Data Communications Company

DCC Performance Measurement Report

Performance Measurement Period:

September 2019

Version:	**V1.0**
Date:	**04/11/2019**
Security Classification:	**DCC Controlled – Panel, Ofgem, BEIS and SEC Parties Only**

Table of Contents

Control Sheet **6**
1 Introduction **7**
1.1 Purpose 7
1.2 Content 7
1.3 Scope 8
1.4 Confidential Information 8
2 Executive Summary **9**
3 Code Performance Measures **17**
3.1 Service Levels Attained 17
3.1.1 Service Level below Minimum – CPM1 22
3.1.2 Service Level below Minimum – CPM3 22
3.1.3 Service Level below Minimum – CPM4 23
3.1.4 Category 1 and 2 Incident Resolution – CPM4 23
3.1.5 Category 3, 4 and 5 Incident Resolution - CPM5 24
3.1.6 CPM4 and CPM5 – Incidents Re-Opened after Closure 24
3.1.7 Incident Resolution Information – CPM 4 & 5 24
3.2 Performance Level Exemptions 26
3.2.1 CPM4/5 - Incidents which the DCC is responsible for resolving and are resolved in accordance with the Incident Management Policy within the Target Resolution Time. 27
4 Reported List of Service Provider Performance Measures DSP **28**
4.1 Service Levels Attained 28
4.2 Performance Measurement Exceptions 29
5 Reported List of Service Provider Performance Measures CSP North **30**
5.1 Service Levels Attained 30
5.2 Performance Measurement Exceptions 32
5.2.1 PM1.4 SMWAN Connectivity Level 32
6 Reported List of Service Provider Performance Measures CSP Central **35**
6.1 Service Levels Attained 35
6.2 Performance Measurement Exceptions 37
6.2.1 PM1.1 First Time SMWAN Connectivity 37
6.2.2 PM1.3 SMWAN Connectivity Level 38
6.2.3 PM11 Accuracy of Coverage Database 39
7 Reported List of Service Provider Performance Measures CSP South **40**
7.1 Service Levels Attained 40

7.2 Performance Measurement Exceptions 42
7.2.1 PM1.1 First Time SMWAN Connectivity 42
7.2.2 PM1.3 SMWAN Connectivity Level 43
7.2.3 PM11 Accuracy of Coverage Database 43
8 Reported List of Service Provider Performance Measures S1SP SIE 45
8.1 Service Levels Attained 45
8.2 Performance Measurement Exceptions 45
9 Reported List of Service Provider Performance Measures S1SP Capgemini 46
9.1 Service Levels Attained 46
9.2 Performance Measurement Exceptions 46
10 Reported List of Service Provider Performance Measures S1SP Vodafone. 47
10.1 Service Levels Attained 47
10.1.1 Service Level Below Target Service Level 47
10.1.2 Service Level Below Target Service Level 47
10.2 Performance Measurement Exceptions 48
11 Service Credits 49
12 DCC's Internal Costs and/or External Cost 51
13 Appendices 52
13.1 Appendix A – Open Problem & Incidents relating to Prior Periods 52
13.1.1 52
13.1.2 52
13.1.3 53
13.1.4 53
13.1.5 54
13.1.6 54
13.1.7 55
13.1.8 55
13.1.9 56
13.1.10 56
13.1.11 56
13.1.12 57
13.1.13 58
13.1.14 59
13.1.15 59
13.1.16 59

13.1.17 60
13.1.18 60
13.1.19 61
13.1.20 61
13.1.21 62
13.1.22 62
13.1.23 63
13.1.24 63
13.1.25 64

Control Sheet

Table below details all enduring changes made to the report this month.

Page No.	Change
28	Section 4.1 – Monthly and Quarterly Performance Measures separated in DSP Performance Measures table
30/31	Section 5.1 – Monthly and Quarterly Performance Measures separated in CSPN Performance Measures table
35/36	Section 6.1 – Monthly and Quarterly Performance Measures separated in CSPC Performance Measures table
40/41	Section 7.1 – Monthly and Quarterly Performance Measures separated in CSPS Performance Measures table
45	Section 8.1 – Monthly and Quarterly Performance Measures separated in S1SP SIE Performance Measures table
47	Section 10 added for S1SP Vodafone

1 Introduction

1.1 Purpose

The Smart Energy Code (SEC) sets out the operational Service Levels which DCC needs to meet when providing services to DCC Users. This report provides details of the Service Levels achieved in respect of the Code Performance Measures set out in Sections H13.1 and L8.6 of the SEC and such Service Provider Performance Measures as are specified in the Reported List of Service Provider Performance Measures document[1].

Service Levels are reported following the end of each calendar month and this report is provided within 25 working days following the end of each calendar month.

This report is provided to the Panel, SEC Parties, the Authority and (on request) the Secretary of State.

1.2 Content

A Target Service Level and Minimum Service Level apply to each of the Code Performance Measures and to the Service Provider Performance Measures in the Reported List of Service Provider Performance Measures[2]. This report sets out the Service Levels achieved in respect of each Performance Measure[3].

Where the Service Level achieved for a Performance Measure is less than the Target and/ or Minimum Service Level, the report provides the reasons for this. Where the Service Level achieved is less than the Minimum Service Level the report also outlines the mitigating actions DCC is taking to prevent re-occurrence.

Where the Service Level achieved is less than the Target Service Level, Service Points are accrued by the DCC Service Provider. Service Points are then converted into Service Credits (monetary amount). Any Service Credits due from the DCC Service Provider are treated as a reduction in their charges and may be reflected in a reduction in DCC's Internal Costs and/ or External Costs. The method for calculating Service Points and Service Credits is detailed in the DCC Service Provider contracts in Schedule 2.2.

[1] The Reported List of Service Provider Performance Measures document was provided 18th December 2015 to Parties, the Panel and the Authority by the Secretary of State and identifies itself as being produced for the purposes of Section H13; it can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures.
[2] The Target and Minimum Service Levels are defined in Sections H13.1 and L8.6 of the SEC and in the Reported List of Service Provider Performance Measures document.
[3] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

1.3 Scope

This document reports on the performance of the DCC Service against the Performance Measures for September 2019.

1.4 Confidential Information

This report is classified as DCC Controlled in accordance with the confidentiality provisions under Section M of the SEC. Where the Service Level achieved is below the Target / Minimum Service Level and the reasons for this or the mitigating actions being taken by DCC are classified as DCC Confidential, this shall be reported in an annex to this report which shall be available on request.

2 Executive Summary

Code Performance Measure (CPM) Summary

CPM1 measures Percentage of On-Demand Service Responses delivered within the applicable Target Response Time, the Service Level achieved is 97.82% and is below the Target Service Level, further details provided in Section 3.1.1.

CPM3 measures Percentage of Alerts delivered within the applicable Target Response Time, the Service Level achieved is 98.85% and is below the Target Service Level, further details provided in Section 3.1.2.

CPM4 measures Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time, the Service Level achieved is 83.33% and is below the Minimum Service Level, further details provided in Section 3.1.3.

The Service Levels achieved for CPM2, CPM5, CPM6, CPM7 and CPM8 are all above the Target Service Level.

Service Provider Performance Measures Summary

S1SP Vodafone Combined monthly IoT Core and Management Service Availability, the Service Level achieved is 99.48% and is below the Minimum Service Level.
Further details are provided in Section 10.1.1.

S1SP Vodafone Monthly Management Service Availability (API, Reporting, Provisioning, GUI, Portal), the Service Level achieved is 99.57% and is below the Minimum Service Level. Further details are provided in Section 10.1.2.

Where the Performance Measure is reportable, all other Service Provider Performance Measures are above the Target Service Level.

Any Service Credits accrued for this measurement period are detailed in Section 8 of the report.

Key Incidents – September Closed in Period

Incident Reference	**INC000000477267 – Category 2**
Problem Reference	**PBI000000117100**
System(s) Impacted	Install and commissions
Incident Start Date / Time (Logged in Remedy)	01/08/2019 12:24
Incident Resolved Date / Time	29/08/2019 11:22
Major Incident Duration	27 days 22 hrs 58 mins Pending – User Action for 26 days 19 hrs 23 mins Actual Major Incident Duration = 1 days 3 hrs 34 mins
Region Impacted	South / Central
Resolved within SLA	No
Summary of High Category Incident	

On 1st August at 12:24 a Service User reported multiple devices not changing to Commissioned state in SSI and returning “Unexpected Device” failure messages.
Customer Impact
Due to the orchestration method employed by the Service User installs and commissions could not be completed for affected devices, impacting a key business aspect.

Incident Reference	**INC000000486219 – Category 2**
Problem Reference	**PBI000000117102**
System(s) Impacted	CSP North RNI infrastructure (Degradation)
Incident Start Date / Time (Logged in Remedy)	30/08/2019 10:27 30/08/2019 12:27 raised to a CAT2 due to Service Users advising they were experiencing delays in installing
Incident Resolved Date / Time (Logged in Remedy)	30/08/2019 15:34
Major Incident Duration	5 Hours 7 Minutes
Region Impacted	North
Resolved within SLA	Yes
Summary of High Category Incident	
At 08:48 DSP SME flagged an increase in E21’s being generated from CSP North infrastructure to DCCMIM. This was escalated into CSP North MIM at 09:00 for them to carry out preliminary investigations. Installs could still be seen happening in the Northern Region. Initial ticket was raised by Service Users at 10:27 with limited information and 3 example install attempts in the Northern Regions and it was confirmed that only one out of the three SEC parties under that particular Service User’s umbrella were experiencing issues and the other 2 were working as normal.	
Customer Impact	
One Service User reported that one out of 3 of their SEC parties was experiencing issues installing in the North. Further Service Users started to report a degraded impact to their installation process in the North region only. An estimated 600 installs in the North were impacted.	

