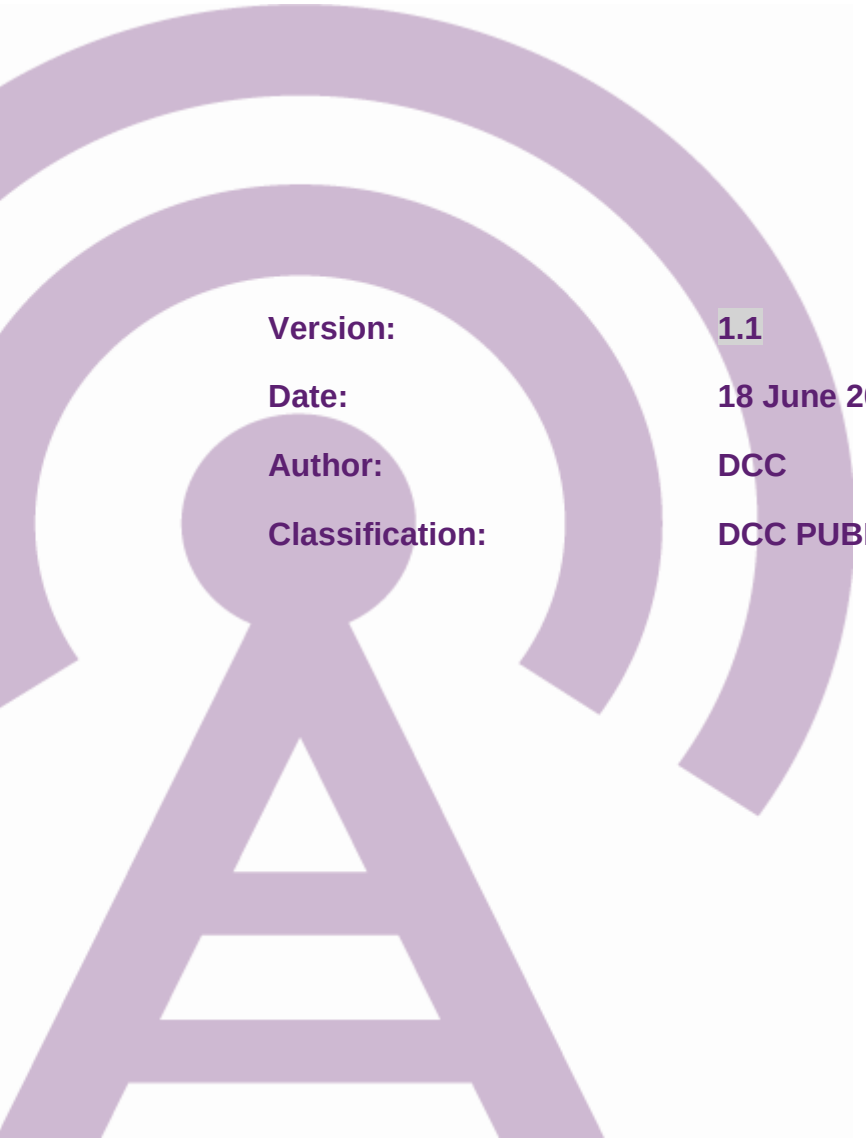
Data Communications Company

SEC Modification Proposal, SECMP0067

Service Request Traffic Management

DCC Preliminary Impact Assessment



Version:	**1.1**
Date:	**18 June 2019**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Contents

1 Introduction

1.1 Document Purpose

The purpose of this DCC Preliminary Impact Assessment (PIA) 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

This DCC Preliminary Assessment was requested of DCC on 01/05/2019.

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

1.5 Requirements

The requirements for this modification have been developed by the Working Group during the Refinement phase. The impact on DCC has been assessed against the Business Requirements.

Business 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.

Business Requirement 2

The DCC System will include a clearly defined and configurable list of Priority and non-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.

Business 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.

Business 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.

Business 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 DCC will also provide a means of notifying Service Users when they are 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.

