Data Communications Company

DCC Performance Measurement Report

Performance Measurement Period:

January 2020

Version:	**V1.0**
Date:	**06/03/2019**
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 **24**
3.1 Service Levels Attained 24
3.1.1 Service Level below Minimum – CPM1 29
3.1.2 Service Level below Minimum – CPM4 29
3.1.3 Category 1 and 2 Incident Resolution – CPM4 30
3.1.4 Category 3, 4 and 5 Incident Resolution - CPM5 31
3.1.5 CPM4 and CPM5 – Incidents Re-Opened after Closure 31
3.1.6 Incident Resolution Information – CPM 4 & 5 31
3.2 Performance Level Exemptions 33
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. 34
4 Reported List of Service Provider Performance Measures DSP **35**
4.1 Service Levels Attained 35
4.1.1 Service Level Below Target Service Level 36
4.2 Performance Measurement Exceptions 36
5 Reported List of Service Provider Performance Measures CSP North **37**
5.1 Service Levels Attained 37
5.2 Performance Measurement Exceptions 39
5.2.1 In Period Exceptions 39
5.2.1.1 PM1.4 SMWAN Connectivity Level 39
5.2.2 Total Estate Exceptions 40
6 Reported List of Service Provider Performance Measures CSP Central **41**
6.1 Service Levels Attained 41
6.2 Performance Measurement Exceptions 43
6.2.1 In Period Exceptions 43
6.2.1.1 PM1.1 First Time SMWAN Connectivity 43
6.2.1.2 PM11 Accuracy of Coverage Database 44

6.2.2 Total Estate Exceptions 44
6.2.2.1 PM1.3 SMWAN Connectivity Level 44
7 Reported List of Service Provider Performance Measures CSP South 46
7.1 Service Levels Attained 46
7.2 Performance Measurement Exceptions 48
7.2.1 In Period Exceptions 48
7.2.1.1 PM1.1 First Time SMWAN Connectivity 48
7.2.1.2 PM11 Accuracy of Coverage Database 49
7.2.2 Total Estate Exceptions 49
7.2.2.1 PM1.3 SMWAN Connectivity Level 49
8 Reported List of Service Provider Performance Measures S1SP SIE 51
8.1 Service Levels Attained 51
8.1.1 Service Level Below Target Service Level 51
8.2 Performance Measurement Exceptions 52
9 Reported List of Service Provider Performance Measures S1SP Capgemini 53
9.1 Service Levels Attained 53
9.2 Performance Measurement Exceptions 53
10 Reported List of Service Provider Performance Measures S1SP Vodafone . 54
10.1 Service Levels Attained 54
10.2 Performance Measurement Exceptions 54
11 Service Credits 55
12 DCC's Internal Costs and/or External Cost 56
13 Appendices 57
13.1 Appendix A – Open Problem & Incidents relating to Prior Periods 57
13.1.1 PBI000000113808 57
13.1.2 PBI000000113813 57
13.1.3 PBI000000115702 58
13.1.4 PBI000000116409 58
13.1.5 PBI000000116812 59
13.1.6 PBI000000117102 59
13.1.7 PBI000000117205 60
13.1.8 PBI000000117128 60
13.1.9 PBI000000117305 61
13.1.10 PBI000000117135 62
13.1.11 PBI000000117240 62

13.1.12 PBI000000117601 63
13.1.13 PBI000000117610 64
13.1.14 PBI000000117408 64
13.1.15 PBI000000117609 65
13.1.16 PBI000000117612 65
13.1.17 PBI000000117807 66
13.1.18 PBI000000117900 66
13.1.19 PBI000000118607 66
13.1.20 PBI000000118516 67
13.1.21 PBI000000118411 67
13.1.22 PBI000000118605 68
13.1.23 PBI000000118518 68
13.1.24 PBI000000118613 69
13.1.25 PBI000000118616 69
13.1.26 PBI000000118704 69
13.1.27 PBI000000118619 70
13.1.28 PBI000000118804 70
13.1.29 PBI000000118916 71
13.1.30 PBI000000119002 71
13.1.31 PBI000000118430 71
13.1.32 PBI000000119007 72
13.1.33 PBI000000118924 72
13.1.34 PBI000000118919 73

Control Sheet

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

Page No.	Change

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 January 2020.

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 98.41% and is below the Target Service Level, further details provided in Section 3.1.1.

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 66.67% and is below the Minimum Service Level, further details provided in Section 3.1.2.

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

Service Provider Performance Measures Summary

DSP PM7 Notification of Planned Maintenance events within required target, reported Service Level is 93.33% and is below Target Service Level.
Further details are provided in Section 4.1.1

S1SP SIE PM3.1 Number of Severity Level 1 or 2 Incidents directly related to a Change Release occurring within 30 days of release of the Change Release, reported Service Level Events is 1 and is below Target Service Level.
Further details are provided in Section 8.1.1

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 11 of the report.

Key Incidents – January Closed in Period

Incident Reference	**INC000000532006 – Category 2**
Problem Reference	**PBI000000118613**
System(s) Impacted	CH Devices dropping off the HAN
Incident Start Date / Time (Logged in Remedy)	18/12/2019 11:53
Incident Resolved Date / Time	10/01/2020 08:31
Outage Start	N/A
Outage End	N/A - Actions ongoing and tracked by Problem Management
Incident Closure Date	16/01/2020
Major Incident Duration	22 days 20 hours 38 minutes

Regions Impacted	CSP Central and South
Resolved within SLA	No
Summary of High Category Incident	
DCC identified a trend of issues with both Comms Hub devices in the CSP Central & South Region dropping of the HAN (Home Area Network). DCC will attempt to trigger a re-join and maintain service of those affected devices by sending the device the command to reboot. Upon reboot the ESME devices regain connectivity to the Comms Hub. To deliver this operation CSP Central and South rebooted 17,300 Comms Hubs on the night of the 23/12/2019 that had already lost HAN connectivity (due to this specific condition) and then to continue to perform this reboot operation as it is identified until further notice. The issue affected both credit and prepayment modes and priority will be directed to rebooting Comms Hubs in prepayment mode before rebooting credit mode Comms Hubs. DCC Technical Operations Centre (TOC) produced a report based on E58 (new response code in DUIS 3) and Alert Code 8F84 (Failure to Deliver Remote Party Message to ESME) which are highlighting the impacted devices. TOC also supplied each impacted Service User with a list of impacted GUIDS including mode of operation. Upon incident resolution approximately 20,000 premises were impacted, DCC proactively identified any impacted premises via daily maintenance. A reboot of affected devices identified during the previous 24-hour period took place. This was originally identified by one Service User; further investigations have shown that there are multiple Users affected. DCC therefore raised the category from a 3 to a category 2. There is no risk to PPMID customers over night due to Emergency Credit and the Social Disconnect function that power suppliers have in place (No power loss during the hours of darkness).	
Reported Customer Impact	
Two Service Users reported devices falling off the HAN. Primarily ESME devices with some GSME.	

Actions Completed to Recover Service		
Item	Description.	Owner

1	Tactical Fix in place to reboot impacted devices, carried out daily	DCC TOC/CSP C&S.

Incident Reference	**INC000000534308 – Category 2**
Problem Reference	**PBI000000118616**
System(s) Impacted	Install and Commissioning failures
Incident Start Date / Time (Logged in Remedy)	23/12/2019 14:47
Incident Resolved Date / Time	27/12/2019 10:04
Outage Start	23/12/2019 13:41
Outage End	23/12/2019 19:51
Incident Closure Date	02/01/2020
Major Incident Duration	6 hours 10 minutes
Regions Impacted	CSP Central and South
Resolved within SLA	Yes
Summary of High Category Incident	
At 13:41 (23/12/2019) a single Service User reported errors being returned for SRVs (e.g. 8.11 and 8.1.1) sent during the commissioning process for all devices. Approximately 30% of their installs were impacted. Analysis by CSP C&S of the examples provided showed that SRVs were being sent to the devices successfully. During a Technical bridge with DCC, DSP and CSP C&S it was found that the UDP throughput being sent from CSP C&S to DSP had doubled resulting in DSP F5 overload protection. This meant that some SRV traffic was being blocked. When the SR retried an error was returned as the initial SR had successfully completed. Traffic volumes stabilised at 19:51 with no manual intervention.	
Reported Customer Impact	
Service Users reported that SRVs were not getting responses which resulted in an impact to Install and Commissioning activities	
Actions Completed to Recover Service	