Incident Reference	**INC000000487108 – Category 2**
Problem Reference	**PBI000000117106**
System(s) Impacted	Birthing Events
Incident Start Date / Time (Logged in Remedy)	04/09/2019 09:13 04/09/2019 09:18 (Escalated to CAT2)
Incident Resolved Date / Time	04/09/2019 09:58

Major Incident Duration	48 minutes
Region Impacted	South / Central
Resolved within SLA	Yes
Summary of High Category Incident	
On 4th September at 08:48 Service User experienced incorrect states being reported for newly-birthed meters. Indicator lights on the meter showed the device as birthed yet sending SRV 8.2 confirmed the device in the wrong state. Over 30 meters were known to have experienced this behaviour when the incident was raised with DCC Service Centre.	
Customer Impact	
The issue was reported by 2 service users and only affected installs in the Central & South region. No other impact to any other service, or service user, was reported.	

Incident Reference	**INC000000491661 – Category 2**
Problem Reference	**PBI000000117205**
System(s) Impacted	Service Requests
Incident Start Date / Time (Logged in Remedy)	12/09/2019 23:24
Incident Resolved Date / Time	13/09/2019 01:31
Major Incident Duration	2 hrs 7 mins
Region Impacted	All Regions
Was the Incident prioritised correctly?	Yes
Resolved within SLA	Yes
Summary of High Category Incident	
Connectivity lost between DSP and CSP, Service Users. Service was restored by DSP failing over their F5 services from their secondary Data Centre to the Primary.	
Customer Impact	
1. Traffic between SUs and DSP was slow for a period and then was interrupted. SUs would have received some http500 errors from SRVs submitted to DSP. Additionally, there was a delay in receiving responses and device alerts from DSP. These were queued and delivered later. 2. Traffic to Arqiva was affected for a period. This was already of a reduced volume due to the first point. 3. The DSP Motorway successfully processed messages that it received, scheduled requests and future dated requests for Telefonica were successful and queued northbound, however scheduled requests and future dated requests for Arqiva were affected as per point 2. 4. TEF traffic continued to flow.	

Incident Reference	**INC000000493155 – Category 2**
Problem Reference	**PBI000000117128**
System(s) Impacted	Comms Hub birth events in the CSP North region
Incident Start Date / Time (Logged in Remedy)	17/09/2019 14:26
Incident Resolved Date / Time	17/09/2019 15:58
Major Incident Duration	49 minutes
Region Impacted	North region only
Resolved within SLA	Yes
Summary of High Category Incident	
Service Centre received reports from a service user of comms hubs not birthing in CSP North region only. Arqiva confirmed an issue on a process within their Comms Hub Manager that was preventing installs to be posted to DSP. This was also confirmed to have impacted multiple Service Users, although not all SUs reported issues and those that did advised that workarounds were available (by sending SR 8.4s).	
Reported Customer Impact	
Multiple Service User experienced delays when birthing comms hubs in the CSP North region. The impacted Service Users had a workaround in place to birth the comms hubs, but this required a lot of manual intervention.	

Incident Reference	**INC000000493559 – Category 2**
Problem Reference	**PBI000000117309**
System(s) Impacted	SMETS1 Service Requests
Incident Start Date / Time (Logged in Remedy)	DSP Truesight generated at 18:30 18/09/2019 DCCMIM CAT2 – 20:44
Incident Resolved Date / Time	00:58 (19/09/2019)
Major Incident Duration	6 Hours 28 Minutes
Region Impacted	All SMETS1 meters
Resolved within SLA	Yes
Summary of High Category Incident	
SMETS1 – DCC TOC identified that all SMETS1 Service Request activity was failing from 18:17 UTC with full service being restored by the DSP at 23:04BST for all SMETS1 devices. This affected a small subset of migrations (13) on the 18/09/2019.	
Customer Impact	
No Customer Impact as service was restored before the 4.6.1 meter reads were scheduled. There was a small subset of migrations (13) which froze which may have been impacted due to the CRL expiring. Fixed Forward today.	

Key Incidents Excluded Through PMEL

Incident Reference	**INC000000487105 – Category 2**
Problem Reference	**PBI000000117106**
System(s) Impacted	Birthing Events
Incident Start Date / Time (Logged in Remedy)	04/09/2019 08:41:06
Incident Resolved Date / Time	04/09/2019 09:25:27
Major Incident Duration	44 mins
Region Impacted	South / Central
Resolved within SLA	Yes
Summary of High Category Incident	
Following the resolution of this alarm, it was identified that it was related to INC000000487108.	
Customer Impact	
The issue was reported by 2 service users and only affected installs in the Central & South region. No other impact to any other service, or service user, was reported.	

Incident Reference	**INC000000488824 – Category 2**
Problem Reference	**PBI000000117115**
System(s) Impacted	SSI / SSMI unavailable
Incident Start Date / Time (Logged in Remedy)	07/09/2019 12:42
Incident Resolved Date / Time	07/09/2019 15:14
Major Incident Duration	2 Hours 32 Minutes
Region Impacted	All Regions
Resolved within SLA	Yes
Summary of High Category Incident	
On 7th September at approximately 12:40 DCC identified an error message was being returned when attempting to access services in SSMI. Service users also called into the Service Centre advising SSI was unavailable. DSP had received an automated alert 488812 at approximately 12:30 and had escalated to their SME at the point DCC became aware of the system issue.	
Customer Impact	
This impacted Service Users ability to troubleshoot any issues with existing or new installations. DCC could not conduct troubleshooting and triage of new incidents. There was no impact to the DSP 'Motorway', only reporting and a delay to SAT file transfers	

Incident Reference	**INC000000488712 – Category 2**
Problem Reference	**PBI000000117115**
System(s) Impacted	SSI / SSMI unavailable
Incident Start Date / Time (Logged in Remedy)	07/09/2019 12:43
Incident Resolved Date / Time	07/09/2019 15:14
Major Incident Duration	2 Hours 31 Minutes
Region Impacted	All Regions
Resolved within SLA	Yes
Summary of High Category Incident	
Identified as the same issue as INC000000488824 and related at 07/09/2019 14:40.	
Customer Impact	
This impacted Service Users ability to troubleshoot any issues with existing or new installations. DCC could not conduct troubleshooting and triage of new incidents. There was no impact to the DSP 'Motorway', only reporting and a delay to SAT file transfers	

Incident Reference	**INC000000488812 – Category 2**
Problem Reference	**PBI000000117115**
System(s) Impacted	SSI / SSMI unavailable
Incident Start Date / Time (Logged in Remedy)	07/09/2019 12:30
Incident Resolved Date / Time	13:35 07/09/2019
Major Incident Duration	2 Hours 32 Minutes
Region Impacted	All Regions
Resolved within SLA	Yes
Summary of High Category Incident	
Identified as the same issue as INC000000488824 and related at 07/09/2019 13:48.	
Customer Impact	
This impacted Service Users ability to troubleshoot any issues with existing or new installations. DCC could not conduct troubleshooting and triage of new incidents. There was no impact to the DSP 'Motorway', only reporting and a delay to SAT file transfers	

Non DCC Service Impacting

Incident Reference	**INC000000487736 – Category 2**
Problem Reference	**PBI000000117117**
System(s) Impacted	SMETS 1 Migrations are failing with error ET08
Incident Start Date / Time (Logged in Remedy)	06/09/2019 09:42 (CAT2 11:34)
Incident Resolved Date / Time	09/09/2019 12:56:11
Major Incident Duration	3 Days 3 hours 14 minutes
Region Impacted	All Regions
Resolved within SLA	No
Summary of High Category Incident	
On Friday 6th September an issue was identified by the MCC team advising they had seen failed Migrations due to an ET08 failure code. 27 of the 119 planned migrations failed with the ET08 error. The remaining migrations were then paused to stop any further failures whilst a fix was developed and Implemented.	
Customer Impact	
There was no direct customer impact as a result of this incident.	

Incident Resolution not DCC Responsibility

Incident Reference	**INC000000491743 – Category 2**
Problem Reference	**PBI000000117305**
System(s) Impacted	Motorway Northbound message queue
Incident Start Date / Time (Logged in Remedy)	13/09/2019 08:10
Incident Resolved Date / Time	13/09/2019 13:40
Major Incident Duration	5hrs 30mins
Region Impacted	All regions
Resolved within SLA	Yes
Summary of High Category Incident	
On 13th September at 08:10 DSP raised a Category 3 ticket, as they could see message queues for a specific set of service users increasing. Initial checks by DSP indicated that the issue could be due to how the Service User is handling message acknowledgements, as all the affected service users are hosted through their connection. DSP engaged DCC MIM to advise, as other Service Users were continuing to manage message queues and install without issue. While DCC MIM were engaging contact points at the Service User a number of the Service User-hosted service users raised calls for failed SRVs and impact to installs and commissioning. The incident was upgraded to Category 2 and a technical bridge call held between DCC, DSP and Service User. During the technical bridge call it was discovered that the message acknowledgement service at the Service User was working as designed but struggling to handle the increased volume (backlog) of messages resulting from a 90-minute interruption to the DSP service provision overnight.	

The Service User made changes to their acknowledgement process and the backlog reduced as message throughput increased.
Customer Impact
As message acknowledgement was delayed, service users were not receiving responses to Service Requests in a timely manner. This affected normal business operations, including Install and Commissioning activity.

3 Code Performance Measures

3.1 Service Levels Attained

This section reports the Service Levels achieved in September 2019 against the targets specified in Sections H13.1 and L8.6 of the SEC.