Business Requirement 6

The DCC will impact and provide a separately costed option to add a buffering mechanism to the solution, such that during a peak overload Service Requests would normally be absorbed by the buffering mechanism and Users would not receive a Busy response.

The DCC will provide a separate and fully costed alternate version of the proposed solution with the addition of a buffering mechanism. This alternate should be designed such that it will accept and queue Non-Priority Service Requests, rather than returning a HTTP503 notification whilst the buffer is active and has capacity. When the available buffer is consumed, a HTTP503 notification will be sent in response until buffer space becomes available.

Determination of the buffer size will be provided by the DCC.

Based on the discussions at the Working Group and the Business Requirements as set out in the Business Requirements Document, DCC assume the requirements for SECMP0067 to be **STABLE**. Where the requirements or SEC obligations change, DCC will be required to carry out a further impact assessment.

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

At any point in time, the DCC System will have a stated capacity for processing Service User requests. This capacity will be stated as a value in "requests per second" and may change over time as the scale of the DCC System increases and more capacity is added.

Service Users will be notified of the DCC System Capacity by the DCC and each Service User will be allocated a proportion of the available capacity based on an agreed algorithm as described in response to Business Requirement 1.

The DCC will notify the DSP of the agreed 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 DCC 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 System Capacity and Service User Capacity, which shall form the basis of the invocation of traffic management.

Two new sets of values will be recorded 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 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 time period shall determine a requests/sec usage value for the System as a whole and for each Service User. These requests/sec usage values will be compared against the System Capacity and the Service User Capacity as follows:

- If the System usage exceeds the amber threshold for 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 System usage remains below the red threshold for 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 System usage exceeds the red threshold for 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 System usage exceeds the red threshold for 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.