Item	Description.	Owner
1	None - Traffic volumes stabilised at 19:51 with no manual intervention.	-

Incident Reference	**INC000000540421 – Category 2**
Problem Reference	**PBI000000118704**
System(s) Impacted	Degradation during Install and Commission
Incident Start Date / Time (Logged in Remedy)	10/01/2020 09:16
Incident Resolved Date / Time	15/01/2020 11:52
Outage Start	10/01/2020 07:00
Outage End	10/01/2020 09:48
Incident Closure Date	21/01/2020
Major Incident Duration	2 hours 48 minutes
Regions Impacted	CSP Central and South
Resolved within SLA	Yes
Summary of High Category Incident	
CSP Central and South confirmed this issue which is occurring because of a fault with the Operational intelligence and orchestration tool (Vitria OI/OT) application/database impacting the smart metering program. The following were impacted: • Birth Events and Installations • Power Outage Notifications • Incoming Shipments • Stock Movements • Outbound Shipments Birth Events not being processed successfully impacts the installation and commission of Communication Hubs and Smart Meters. A faulty domain server was identified and was restarted to the resilient server.	

CSP Central and South experienced infrastructure problems and carried out a reboot of their Operational Intelligence platform at 09:48.		
Reported Customer Impact		
No Service User reports as the E20 issue was masking this OI/OT platform failure.		
Actions Completed to Recover Service		
Item	Description.	Owner
1	Reboot of 1 of the domain servers in the OI/OT platform	CSP C&S

Incident Reference	**INC000000541487 – Category 2**
Problem Reference	**PBI000000118704**
System(s) Impacted	Degradation for all SRVs
Incident Start Date / Time (Logged in Remedy)	13/01/2020 11:14
Incident Resolved Date / Time	14/01/2020 17:33
Outage Start (impact)	10/01/2020 01:15
Outage End	13/01/2020 15:00
Incident Closure Date	20/01/2020
Major Incident Duration	3 days 13 hours 45 minutes
Regions Impacted	CSP Central and South
Resolved within SLA	No
Summary of High Category Incident	
Following an issue affecting a core network element in the Central and South Region on the 09/01/2020 there was an increase in E20 alerts (E20 - Communications Failure – Unable to Communicate with Device) which was intermittently impacting SRVs in the Central and South region. This was initially investigated under INC000000540421 as it was thought to have been caused by CSP Central and South connection pool to their Operational Intelligence Database becoming exhausted, which resulted in the loss of connectivity. It was determined later that this was not the cause of the increase in E20s and ongoing investigations would be tracked under INC000000541487.	

It was confirmed that 1 of 8 MME elements started flapping at 08:15 on 09/01/2020. This resulted in 1/8 of the comms hub base losing network connection (potentially c.240k hubs). Although comms hubs are designed to automatically re-join the network, approximately 430 Comms Hubs lost their DNS entry and were unable to re-connect. When DSP receive a DNS failure they retry as per the retry pattern for the Service Request Variant (SRV)/Device Type. However, if the retry also fails then the DNS request will take longer than the SRV timeout and results in an E20. The devices that did not have DNS entries after the network outage therefore caused a backlog of requests and time-outs (E20s) of other SRVs for other devices. On Friday Morning (10/01/2020) by 10am there was an increase of over 103k in E20s compared to the previous day. DSP took an action to improve the efficiency of DNS lookups by removing a non-prod domain entry on the Application Server. This resulted in failures completing quicker, allowing 'real' messages to complete within expected timescales. While this did not resolve the core issue with this incident it did allow service to restore to BAU levels.
Reported Customer Impact
Service Users reported an increase in Install and Leave actions, which result in repeat visits for the customer, longer install times (due to failed SRVs being retriggered until they're successful), poor customer experience and an increase in Pre-pay vends receiving E20s.

Actions Completed to Recover Service		
Item	Description.	Owner
1	DSP improved the efficiency of DNS lookups by removing a non-prod entry from the Application Server.	DSP

Incident Reference	**INC000000541556 – Category 2**
Problem Reference	**PBI000000118619**
System(s) Impacted	UIT A SRs not being sent
Incident Start Date / Time (Logged in Remedy)	13/01/2020 09:41
Incident Resolved Date / Time	13/01/2020 12:14
Outage Start	13/01/2020 08:00
Outage End	13/01/2020 10:55
Incident Closure Date	19/01/2020
Major Incident Duration	2 hours 55 minutes

Regions Impacted	All
Resolved within SLA	Yes
Summary of High Category Incident	
An Internal DSP change on the evening of 12/01/2020 resulted in the SQL database being turned off. SMKI Repo and MKs were also impacted due to this change. All SMETS1 SRs and installation SRs for SMETS2 were impacted within UIT A. DSP reported an issue with UIT A SMETS1 Motorway 08:59 13/01/2020. Investigations found that the My SQL Database was down. Once started service appeared to be restored. However, further health checks identified issues with SRs, application components were restarted (MKS, SGN and Apache). Once restarted service was restored at 10:55 13/10/2020.	
Reported Customer Impact	
All SMETS1 SRs would have been impacted with a subset of SMETS2 SR also being impacted (installations/update credential/certificates) within the UIT A testing environment.	

Actions Completed to Recover Service		
Item	Description.	Owner
1	MY SQL Database restarted	DSP
2	Application components restarted (MKS, SGN and Apache)	DSP

Incident Reference	**INC000000542187 – Category 2**
Problem Reference	**PBI000000118804**
System(s) Impacted	Single Service User Install & Commission failures in the North
Incident Start Date / Time (Logged in Remedy)	14/01/2020 09:00
Incident Resolved Date / Time	14/01/2020 14:31
Outage Start	14/01/2020 09:00
Outage End	14/01/2020 10:15
Incident Closure Date	20/01/2020
Major Incident Duration	1 hours 15 minutes
Regions Impacted	CSP North
Resolved within SLA	Yes

Summary of High Category Incident		
A Single Service User reported an increase in E20 errors being returned from Service Requests sent during the Install and Commissioning process. DCC TOC monitoring also identified that this Service User was down on installs. Investigations show that this is related to an ongoing issue with a Service User sending On-Demand requests rather than Scheduled requests through the night. This has a knock-on effect to the next day's processing of service requests causing a queue. Once the backlog was clear, SRs were being processed as normal and installs continued.		
Reported Customer Impact		
Single Service User reported this as an issue however this would have impacted all the CSP North Service Users.		
Actions Completed to Recover Service		
Item	Description.	Owner
1	Backlog of SRs reduced to normal levels without manual intervention	CSP N

Key Incidents – January Excluded Through PMEL

Not DCC Resolution

Incident Reference	**INC000000543758 – Category 2**
Problem Reference	**PBI000000119002**
System(s) Impacted	Single Service User - Delays during Install and Commission
Incident Start Date / Time (Logged in Remedy)	17/01/2020 10:42
Incident Resolved Date / Time	17/01/2020 12:58
Outage Start	17/01/2020 10:00
Outage End	17/01/2020 13:00
Incident Closure Date	23/01/2020
Major Incident Duration	3 hours
Regions Impacted	All
Resolved within SLA	Yes
Summary of High Category Incident	

On 17/01/2020 at 10:42 An MSP (Managed Service Provider) reported that a Service User's install and commissions were taking significantly longer than usual across all regions. Delays in excess of 5 minutes for SRV responses were resulting in I&Cs taking over 90 minutes to complete. Examples provided indicated showed the time taken between the DUIS request, DUIS response and MMC responses. Although the time of the request was not included. DSP analysed the examples provided and could see prompt responses for all. DCC MIM contacted the MSP to investigate the adapter. It was then identified there was a backlog in Service Requests and alerts on the adapter which was leading to the delays experienced. The backlog cleared at approx. 12:30 and Install and Commissioning activities then completed as normal.		
Reported Customer Impact		
A single Service User reported delays in completing Install and Commissioning activities across all regions. A delay in the Service Requests responses used in the process was leading to a delay in completion.		
Actions Completed to Recover Service		
Item	Description.	Owner
1	Enhanced monitoring and increased level of service on one of the queues to process alerts quicker	MSP

