Data Communications Company

Service Request Traffic Management

SECMP0067

Business Case

Version:	0.1
Date:	01/08/2019
Author:	Graeme Liggett
Classification:	DCC Controlled

Document Control

Documentation Control

Version	Date	Description	Author
0.1	02/09/2018	Initial Draft	Graeme Liggett

Documentation Location

This document and related artefacts are located

Table of Contents

1 Introduction

1.1 Summary

As there are currently no constraints placed on Service Users, the demand on the DCC solution could be unbounded. It is not feasible to provide a technical solution with infinite capacity, we therefore require a mechanism by which the rate of Service Requests accepted at the Message Gateway can be controlled to prevent a severe and sustained deterioration in performance or a failure in the service.

Current Gamma connections to the DCC System are capable of transmitting the equivalent of 30,000 Service Requests per second, based on an average Service Request payload of 2Kbytes. This is equivalent to some 80 billion Service Requests per month, or 10 times the contracted capacity of the service at scale. Additionally, a single Service User with a 100Mb connection could introduce up to 5000 Service Requests per second into the DCC System, potentially consuming over half of DCC System resources at scale and a greater proportion of System resources prior to the DCC system reaching full scale over the coming years.

Ofgem reports that there are currently 50 active domestic fuel suppliers in the UK and growing, not all of these currently have a gamma connection. The risk of a single Service User experiencing issues with their back-end systems or human error triggering the transmission of concentrated bursts of large volumes of Service Requests, increases as traffic volumes increase and the number of active Service Users with a Gamma connection increases. The impact of which could be a severe and sustained deterioration in performance for all Service Users as a single Service User crowds out the activities of others or a failure in the service for all.

This paper summarises the business case for the proposed SECMP0067 ‘Service Request Traffic Management’.

1.2 System Usage

Currently half of on-demand Service Requests are received before 8am, as shown in Figure 1.2, with the majority of this traffic being the Service Requests 4.6.1 Retrieve Import Daily Read Log and 4.8.1 Read Active Import Profile Data, as shown in Figure 1.2. Scheduled Service Requests are also distributed across this window by the DSP.

This period of concentrated service traffic is when the service is most at risk from environmental shocks such as freak weather events or Service User incidents as utilisation will be at its highest, reducing the services ability to absorb or withstand these events.

In contrast while the service load is typically concentrated into the first 8 hours of the day, the timing of the peak event within each day is transient and shifts from day to day depending on the specific activities of Service Users on that day. Peak load within a day can be anywhere between 3 and 4 times the average load during that day. If any environmental shock or Service User incident collides with this peak, again the services ability to absorb or withstand these events will be reduced.

While Service Request volumes are low today, at some 66 million Service Requests in July 2019, they’re predicted to grow nearly ten-fold over the next 12 months, to reach above 500 million a month in July 2020 and exceed 1 billion a month by the end of 2020. Utilisation of the service today is below 10% of the current available infrastructure, while at scale both from an infrastructure and traffic perspective, average utilisation will likely be closer to 50%, once again reducing the services ability to absorb or withstand environmental or Service User events.

These factors combine to increase the risk over time of environmental shocks or Service User incidents, indescriminatly crowding out the activities of all, irrespective of a Service User being at fault or not, with no consideration of the importance of the Service Request to the Service User and their customers.

Figure 1-1. Aggregate On-Demand Service Requests Per Second (15th July to 19th July 2019)

