Data Communications Company

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.

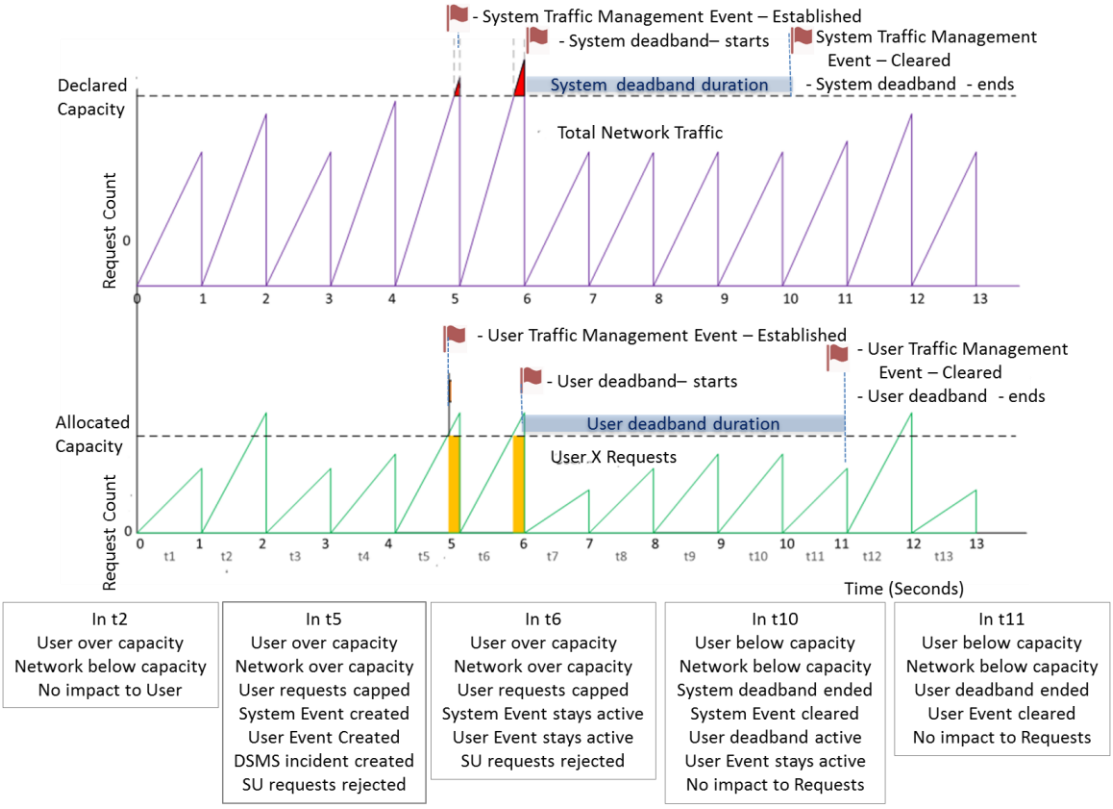

Figure 1 Southbound Traffic Management Processing

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

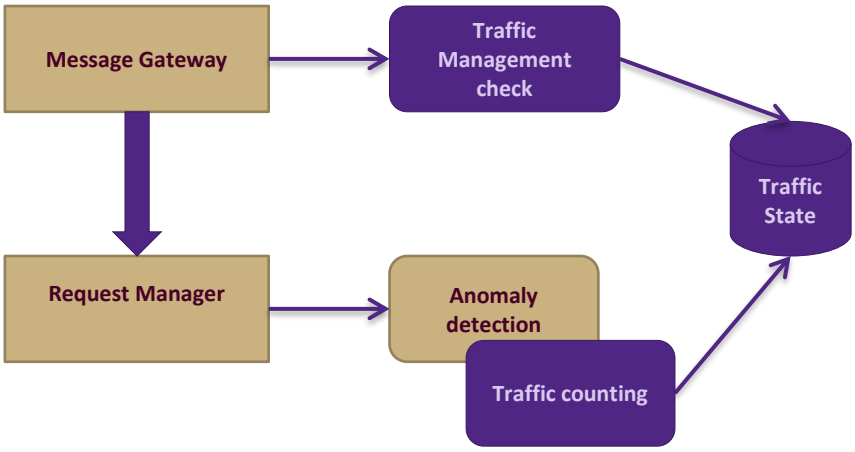

Figure 2 Southbound Traffic Management within DCC Systems

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 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 SSMI 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 SSMI 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	1,406345	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**" (THRu) shall be determined as follows;

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

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)
- $\sum euTMu$ 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 = TSCw - BSCw

Where;

TSCw is the Total System Capacity

BSCw 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 diving 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;

Σe 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 ($e.g.\mathbf{0.466}$) from Table 7, by the adjusted number of meters that Service User is responsible for in that role ($e.g.\ \mathbf{5,960}$), 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;

$$\mathbf{0.466\ \times 5,960 = 2,774}$$

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:

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

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