Incident Reference	**INC000000538993 – Category 2**
Problem Reference	**PBI000000118430**
System(s) Impacted	DCC Service Requests impacting commissioning of devices
Incident Start Date / Time (Logged in Remedy)	07/01/2020 14:09
Incident Resolved Date / Time	07/01/2020 15:28
Outage Start	07/01/2020 13:18
Outage End	07/01/2020 14:43
Incident Closure Date	13/01/2020
Major Incident Duration	1 hour 25 minutes
Regions Impacted	All
Resolved within SLA	Yes
Summary of High Category Incident	

At 13:20 DCC IM noticed that the motorway component on the SSMI dashboard had turned amber, with sub-components MGS-1, MGS-2, RMS-1, RMS-2 turning red. A call was placed to the SME at DSP who instigated an internal technical call at 13:40. At 13:59 a Service User advised that they were seeing delays in install and commissions. DSP advised that they could still see install and commissions happening. They suspected that the fault lies with the DMA servers and that they would start the restart process for them immediately. DSP SDM called DCC IM at 14:08 to advise that this would affect DCC SRVs only. The MCC advised at 14:26 that this incident was also impacting the ability to migrate SMETS1 devices. DCC IM were merged with the ongoing technical call by DSP SDM at 14:40 and service was restored at 14:43, following the restart and reintroduction of both the DMA servers. This only affected HTTP500 to DSP SRVs but was further impacted by an increase in 8F12 alerts. Expectation is ~20k per day, but the service received over 3 million in this case.		
Reported Customer Impact		
Service Users experienced delays in install and commissioning activities in all regions. SMETS1 migrations were failing.		
Actions Completed to Recover Service		
Item	Description.	Owner
1	The DMA Servers were restarted and reintroduced.	DSP

Incident Reference	**INC000000544951 – Category 2**
Problem Reference	**PBI000000118916**
System(s) Impacted	Single Service User Install & Commission failures in the North
Incident Start Date / Time (Logged in Remedy)	21/01/2020 09:54
Incident Resolved Date / Time	21/01/2020 16:45
Outage Start	21/01/2020 09:54
Outage End	21/01/2020 12:17

Incident Closure Date	27/01/2020
Major Incident Duration	2 hours 23 minutes
Regions Impacted	CSP North
Resolved within SLA	Yes
Summary of High Category Incident	
A Single Service User reported an increase in E20 errors which were impacting Install and Commission in the North. A Second SU reported they were also impacted. Investigations by the CSP North and DCC TOC could not see any increase in E20 errors or a drop in Installs. Both Service Users confirmed internal issues as the cause of the issue.	
Reported Customer Impact	
Single Service User reported this was impacting Install and commission, however investigations show the ecosystem was not at fault.	

Actions Completed to Recover Service		
Item	Description.	Owner
1	None	-

Incident Reference	**INC000000545509 – Category 2**
Problem Reference	**PBI000000119007**
System(s) Impacted	Multiple Service Users Receiving E20 Errors
Incident Start Date / Time (Logged in Remedy)	22/01/2020 09:32
Incident Resolved Date / Time	23/01/2020 12:16
Outage Start	22/01/2020 02:48
Outage End	22/01/2020 17:00
Incident Closure Date	29/01/2020
Major Incident Duration	14 hours 12 minutes
Regions Impacted	CSP Central and South
Resolved within SLA	No

Summary of High Category Incident
On 22nd January multiple SEC Parties raised incident tickets for increases in E20 errors which, in turn, had an intermittent impact on key business operations; most notably install & commission, pre-pay top-up, change of supply and other on-demand service requests. A call was raised with DSP and CSP Central & South (C&S). DSP confirmed that they were already investigating the issue and an automated alerting ticket had been raised at 09:21 – INC000000545506. During the Post Incident Review DSP confirmed that this tied into an event at 02:48 where a drop in Scheduled Reads for CSP Central & South (C&S), from 6,000/min to 400/min was seen. The start of impact for this incident has been set to this first-noticed time of 02:48. Extensive investigations took place with both DSP and CSP C&S working closely and providing data to establish where the issue may be originating. Following a mandatory upgrade of Trend Security Agent, from v9.6 to v11, the setting for maximum UDP connections became 'enforced,' limiting these connections to 1,000. Ordinarily this would not cause an issue. However, once the CSP C&S scheduled reads started the maximum number of connections was exceeded, resulting in time-outs. This would not have been evident immediately after the upgrade as the CSP C&S scheduled reads had completed for that day. It should be noted that those scheduled reads which timed out would have automatically retried two hours later. DSP monitored the level of E20s at the next retry point (16:55) and mitigated the impact by manually turning off the Security Agent. Once the Security Agent had been restarted, the maximum UDP connections limit was raised to 10,000 and the service monitored overnight to ensure no further issues arose. During the checkpoint call at 09:00 on 23/01/2020 DSP confirmed that the service had operated as expected and no further issues had been reported.
Reported Customer Impact
Service users in the Central & South Region experienced delays in install & commissioning activities (resulting in missed installations), pre-payment top-ups and change of supply, along with other on-demand service requests. Impact would have been seen every 2 hours (when the scheduled reads re-try queue runs) and would last for approximately 30 minutes.

Actions Completed to Recover Service		
Item	Description.	Owner
1	DSP initially turned off the Trend Security Agent service before changing the maximum UDP connections limit from 1,000 to 10,000.	DSP

None Service Impacting

Incident Reference	**INC000000545619 – Category 2**
Problem Reference	**PBI000000118924**
System(s) Impacted	SMETS1 Migrations
Incident Start Date / Time (Logged in Remedy)	22/01/2020 12:06
Incident Resolved Date / Time	23/01/2020 15:49
Outage Start	22/01/2020 09:00
Outage End	22/01/2020 21:10
Incident Closure Date	29/01/2020
Major Incident Duration	12 hours 10 minutes
Regions Impacted	CSP Central and South
Resolved within SLA	Yes
Summary of High Category Incident	
Following the deployment of a S1SP change on 21/01 (ref120604) migrations were stalling. The change involved adding a validation step (5.9.10 check) on the MCF (Migration Common File) that all Supplier certs (if provided) belong to same SEC Party. But it also had a condition that at least one Supplier certificate to be present per MCF, otherwise the check fails Supplier certs are not included on MCF files for dormant meters therefore this scenario caused migrations to fail, impacting 995 in flight migrations. S1SP developed a patch to correct the validation. This completed PIT testing and was deployed into production 22/01 at 21:10. Migrations completed the following day proved this successfully resolved the issue.	
Reported Customer Impact	

The migration of SMETS1 Dormant devices was impacted		
Actions Completed to Recover Service		
Item	Description.	Owner
1	Deployment of a new version of SECMOD with the additional validation check disabled	S1SP

Incident Reference	**INC000000545763 – Category 2**
Problem Reference	**PBI000000118919**
System(s) Impacted	Active and Dormant SMETS1 Migrations stalled
Incident Start Date / Time (Logged in Remedy)	22/01/2020 18:01
Incident Resolved Date / Time	23/01/2020 15:20
Outage Start	22/01/2020 17:50
Outage End	23/01/2020 13:40
Incident Closure Date	29/01/2020
Major Incident Duration	19 hours 50 minutes
Regions Impacted	All
Resolved within SLA	Yes
Summary of High Category Incident	
SMETS1 migrations for 9 Active devices attempted on the 22/01/2020 are currently stalled due to GSME meters failing at the 12.2 SRV (Device Pre - Notification). During the Go/NoGo on the 23/01/2020 a No Go decision was made due to this incident being outstanding with no Root Cause. Due to the Root Cause not being known this is also holding up migrations for the 1990 dormant and 10 active installations planned for today.	
Reported Customer Impact	
All SMETS1 activity was stalled	
Actions Completed to Recover Service	

Item	Description.	Owner
1	CP removed the affected App Server	Commissioning Party (CP)
2	CP removed the containers from App Server 6 and moved them to the healthy App Servers within the cluster to ensure no loss of capacity for the planned migrations.	Commissioning Party (CP)

