.
E.ON	Large Supplier	Yes	Costs unknown at this stage. Costs will be subject to commercial assessment by E.ON third party service provider, but will be significant to implement automated changes to the handling of all commands for this scenario.
UK Power Networks	Electricity Network Party	No	There are no cost savings to UKPN by the implementation of this modification. The cost of changing the DCC Adaptor would be in excess of £150k as changes would be required to the entire system, processes, and business models. This is an estimate based on other changes made in recent years. We estimate it would take 12 months to implement these changes.
Utilita	Large Supplier	Yes	these are undeterminable at this present time due to a lack of transparency relating to system capacity.
British Gas	Large Supplier	Yes	As above (Q2), there would be minor implementation costs to accommodate new http error code. This would be wrapped up in a DUIS release so would form part of a bigger scheduled release / implementation. The incremental delivery costs for this modification would be very minor. We would expect this to be implemented via a scheduled DUIS uplift (e.g. v4.1 or v5.0).

Question 4: Do you believe that SECMP0067 would better facilitate the General SEC Objectives?

Question 4			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	No	While we understand the intent of this proposed modification we are not convinced that any General SEC Objectives will be better facilitated by its implementation.
SSEN	Electricity Network Party	No	We agree that it is not feasible or economically viable to provide a System with infinite capacity. Noting proposed costs, we would like to ensure full analysis confirms that this mechanism is the most suitable solution and would best deliver SEC objectives (a) and (e), as per the SECMP0067 consultation.
Northern Powergrid	Electricity Network Party	No	We agree that it is not feasible or economically viable to provide a System with infinite capacity. Noting proposed costs, we would like to ensure full analysis confirms that this mechanism is the most suitable solution and would best deliver SEC objectives (a) and (e), as per the SECMP0067 consultation.
Western Power Distribution	Electricity Network Party	No	<p>We don't agree that this modification would better facilitate SEC Objective (a) by ensuring an efficient operation of Smart Metering Systems as we don't feel that it fully addresses the problem.</p> <p>We disagree that this modification better facilitates SEC Objective (e) as we do not feel that it facilitates Network Operators in innovating the design and operation of their networks to ensure a secure and sustainable supply of energy, especially as Network Operators cannot send SRVs that control the supply to a premise.</p>

Question 4			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	No	The modification appears to offer additional protection to the DCC System in times of high demand. However, the level of information outlined impedes our ability to complete a full impact assessment.
UK Power Networks	Electricity Network Party	No	UKPN cannot identify any SEC objectives that would be better facilitated by this proposed modification.
Utilita	Large Supplier	Yes	SECMP0067 plus the solution (or equivalent solution) from SECMP0028 would better facilitate Objectives A and E.
British Gas	Large Supplier	Yes	We agree that implementation would better facilitate General SEC Objectives (a) and (e) as indicated in the Modification Report.

Question 5: Noting the costs and benefits of this modification, do you believe SECMP0067 should be approved?

Question 5			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	No	Please see our responses to Question 1, 2,3 & 4.
SSEN	Electricity Network Party	No	Please see Question 1
Northern Powergrid	Electricity Network Party	No	Please see our responses to Question 1, 2 and 3.
Western Power Distribution	Electricity Network Party	No	<p>We do not believe that the Authority's request for 'clear succinct and complete assessment of the costs and benefits of the three options' has been addressed.</p> <p>We would also like to understand the industry costs involved with this change in addition to the DCC costs as we feel that this could be significant.</p> <p>We currently cannot see a cost versus benefit cast for this modification.</p>
E.ON	Large Supplier	No	Delivery of http 429 should not be separate to the main body of changes.
UK Power Networks	Electricity Network Party	No	The DCC system should be correctly scaled to meet the demand of the Smart Meter roll out, and to cater for events that result in an increase in Service Requests. The number of meters and Service Requests are not a surprise and the DCC system should be sized accordingly to cope with this, instead of impacting its customers with additional costs and a reduction of our ability to provide the customer benefits that each DNO has declared. There

Managed by

Question 5			
Respondent	Category	Response	Rationale
			would a number of negative customer impacts if customers are unable to rely on smart meters, e.g. to seamlessly notify their DNO in the event of a loss of supply incident.
Utilita	Large Supplier	Not in isolation or as drafted - the addition of SECMP0028 must be included before this could be considered as a solution to the identified problem.	See question 1
British Gas	Large Supplier	Yes	We do however disagree with the cost estimate that has been provided for the alternative 'motorway' solution by the DCC. The 'sizing' for additional motorways has been carried out using all User traffic to establish the cost – this wouldn't be necessary as the motorways would only need to cater for the increased demand of the User that has been compromised / has an issue. On this basis the cost of the alternative solution should be much lower. However, we do not think that the lower cost would be less than the implementation cost for the proposed solution (or not significantly lower) and we therefore support implementation of the proposed solution.

Question 6: How long from the point of approval would your organisation need to implement SECMP0067?