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
CPM1	**Percentage of On-Demand Service Responses delivered within the applicable Target Response Time.**			**92.42%**	**97.82%**	**99.00%**	**96.00%**
	PM1.1	Percentage of DSP Service Request Times within relevant TRT	DSP	99.83%	98.91%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP SIE	84.57%	92.60%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP Capgemini	99.96%	99.75%	99.00%	96.00%
	PM1.4	Percentage of DCC Service Request Times within relevant TRT	DSP	99.93%	99.94%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPN	99.67%	88.70%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPC	75.69%	99.03%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPS	64.65%	98.50%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPN	100.00%	100.00%	85.00%	80.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPC	99.97%	99.95%	99.00%	90.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPS	99.96%	99.95%	99.00%	90.00%
CPM2	**Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time**.			**99.92%**	**99.88%**	**99.91%**	**96.00%**
	PM1.2	Percentage of DSP Service Response Times within relevant TRT	DSP	100.00%	100.00%	99.00%	96.00%
	PM1.3	Percentage of DSP Service Request Scheduling Times within relevant Target Response Time (as set out in Part C of this Appendix 1)	DSP	100.00%	100.00%	99.00%	96.00%
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPN	99.09%	98.71%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPC	100.00%	100.00%	99.00%	96.00%
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPS	100.00%	100.00%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPN	100.00%	100.00%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPC	100.00%	100.00%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPS	100.00%	100.00%	99.00%	96.00%
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPN	100.00%	100.00%	99.00%	96.00%
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPC	100.00%	99.99%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPS	99.99%	99.99%	99.00%	96.00%
CPM3	**Percentage of Alerts delivered within the applicable Target Response Time.**			**98.37%**	**98.85%**	**99.00%**	**96.00%**
	PM1.5	Percentage of DSP Alert Response Times within relevant Target Response Time (as set out in Part C of this Appendix 1)	DSP	99.20%	99.93%	99.00%	96.00%
	PM1.5	Percentage of S1SP SMETS1 Alert Response Times within relevant Target Response Time	S1SP SIE	No Events	99.94%	99.00%	96.00%
	PM1.7	Percentage of S1SP SMETS1 UTRN Response Times within relevant Target Response Time	S1SP SIE	No Events	No Events	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPN	94.55%	94.66%	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPC	99.88%	99.89%	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPS	99.86%	99.84%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
CPM4	**Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.**			**33.33%**	**83.33%**	**100.00%**	**85.00%**
CPM5	**Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 3, 4 or 5 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.**			**92.72%**	**91.25%**	**90.00%**	**80.00%**
CPM6	**Percentage Availability – Self Service Interface**			**100.00%**	**100.00%**	**99.50%**	**98.00%**
	PM2.4	Percentage Service availability – Self Service Interface (Production Services)	DSP	100.00%	100.00%	99.50%	98.00%
CPM7	**Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services.**			**100.00%**	**100.00%**	**99.00%**	**96.00%**
	PM1.1	Batch requests for device certificates maximum 375,000 for RA system received 07:00-18:00 available by 06:59 next day	TSP	100.00%	100.00%	100.00%	95.00%
	PM1.4	Single certificate requests via RA System 100% within 30 seconds	TSP	100.00%	100.00%	100.00%	99.00%
	PM1.7	Single certificate request via system to system interface in Core Service Hours (maximum 12 certificate requests/second) 100% within 15 seconds	TSP	100.00%	100.00%	100.00%	99.00%
CPM8	**Percentage of documents stored on the SMKI repository delivered within the applicable Target Response Time for the SMKI Repository Service.**			**100.00%**	**100.00%**	99.00%	100.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM13	Percentage of documents stored on the SMKI Repository delivered within the applicable Target Response Time for the SMKI Repository Service.	DSP	100.00%	100.00%	99.00%	96.00%
	PM1.8	Processed certificate or binding is made available to PKI repository within 10 seconds	TSP	100.00%	100.00%	99.00%	96.00%

Table 1 - DCC Code Performance Measures

3.1.1 Service Level below Minimum – CPM1

Percentage of On-Demand Service Responses delivered within the applicable Target Resolution Time

The Service Level reported for CPM1 is 97.82% and is below the Target Service Level.

CSPN PM2 reported Service Level was 88.70% and is below Minimum Service Level This measure has gone to red this month due to 1.4 million firmware payloads missed out of 12.4 million. This was due to errors occurred on the CSPN RNI, patches have been applied and the issue has been resolved.

CSPS PM2 reported Service Level was 98.50% and is below Target Service Level

This measure has improved to Amber this month due to the Smart M2M release 8.5. There is still work ongoing to resolve the issues which are preventing CSPS from meeting the target. The largest proportion of these failures should be remedied with the implementation of Smart M2M release 9.

S1SP SIE PM1.1 reported Service Level was 92.60% and is below Minimum Service Level. A defect with the SIE message processing system was identified under Problem Investigation PBI000000117104, and an enduring solution implemented on 30 September 2019. Monitoring of this fix will continue throughout October.

3.1.2 Service Level below Minimum – CPM3

Percentage of Alerts delivered within the applicable Target Resolution Time

The Service Level reported for CPM3 is 98.85% and is below the Target Service Level.

CSPN PM3.2 reported Service Level was 94.66% and is below Minimum Service Level. Over 12 million Cat 3 alerts on the CSPN region CH installs, Arqiva estimate that this is being caused by around 100 meters. Of the 12 million alerts, 600k alerts were missed, Arqiva was unable to process the exclusions of the majority of these 600k alerts. This is

due to Arqiva's system which can only run 15k duplicates per day. Arqiva is working with Service Users to get these devices investigated. With over 80% of the of the alerts coming from a single Service Users meters. Work is also underway to remove duplicate alerts and Release 2 is will fix several defects that are causing alerts. Problem record PBI000000116412. Arqiva has requested a let for this service measure which is being investigated by DCC.

3.1.3 Service Level below Minimum – CPM4

Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.

The Service Level reported for CPM4 is 83.33% and is below the Minimum Service Level. This was as a result of one failure to meet SLA on Category 2 Incidents.

The aforementioned incident that failed to meet SLA was INC000000477267, which spent the majority of its life-cycle as a Category 2 Incident. However, in review, it was agreed that the incident should have been escalated to a retrospective Category 2 Incident because this would have impacted multiple Service Users when birthing CH's.

3.1.4 Category 1 and 2 Incident Resolution – CPM4

Incident Volumes – Closed in Measurement Period

CPM4 measures Incident resolution performance for Category 1 and 2 Incidents that were Closed in the Measurement Period. The table below illustrates how many of the Incidents were closed in the Measurement Period and of those, how many failed to meet the Service Level Requirements defined in the SEC.

Category	Total Incident Count	Within SLA	Failed SLA
Category 1	0	0	0
Category 2	6	5	1
Total	**6**	**5**	**1**

Table 2 - CPM4 Incident Count

For Information only:

Prior to any Performance Measurement Exclusions Applied (3 Incidents excluded that were internal to DCC)

Category	Total Incident Count	Within SLA	Failed SLA
Category 1	0	0	0
Category 2	12	10	2
Total	**12**	**10**	**2**

Table 3 – CPM4 Pre-PMEL Incident Count

3.1.5 Category 3, 4 and 5 Incident Resolution - CPM5

Incident Volumes – Closed in Measurement Period

CPM5 measures Incident resolution performance for Category 3, 4 and 5 Incidents that were Closed in the Measurement Period. The table below illustrates how many of the Incidents were closed in the Measurement Period and of those, how many failed to meet the Service Level Requirements defined in the SEC.

Category	Total Incident Count	Within SLA	Failed SLA
Category 3	59	46	13
Category 4	82	68	14
Category 5	1,322	1,221	101
Total	**1,463**	**1,335**	**128**

Table 4 - CPM5 Incident Count

3.1.6 CPM4 and CPM5 – Incidents Re-Opened after Closure

Where an incident that has been closed and their Service Level reported on in a previous period, and re-opened and Closed in this reporting period, the Service Level reported may be subject to change. The new Service Level will be documented below:

No Incidents Closed in this period have been re-opened and reported in a previous period.

3.1.7 Incident Resolution Information – CPM 4 & 5

For information only

Incident Volumes - Raised at any point in time and in a Resolved Status at the point of extract. (Point of Extract: 1st of the Month following the reporting period)

Category	Within SLA	Failed SLA	SLA Pass %
Category 1	0	0	N/A
Category 2	1	0	100.00%
Total	**1**	**0**	**100.00%**

Table 5 - Incidents Relating to CPM4

Category	Within SLA	Failed SLA	SLA Pass %
Category 3	10	4	60.00%
Category 4	21	4	80.95%
Category 5	168	32	80.95%
Total	**199**	**40**	**79.90%**

Table 6 - Incidents Relating to CPM5

Incident Volumes assigned to Service Users – Tickets not Closed (Raised at any point in time - Point of Extract: 1st of the Month following the reporting period)

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2018 June					1	**1**
2018 July					2	**2**
2018 August					51	**51**
2018 September					75	**75**
2018 October					148	**148**
2018 November				1	245	**246**
2018 December					383	**383**
2019 January				1	647	**648**
2019 February			2	1	454	**457**
2019 March			1	1	640	**642**
2019 April					803	**803**
2019 May			5	2	697	**704**
2019 June			7	2	1,626	**1,635**
2019 July			15	3	1,773	**1,791**
2019 August			14	4	2,112	**2,130**
2019 September			51	7	2,922	**2,980**
Total			**95**	**22**	**12,579**	**12,696**

Table 7 - Aged Incidents Assigned to Service Users

Analysis of these aged incidents show that the top 3 issues are;

Incorrect Communications Hub Variant Installed – 6,823
Incorrect Credentials Loaded on to Device – 3,391
DUIS Service Request 8.14. not received – 1,034

** As 89% of the total number of Incidents considered aged the due to the three reasons above, these items will be discussed at length during the SECOPS meeting scheduled for 04/11/2019. During which, all possible solutions will be considered and an appropriate action plan will be generated.