3 Code Performance Measures

3.1 Service Levels Attained

This section reports the Service Levels achieved in January 2020 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.**			**98.05%**	**98.41%**	**99.00%**	**96.00%**
	PM1.1	Percentage of DSP Service Request Times within relevant TRT	DSP	99.65%	99.52%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP SIE	99.13%	99.47%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP Capgemini	99.98%	99.95%	99.00%	96.00%
	PM1.4	Percentage of DCC Service Request Times within relevant TRT	DSP	99.96%	99.93%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPN	84.71%	87.20%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPC	98.89%	99.32%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPS	98.74%	99.30%	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	99.74%	99.72%	99.00%	90.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPS	99.73%	99.73%	99.00%	90.00%
CPM2	**Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time**.			**99.92%**	**99.92%**	**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	99.30%	99.21%	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	99.99%	99.99%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPS	99.98%	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	99.94%	99.93%	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	99.94%	99.94%	99.00%	96.00%
CPM3	**Percentage of Alerts delivered within the applicable Target Response Time.**			98.84%	99.17%	**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	99.98%	99.94%	99.00%	96.00%
	PM1.5	Percentage of S1SP SMETS1 Alert Response Times within relevant Target Response Time	S1SP SIE	99.59%	99.66%	99.00%	96.00%
	PM1.7	Percentage of S1SP SMETS1 UTRN Response Times within relevant Target Response Time	S1SP SIE	No Events	100.00%	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	94.74%	95.46%	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	99.94%	99.98%	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	99.95%	99.98%	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.**			**75.00%**	**66.67%**	**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.**			**93.64%**	**92.77%**	**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 98.41% and is below the Target Service Level.

CSPN PM2 reported Service Level was 87.20% and is below Minimum Service Level.

The above measures have been affected by the volume of alerts coming across to the CSPN from a small percentage of the estate. The volumes of these are 30x that specified in the design. A Problem record PBI000000116412 has been raised. The issue requires a firmware upgrade to resolve but this can't be done over the air and requires the service user to visit the site. Other alerts (8F3E's) are being investigated within the test labs along with the meter manufacturer.
Service Users have been advised not to install this model of Communications Hub whilst investigations are on-going.

3.1.2 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 66.67% and is below the Minimum Service Level.

This was impacted by INC000000532006 and INC000000541487

INC000000532006 was under investigation as a category 3 however analysis by DCC Incident Management determined that a number of Service Users were affected and the incident was reclassified as a Cat 2 based on the increased impact. The incident concerned devices dropping of the HAN (Home Area Network) in the CSP Central &

South Region. To mitigate the issue DCC TOC generated daily reports of impacted devices and CSP Central and South carried out reboots of the devices to restore HAN connectivity. This work was completed daily under the Incident until the impact had reduced significantly. The ongoing activity of completing this tactical fix was then tracked by Problem Management under PBI000000118613

INC000000541487 occurred due to a failure on 1 of the 8 MME elements, within CSP Central and South's infrastructure. This resulted in approximately 430 Comms Hubs losing their DNS entry and being unable to re-connect. This had a knock-on effect to DNS checks for SRVs as there were being queued and timing out before completion and returning E20 errors. Complex investigations were required by CSP Central and South and DSP to first identify the root cause of the increase in E20 errors and to identify a resolution. Technical restoration was achieved by DSP removing a non-prod domain entry on the Application Server that handles the DNS requests.

Please see section 2 "Key Incidents" for further details of this event.

3.1.3 Category 1 and 2 Incident Resolution – CPM4

For clarity please note, to ensure operations boards are furnished with the most recent information, data provided to them utilises the "Start Date". The PMR utilises the "Closed Date" as the formal service level performance on Incident Resolution can only be calculated on closure. This can result in discrepancies between operational reporting and contractual reporting in instances where Incidents are Opened in one month and Closed in another.

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	4	2
Total	**6**	**4**	**2**

Table 2 - CPM4 Incident Count

For Information only: Prior to any Performance Measurement Exclusions Applied

Category	Total Incident Count	Within SLA	Failed SLA
Category 1	0	0	0
Category 2	12	9	3
Total	**12**	**9**	**3**

Table 3 – CPM4 Pre-PMEL Incident Count

3.1.4 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	78	70	8
Category 4	68	64	4
Category 5	877	815	62
Total	**1,023**	**949**	**74**

Table 4 - CPM5 Incident Count

3.1.5 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.

3.1.6 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	2	1	66.67%
Total	**2**	**1**	**66.67%**

Table 5 - Incidents Relating to CPM4

Category	Within SLA	Failed SLA	SLA Pass %
Category 3	16	5	76.19%
Category 4	17	1	94.44%
Category 5	310	31	90.91%
Total	**343**	**37**	**90.26%**

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					48	48
2018 September					74	74
2018 October					137	137
2018 November				1	226	227
2018 December					337	337
2019 January					551	551
2019 February			1	1	391	393
2019 March				2	544	546
2019 April					657	657
2019 May				2	533	535
2019 June				4	1,328	1,332
2019 July				11	1,449	1,460
2019 August			1	4	1,603	1,608
2019 September			1	1	2,443	2,445
2019 October			7	1	2,804	2,812
2019 November			20	3	2,724	2,747
2019 December			6	8	3,992	4,006
2020 January			35	2	2,137	2,174
Total			**71**	**40**	**21,981**	**22,092**

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 – 10,186
Incorrect Credentials Loaded on to Device – 8,446
DUIS Service Request 8.14. not received – 1,423

Following positive feedback from the Customer Operations Forum the Incident into Problem proposal was due to be discussed in February's OPSG meeting but was dropped from the agenda due to various reasons. A verbal update has been given to the March OPSG meeting but members have asked for additional information so will now be rolled forward into April's meeting where it will be discussed along with wider problem management changes

In February SIP525 'Interested Parties' functionality went live which will result in a reduction in duplicate incidents needing to be raised to keep multiple parties updated on progress. The DCC have engaged the DSP to see if open duplicate tickets can be closed in bulk to reduce the time and effort to cleanse. An update is due to be provided to the OPSG meeting in April on progress.

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					1	1
2018 August					1	1
2018 September					3	3
2018 October					2	2
2018 November					19	19
2018 December					34	34
2019 January					101	101
2019 February					36	36
2019 March					109	109
2019 April					86	86
2019 May			1		82	83
2019 June					141	141
2019 July				1	194	195
2019 August				2	301	303
2019 September			1	1	146	148
2019 October				1	258	259
2019 November			2	4	171	177
2019 December			2	3	253	258
2020 January	1		19	19	935	974
Total	**1**		**25**	**31**	**2,873**	**2,930**

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	367
Total	**367**
Exclusion Type	
Alert / Event Monitoring (For Information only)	2,555
Duplicate	237
Cancelled	41
Production Proving / Testing	3
Internal to DCC – Non DCC Impacting	24
Total	**2,860**
Grand Total	**3,227**

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	100.00%	99.95%	99.95%	99.00%
	2.3	Service availability – DCC Service Management	Monthly	100.00%	100.00%	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	100.00%	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 2019 Q3	Latest Qtr. Service Level 2020 Q1	Target Service Level	Minimum Service Level
Service Management	7	Notification of Planned Maintenance events[5]	Quarterly	92.31%	93.33%	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

4.1.1 Service Level Below Target Service Level

PM7 Notification of Planned Maintenance events, reported Service Level is 93.33% and is below Target Service Level.

This is measured on a quarterly basis and out of the 30 applicable changes, there were 2 changes which failed the measure. One was related to the November maintenance release and the other was with the associated SSI/SSMI sprint release on the same date. In both cases, although planned with DCC and testing teams took place within the required timescale, the change was not officially submitted to DCC with 20 days' notice. This was an oversight in the planning. Since November DSP have updated their Change Management processes and introduced an additional internal Change Board to ensure this oversight is not repeated.

4.2 Performance Measurement Exceptions

During the period the following Exceptions were agreed for DSP reported Service Levels:

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Availability	PM2.2 (DSP)	2	Events Beyond Service Provider Control	During the national Gamma network incident (INC000000549963) 2 Service Users experienced outages to their Gamma service for a combined total of 1,078 minutes in January 2020. Upon DSP investigation it was found that Gamma resilience had failed due to issues within those Service Users' internal infrastructure. It should be noted that a 3rd Service User also experienced outage during this event due to both of their Gamma links being impacted by the incident. This outage is included in the PM2.2 results.