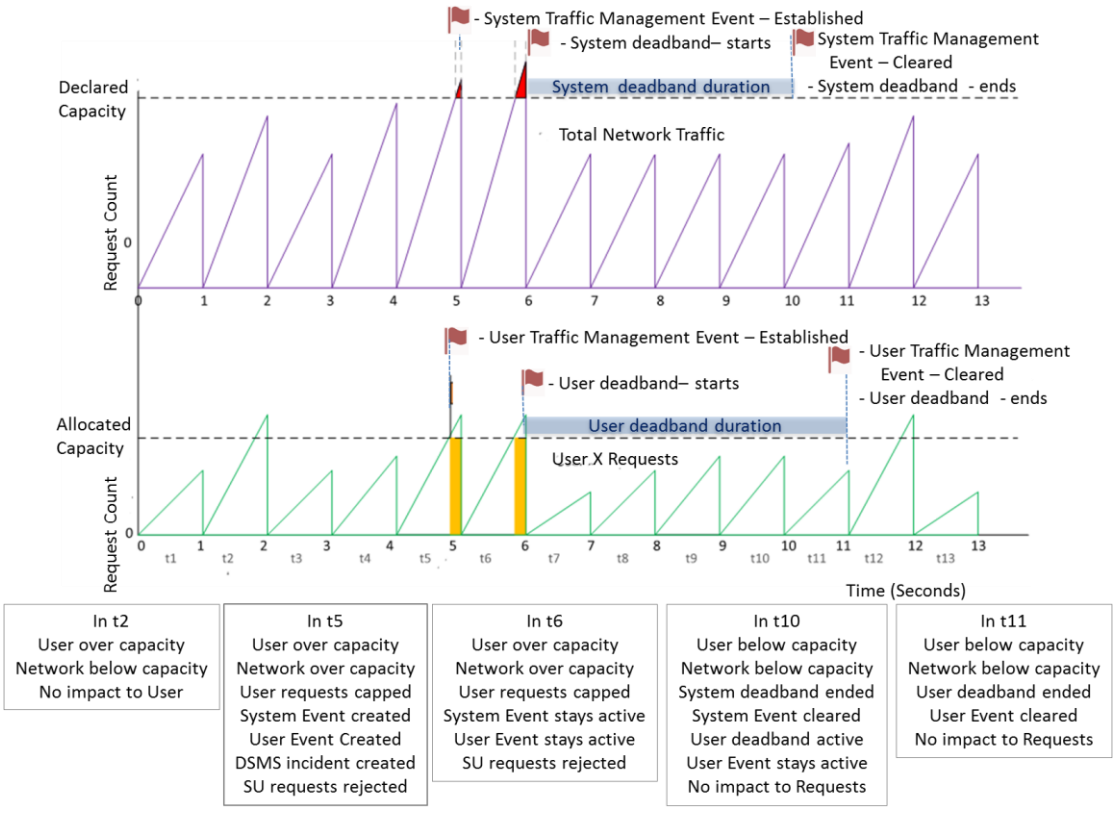


Figure 1 Southbound Traffic Management Processing

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 and an HTTP 503 System Busy response will be returned;
- 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.

The processing under Traffic Management mode will continue until the System usage returns below the red threshold for System Capacity and stays there for a period greater than the system deadband duration. During the system deadband period if the 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, the period will be refined during the testing phases but it is anticipated that this will initially be set to 60 minutes.

(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 System usage returns below the red threshold then that Service User will be cleared of being subject to Traffic Overload.

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

In addition, the current state of System usage and Service User usage will also be made available to the DSP Monitoring solution so that it can be displayed and, if required, exported to other systems.

2.1.2 Business 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.

Traffic Management Allocation Formula

System Parameters

There will be a number of commissioned and installed smart meters to which Service Users will be sending service requests. The implication here is that the greater the number of smart meters for which the service user is responsible, the greater the aggregate volume of service requests required to support them. We'll denote the number of smart meters for each service user by **N,** over the period in question.

Each Service User has potentially multiple (up to 7) user roles. To reflect the varying range of service requests available to each user role and by implication the aggregate volume of service requests a service user can send, 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. We'll denote them by **W**.

The Charging Group Weighting Factors specify the ratio of costs to be incurred in respect of each Smart Metering System (without regard to the number of Smart Metering Systems). These weighting factors are based on an estimate of the demand for DCC Services within each Charging Group in accordance with the Charging Methodology. This estimate is derived from:

- Forecast of Smart Metering Systems rollout volumes;
- Service Request cost assumptions; and
- Forecast of Service Request volumes for RY2021/22.

DCC has derived these Charging Group Weighting Factors using aggregated demand and rollout profiles provided by energy suppliers and network operators to DECC at the bid stage combined with the contracted variable costs of External Service Providers.

These Charging Group Weighing Factors do not provide three Charging Groups with a weighting, these are Gas Transporters, Other Users and Registered Supply Agent (RSA). A process to distribute these Charging Group weightings across all 7 user roles will need to be established.

Finally, it has been proposed that as pre-payment customers on average consume a higher number of messages that these higher volumes should be factored in the formula

Calculations of Threshold Matrices

For each threshold, a matrix will be calculated, where the rows will correspond to the User Roles and the columns to the Service Users. For this matrix, each cell element will contain the allocated threshold of smart meters according to the distribution of User roles and the number of smart meters being served per Service User and User Role.

The number of Service Users may vary. For example, if we consider two service users, with a single user role then the THRj Threshold matrix would have the following form:

$$THR_j = \frac{STT\_DM_j}{W \cdot (N1 + N2)} * \left\{ W_p \times N_1^T \middle| W_p \times N_2^T \right\}$$

DefinitionsVariable	Description
THR_j	Service User Allocated Share
STT_DM_j	Defined Total Capacity
$W \cdot (N1 + N2)$	Total smart meter volumes weighted by user role

$\{W_p \times N_1^T \mid W_p \times N_2^T\}$	Total smart meter volumes for that service user weighted by user role and pre-payment uplift

Worked Example

The worked example below, illustrates the steps in calculating the threshold for six Service Users with the notional User Roles of Electricity Supplier – Import, Gas Supplier, Electricity Supplier – Export, DNO, Gas Transporter, RSA and Other Users. The values are provided as an example only.