Incident Volumes assigned to Service Providers or DCC Resolver Teams – Tickets not Closed (Raised at any point in time - Point of Extract: 1st of the Month following the reporting period)

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2018 May					2	**2**
2018 July					1	**1**
2018 September				1	7	**8**
2018 October					1	**1**
2018 November					24	**24**
2018 December					32	**32**
2019 January					90	**90**
2019 February					37	**37**
2019 March			2		108	**110**
2019 April					73	**73**
2019 May			1		77	**78**
2019 June				2	124	**126**
2019 July					171	**171**
2019 August			1	4	247	**252**
2019 September			12	11	269	**292**
Total			**16**	**18**	**1,263**	**1,297**

Table 8 - Aged Incidents Assigned to Service Providers or DCC

**DCC Incident Management have a process whereby the aged incidents are split into Service User and Service Provider. These are worked through on a daily basis in an attempt to bring the number of aged incidents down.

3.2 Performance Level Exemptions

In accordance with the Performance Measurement Methodology document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below.

No Service Providers requested exemptions this period.

3.2.1 CPM4/5 - Incidents which the DCC is responsible for resolving and are resolved in accordance with the Incident Management Policy within the Target Resolution Time.

Exception Type	Total Incidents
User Responsibility	498
Total	**498**
Exclusion Type	
Alert / Event Monitoring (For Information only)	2,216
Duplicate	638
Cancelled	93
Production Proving / Testing	10
Internal to DCC – Non DCC Impacting	9
Total	**2,966**
Grand Total	**3,464**

Table 9 - PMEL Exclusions Detail

4 Reported List of Service Provider Performance Measures DSP

4.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service availability – DCC Data Service	Monthly	100.00%	100.00%	99.95%	99.00%
	2.2	Service availability – DCC User Interface	Monthly	99.99%	99.99%	99.95%	99.00%
	2.3	Service availability – DCC Service Management	Monthly	100.00%	99.85%	99.50%	98.00%
	2.4	Service availability – Self Service Interface	Monthly	100.00%	100.00%	99.50%	98.00%
	2.5	Service availability – Average Interface (DCC Internal availability	Monthly	100.00%	100.00%	95.00%	90.00%
	2.7	Service availability - Test services	Monthly	97.95%	100.00%	99.00%	98.00%
Application Management	3	Category 1 or 2 Incidents directly related to a change release within 30 days of release[4]	Monthly	0	0	0	5
Anomaly Detection	11	Anomalous Service Requests	Monthly	100.00%	100.00%	99.00%	96.00%
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level	Latest Qtr. Service Level	Target Service Level	Minimum Service Level
Service Management	7	Planned Maintenance events[5]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 10 - DSP Reportable Performance Measures

[4] DCC are reviewing the contractual definition of this DSP Performance Measure
[5] Measurement Period is a Calendar Quarter

4.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

5 Reported List of Service Provider Performance Measures CSP North

5.1 Service Levels Attained

*Performance Measures are reported monthly unless otherwise specified.

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

During Q3 2018 a major incident occurred affecting the returns process. This has led to exceptions to obligations for both service users and service providers. The situation is being recovered and this will result in a bulk of returns being reported in a single period. The reporting considerations of this will be agreed across CSPs.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	99.71%	99.46%	80.00%	70.00%
	1.2	First time SMWAN connectivity within 30 days	Monthly	99.97%	99.90%	90.00%	80.00%
	1.4	SMWAN connectivity Level	Monthly	99.98%	99.97%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	99.98%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	99.78%	99.65%	99.00%	95.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	100.00%	99.90%	99.00%	96.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	384.86%	364.09%	99.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	100.00%	100.00%	99.90%	99.50%
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	No Events	No Events	99.00%	95.00%
Performance Area	**Performance Measure Number**	**Performance Measure Name**	**Measurement Period**	**Previous Qtr. Service Level**	**Latest Qtr. Service Level**	**Target Service Level**	**Minimum Service Level**
Communications Hub Connectivity	1.3	First time SMWAN connectivity within 90 days	Quarterly	99.99%	99.99%	99.00%	95.00%
Service Management	10	Notification of Planned Maintenance events within required target[6]	Quarterly	75.00%	100.00%	100.00%	90.00%

Table 11 - CSPN Reportable Performance Measures

[6] Measurement Period is a Calendar Quarter

PM12.2 - The calculation results for PM 12.2 comes as 364.09%. CSPN had a total of 1,521 CH power outages reported, in August, and all were sent to DSP within SLA. CSPN have 1,521 as MET (100%).

The formula (below) as given in Schedule 2.2.

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$\text{PM12.2} = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{\text{((Number of Communications Hub Power Loss Alerts - 50) x 0.25) + 50}} \right)$$

Using the calculation above PM12.2 = 100 * (1521/ ((1521 – 50) * 0.25) + 50) = 364.09%

5.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[7] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

5.2.1 PM1.4 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.4 (CSPN)	37,520	Failure to follow maintenance as per CHIMSM	These figures are for the reporting period (not cumulative)

Table 12 - CSPN PM1.4 Exclusions

[7] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

37,520 x CH excluded for September 2019 due to several reasons, covering: -

- Incomplete Communication Hub Install – 4,659
- Communication Hub installed on non-consumer premises e.g. Live Lab – 11
- Communication Hub in Low Coverage database – 1
- Communications Hubs where JSR is incomplete – 484
- Communications Hubs where no incident has been raised for outage – 30,847
- Communication Hubs has an incident open which is being investigated, not by Arqiva – 1
- Issue started and ended in prior month – 1,517

Explanations for the exclusions mentioned above are as follows:

Communications Hubs where no incident has been raised for outage

CSPN see the comms hub appear on its network but then do not see any traffic to or from the comms hubs for more than 10 days. This is mostly driven by service users powering on a comms hub and either not completing the install or correctly decommissioning it. As soon as the CSPN system sees the CH on the network, it will be looking for it forever. This is being investigated as part of problem ticket, data is being rationalised with the TOC. Once this has been completed the service users will be contacted to confirm the status of the CH.

Incomplete Communication Hub Install

Installations that have been aborted by the service user, but no service requests submitted. If the installation results in an install and leave then the SU should be submitting and 8.14.2 service request. If the install is fully aborted then an 8.14.3 service request should be submitted. This is being investigated as part of problem ticket, data is being rationalised with the TOC. Once this has been completed the service users will be contacted to confirm the status of the CH.

Issue started and ended in prior month

Comms Hubs where the outage incident started and ended in a previous month but are showing the in current reporting month.

Communications Hubs where JSR is incomplete

CH insufficient address details / none at all provided in order to determine if the install was compliant and in line with CSPN recommendation. This is caused by address field being optional in DUIS but in the CSPN contract it states that this is a Mandatory requirement.

Communication Hub installed on non-consumer premises e.g. Live Labs

Hubs install is confirmed as not in scope because it not installed on a consumer's premises, i.e. Live Labs.

Communication Hub in Low Coverage database

Comms Hub is installed in a low coverage area.

Communication Hubs has an incident open which is being investigated, not by Arqiva

Comms Hub has an incident related to the Outage, but this is assigned to the Service User to investigate.

6 Reported List of Service Provider Performance Measures CSP Central

6.1 Service Levels Attained

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

During Q3 2018 a major incident occurred affecting the returns process. This has led to exceptions to obligations for both service users and service providers. The situation is being recovered and this will result in a bulk of returns being reported in a single period. The reporting considerations of this will be agreed across CSPs.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	99.98%	99.98%	90.00%	80.00%
	1.3	SMWAN connectivity Level	Monthly	100.00%	100.00%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	100.00%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	99.20%	99.09%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	96.65%	99.97%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	359.89%	396.14%	98.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	No Events	No Events	99.90%	99.50%
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	No Events	No Events	99.00%	95.00%
Performance Area	**Performance Measure Number**	**Performance Measure Name**	**Measurement Period**	**Previous Qtr. Service Level**	**Latest Qtr. Service Level**	**Target Service Level**	**Minimum Service Level**
Communications Hub Connectivity	1.2	First time SMWAN connectivity within 90 days	Quarterly	100.00%	100.00%	99.00%	90.00%
Service Management	10	Notification of Planned Maintenance events within required target[8]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 13 - CSPC Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 396.14%. CSPC had a total of 15,393 CH power outages reported, in September, and all were sent to DSP within SLA.

The formula (below) as given in Schedule 2.2.