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.

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	99.24%	98.01%	80.00%	70.00%
	1.2	First time SMWAN connectivity within 30 days	Monthly	99.82%	99.83%	90.00%	80.00%
	1.4	SMWAN connectivity Level	Monthly	99.99%	99.99%	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	99.07%	99.04%	99.00%	95.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	99.71%	99.85%	99.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	385.39%	388.10%	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
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 2019 Q3**	**Latest Qtr. Service Level 2019 Q4**	**Target Service Level**	**Minimum Service Level**
Communications Hub Connectivity	1.3	First time SMWAN connectivity within 90 days	Quarterly	99.99%	100.00%	99.00%	95.00%
Service Management	10	Notification of Planned Maintenance events within required target[6]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 11 - CSPN Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 388.10%. CSPN had a total of 4,891 CH power outages reported, in January, and 4,891 were sent to DSP within SLA. CSPN 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:

$$PM12.2 = 100\% \times \frac{\text{Number of Power Outage Event alerts}}{}$$

[6] Measurement Period is a Calendar Quarter

$$\left(\frac{}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

Using the calculation above PM12.2 = 100 * (4891/ ((4891 – 50) * 0.25) + 50) = 388.10%

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 In Period Exceptions

5.2.1.1 PM1.4 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.4 (CSPN)	41,437	Failure to follow maintenance as per CHIMSM	These figures are for the reporting period (not cumulative)

Table 12 - CSPN PM1.4 Exclusions

41,437 x CH excluded for January 2020 due to several reasons, covering: -

- Incomplete Communication Hub Install – 9,265
- Communication Hub installed on non-consumer premises e.g. Live Lab – 17
- Communication Hub in Low Coverage database – 151
- Communications Hubs where JSR is incomplete – 121
- Communications Hubs where no incident has been raised for outage – 13,085
- Issue started and ended in prior month – 9,107
- Data Error – 9,675

[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

- Not Active – 16

Explanations for the exclusions mentioned above are as follows:

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.

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.

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.

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.

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. This reporting issue is being investigated by CSPN.

Data Error

Comms Hubs where the data shows that an additional outage started prior to the previous one ending. This is an error and is under investigated by CSPN.

Not Active

Comms Hubs where the Operational Status in the CSPN system is not set to Active, to be included in PM1.4 the device must be Active. These are devices where the SU has started the Returns Process

5.2.2 Total Estate Exceptions

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

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.

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%	99.97%	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	99.02%	98.95%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	100.00%	100.00%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	396.23%	394.96%	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%
	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%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
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 2019 Q3**	**Latest Qtr. Service Level 2019 Q4**	**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 394.96%. CSPC had a total of 11,756 CH power outages reported, in January, and all were sent to DSP within SLA (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 * (11756/ ((11756– 50) * 0.25) + 50)) = 394.96%

[8] Measurement Period is a Calendar Quarter

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 In Period Exceptions

6.2.1.1 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)	7,259	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

7.259 x CH excluded for January 2020 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,605
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 375
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 47
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 237
- CHIMSM Not Followed – Associated with NEP – 6
- CHIMSM Not Followed – 8.14.2 on Cellular – 11
- There were no, or incomplete address details provided by the Service User – 4,978 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

[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

6.2.1.2 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPC)	7,259	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 PM11 Exclusions

7.259 x CH excluded for January 2020 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,605
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 375
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 47
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 237
- CHIMSM Not Followed – Associated with NEP – 6
- CHIMSM Not Followed – 8.14.2 on Cellular – 11
- There were no, or incomplete address details provided by the Service User – 4,978 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

6.2.2 Total Estate Exceptions

6.2.2.1 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	60,200	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 PM1.3 Exclusions

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

60,200 x CH excluded for January 2020 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 10,341
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 4,319
- Aborted Installation – 135
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 796
- Installed out of region – 5
- Test Lab installations – 2
- There were no, or incomplete address details provided by the Service User – 44,602 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

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.

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%	99.97%	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	99.01%	99.10%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	100.00%	100.00%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	396.86%	395.43%	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%
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	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 2019 Q3	Latest Qtr. Service Level 2019 Q4	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 395.43%. CSPS had a total of 12,975 CH power outages reported in January, and all were sent to DSP within SLA (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:

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

[10] Measurement Period is a Calendar Quarter

Using the calculation above PM12.2 = 100 * (12975 / ((12975 – 50) * 0.25) + 50)) = 395.43%

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 In Period Exceptions

7.2.1.1 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)	5,713	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

5,713 x CH excluded for January 2020 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,628
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 568
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 40
- CHIMSM Not Followed – 8.14.2 on Cellular – 11
- CHIMSM Not Followed – Associated with NEP – 6
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 206
- There were no, or incomplete address details provided by the Service User – 3.254 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

[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

7.2.1.2 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPS)	5,713	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 19 - CSPS PM11 Exclusions

5,713 x CH excluded for January 2020 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,628
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 568
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 40
- CHIMSM Not Followed – 8.14.2 on Cellular – 11
- CHIMSM Not Followed – Associated with NEP – 6
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 206
- There were no, or incomplete address details provided by the Service User – 3.254 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

7.2.2 Total Estate Exceptions

7.2.2.1 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	63,492	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 20 - CSPS PM1.3 Exclusions

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

63,492 x CH excluded for January 2020 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 10,528
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 4,850
- Aborted Installation – 76
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 602
- Installed outside of region – 2
- CHIMSM Not Followed – Given UPRN is not available – 1
- Test Lab installations – 1
- There were no, or incomplete address details provided by the Service User – 47,378 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

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	1	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	100.00%	100.00%	90.00%

Table 21 – S1SP SIE Reportable Performance Measures

8.1.1 Service Level Below Target Service Level

PM3.1 Category 1 or 2 Incidents directly related to a change release within 30 days of release, reported Service Level is 1 and is below Target Service Level.

During the period, a Category 2 Incident (INC000000545619) was caused due to an additional migration validation step preventing migrations. The additional validation was introduced by the SIE January maintenance release (CRQ000000120604)

with an incorrect configuration. The configuration was corrected as part of the Incident response, and a Problem Investigation (PBI000000118924) was initiated to prevent future repeats.

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	100.00%	100.00%	99.99%	99.17%
	2.2	Percentage Service availability – CP Service (Production Environment)	Monthly	99.81%	100.00%	99.95%	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

able 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	99.69%	99.71%	99.00%	99.00%
		Combined monthly IoT Core and Management Service Availability	Monthly	99.90%	99.97%	99.70%	99.70%
		Monthly IoT Core availability (Voice/Data/SMS)	Monthly	99.95%	100.00%	99.90%	99.90%
		Monthly Management Service Availability (API, Reporting, Provisioning, GUI, Portal)	Monthly	99.95%	99.97%	99.70%	99.70%
		Monthly Availability of DCC dedicated fixed links	Monthly	No Data	No Data	99.95%	99.95%

Table 23 – S1SP Vodafone Reportable Performance Measures

10.2 Performance Measurement Exceptions

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

Please note that “dedicated fixed links” are not currently implemented as a solution therefore no data to report.

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.

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 three Performance Measures. These Performance Measures are:

CSP 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 87.20%. This failure resulted in the accrual of 175 Service Credit points which equate to Service Credits of £45,377. (This Performance Measure contributes to DCC Performance Measure 1.)

CSP 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 95.46%. 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 CSP PMs 2 & 3.2, discussions are ongoing between DCC and CSPN regarding the installation by Service Users of meters outside of the agreed derogation areas. Until Phase 2 of ARQCR1028 is implemented, CSPN 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.

CSP PM7.4 – Percentage Incident Resolution of Severity 3, Severity 4 and Severity 5 Incidents within requirement based on Severity Level. The Target Service Level for this PM is 90% and the Actual Service Level achieved was 78.95%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

These failures equate to Service Credits of £113,571

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

CSP PM7.3 – Percentage Incident Resolution of Severity 1 and Severity 2 Incidents within requirement based on Severity level. The Target Service Level for this PM is n-1 and the Actual Service Level achieved was n-2. The Service Credit Points for this measure is 100, with Service Credits of £36,405,43. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

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

CSP PM7.3 – Percentage Incident Resolution of Severity 1 and Severity 2 Incidents within requirement based on Severity level. The Target Service Level for this PM is n-1 and the Actual Service Level achieved was n-2 The Service Credit Points for this measure is 100, with Service Credits of £29,548.07 (This Performance Measure does not contribute to any DCC Code Performance Measure.)