Step 1: Establish Core Parameters

Table 1. Core Parameters

SEC Party Details	SEC Party ID	Network Operator (DNO or Gas Transporter)	Charging Group ID	Charging Group Weighting
Service User A	A001	Electricity Supplier - Import	g1	0.490
Service User A	A002	Gas Supplier	g3	0.370
Service User B	A003	Electricity Supplier - Export	g2	0.080
Service User C	A004	DNO	g4	0.060
Service User D	A005	Gas Transporter	g5	0.000
Service User E	A006	RSA		0.000
Service User F	A007	Other User		0.000

Step 2: Establish installed smart meter volumes for each service user over the period the allocation applies

Table 2. Number of Meters Associated with Each Service User at the end of the period

SEC Party Details	SEC Party ID	Number of Installed Meters at time t	Number of Forecast Meters to be Installed in time t+1	Total Meters at time t+1
Service User A	A001	4,000	1,000	5,000
Service User A	A002	3,000	500	3,500
Service User B	A003	1,000	200	1,200
Service User C	A004	6,000	1,200	7,200
Service User D	A005	7,000	250	7,250
Service User E	A006	2,000	1,000	3,000
Service User F	A007	-	-	-

Step 3: Define Overall Capacity. This Corresponds to STT_DM_j in Equation 1. As this traffic management proposal requires that agreed service requests are not constrained by this solution, a portion of capacity needs to set aside to accommodate these unconstrained service requests. This portion of capacity is referred to as the headroom and is deducted from the defined capacity figure in the calculation.

Table 3. Defined Capacity for the Message Type

Capacity	Defined Capacity (Transactions per Second)	Headroom
System Capacity	300	30

Step 4: Charing Group Weighting Factors are distributed across all user roles by allocating an agreed portion of the current Weighting Factors to those user roles not covered by current Weighting Factors.

Table 4. Charging Group Weighting Redistribution

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

Table 5. Charging Group Weighting Redistribution Multiplied by Weighting Factor

SEC Party Details	SEC Party ID	Role	Charging Group	Final Weighting
Service User A	A001	Electricity Supplier – Import	g1	0.466
Service User A	A002	Gas Supplier	g3	0.352
Service User B	A003	Electricity Supplier – Export	g2	0.076
Service User C	A004	DNO	g4	0.057
Service User D	A005	Gas Transporter	g5	0.040
Service User E	A006	RSA		0.010
Service User F	A007	Other User		0.000

Step 5: Adjust smart meter volumes by the pre-payment multiplier to reflect the higher traffic volume of pre-payment customers. The proportion of a service users customers who are pre-payment customers are multiplied by the pre-payment multiplier (the agreed factor that represents the additional service requests required to manage pre-payment customers relative to non-prepayment customers).

Table 6. Charging Group Weighting Redistribution Multiplied by Weighting Factor

SEC Party Details	SEC Party ID	Percentage Pre-Pay Customers	Pre-Pay Multiplier	Adjusted Meter Volumes at time t+1
Service User A	A001	16%	1.2	5,960
Service User A	A002	16%	1.2	4,172
Service User B	A003		-	1,200
Service User C	A004		-	7,200
Service User D	A005		-	7,250
Service User E	A006		-	3,000

Service User F	A007		-	-
Total			2.4	28,782

Step 6: Calculate the weighted number of smart meters associated with a user role

Table 7. Number of Smart Meters Weighted by User Role

Role	Adjusted Meter Volumes at time t+1	User Role Weights	Weighted Smart Meter Volumes at time t+1
Electricity Supplier – Import	5,960	0.466	2,774
Gas Supplier	4,172	0.352	1,466
Electricity Supplier – Export	1,200	0.076	91
DNO	7,200	0.057	410
Gas Transporter	7,250	0.040	290
RSA	3,000	0.010	30
Other User	-	0.000	-
Total	**28,782**		**5,062**

Step 7: Multiply the number of smart meters by the user role weighting factor for each service User