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{\text{((Number of Communications Hub Power Loss Alerts - 50) x 0.25) + 50}} \right)$$

[8] Measurement Period is a Calendar Quarter

Using the calculation above PM12.2 = 100 * (15393/ ((15393– 50) * 0.25) + 50)) = 396.14%

6.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[9] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

6.2.1 PM1.1 First Time SMWAN Connectivity

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.1 (CSPC)	2,316	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 14 - CSPC PM1.1 Exclusions

2,316 x CH excluded for September 2019 due to a number of reasons, covering: -

- There were no, or incomplete address details provided by the Service User – 1,080
- CHIMSM Not Followed - No aerial is attached for installed SKU2 Device – 821
- CHIMSM Not Followed - SKU1 Device installed when SKU2 Device is recommended - 386
- CHIMSM Not Followed - CH Never connected but received 8.14.1 - 10
- Aborted Installation – 2
- CHIMSM Not Followed - Outside TEF Committed Coverage Area – 16
- CHIMSM Not Followed - Associated with NEP – 1

[9] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

6.2.2 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	32,191	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 15 - CSPC PM1.3 Exclusions

NOTE: these exception volumes relate to the whole estate not just CH's connected in the reporting period

32,191 x CH excluded for September 2019 due to a number of reasons, covering: -

- There were no, or incomplete address details provided by the Service User – 24,043
- CHIMSM Not Followed - No aerial is attached for installed SKU2 Device – 4,931
- CHIMSM Not Followed - SKU1 Device installed when SKU2 Device is recommended – 2,943
- Aborted Installation – 166
- CHIMSM Not Followed - Outside TEF Committed Coverage Area – 82
- Partial address match – 19
- Installed out of region – 5
- Test Lab installations – 2

6.2.3 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPC)	2,316	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 16 - CSPC PM11 Exclusions

2,316 x CH excluded for September 2019 due to a number of reasons, covering: -

- There were no, or incomplete address details provided by the Service User – 1,080
- CHIMSM Not Followed - No aerial is attached for installed SKU2 Device – 821
- CHIMSM Not Followed - SKU1 Device installed when SKU2 Device is recommended - 386
- CHIMSM Not Followed - CH Never connected but received 8.14.1 - 10
- Aborted Installation – 2
- CHIMSM Not Followed - Outside TEF Committed Coverage Area – 16
- CHIMSM Not Followed - Associated with NEP – 1

7 Reported List of Service Provider Performance Measures CSP South

7.1 Service Levels Attained

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

During Q3 2018 a major incident occurred affecting the returns process. This has led to exceptions to obligations for both service users and service providers. The situation is being recovered and this will result in a bulk of returns being reported in a single period. The reporting considerations of this will be agreed across CSPs.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	99.97%	99.98%	90.00%	80.00%
	1.3	SMWAN connectivity Level	Monthly	100.00%	100.00%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	99.98%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	98.84%	98.98%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	96.56%	99.96%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	361.07%	395.82%	98.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	No Events	No Events	99.90%	99.50%
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	No Events	No Events	99.00%	95.00%
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level	Latest Qtr. Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.2	First time SMWAN connectivity within 90 days	Quarterly	100.00%	100.00%	99.00%	90.00%
Service Management	10	Notification of Planned Maintenance events within required target[10]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 17 - CSPS Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 395.82%. CSPS had a total of 14,188 CH power outages reported in September, and all were sent to DSP within SLA.

The formula (below) as given in Schedule 2.2.

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

[10] Measurement Period is a Calendar Quarter

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

Using the calculation above PM12.2 = 100 * (14188 / ((14188 – 50) * 0.25) + 50)) = 395.82%

7.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[11] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

7.2.1 PM1.1 First Time SMWAN Connectivity

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.1 (CSPS)	9,687	Failure to follow installations as per CHIMSM	SU's have not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 18 - CSPS PM1.1 Exclusions

9,687 x CH excluded for September 2019 due to a number of reasons, covering: -

- There were no, or incomplete address details provided by the Service User – 7,731
- CHIMSM Not Followed - No aerial is attached for installed SKU2 Device – 1,373
- CHIMSM Not Followed - SKU1 Device installed when SKU2 Device is recommended - 495
- CHIMSM Not Followed - CH Never connected but received 8.14.1 - 52
- CHIMSM Not Followed - 8.14.2 on Cellular – 23
- CHIMSM Not Followed - Outside TEF Committed Coverage Area – 11

[11] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

- Aborted installs – 1
- CHIMSM Not Followed – Associated with NEP – 1

7.2.2 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	37,901	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 19 - CSPS PM1.3 Exclusions

NOTE: these exception volumes relate to the whole estate not just CH's connected in the reporting period

37,901 x CH excluded for September 2019 due to a number of reasons, covering: -

- There were no, or incomplete address details provided by the Service User – 30,548
- CHIMSM Not Followed -No aerial is attached for installed SKU2 Device – 4,339
- CHIMSM Not Followed -SKU1 Device installed when SKU2 Device is recommended – 2,865
- Aborted Installation – 86
- CHIMSM Not Followed -Outside TEF Committed Coverage Area – 56
- Partial address match – 3
- Installed outside of region – 2
- CHIMSM Not Followed -Given UPRN is not available – 1
- Test Lab installations – 1

7.2.3 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPS)	9,687	Failure to follow installations as per CHIMSM	SU's have not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 20 - CSPS PM11 Exclusions

9,687 x CH excluded for September 2019 due to a number of reasons, covering: -

- There were no, or incomplete address details provided by the Service User – 7,731
- CHIMSM Not Followed - No aerial is attached for installed SKU2 Device – 1,373
- CHIMSM Not Followed - SKU1 Device installed when SKU2 Device is recommended - 495
- CHIMSM Not Followed - CH Never connected but received 8.14.1 - 52
- CHIMSM Not Followed - 8.14.2 on Cellular – 23
- CHIMSM Not Followed - Outside TEF Committed Coverage Area – 11
- Aborted installs – 1
- CHIMSM Not Followed – Associated with NEP – 1

8 Reported List of Service Provider Performance Measures S1SP SIE

8.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service Availability – S1SP Data Service (Production Services)	Monthly	100.00%	100.00%	99.99%	99.17%
	2.2	Service Availability – RPS Data Service (Production Services)	Monthly	100.00%	100.00%	99.99%	99.17%
	2.4	Percentage Service availability – S1SP Management Interface Availability (Production Services)	Monthly	100.00%	100.00%	99.50%	98.00%
	2.7	Service Availability - Test services	Monthly	100.00%	100.00%	99.00%	98.00%
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	5
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level	Latest Qtr. Service Level	Target Service Level	Minimum Service Level
Service Management	7	Planned Maintenance events	Quarterly	N/A	No Events	100.00%	90.00%

Table 21 – S1SP SIE Reportable Performance Measures

8.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

9 Reported List of Service Provider Performance Measures S1SP Capgemini

9.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service Availability – S1SP Data Service (Production Services)	Monthly	98.15%	100.00%	99.99%	99.17%
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	5

Table 22 – S1SP Capgemini Reportable Performance Measures

9.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

10 Reported List of Service Provider Performance Measures S1SP Vodafone

10.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability		Monthly availability of the Radio Network across VF-UK network	Monthly	N/A	No Data	TBC	TBC
		Combined monthly IoT Core and Management Service Availability	Monthly	N/A	99.48%	99.70%	99.70%
		Monthly IoT Core availability (Voice/Data/SMS)	Monthly	N/A	99.91%	99.90%	99.90%
		Monthly Management Service Availability (API, Reporting, Provisioning, GUI, Portal)	Monthly	N/A	99.57%	99.70%	99.70%
		Monthly Availability of DCC dedicated fixed links	Monthly	N/A	No Data	TBC	TBC

Table 23 – S1SP Vodafone Reportable Performance Measures

10.1.1 Service Level Below Target Service Level

Combined monthly IoT Core and Management Service Availability, reported Service Level was 99.48% and is below Minimum Service Level.
Combined monthly IoT Core & Management Service Availability is calculated by combining the IoT Core & Management Service & Monthly Management Service Availability, therefore due to the Management Service Availability target not being met this impacted the overall SLA achievement.

10.1.2 Service Level Below Target Service Level

Monthly Management Service Availability, reported Service Level was 99.57% and is below Minimum Service Level.
The Monthly Management Service Target was not met due to how the availability target is calculated for the platform as a whole as a result of this being a shared environment. Incidents were reported internally within Vodafone for the IoT Reporting section of the IoT Platform. However, reporting is not a service utilised by the DCC, therefore no tickets were raised with the DCC for this issue.

10.2 Performance Measurement Exceptions

The DCC were not impacted by the IoT reporting issues experienced on the IoT platform. No other tickets were raised in respect to availability during the reporting period, therefore the availability target has been met.

11 Service Credits

The calculation of Service Credits is subject to certain contractual exemptions.

The CSPs have exemptions relating to the installation of Communications Hubs as detailed below;

- CSP South, Performance Measure 1.3 (First time SMWAN connectivity within 90 days) and Communications Hub Performance Measures PM1.1 (Number of Communications Hubs delivered to DCC Service Users according to schedule each Delivery Month) and PM1.2 (Number of Communication Hubs accepted by DCC Service Users in each Delivery Month) exempt from Service Credits until the cumulative number of Communication Hubs installed at the end of any measurement period is greater than or equal to 550,000.

- CSP Central, Performance Measure 1.3 (First time SMWAN connectivity within 90 days) and Communications Hub Performance Measures PM1.1 (Number of Communications Hubs delivered to DCC Service Users according to schedule each Delivery Month) and PM1.2 (Number of Communication Hubs accepted by DCC Service Users in each Delivery Month) exempt from Service Credits until the cumulative number of Communication Hubs installed at the end of any measurement period is greater than or equal to 700,000.

- CSP North, Performance Measures 1.2 (First time SMWAN connectivity within 30 days) and 1.3 (First time SMWAN connectivity within 90 days) and Communications Hub Performance Measures PM1.1 (Number of Communications Hubs delivered to DCC Service Users according to schedule each Delivery Month) and PM1.2 (Number of Communication Hubs accepted by DCC Service Users in each Delivery Month), exempt from Service Credits until the cumulative number of Communication Hubs installed at the end of any measurement period is greater than or equal to 700,000.