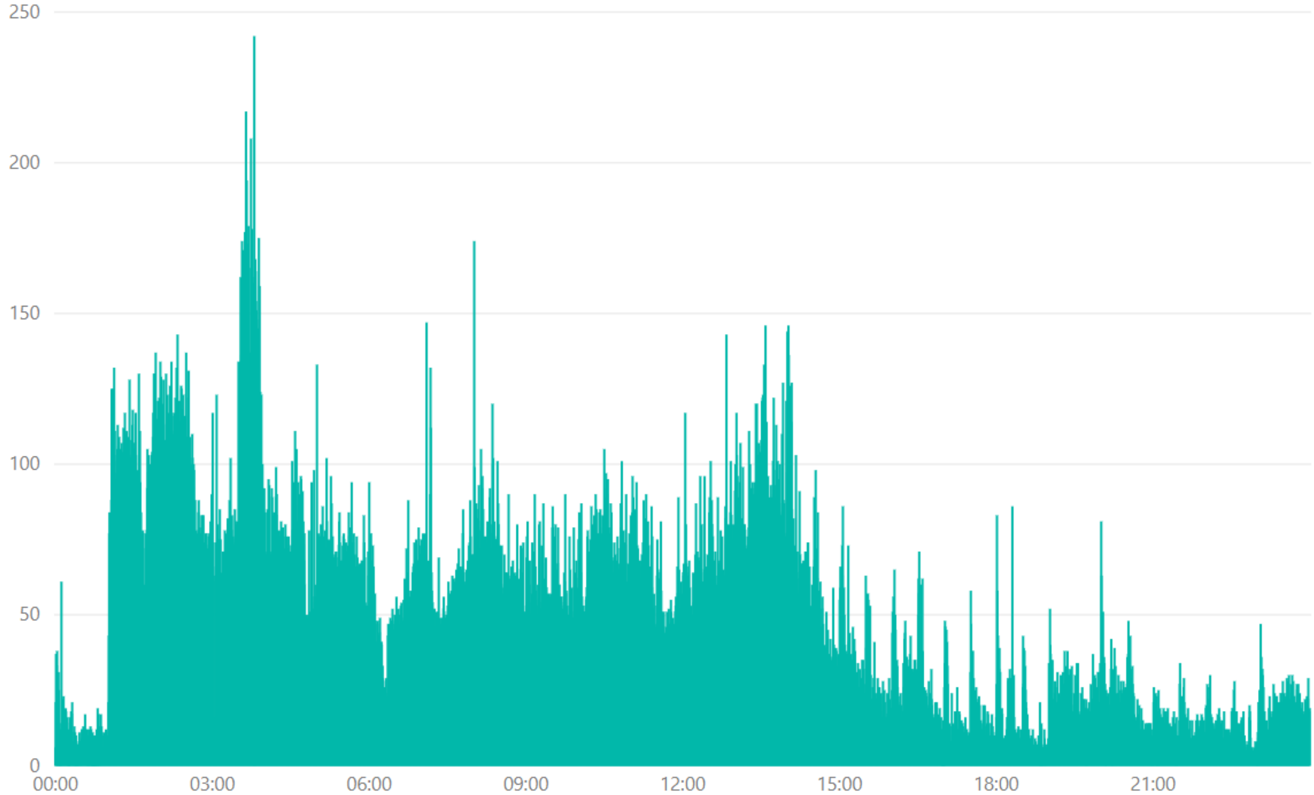
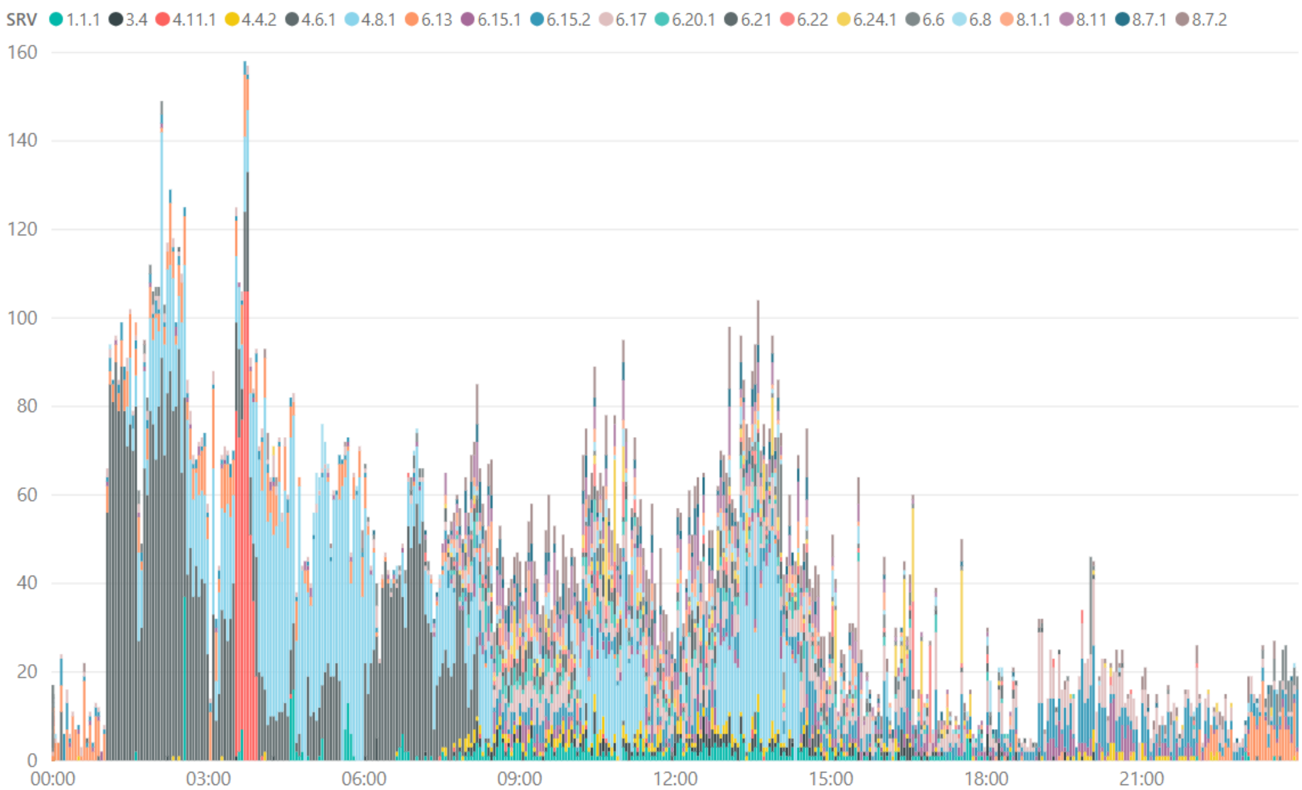