These failures equate to Service Credits of £69,954

DSP No Service Failures have occurred during the month. Therefore, no Service Credits have accrued this month.

Note: Whilst discussions on an appropriate measurement method for PM10 continue, it has been greyed out and will not count as either a pass or a fail. This will be revisited once the PM10 performance measure is agreed.

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

Month	Arqiva	BT	CGI	Telefonica	Total
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**
Oct – 19	£94,125	£0	£20,201	£0	**£114,326**
Nov – 19	£100,607	£0	£0	£44,523	**£145,130**
Dec – 19	£133,019	£0	£0	£49,694	**£182,713**
Jan – 20	£113,571	£0	£0	£69,954	**£183,525**

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 £183,525.

13 Appendices

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

13.1.1 PBI000000113808

February Report 2019 - 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 to complete resolution activities is due in DSP release 43, scheduled for deployment into Production on 14th March 2020.

Latest: Target Completion Date 20/03/2020

13.1.2 PBI000000113813

February Report 2019 - 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. A precautionary restart of the Firewall has been successfully carried out on 19th of December 2019 and will be scheduled periodically via Change Process until the permanent solution is put in place.

Latest: Target Completion Date 30/04/2020

13.1.3 PBI000000115702

June Report 2019 - 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. A code change was required to ensure an appropriate response to Service Users in the event of connection/application performance issues. The fix was included within DSP#36, deployed into Production on 27th August 2019. DCC are working with DSP to ensure mitigation is in place to avoid potential reoccurrences and related issues that service users observe.

Latest: Target Completion Date 27/03/2020

13.1.4 PBI000000116409

June Report 2019 - 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 has been delivered via a code fix.

Latest: Closed

13.1.5 PBI000000116812

August Report 2019 - 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. DSP has confirmed that they have exhausted all testing that can be done without a strategic / planned failover of the F5s with packet captures and sniffers in place. DSP have been unable to see anything other than packet loss / output drops but need to confirm if the loss is enough to have caused this issue. At this stage it is not believed that further testing will add any value to Root Cause Analysis without a failover and captures for analysis. Ahead of any future failover requirements DSP need to provide assurances that a repeat of the impact seen at failover will not be seen, however at this stage no definitive Cause has been confirmed – as a result of the testing completed there has been no fault found to date therefore no further solution to implement in response. What has been identified is that output drops increase only under periods of high traffic output. A recreation of the Incident in a controlled environment is believed to be needed to investigate further, but this will have to be planned and co-ordinated under a planned change. Failover of firewalls is going to be pursued in isolation, under a controlled change, in order to troubleshoot and resolve any outstanding issues with the system management firewalls. DSP are assessing all possible scenarios which could arise during the failover ahead of the change to pre-empt any issues and prepare accordingly. This will include the availability of hardware during the change window and the presence of the required Resolver Groups at both datacentres.

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

13.1.6 PBI000000117102

September Report 2019 - 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. Automatic alert thresholds are being reviewed and long-term solution is still being defined.

Latest: Target Completion Date for this Problem is 31/07/2020

13.1.7 PBI000000117205

September Report 2019 - 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. DSP plan for an enduring fix be completing F5 upgrades across the estate, that programme is very large and will be completed in 3 Phases.

Latest: Target Completion Date for this Problem is 31/03/2020

13.1.8 PBI000000117128

September Report 2019 - Key Incident **INC000000493155** & November Report 2019 - Key Incident **INC000000511840**

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.

Strategic Solution around increased virtual memory capacity commenced on 07th of November 2019, all activities carried out under strict governance and change control. The long term plan is to optimise additional memory allocation for Comms Hub Manager. Database changes to the production environment successfully implemented 18/02, however they highlighted a requirement to add additional CPU's which was followed up with a change on the 19th February. Initial analyse is positive but the situation remains under monitor.

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

13.1.9 PBI000000117305

September Report 2019 - Key Incident **INC000000491743**

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 are coordinating efforts with DSP, DCC Service Management and the Service User to insure repeat incidents don’t occur. Work has been completed for the service user to upgrade their primary gateway bandwidth. The upgrade of the Secondary link has to be coordinated with a relocation of equipment in a datacentre due to capacity constraints, this issue has delayed completion of this Problem.

Latest: Target Completion Date for this Problem is 27/03/2020

13.1.10 PBI000000117135

October Report 2019 - Key Incident **INC000000495738**

CSP Central and South Comms Hubs not birthing with DSP

Problem: A Service User contacted the DCC to advise that Comms Hubs were not birthing in the Central and South region. This was directly affecting Service Users ability to complete install and commissioning activities. The issue was due to a database full-table scan on the CSP Meter Firmware Operation Logging table. This caused other messages to queue while this scan completed. The reasons behind the full-table scan starting and why it was long-running are under investigation.

The Root Cause of this issue was a configuration change from a CSP release. CSP C&S completed a change release (R8.5) where additional logging was introduced to capture 'Force Time Sync' data issues, this caused the table space to increase significantly. This resulted in increased query times when high volumes of requests were submitted in parallel, in this incident single meter firmware jobs, caused extensive queuing. (90 sec + query times across 1000's of transactions).

CSP C&S technical team added Indexes to the table (per their vendors recommendation). Before the Indexes were added each job could took between 90 and 1200 seconds, following the Indexes going in this has dropped to 11 milliseconds. Long term enhancements are also being devised and a change has been raised to address the main issue of optimising the search API query response times. The change required for the fix has been successfully implemented, this change will enable a higher number of bulk uploads to be complete in one go. CSP Central and South are now looking to test to confirm the issues are resolved.

Latest: Target Completion Date 31/03/2020

13.1.11 PBI000000117240

October Report 2019 - Key Incident **INC000000503961**

CSP Central and South Comms Hubs not birthing with DSP

Problem: A Service User contacted the DCC to advise that Comms Hubs were not birthing in the Central and South region. This was directly affecting Service Users ability to complete install and commissioning activities. The issue was due to a database full-table scan on the CSP Meter Firmware Operation Logging table. This caused other messages to queue while this scan completed. The reasons behind the full-table scan starting and why it was long-running are under investigation.

The Root Cause of this issue was a configuration change from a CSP release. CSP C&S completed a change release (R8.5) where additional logging was introduced to capture 'Force Time Sync' data issues, this caused the table space to increase significantly. This resulted in increased query times when high volumes of requests were submitted in parallel, in this incident single meter firmware jobs, caused extensive queuing. (90 sec + query times across 1000's of transactions).

CSP C&S technical team added Indexes to the table (per their vendors recommendation). Before the Indexes were added each job could took between 90 and 1200 seconds, following the Indexes going in this has dropped to 11 milliseconds. Long term enhancements are also being devised. DSP is still working with the Vendor to ascertain the best upgrade options. DSP has confirmed that the HSM (Hardware Security Module) upgrade is still under analysis with the Vendor as testing of the new client software was unsuccessful. At this stage DSP cannot proceed any further without a re-compiled version for the supporting software. A new testing phase / acceptance test review is required; DSP are currently awaiting a timeline and expect this from the Vendor in the coming weeks.

Latest: Target Completion Date 31/03/2020

13.1.12 PBI000000117601

October Report 2019 - Key Incident **INC000000508103**

CHM - Fuse components - Unable to birth in North Region

Problem: This Problem investigates issues with Comms Hub Device Manager related to Fuse components. Install Alerts not progressing through CSP North to DSP on 25th of October 2019 that impacted Service Users (SU's) Comms Hubs installations.