For all other Performance Measures, the Service Credits accrued for this measurement period are as follows:

CSP (N) failed to meet the Target Service Level for six Performance Measures. These Performance Measures are:

CSPN PM2 – Percentage of Category 1 Firmware Payloads completed within the relevant Target Response Time. The Target Service level for this PM is 99.0% and the Actual Service Levels achieved was 88.70%. This failure resulted in the accrual of 50 Service Credit points which equate to Service Credits of £12,965. (This Performance Measure contributes to DCC Performance Measure 1.)

CSPN PM3.1 - Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time. The Target Service level for this PM is 99.0% and the Actual Service Levels achieved was 98.71%. This failure resulted in the accrual of 7 Service Credit points which equate to Service Credits of £1,815. (This Performance Measure contributes to DCC Performance Measure 2.)

CSPN PM3.2 – Category 3 Alerts delivered to the DCC WAN Gateway Interface. The Target Service Level for this PM is 99% and the Actual Service Level achieved was 94.66%. The

Service Credit Points for this measure is 263, with Service Credits of £68,195. (This Performance Measure contributes to Code Performance Measure 3.)

Regarding CSPN PM2 & PM3.2, discussions are ongoing between DCC and Arqiva regarding the installation by Service Users of meters outside of the agreed derogation areas. Until Phase 2 of ARQCR1028 is implemented, Arqiva are unable to automate the exclusion of these non-compliant meters from Performance Measure results. It is therefore proposed that no Service Credits are paid against these Service Measures. DCC to issue a formal position around these performance measures.

CSPN PM6.3 - Percentage Access Node availability. The Target Service level for this PM is 99.80% and the Actual Service Level achieved was 99.26%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSPN PM9 - Delivery of Change Requests Impact Assessments within required target. The Target Service level for this PM is 100% and the Actual Service Level achieved was 83.33%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

Regarding CSPN PM9, this is a quarterly measure, with the figure reflecting performance across all 3 months.

CSP (C) - No Service Failures have occurred during the month. Therefore, no Service Credits have accrued this month.

CSP (S) failed to meet the Target Service Level for one Performance Measure. This Performance Measure is:

CSPS PM2 – Percentage of Category 1 Firmware Payloads completed within the relevant Target Response Time. The Target Service level for this PM is 99.0% and the Actual Service Levels achieved was 98.50%. This failure resulted in the accrual of 28 Service Credit points which equate to Service Credits of £6,188. (This Performance Measure contributes to DCC Code Performance Measure 1.)

DSP failed to meet the Target Service Level for two Performance Measures. These Performance Measures are:

DSP PM4.1 - Percentage of Incident Responses provided to DCC Service Desk within requirement based on Incident Category Level. The Target Service Level for this PM is 99% and the Minimum Service Level is 85%. The Actual Service Level achieved was 97.10%%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

DSP PM10 - Number of Incidents of mis-alignment of DCC Industry Data. The Target Service Level for this PM is zero and the Minimum Service Level is two. The Actual Service Level achieved was two. This failure resulted in the accrual of 140 Service Credit points, which equates to Service Credits of £17,005. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

A summary of last 12 months Service Credits is provided in the table below:

Month	Arqiva	BT	CGI	Telefonica	Total
Oct-18	£0	£0	£12,146	£0	**£12,146**
Nov-18	£0	£0	£2,429	£15,928	**£18,357**
Dec-18	£0	£0	£18,219	£0	**£18,219**
Jan-19	£0	£0	£2,235	£82,097	**£84,332**
Feb-19	£21,402	£0	£0	£0	**£21,402**
Mar-19	£16,510	£0	£2,429	£93,216	**£112,155**
Apr-19	£14,369	£0	£9,333	£93,230	**£116,933**
May-19	£30,078	£0	£4,859	£93,185	**£128,122**
June-19	£53,883	£0	£12,146	£41,975	**£108,004**
July-19	£75,974	£0	£14,771	£86,321	**£177,066**
Aug - 19	£0	£0	£29,758	£86,321	**£116,079**
Sep - 19	£82,975	£0	£17,005	£6,188	**£106,168**

Table 24 – Service Credits

12 DCC's Internal Costs and/or External Cost

There is no impact on DCC's Internal Costs.

DCC's External Costs in the period of this report are reduced by the Service Credit total of £106,168.

13 Appendices

13.1 Appendix A – Open Problem & Incidents relating to Prior Periods

13.1.1

PBI000000113620

March Report - Key Incident **INC000000432999**

SU observed 8.1.1 Unreliable Clock Sync.

Problem: Service User (SU) observed in Installation and Commissioning that there was a job running on SM2M platform which slowed down the response of 8.1.1 (Commission Device).

This Problem Record is with CSP South. Root Cause was confirmed as a report that started running in the early hours of 1st March 2019 slowed down the Smart Machine to Machine (SM2M) platform, invoking a delay with the response to the 8.1.1 (Commission Device) Service Request.

An updated version of Smart Machine to Machine (SM2M) is required. The upgrade will contain a fix for 'Force Time Sync', which will help alleviate unreliable Clock Sync. The update was deployed on the 3rd September 2019, which will support a marked improvements to the functionality.

Latest: Problem Closed

13.1.2

PBI000000113808

February Report - Key Incident **INC000000429217**

Device Searches Outage - Invalid Business Objects

Problem: Device searches were not returning any information within SSI (Self Service Interface) and SSMI (Self Service Management Interface). This query allows the users to search for Smart Metering devices by various inputs, then view full details of any devices that the search locates. Users are unable to perform the searches to locate the devices.

Root Cause was confirmed as Objects are becoming invalidated in reporting databases as a symptom of a workaround for application/database Production triggered processes not being able to be fully applied to Disaster recovery. This is a workaround that was developed early on in the development phase by DSP, it has always existed and was not introduced following go-live or under a problem or change. This is the first time the skip rules cause an issue like this and it’s being investigated by DSPs Vendor. Transactions are skipped from applying on the reporting databases to prevent synchronisation halting and the Transactions that contain DDL (Data Definition Language) on certain tables are causing packages/views to become invalid at 10pm and 1am.

A fix has been implemented by the DSP to correct the issue at 10pm which was caused by a maintenance job and it was this view becoming invalid that caused the Incident. Mitigating has been completed to introduce new alerting to catch invalid objects before they cause a service impact. A fix has been defined to correct the issue at 1am for the possibility of the ERROR_LOG functionality to be separated out to dedicated tables within the database. The code fix has been scheduled for release in DSP 41, which is currently planned for 21/01/2020 however this date may be subject to change

Latest: Target Completion Date 24/01/2020

13.1.3

PBI000000113813

February Report - Key Incident INC000000430724

Problem: Failure of inbound SR's from DSP to CSP North. This Problem Record is with CSP North. Loss of Inbound SR (Service Request) traffic from DSP to CSP North approx. 15:05 - 17:17 on Monday 18th February 2019. Outbound service was unaffected. No customer impact reported by SU's (Service Users).

The Root Cause has been confirmed as a bug in a Firewall software that caused memory leak [due to unnecessary logging profile configuration updates]. This led to Out of Memory Killer having been invoked 3 times in an attempt to free up swap memory which closed off enough processes to result in the Firewall crashing and going offline.

The fix for this issue requires the unnecessary logging profile configuration updates bug to be fixed. Software upgrade/patching and testing to confirm the fix has begun. This issue is not service affecting, unless a device crashes again before fixed, but the last two times it has been tested it has failed over without impact. The enduring fix will require a prolonged test phase across multiple environments before promoting to Production which may ultimately coincide with Technology refresh in April 2020. No impact has been seen post incident.

Latest: Target Completion Date 30/04/2020

13.1.4

PBI000000115702

June Report - Key Incident **INC000000456123**

SR's returning an error status on the 24th May due to Master Key Store (MKS) issue.

Problem: This Problem Record is with the DSP. On Friday 24th May an issue arose within the DSP infrastructure which impacted the flow of traffic, Northbound and Southbound, through the DSP Motorway. It was discovered that a network connection to the Master Key Store (MKS) was causing issues, a restart of the MKS application was carried out to restore service. Some Service Requests (SR's) that required a cert from MKS failed, however instead of returning an error to the Service User, they timed out after 60 seconds.

The Root Cause has been identified as a behavioural/code issue. After the initial 60-second time-out DSP systems completed a number of retries and waits for those to also fail before sending any final error message back to the Service User. It seems in this case that the Service User didn't wait for the full DSP-retry cycle before deciding that the SR had failed. So, DSP believe the behaviour experience was correct according to the design. The overall DSP timeout (including all retries) will be communicated by DCC in order to set the Service User's expectation on when they will receive error messages for this scenario.

Latest: Target Closure Date 08/11/2019

13.1.5

PBI000000116300

June Report - Key Incident **INC000000457237**

Document Management system not accessible for Service Users

Problem: This Problem Record is with the DCC. Service Users were unable to access DCC Document Management System which prevented them from raising Service Management Service Requests and accessing key information.

The Root Cause has been found. The incident was caused by human error. Amendments were being made to the DCC Document Management System sharing settings. These amendments were made at the incorrect level and caused mass permission changes.

Any SharePoint global/tenant level changes in the future will require DCC Change control. Training on the new process has been completed.

Latest: Problem Closed

13.1.6

PBI000000116404

June Report - Key Incident **INC000000452354**

Reporting Delays - Daily, Weekly and monthly regulatory reports

Problem: This Problem Record is with the DCC. On 14th May a member of the DCC Ops Reporting Team reported that the daily ETL data had been sporadic for approximately 1 week, with some aspects having to be suspended. Their most recent attempt was stopped after 2.5 days, when the transfer of data should only have taken a few hours to complete. Delays resulted in regulatory breach by the DCC. BEIS, SEC Panel and SEC Security Sub-Committee were chasing delayed reports.