Figure 1-2. Aggregate On-Demand Top 20 Service Requests Per Second (15th July to 19th July 2019)



1.3 Traffic Scenarios

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

Table 1-1. Traffic Scenarios

Scenario	Description	Risk of Occurance
Service User Technical or Human Error	A technical or human error within a Service Users systems triggers a Service User to submit a days or a months volume of Service Requests in a matter of minutes or seconds.	Service User issues with their back-end systems are monthly events. New entrants to the market increase this risk as their back-end systems may not be as developed as existing Service Users. At least one event in the past 12 months led to a Service User trigerring the submission of Service Request volumes many times their expected volume
Environmental Factors	Extreme weather (e.g. storms, floods) will likely create periods of concentrated and additional traffic pre and post such events	Extreme weather events could trigger the failure of part of the National Grid Transmission System or a Grid Supply Point (GSP) substation, which could impact upwards of 100,000 households. These events typically occur between 5 and 10 times a year
Denial of Service Attack	Denial of sevice events in which the perpetrator seeks to make network resource unavailable by temporarily or indefinitely disrupting services may prevent service users from submitting priority service requests and responding to the needs of vulnerable customers	Denail of Service Attacks grow in frequency and impact each year, especially targeting critical infrastructure. A recent attack on a US energy company in March 2019 led to *"interruptions of electrical system operations"* for more than 10 hours. The risk to of such attacks only increase as the service scales, with at least one likely in the next two years
DCC System Failure	System failure over extended periods may create a backlog of priority service requests that under the current system would not be prioratised above other service requests	DCC's target availability measure of 99.99% implies the equivalent of a service outage of 1 hour each year. Environmental factors creating physical damage to key components or critical events such as Telefonica's network outage in December 2018 could see a service outage for an extended period of time

1.4 Business Case

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

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

Table 1-2. Business Case

Business Case	Financial Impact
Delays to the Installation and Commission Process	A one hour delay to the installation and commission process across a workforce of 10,000 engineers would result in the loss of 10,000 workforce hours, which at a cost of £20 per hour per engineer, is equivalen to £200,000. This may result in additional costs in the form of missed appointments, which would need to be rebooked, to the frustration of customers and require engineers to work overtime to complete their target number of installations
Vulnerable Consumers May be Unable to Top-Up Their Pre-Payment Meters	A one hour delay to consumers being unable to top-up their meters could create thousands of additional calls to the affected Service Users call centre. With nearly 5 million pre-payment customers, if 1% of these are unable to top-up and call a Service Users call centre this could create an additional 50,000 calls to the call centre, at a typical cost of a call made to a call centre of £5, this would equate to £250,000. Additionally the call centre would be unable to assist these customers as they could not interact with the meter
Disruption to Business Processes	A one hour delay to business processes at critical times may push these outside of the operational windows of a Service User which may disrupt a Service Users internal data processing processes. Industry wide disruption to the timing of business process would likely be in excess of £250,000
Inability to Respond to and Address Customer Issues Efficiently	Service Users may not be able to respond to consumers who have directly contacted them due to issues or questions related to their smart meters which could lead to customer dissatisfaction. Across industry this could result in lost efficiency gains from Smart Meters in excesss of £100,000
Negative Press coverage	Disruption to the service and any associated negative or harmful consumer experiences reported by the press could supress customer interest in smart meters and slow the roll-out and delay consumers and Service Users sharing the benefits of the Smart Metering Programme. Smart Energy GB, reportedly spent £20m on advertising in 2016. If negative publicity around any events is only equivalent to 1% of this budget, its value would be £200,000

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

With environmental shocks alone likely to occur multiple times a year, this modification could shield Service Users from millions of pounds of additional costs at scale.