Table 8. Number of Smart Meters Weighted by Each Service User

SEC Party Details	SEC Party ID	Charging Group Weighting	Number of Installed Meters at time t+1	Weighted Smart Meter Volumes at time t+1
Service User A	A001	0.466	5,960	2,774
Service User A	A002	0.352	4,172	1,466
Service User B	A003	0.076	1,200	91
Service User C	A004	0.057	7,200	410
Service User D	A005	0.040	7,250	290
Service User E	A006	0.010	3,000	30
Service User F	A007	0.000	-	-

Step 8: Divide the available capacity by the sum of user role weighted smart meters for each service user and multiply by the total user role weighted number of meters for each service user

Table 9. Number of Smart Meters Weighted by Each Service User

SEC Party Details	SEC Party ID	Capacity Allocation (Transactions Per Second)	Percentage Allocation for time t+1
Service User A	A001	226.18	83.8%
Service User B	A003	4.86	1.8%
Service User C	A004	21.89	8.1%
Service User D	A005	15.47	5.7%
Service User E	A006	1.60	0.6%
Service User F	A007	-	0.0%
Total		**270.00**	**100%**

This calculation provides the service user with an allocated share of capacity measured as a percentage of total available capacity. By stating the allocated capacity for each service

user as a percentage of available capacity, this ensures that the DSP can make capacity enhancements during the period to which the allocated share applies without having to recalculate the formula.

Business Processes

Allocation Process

The DCC proposes a monthly cycle of updates to the calculated capacity allocation of service users. Explicit approval from the delegated SEC Panel committee will be required before its publication on SSI and publication will take place at least two weeks before the allocated capacity for each service user is active on the solution.

Amendments to the allocated capacity of each service user within the monthly cycle is permitted where the SEC Panel committee agrees with any recalculated allocations.

This allocation formula and associated processes will be reviewed regularly in consultation with the delegated SEC Panel committee. The formula will be published on the DCC website, together with the outcome of the most recent consultation undertaken in respect of such methodology.

Changes to the Capacity Allocation formula

The DCC will develop appropriate Business Processes in support of Business Requirement 10, to ensure that changes to the Capacity Allocation formula includes explicit approvals from the delegated SEC Panel committee.

Amendments to the Capacity Allocation formula parameters

DCC will develop appropriate Business Processes in support of Business Requirement 10, to ensure that changes to the Capacity Allocation formula parameters include explicit approval from the delegated SEC Panel committee.

These parameters include the reweighting of Charging Group Weighting factors and pre-payment uplift.

2.1.3 Business Requirement 2

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

DCC understands that TABASC will provide an approved list of Priority Service Request Variants that will be not be subject to capping, all other SRV's will be treated as non-Priority and will be subject to capping.

This list may be amended by TABASC when required and notified to DCC. A mechanism will be provided for the verification of the revised list and the secure loading of the new configuration into the DSP solution.

2.1.4 Business Requirement 3

Service user capacity allocations will be updated monthly.

The DCC proposes a monthly cycle of updates to the calculated capacity allocation of service users. Explicit approval from the delegated SEC Panel committee will be required before its publication on SSI and publication will take place at least two weeks before the allocated capacity for each service user is active on the solution.

2.1.5 Business 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.

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

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.

Response Code	Interpretation
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
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.
500	Internal Server Error – Indicates that the DCC Systems are malfunctioning.
503	Service Unavailable – The DCC Systems are currently unavailable (because they are overloaded or down for maintenance).

If the DSP system is unavailable due to maintenance, fault, or overload then an HTTP 503 response should be returned. At this point it is the responsibility of the calling system to handle the error condition.

If the calling system (the User) immediately retries the Service Request then there is a chance this may fall within the same Traffic Management window and result in a further 503 response.

If it is desired to retry a Service Request, then normal design practice would be to implement a retry strategy that includes a backoff algorithm (e.g. exponential backoff) such that successive retries are submitted in a managed way that will minimise the number of attempts needed and avoid overloading the service being requested. The retry strategy should include a mechanism to limit the total number of retry attempts and to report back a failure to the calling system. For information, the DSP solution incorporate retry strategies on its interfaces to Service Users and to the CSP's.