The Root Cause has been found. The increase in requirements (load of data) for the service has outgrown the service capability. The issues are being addressed under a Change Request to ensure infrastructure is in place to deal with the long-term growth but delays in delivery has meant an impact to service. Two performance fixes were identified during the incident and implemented. The enduring fix will be delivered by DCC Project Management via new infrastructure.

Latest: Target Completion Date 27/12/2019

13.1.7

PBI000000116409

June Report - Key Incident **INC000000459622**

Service Users unable to run SMI and SAT queries

Problem: This Problem Record is with the DSP. Multiple Service Users were unable to run SMI (Service Management Interface) and SAT (Standard Acis Text file) queries. The queries were running but not completing due to the request timeouts. No corrective action was taken to restore service as the incident self-cleared.

The Root Cause has been found. ESI reports run long running queries on the reporting database and lock tables whilst doing so, this prevents online queries from returning within expected timeframe however, some of the ESI reports were not designed to run with the volume of data now present in the system which is contributing to the long running queries. A workaround to run the ESI reports on the DR Reporting DB server is being used until a permanent fix can be devised.

The solution is currently being investigated and progressed under a code fix and the target is to complete the work within DSP release 41.

Latest: Target Completion Date 24/01/2020

13.1.8

PBI000000116206

June Report - Key Incident **INC000000461110**

Service Requests (SRs) are failing with E20/N12 errors

Problem: This Problem Record is with the CSP (Central & South). In the morning of 18th June 2019 (around 07:35am) Service users reported that all Service requests for devices in the Central and South regions were receiving E20/N12 error responses. Service users confirmed at 08:19am Service was restored. The CSP (Central and South region) are investigating their core infrastructure to identify the Root Cause and they are also troubleshooting with the DSP.

The Root Cause has not been found. The issue self-cleared before logs could be captured to isolate the cause of this incident. Mitigation has taken place to ensure capture of data if a similar incident occurs again.

Latest: Target Root Cause Date Expired 09/07/2019

13.1.9

PBI000000116302

July Report - Key Incident **INC000000457675**

An intermittent fault on the CSP Central & South Smart Metering Wide Area Network service

Problem: This Problem Record is with the CSP (Central & South). This has been raised to track investigation for the High priority incident on 03/6/19. The EPG (Evolved Packet Gateway) failed on the previous night. The incident was mitigated by draining the Comms hub off the EPG. As a result, this caused the Comms Hub to perform reboots. The high number of reboots caused an influx of Service Requests to be sent causing a backlog.

The Root Cause has been identified. The large influx of messages onto the system was due to CH (Comms Hub) behaviour post a vEPG (virtual Evolved Packet Gateway) drain. This influx of traffic caused queues on the CSP servers, which delayed Birth Event traffic and other System and Service User requests. The traffic loss on the EPG was due to protocols failing that direct traffic through the system. A configuration issue was identified and fixed on all 4 of the links.

Latest: Target Closure Date 08/11/2019

13.1.10

PBI000000116500

July Report - Key Incident **INC000000465166**

Birth events processing delays 25/06

Problem: This Problem Record is with the CSP (Central & South). Birth events were processing slowly for the CSP Central & South Regions. In order to restore service, the CSP for Central and South restarted a workflow in their Orchestration Tool.

The Root Cause has not been identified. The CSP have investigated the possibility of anti-virus protection and backups causing this issue but have been unable to confirm. To mitigate the risk of further occurrences the CSPs network team has setup throttling at switch level.

Latest: Target Root Cause Date Expired 24/07/2019

13.1.11

PBI000000116709

July Report - Key Incident **INC000000472537**

Host connectivity issues post Storage Area Network (SAN) switch firmware upgrade

Problem: This Problem Record is with the DSP. Multiple hosts lost connectivity to their Storage Area Network (SAN) switch storage during a planned firmware upgrade.

The Root Cause has not been identified. The issue was caused by a configuration issue. The Light Pulse Fibre Channel (LPFC) drivers encountered issues at the time of the hosts losing connection to their storage. The driver events were observed on all hosts which were affected by the upgrade. This issue was isolated to these hosts. The solution is to upgrade the Light Pulse Fibre Channel (LPFC) driver versions on the affected hosts.

A change has successfully implemented the update to Light Pulse Fibre Channel (LPFC) drivers on 2 clusters in non-Prod (including the affected cluster). Non-Prod environments have now been completed. DSP are now planning changes for DR and Production environments.

Latest: Target Completion Date for this Problem Record is 29/11/2019

13.1.12

PBI000000116600

July Report - Key Incident **INC000000459540 & INC000000467197**

SR Data Forecast vs Actuals for June data was not available

Problem: This Problem Record is with Capita ITES. On 2nd July a member of the DCC Ops Reporting Team reported that the monthly SR Data Forecast vs Actuals for June data was not available in Cognos. The report is due on the morning of the 2nd working day of each month so that DCC Ops reporting can get the regulatory reporting out by the 10th working day of that particular month. The lack of this reported generated a SEV2 Incident

The Root Cause has been identified. Due to the huge increase in the volume of SAT (Service Audit Trail) files early this year the automated process became unable to produce the data for the report in an acceptable time. A workaround was created and was run each month to populate the report, while a new version of the automated routine was being worked on. This workaround was run until May, when the workaround itself became too slow to use. A new version of the workaround was completed, this calculates the totals on a daily basis and at the end of the month has to be loaded manually to create the data set required. The day that the incident for June data was raised was going to be the day of hand over of the process within the supplier's teams. The handover of the data was missed due to resourcing issue and human error reasons. When the incident was logged to the supplier, they quickly looked to run the data and provide the info to the DCC. The second workaround will continue to be run until the permanent fix in in place.

A fix has been delivered and vigorous testing is underway to confirm that the solution functionality fully works. It has been found that a level of manual intervention is still required and that a full fix will be delivered by moving to a new solution.

Latest: Target Completion Date for this Problem Record is 29/11/2019

13.1.13

PBI000000116808

August Report - Key Incident **INC000000478818**

Service Request 6.23 Change of Supplier failing due to update Security Credentials not working

Problem: This Problem Record is with DSP. Numerous 'HTTP 500' errors were observed following Service Request 6.23 (Update Security Credentials (CoS)) on Electricity Smart Metering Equipment (ESME) in the Change of Supplier environment. This meant that the gaining Suppliers were unable to place their certificates on the devices they gained via Change of Supplier and hence were unable to send any critical commands to that device. This impacted no other Service Requests and had no impact on Installation and Commissioning.

The Root Cause has not been identified. The failure observed was triggered by a switch restart. The firewall failed over to DR as the switches went down, on restarting, the peer setting i.e. Border Gateway Protocol (BGP) neighbouring function did not resolve correctly and got stuck in DR. This caused the physical comms device to go offline. The network virtualization platform (NSX) and physical infrastructure had no issues. The issue encountered was a failure where there is a touchpoint of the physical connection between the firewall and the Unidirectional Link Routing (UDLR). Prior to redeploying the Unidirectional Link Routing (UDLR) image, the firewall configuration was reapplied with both sides restarted on the demilitarised zone (DMZ) and the electronic messaging firmware (DataPower). The Unidirectional Link Routing (UDLR) deployment was the ultimate resolving action for the Incident. All items were required however arguably the Unidirectional Link Routing (UDLR) redeployment, had this been done earlier, may have negated the requirement to restart firewalls. The issues observed were linked with the Unidirectional Link Routing (UDLR) attempting to connect to the DR firewall following the switch restart, which is what brought itself back up first. This is a potential redesign requirement which is being investigated via DSP Project Management with DSP Technical Architects.

To mitigate this issue, in the event of a recurrence DSP would redeploy Unidirectional Link Routing (UDLR) to resolve the connectivity issues, retain the management interface only i.e. remove DR firewall connection as part of planned changes to core switches where a restart would be required (isolate the DR link for certain ports) - ultimately ensuring that the Production firewall is available and takes priority for switch connection (in the event of any future Changes requiring a restart of the switch stack).

An upgrade of the operating system on the virtualisation hosts and the code was successfully progressed via Change. During these upgrades the resiliency was also successfully tested. Additional monitoring has been added to more easily identify this type of issue. Enhancements have been made to the post Change verification process to ensure issues such as this are identified at the time the change has been made. Future Changes of this type will more clearly identify the impact/risk of the Change.

Latest: Problem Closed

13.1.14

PBI000000116812

August Report - Key Incident **INC000000479406**

DCC SMS, SSI and SSMI service degradation

Problem: This Problem Record is with DSP. DCC Service Management System, Service Management Interface and Self-Service Management Interface observed service degradation when a power outage was experienced throughout the UK which impacted a single rack in DSP Data Centre causing multiple DCC systems to alert.

The Root Cause has not been identified. Fluke analyser testing has been completed in a change window and no issues has been identified with the links since the tests were undertaken. Switch testing will now be planned.

Latest: Target Root Cause Date Expired 27/08/2019

13.1.15

PBI000000116918

August Report - Key Incidents **INC000000480076/480350**

SMETs 1 Migrated Devices - Service requests failing

Problem: Service requests were failing in Dual Control Organisation (DCO) with Error "500 internal service error". This prevented the Dual Control Organisation application from processing Service requests.

The Root Cause has been identified. The errors were due to a router service bug. Changes will be completed to update the router service on the application servers across the Dual Control Organisation (DCO) estate.

Changes have been completed to update the router service on the application servers across the DCO estate.