The Root Cause is under investigation. A series of changes has been completed by the CSP North:

1 - Automatic Reboots of the Nodes (4 hourly) - Implemented - Provided the stability and resilience to the systems
2 - CHM Fuse and ActiveMQ JVM optimisation Change 1 - Implemented - Memory utilisation has improved
3 - CHM Fuse and ActiveMQ JVM optimisation Change 2 - Implemented - Memory utilisation has improved
4 - CHM Fuse and ActiveMQ JVM optimisation Change 3 - Implemented - Memory utilisation has improved, No more Hang & Abort of the process routes
5 - Frequency of SLA Cron decreased from 1 Minute to 1 hour to observe the SLA processing - Implemented - No significant improvement observed
6 - Data Fix to invalid data records in the CHM - Implemented - Database contention Improved
7 - Optimisation of Code (CRON SLA) for efficient data processing - Implemented - Resource Utilisation improved as this exclude invalid Records
8 - Throttler Increasing the gap between cycles and the number of SRs per cycle (While Keeping the max count of SR Identical) - Implemented - Improved throughput of the system

The CSP are have looked to reduce the frequency of the reboots currently in place to ensure the changes made have stopped issues reoccurring. In the course of investigation it has been decided to consolidate this Problem record with PBI000000117128.

Latest: Closed

13.1.13 PBI000000117610

November Report 2019 - Key Incident **INC000000510213**

Intermittent Service request failures from DCO

Problem: Following a deployment of a planned DCO (Dual Control Organisation) release in to Production, intermittent Server (error 500) errors were being seen by S1SP in response to the heartbeat service requests (for SMETS1). The deployment was rolled back but issues continued to occur. The Migration of SMETS1 devices could not continue until the incident was resolved.

There are 2 separate unrelated issues within DCO that both contributed to the “Server 500 errors” seen following rollback.

The first was a reoccurrence of the Cryptocontainer issues being investigated in PBI117226 (Bug in the behaviour of the Crypto API (application programming interface) which throws an exception if an error is encountered loading Codesafe against the list of HSMs (Hardware Security Module). An enduring fix is currently being progressed by DCO & its vendor), this was resolved by Container restarts in PROD-B. The second was after the container restarts in PROD-B, any incoming service requests failed, resulting in the error responses seen by S1SP. This issue was due to an application memory issue, there was a memory limit set to 8Gb and the automating application deployment Memory limit was sent to 4 GB. This caused container memory to be throttled at 4GB when the container was expecting to have 8gb available, causing the container to restart when the 4GB memory usage was reached.

There are two issues to resolve:
1) PBI117226 is dealing with the Bug in the behaviour of the Crypto API (application programming interface) which throws an exception if an error is encountered loading Codesafe against the list of HSMs (Hardware Security Module). The solution proposed is a change of behaviour to note the exception and continue to retry the remaining available HSMs (Hardware Security Module) rather than stopping. This is currently being progressed with DCOs & its vendor.
2) Memory Configuration was amended for the pods within the application servers in the PROD B environment.

The HSM Defensive Solution update is progressing via a commercial CR (Change Request)

Latest: Target Completion Date 27/03/2020

13.1.14 PBI000000117408

November Report 2019 - Key Incident **INC000000510226**

CSP-N - UIT-A Environment – No traffic received from Firewall

Problem: Traffic coming to CSP's North UIT-A (User Integration Testing) environment through fronthaul Firewall was being dropped, resulting in Service Users not being able to utilise UIT-A Environment.

The Root Cause is under investigation. CSP North carried out investigations into root cause, which could not be identified.

Firewall policies have been reapplied to restore the service and can be reapplied at any time given issues reoccur. There is monitoring in place, but it is currently impossible to capture the issues before the impact is noticeable. Service has been stable since.

Contractual agreements regarding testing environment are being reviewed by DCC Service Management.

Latest: Target RCA date breached 22/11/2019

13.1.15 PBI000000117609

November Report 2019 - Key Incident **INC000000510715**

Delay with Install and Commissions across all regions

Problem: Service Users reported latency with installs and monitoring identified a reduction in Install and Commissions in all regions.

The Root Cause was identified as latency being observed and caused by available sockets. The socket timeout settings are under analysis as if these timeout quicker, they release quicker, leading to sockets being more readily available. On this occasion, the sockets were held for too long, which led to latency and impact on the motorway. Due to resources running out as a result of blocking procedures currently in place. Queries and associated threads to database should be 'non-blocking'.

Making the second Database call asynchronous would resolve this issue. This should mean that DSP don't run out of threads, and although a slow response back to be invoked, it is within the http timeout so calls actually succeed. The fix is currently targeted for DSP#43 Release, scheduled for deployment into Production on 14th March 2020.

Latest: Target Completion Date 20/03/2020

13.1.16 PBI000000117612

November Report 2019 - Key Incident **INC000000510869**

UIT-A Not Available For Testing

Problem: On 31st October at 18:49 an incident ticket was raised for the UIT-A environment as users were unable to carry out testing activities. The incident was due to a service user's ESME device in the CSP North UIT-A area generating an excessive amount of alerts (approximately 18,000 alerts). Once this device was turned off normal service resumed. Testing activities in UIT-A had to be suspended until the issue was resolved.

The Root Cause was due to capacity limit being breached. One service user ESME device in the CSP North UIT-A area of the DCC North Test Lab was generating excessive

alerts (approximately 18,000 alerts). Once this device was turned off normal service resumed.

DCC are working with DSP to determine what can be done differently to spot and stop these nuisance alerts from impacting the UIT test environments in the future. Contractual agreements regarding testing environment are also being reviewed by DCC Service Management.

Latest: Target Completion Date 30/03/2020

13.1.17 PBI000000117807

November Report 2019 - Key Incident **INC000000514505**

CSP-N Production Core Firewall high CPU usage and on demand SR's failing

Problem: High CPU (Central Processor Unit) usage on CSP-N Production Core Firewall and high number of connections impacted live service with all on demand Service Requests failing for Service Users.

CSP North vendor identified a memory leak issue within the upgraded firmware that was causing the CPU spike.

CSP Norths vendor has confirmed they now have fixes ready and are looking to implement them in change windows.

Latest: Target Completion Date 13/03/2020

13.1.18 PBI000000117900

November Report 2019 - Key Incident **INC000000515630**

CSP-N loss of connectivity to multiple 3G sites

Problem: Over a hundred 3G sites have dropped off the network.

The Root Cause has been identified as incorrect roaming load on the cellular network with CSP North's Vendor. Once the load issue was resolved there was a prolonged impact as the CSP Norths vendors fault left additional manual work to be carried out by CSP North in order for full connection to re-establish between onsite routers and CSP North's infrastructure.

Investigations are ongoing to look at how similar issues can be prevented in the future and to ensure the correct impact is identified under Incident Triage.

Latest: Target Completion Date 27/03/2020

13.1.19 PBI000000118607

December Report 2019 - Key Incident **INC000000526144**

RNI failure following Server patching change

Problem: Failure of multiple RNI (Radio Network Infrastructure) nodes was spotted on the monitoring resulting in no incoming or outgoing traffic on the CSP-North Network. Monitoring also showed shutdown/ heartbeat failures.

The Root Cause has been identified as Human Error during the implementation of a low impacting Planned patching change. The change went through the Non impacting change process however human error lead to an impact.

CSP North change process has been updated to accommodate changes to work instructions, work patterns and supervision of change implementers as well as improvements to the current process.

Latest: Target Closure Date 06/03/2020

13.1.20 PBI000000118516

December Report 2019 - Key Incident **INC000000530859**

SAT Query Delay

Problem: It was reported that Service Users were experiencing delays when running SAT queries which impacted the ability to view the history of Service Requests on their devices, however, Installs and commissions were not impacted. It was identified that a server had unexpectedly rebooted and required a restart of the application to successfully restore Service.

The Root Cause has been identified as Human Error. The server restart was completed by a technical team member entering the wrong command to a machine.

A change has been created to disable the command on the virtual machines to avoid a repeat issue.

Latest: Target Completion Date 31/03/2020

13.1.21 PBI000000118411

December Report 2019 - Key Incident **INC000000518930**

High Volume of 'Too Busy' errors – CSP North

Problem: An increase in of 'Too Busy' errors were witnessed along with a spike in E20 (Communications Failure – Unable to Communicate with Device) and E21 (Communications Failure – No Response Received from Device) errors.

The Root Cause was that the CSP North network was unable to handle the throughput of messages that were being sent. This caused an inability to handle excessive alerts traversing the network as all CSP North traffic is on a single channel on their transmitter equipment.

CSP North continues to perform on-going manual tuning activities on the network to alleviate congestion.