The use of retry strategies will help to prevent 'tidal wave' effects of Service Requests when systems become available again. It would be helpful if Users could provide details of their retry strategies to either the DCC or the SECMP0067 Working Group.

2.1.6 Business Requirement 5

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

Users will receive synchronous responses to Service Requests, and if the request is subject to throttling an HTTP 503 response will be received.

The DSP solution will also record events generated from the Traffic Management solution.These events will be forwarded to the DCC for the purposes of analytics and reporting.

Reporting will be provided on a monthly basis and will include information on:

- When the system capacity thesholds have been reached or exceeded.
- Which Service Users have exceeded their capacity allocation.
- When throttling of Service Requests has been used and for how long.
- Identification of any trends or particular events.

As requested these reports will not be made public by the DCC, but will be provided to the SEC Panel or delegated subcommittee in confidence.

An early warning system may be feasible by means of either:

- Triggering from the 'amber thresholds' within the DSP. This would require an additional notification mechanism to be identified.
- The analytics and reporting capabilities could be leveraged to provide trending and warning notifications.

We will provide additional analysis of this as part of the Full Impact Assessment.

2.1.1 Business Requirement 6

The DCC will impact and provide a separately costed option to add a buffering mechanism to the solution, such that during a peak overload Service Requests would normally be absorbed by the buffering mechanism and Users would not receive a Busy response

If this option is progressed then DSP will build a buffering mechanism to avoid rejecting Service Requests during a short-term surge above the allocated capacity of a Service User. This buffer will be called the 'Service Request Buffer' and will be implemented as queues managed within a given instance of the Message Gateway component. The Service Request Buffer will not be implemented as shared queues across all instances of the Message Gateway component. This approach may lead to Service Requests being processed in a different order than originally submitted by an affected Service User, but has been selected as it greatly simplifies the technical solution.

There will be a separate Service Request Buffer for each affected Service User within each Message Gateway instance. DSP expects that only a small number of Service Users will simultaneously require the Service Request buffer at a given point in time. The maximum number of Service Request Buffers that need to be supported simultaneously and the size of each of these buffers will be managed through configuration. The details of the configuration will be stated in the Final Impact Assessment (FIA).

It is assumed that Service Request Buffer will be designed, implemented and tested at the same time as the rest of the solution for SECMP0067. The mechanism for activating Service Request capping is defined by the response to SECMP0067 Business Requirements 1 to 5, therefore it will require implementation before, or at the same time as the Service Request Buffer. When Service Request capping is activated, non-priority Service Requests in excess of their allocated capacity will be directed into the Service Request Buffer. The messages in the Service Request Buffer will be processed at the start of the next time window in a first in, first out (FIFO) manner. All subsequently received Service Requests will be added to the back of the queue until the Service Request Buffer becomes empty. If the Service Request Buffer reaches its maximum size, DCC Data Systems will stop buffering the Service Requests and they will be rejected with an HTTP 503 response.

Please note that every message stored in the Service Request Buffer will hold a connection for the Service User through the F5 and Data Power services to the Message Gateway therefore resulting in an increased number of concurrent connections. Further analysis will be required as part of the Full Impact Assessment stage to determine how many concurrent connections the F5, Data Power and Message Gateway can have open at once and what resource (for example CPU, RAM) usage this will entail.

2.1.2 Affected Components

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. The Message Gateway will use the new Traffic Management component to determine the traffic overload status.

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. The traffic rate will be shared with the DSP monitoring solution.

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.

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.

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.

Transform

The Transform component will not require any changes.

Incident Client

The existing interface for creating incidents will not require any changes.

Reporting Services

The Reporting Application Server will need a new upload process to load the traffic counts for operational monitoring. It will also provide a new service for SSMI to retrieve data to display in the operational dashboard.

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.

SSMI will also be enhanced to present the traffic management information within the Operational Dashboard. This will allow DCC Service Desk users to view the traffic state information for both Service Users and the DCC System as a whole.

DSMS

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

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.

Dependency Management/Feature Switch

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.