Latest: Target Completion Date for this Problem Record is 04/11/2019

13.1.16

PBI000000117104

August Report - Key Incident **INC000000485618**

SMETS1 Migration: S1SP to DCO Communication Failures

Problem: This Problem Record is with SIE/DSP. Some service requests and communications were failing between DCO infrastructure and S1SP Infrastructure. This caused the DCC to put a hold on migrations as it was unclear whether there was a widespread issue. To triage the issue, the S1SP Network Team failed services over to the secondary F5 (Load Balancer) and completed the tests and no failures were experienced.

They further failed services back to the primary and the connections were refused confirming that the issue was with the primary load balancer.

The Root Cause of the service requests failing between DCO infrastructure and S1SP infrastructure was due to a software bug on a Traffic Management device. An upgrade to the software on the traffic management device has been completed.

Latest: Target Completion Date for this Problem Record is 31/10/2019

13.1.17

PBI000000117100

September Report - Key Incident **INC000000477267**

Failed Commissions for a Single Service User

Problem: This Problem Record is with CSP Central and South. Unexpected Device Failures on Service Request 8.2 (Read Inventory) were observed on the 1st of August 2019, which led to failed commissions for a single Service User.

Root Cause Analysis investigations continue for this issue. The CSP are looking into a change that they believe caused this issue.

Latest: Target RCA Date for this Problem Record breached on 18th September 2019.

13.1.18

PBI000000117102

September Report - Key Incident **INC000000486219**

CSP North RNI infrastructure (Degradation)

Problem: This Problem Record is with CSP North. On 30th August 2019 DSP flagged an increase in E21's being generated from CSP North infrastructure. Degradation of the Radio Network Interface (RNI) was found and DCC estimate 600 installs in the North were impacted. Service was declared restored following a number of restorative actions being carried out by CSP North. Mitigation for this issue involves 4 hourly checks of Network Controller disk space with check point actions marked should disk space increase pass a threshold. Disk space was also doubled to 300Gb.

The Root Cause has due to CSP North disk space become full. An increase in installs and daily throughput through the NC's (Network Controllers) caused Partition File sizes to gradually increase over time. The log rotation configuration has worked correctly over the last year or so (since its introduction due to a previous incident). However, the increase in file size now means the rotation configuration was no longer suitable and allowed the Partition to fill. Monitoring was in place to capture Partition disk space issues but it had incorrect thresholds settings resulting in the CSP not receiving alerts prior to the issue becoming service impacting.

A further 150GB has been added to each NCs (Network Controllers) since the incident (300GB in total including a 150GB increase to restore the incident). There has been a

recommendation to increase by a further 250GB per NC taking total storage for the partition up to 700GB. The CSP have been reviewing requirements for enhanced alerting and are raising amending the threshold alerts from 95% to 70%. This will be requested across all partitions and will need to be tested after to confirm the alerts correctly pull through at the right times.

Latest: Target Completion Date for this Problem is 22/11/2019

13.1.19

PBI000000117106

September Report - Key Incident **INC000000487108**

Birthing Events in the CSP Central and South Region

Problem: This Problem Record is with CSP Central & South. On 4th September at 08:48 a Service User experienced incorrect states being reported for newly-birthed meters. Indicator lights on the meter showed the device as birthed yet sending SRV 8.2 confirmed the device was in the wrong state. The issue was reported by a further 2 service users and impacted installs in the Central & South region.

Root Cause Analysis investigations continue for this issue. The CSP have linked the issue to a Database. As part of this upgrade it was advised inactive sessions were required to be killed, which in turn led to a restart of the Database. Following this restart, the Birth Event Workflow which processes birth events was automatically moved to a different runtime server which did not have Datasource configured. Therefore, the Workflow did not establish a connection to the Database.

Latest: Target RCA Date for this Problem Record breached on 26th September 2019

13.1.20

PBI000000117205

September Report - Key Incident **INC000000491661**

Primary host down invoking failover

Problem: This Problem Record is with DSP. A host failover occurred in the late hours of 12th September 2019. The primary core host for the North, Central and South went down at 23:05, which recovered with no corrective action required.

Root Cause was confirmed as a capacity issue. The primary Host failed over to the secondary due to swap memory exhaustion. The North switch failed to work correctly due to missing Hardware Security Module (HSM) keys, added under a Change via Problem Record PBI000000117120, that had not been replicated to the secondary nodes due to a missing step in the Process (now rectified).

The switch vendor has stated that the swap memory exhaustion is related to disk space exhaustion. The ‘BIG IP Analytics’ process was sending tens of thousands of temporary files to be processed by the 'MySQL' process. The 'MySQL' process also appeared to crash due to disk exhaustion (a single mysql.err.log at 1.5GB). This prevented the

processing of the temp files, which resulted in the continual growth of the disk space until it had also been exhausted. A system upgrade to latest version is currently under review, which may resolve the issue with the 'MySQL' process that played a part in the failure. This work needs to be considered in conjunction with Hardware Security Module (HSM) and Load Balancer upgrades currently being progressed across the environments.

Latest: Target Completion Date for this Problem is 29/11/2019

13.1.21

PBI000000117128

September Report - Key Incident **INC000000493155**

Delays when birthing Comms Hubs in the CSP North region

Problem: This Problem Record is with CSP North. Multiple Service Users experienced delays when birthing Comms Hubs in the CSP North region. Service was restored by restarting the nodes one at a time in the Comms Hub Manager (CHM) infrastructure where a hung process was identified.

Root Cause Analysis investigations continue for this issue. Hourly monitoring of Comms Hub Manager was put in place until an automated monitoring notification would be implemented. This was implemented 26/09/2019 and provides CSP-North with an early warning notification in case of future issues.

Latest: Target RCA Date for this Problem Record breached on 22nd October 2019

13.1.22

PBI000000117309

September Report - Key Incident **INC000000493599**

SMETS-1 Service Requests failing

Problem: This Problem Record is with DSP. DCC identified that all SMETS-1 Service Request activity was failing from 19:17pm on 18th September 2019 with full service being restored by DSP at 23:04pm (BST) for all SMETS-1 devices. This impacted a small subset of migrations (14) that have subsequently been fixed forward. No Customer Impact was observed as Service was restored before the meter reads were scheduled.

The Root Cause of this issue was a failure with the CRL (Certificate Revocation List) renewal process, whereby the change required to complete the renewal did not progress through the process as expected resulting in a new certificate not being applied before the original one expired. When the CRL expired, this caused service requests between DSP and SIE to fail until a new CRL was deployed.

The issue was with the CRL process and DSP are completing changes to improve the process. Improvements have been made and further improvements are under review.

Latest: Target Completion Date for this Problem is 15/11/2019

13.1.23

PBI000000117115

September Report - Key Incident **INC000000488824**

SSMI issue

Problem: This Problem Record is with DSP. Self Service Management Interface functionality was reported as not working upon the launch screen when attempting to log in. A database error occurred that prevented the request from being fulfilled.

The Root Cause was confirmed as a Process issue. The Security protocol (IPSec) restart causing a knock on with the application. In theory, the IPSec restarts (multiple times) should only take out the SSI and SSMI for a very short period of time. However, the application was down for 58 minutes. It was thought prior to the Change that the service for SSI and SSMI was resilient, which was a mistake and it should have been anticipated that if IPSec was not restarted immediately then service would be lost. The application behaved as expected, but the restart of the IPSec was a manual task, which on the day proved difficult for two engineers to restart all IPSec services at the same time.

An IPSec script has been created to ensure that the restarts are quicker in order to successfully implement relating Changes.

Latest: Target Completion Date for this Problem is 31/10/2019

13.1.24

PBI000000117117

September Report - Key Incident **INC000000487736**

SIE Migration failures due to Key Rotation Error

Problem: This Problem Record is with SIE/S1SP. SMETS 1 migrations were suffering from failure with the error message ETO8. On Friday 7th September 27 of the 119 planned migrations failed with the ET08 error. The remaining migrations were then paused to stop any further failures whilst a fix was developed and Implemented.

The Root Cause of this issue was due to the sub sessions being opened with DCO. These sessions were required to be opened separately, however, they were opening at the same time which was causing the connections to be refused. Other contributory factors have been identified:
1. It was found that there were 4000 open connections on the active load balancer.
2. A race condition was identified between the session managements on two of the S1SP components: Foundation Engine and Migration Manager.

A configuration change was progressed to add a delay into the Foundation Engine component to avoid both sessions to DCO being opened simultaneously. Measures have also been to be completed to deal with contributory factors. SIE are looking to complete information tasks before moving this Problem to completed.

Latest: Target Completion Date for this Problem is 31/10/2019

13.1.25

PBI000000117305

September Report - Key Incident **INC000000491743**

PROJECT: Service User Message queue increase

Problem: On 13th September at 08:10 DSP reported that they could see message queues for a specific set of Service Users increasing. Initial checks by DSP indicated that the issue could be due to how a Service User was handling message acknowledgements, as all the affected Service Users are hosted through their connection.

The Root Cause is confirmed to be a configuration issue. The Service Users capacity for handling uncharacteristically large queue sizes. For BAU activity this is not an issue, however, should an event happen in any space that results in increased queue sizes, the Service User could experience similar issues in the future.

It was discovered that the message acknowledgement service at the Service User was working as designed but struggling to handle the increased volume (backlog) of messages resulting from a 90-minute interruption to the DSP service provision overnight. The Service User made changes to their acknowledgement process and the backlog reduced as message throughput increased. DCC coordinating efforts working with DSP, DCC Service Management and the Service User to insure repeat incidents don't occur.

Latest: Target Completion Date for this Problem is 08/11/2019