Question 6			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	At least 12 months.	Based on any final solution we would need to review our systems and processes and complete any relevant changes.
SSEN	Electricity Network Party	>12 Months	As this Mod would require substantial system changes as noted in question 3, this would require enough lead time to build and test functionality and performance.
Northern Powergrid	Electricity Network Party	>12 Months	As this Modification would require substantial system changes as noted in Question 3, this would require enough lead time to build and test functionality and performance.
Western Power Distribution	Electricity Network Party	12 months	As this would require system changes we would require a minimum lead time of 12 months.
E.ON	Large Supplier	9-12 months	Based on current limited information available and delivery of the http 429 error code being separated from the main delivery, there would be little point in delivering any changes before November 2021.
UK Power Networks	Electricity Network Party	12-15 months at least.	Significant DCC Adaptor change would be required. Fault system processes would require amendment. Business processes would require change.
Utilita	Large Supplier		
British Gas	Large Supplier	<1 month (phased implementation)	If the modification were to be implemented in two parts, we would not require much time (if any) to implement based on the use of the existing http 503 error codes. Standard SEC

Question 6			
Respondent	Category	Response	Rationale
			implementation timescales would need to apply for the enduring part of the solution as that would need to be part of a scheduled DUIS release (e.g. November 2021).

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

Question 7			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	No comment	No comment
SSEN	Electricity Network Party	No	SSEN feel that if the modification is approved, an implementation date of 24 June 2021 does not provide enough time to build, implement and test the required solution within SSEN.
Northern Powergrid	Electricity Network Party	No	Northern Powergrid feel that if the Modification is approved, an implementation date of 24 June 2021 does not provide enough time to build, implement and test the required solution within Northern Powergrid.
Western Power Distribution	Electricity Network Party	Yes	We can understand the argument for the implementation approach detailed in the modification.
E.ON	Large Supplier	No	The DSP uplift to introduce the http 429 must be delivered at the same time as the other changes – it's an integral part of the solution.
UK Power Networks	Electricity Network Party	No	There is more information required before this question can be answered – once again visibility of the DCC system capacity is needed. In addition UKPN needs to understand what share of the overall capacity will be available to UKPN during a period of "Throttle".
Utilita	Large Supplier	No, we disagree with the implementation	See Question 1.

Question 7			
Respondent	Category	Response	Rationale
		approach because the solution set out in SECMP0067 is not a full solution.	
British Gas	Large Supplier	No	If a phased approach, we would support an earlier implementation (with the required DUIS changes following in November 2021).

Question 8: Do you agree that the legal text will deliver SECMP0067?

Question 8			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	No comment	No comment
SSEN	Electricity Network Party	No	The legal text refers to rejecting non-Priority Service requests but does not detail anything further about a Priority List. It has been confirmed that the functionality will exist but will be turned off at implementation. The legal text does not allow for this functionality to be used or managed at any point.
Northern Powergrid	Electricity Network Party	No	The legal text refers to rejecting non-Priority Service requests but does not detail anything further about a Priority List. It has been confirmed that the functionality will exist but will be turned off at implementation. The legal text does not allow for this functionality to be used or managed at any point.
Western Power Distribution	Electricity Network Party		We have not fully reviewed the legal text at this time.
E.ON	Large Supplier	Yes	The text accurately reflects the proposed changes
UK Power Networks	Electricity Network Party	No comment.	No comment.
Utilita	Large Supplier	The legal text fails to deliver a fit for purpose	

Question 8			
Respondent	Category	Response	Rationale
		solution for prioritisation.	
British Gas	Large Supplier	Yes	The legal text supports the intent of the modification proposal.

Question 9: Do you believe there will be any impacts on or benefits to consumers if SECMP0067 is implemented?

Question 9			
Respondent	Category	Response	Rationale
Electricity North West Limited	Electricity Network Party	No comment	No comment
SSEN	Electricity Network Party	Yes	If SRV's that relate to Supply Management (7.4) are rejected, this will have a negative impact on the consumers service.
Northern Powergrid	Electricity Network Party	Yes	If SRV's that relate to Supply Management (7.4) are rejected, this will have a negative impact on the consumers service.
Western Power Distribution	Electricity Network Party		No comment
E.ON	Large Supplier	Yes	Some benefit may be accrued in the event of a denial of service attack being mitigated. Consumers may also be negatively impacted due to the removal of the Priority service request list. Installs may be impacted, which could have been avoided if that element of the solution had been retained.
UK Power Networks	Electricity Network Party	Yes	The impact on our customers will be that in a period of "Throttle" our ability to identify a supply status will be impacted, i.e. for UKPN to ping a meter. This could mean that DNOs would not know when their customers are off supply, and could mean customers contacting DNOs to alert them that they are off supply which would defeat one of the core benefits of having smart meters.

Question 9			
Respondent	Category	Response	Rationale
			<p>This will result in UKPN having to attend site to establish the supply status. This will impact the customer's ability to know as soon as possible that the supply issue is within their property as opposed to a Network issue.</p> <p>We are cognisant that throttling could impair the proliferation of low carbon technology such as EVs and heat pumps. It seems to us, that with the continued transition to Net Zero, it would be sensible to expect service request traffic to increase and therefore the more enduring solution would be to increase the capacity.</p>
Utilita	Large Supplier	Yes, impacts on customers	See question 1.
British Gas	Large Supplier	Yes	Implementation of this modification could prevent a denial of service event that impacts many / all Users. If users are unable to take DCC services then this could have a detrimental impact / consequence for customers, in particular prepayment customers if they are unable to vend / apply additional credit.

Question 10: Please provide any further comments you may have

Question 10		
Respondent	Category	Comments
Electricity North West Limited	Electricity Network Party	No comment
SSEN	Electricity Network Party	N/A
Northern Powergrid	Electricity Network Party	No comment
Western Power Distribution	Electricity Network Party	
E.ON	Large Supplier	
UK Power Networks	Electricity Network Party	
Utilita	Large Supplier	
British Gas	Large Supplier	n/a