Operational Monitoring

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

Events created for specific thresholds being breached or cleared will be tracked and reported in the DSP operational monitoring tools.

3 Impact on Security

This section describes the impact DCC considers SECMP0067 will have on Security of DCC's Total System.

There are no new security patterns introduced as a result of this change and it is not expected that it requires any associated penetration testing or changes to the Protective Monitoring solution on the basis that it introduces no new infrastructure.

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

Systems Integration Testing (SIT) is the testing of the DCC Total System, which brings together the components, e.g., DSP and CSP Systems, to allow testing of the end-to-end solution by DCC. SIT is carried out for every DCC System release and incorporates the test and integration of multiple changes. The SEC Modification and associated system changes will need to be demonstrated and tested as part of the integration test phases.

During the Transitional phase of the Smart Metering Implementation Programme (SMIP) the SIT environment and associated services are primarily used to provide integration testing to support implementation. At this stage in the programme the SIT environment is required to support the integration of SMETS1 systems into the DCC ecosystem, with the associated costs already being incurred by Users. Because Users are already paying for SIT, DCC considers that SIT costs should not be included in this assessment.

4.3 User Integration Testing

User Integration Testing (UIT) is referred to as User Testing in the SEC. User Testing of Modification Proposals is provided using the Modification Implementation Testing Service. It enables Users to run specific tests to support their implementation of a change. DCC expects that User Testing will be required to support User's implementation of this modification.

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 **12 months.**

Phase	Start	End
SECAS approval of SECMOD	June 2019	

Phase	Start	End
PIT Phase	July 2019	December 2019
SIT Phase	January 2020	April 2020
UIT Phase	May 2020	May 2020
Transition to Operations and Go Live	May 2020	June 2020

6 DCC Costs and Charges

6.1 Cost Impact

6.1.1 Implementation Costs

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

Implementation costs							
Phase:	**Design**	**Build**	**Pre-Integration Testing**	**System Integration Testing**	**User Testing**	**Implementation to Live**	**Total**
SECMP0067 BR 1 – 5	*£1,646,355*						
SECMP0067 BR 6	*Between £351,000 and £750,000 in addition to the costs for BR 1 - 5*						

Implementation costs – supplementary information	
Implementation cost assumptions	*A. Costs are exclusive of VAT and any applicable finance charges* *B. Majority of the costs above represent labour costs.* *C. Costs provided for Design, Build and Pre-Integration Testing are quotes provided by the Service Providers and assuming there is no scope change can be considered the final costs. DCC have reviewed and challenged the costs from the Service Providers to ensure this reflects best price to date.* *D. Costs will be refined during future assessments.*
Explanation of Implementation Phases	*DCC's implementation costs are provided by implementation phases. The following describes the purpose of each phase:* • *Design: The production of detailed System and Service design 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: Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.*

- *System Integration Testing: All Service Providers' PIT-complete solutions are brought together and tested as an integrated solution, ensuring all Service Provider solutions align and operate as an end to end solution.*
- *User Integration Testing: Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.*
- *Implementation to Live Costs: The solution is implemented into production environments and ready for use by Users as part of a live service. This service is subject to implementation costs.*

The fixed price cost for a Full Impact Assessment is £18,832

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

7.1 Risks

Ref.	Risk Description	Risk Impact
R-001	User System retry strategies (in respect of Service Request transmission) are not known to the DCC. If the retry strategy uses very short time intervals the requests may be counted as additional submissions within the same traffic management time window	n/a

7.2 Assumptions

Ref.	Description	Impact
A-001	For Business Requirement #2, it is assumed that a list of agreed Service Request Variants will be notified by TABASC.	Low
A-002		Low

7.3 Dependencies

Ref.	Description	Impact
D-001	The option described for Business Requirement 6, is dependant upon the implementation of the solution to meet Business Requirements 1 – 5.	n/a

Appendix A – Priority Service Requests

The list of Priority Service Requesta will be agreed by TABASC and notified to DCC. This list will be loaded into the Trafffic Management solution as configuration data.

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