Latest: Target Completion Date 31/03/2020

13.1.22 PBI000000118605

December Report 2019 (Excluded through PMEL) - Key Incident **INC000000524184**

Gamma link failure

Problem: Gamma link was down leaving 2 Service users unable to communicate with the DSP system, which meant they were unable to perform any installation or commissioning of SMETS-2 devices or process any Service Requests. No service impact reported as this was Northbound queue affecting.

The Root Cause was a failed Change. The Service User bandwidth upgrade required a Third Party to perform a hub switch and for the Vendor to configure the new bandwidth requirement. Investigation has shown that the hub switch did not work successfully due to a software defect with the Third-Party Portal that is used to automatically request and carry out hub switches.

The Vendor have changed their process so that when upgrading bandwidth involving hub switches, they will do the primary link one day and the secondary link a subsequent day to ensure that in the event of an issue, there is always one link available. Additionally, a Process change has been made to ensure that going forward, this type of work goes through the DSP Change Management Process and receives DSP and DCC CAB approval to ensure that everyone is aware of the work and any risks.

Latest: Closed

13.1.23 PBI000000118518

December Report 2019 (Excluded through PMEL) - Key Incident **INC000000530634**

Service User Planned Works - Alert Build-up

Problem: Multiple Service Users carried out internal planned works which has resulted in excessive messages queuing in the DSP Northbound Message store. All SRV's and alerts were not being accepted by the Service User's whilst they are carrying out their planned works, causing DSP's queue to increase.

The Root Cause is a Data Issue. Service User Planned works resulted in a high amount of data alerts being stored by DSP and to mitigate against the alerts crashing their systems they tool mitigating actions. DSP ran 4 scripts in parallel to discard/remove 8F3E alerts for the Service Users. DSP also temporarily shut down the CSP Central and South connections to stop the number of alerts increasing which allowed DSP to reduce their queues to within acceptable levels. There should not be this level of alerts on the system to store during outages.

Solutions are being devised. Dealing with alert volumes and finding and implementing solutions is ongoing already. Storm Alert Protection filters being available to DSP to use are due to be delivered later in the year.

Latest: Target Completion Date 26/06/2020

13.1.24 PBI000000118613

January Report 2020 - Key Incident **INC000000532006**

CSP C&S Progressing CH Defects causing HAN drop offs

Problem: DCC have identified a trend of issues with both Comms Hub devices in the CSP Central & South Region dropping of the HAN (Home Area Network). DCC can attempt to trigger a re-join and maintain service of those affected devices by sending the device the command to reboot. Upon reboot the ESME devices regain connectivity to the Comms Hub. This Problem is to look and identify the Root Cause from a Comms Hub perspective and look to avoid Comms Hubs dropping off the HAN.

The Root Cause is under investigation. Routing issues have been observed with both CHs used in the CSP C&S region. Two defects have been found APS ACK (App Support Layer Acknowledgement) & Link status. Fixes for these issues are planned to go in to testing environments as soon as feasible. Further analysis of data is ongoing to ensure all the triggers for Comms Hub related drops are identified.

Latest: Target RCA Date expired 03/02/2020.

13.1.25 PBI000000118616

January Report 2020 - Key Incident **INC000000534308**

Install and Commissioning failures in the CSP Central and South Region

Problem: Multiple Service Users were reporting Install and Commissioning failures/delays in the CSP Central and South region starting on the 23rd December 2019.

The Root Cause of this Problem is Capacity. Meter traffic through the comms hub that then go on from the CSP to DSP created this issue. The primary alerting source during this issue came from 8F3Es. Due to the heavy load in traffic DSP struggling to send responses back to the CSP and created a backlog of all service requests.

Mitigation to avoid capacity being reached have been implemented and more tasks to reduce traffic are ongoing.

Latest: Target Completion Date 26/06/2020.

13.1.26 PBI000000118704

January Report 2020 - Key Incident **INC000000540421 & INC000000541487**

CSP South & Central Operational Intelligence and Orchestration Tool stopped.

Problem: CSP South & Central Operational Intelligence (OI) and Orchestration Tool (OT) stopped.

The Root Cause has been established as a defect from a software patch applied to the application in December 2019. The defect impacts the connection pool for the application which grows by 1 connection per day and upon reaching the threshold of 20 no further connections can be established and consequently the application malfunctions.

To resolve the defect a hotfix supplied by the provider is being analysed by CSP South & Central, implementation date TBC.

Latest: Target Completion Date 27/03/2020.

13.1.27 **PBI000000118619**

January Report 2020 - Key Incident **INC000000541556**

Service request failures in UIT-A

Problem: An internal Change implemented resulted in a database being turned off impacting SMKI Repo, MKS, all SMETS-1 Service Requests and installation Service Requests for SMETS-2 within UIT-A.

The Root Cause of this Problem was a failed Change. A windows service was not brought back up following a planned and approved Change implemented to patch and reboot UIT-A servers, which subsequently caused service components within UIT-A to go off line.

All Changes which impact SMKI Repo or the MKS are to have further post implementation checks put in place and all issues identified post Change/Release will be highlighted to Service Management to gain approval on next steps.

Latest: Closed

13.1.28 **PBI000000118804**

January Report 2020 - Key Incident **INC000000542187**

Increase in Too Busy/ E20 Errors in North Region

Problem: Regular increase of Too Busy responses being seen on the CSP North region. Potential to cause E20 errors and impact install and commissions.

The Root Cause has been established as one Service User sending an excessive amount of On-Demand service requests causing congestion on the network.

DCC are working with the Service User to move On-Demand reads request traffic to Scheduled Service Requests.

Latest: Target Completion Date 25/03/2020.

13.1.29 PBI000000118916

January Report 2020 - Key Incident **INC000000544951** (Excluded through PMEL)

E20 alerts preventing Installs for 1 Service User in CSP North

Problem: This is a follow on Problem to a CAT 2 incident that impacted install and commission (I&C) for a single service user in the CSP North Region. Initially a Cat 1 was raised by the service user (SU), this was lowered to a Cat 3 for investigations to take place then raised to Cat 2 when SU confirmed I&C impacted. Investigations showed no DSP or CSP related issues that impacted this outage.

The Root Cause is under investigation, it is believed to be a service user issue but they have not confirmed identification of what caused the Problem.

Latest: Target RCA Date expired 02/03/2020.

13.1.30 PBI000000119002

January Report 2020 - Key Incident **INC000000543758** (Excluded through PMEL)

Install & Commission Delays for a Service User

Problem: A Service User report was received, indicating that their install and commissions were taking significantly longer than usual, with the few that had completed having taken over 90 minutes. Delays in excess of 5 minutes could be seen between the DUIS request being sent and the DUIS response being returned and out of 123 install attempts, only 9 had completed.

The Root Cause is a Capacity Issue. The trigger was caused by a backlog of service requests and alerts on a MSP (Multi Service Party) adaptor which resulted in install and commission delays for a service user who communicate via the adapter.

The MSP (Multi Service Provider) advises that monitoring improvement allows them to identify the receipt of alerts (they were not previously monitoring this element of the queues) which will ensure that any delays to Install & Commission requests due to high volumes of device alters will be identified earlier in the troubleshooting process and should not result in a ticket being raised with DCC. The MSP also introduced an increase in processing rate for these service requests to avoid capacity issues occurring again.

Latest: Closed

13.1.31 PBI000000118430

January Report 2020 - Key Incident **INC000000538993** (Excluded through PMEL)

Delay in processing Service Requests.

Problem: Service Users experienced a delay in processing DCC only Service Requests. Service Users would have experienced a delay in completing the installation of SMETS-2 devices. The installations were processing during the course of the Incident; however, there was a service degradation, which means that the number of installations during the Incident were lesser than compare with a normal period.

The Root Cause has been identified as a Data Issue. During the Incident, all SMETS-1 migrations failed whilst attempting to send Service Request 12.2 (Device Pre-notification). The reason for this is that during the Incident, the traffic management on the “execute” pool was triggered and therefore blocking DCC-only Service Requests, of which 12.2 is one. As with previous issue, a significant factor with this, is the volume of '8F12' (CHF Device Log Changed) alerts received.

A code fix to make the second Volt call asynchronous, indicated on the latest edition of the Production Maintenance Schedule as targeted for DSP#43. This should mean that DSP don’t run out of threads, and although DSP get slow response back to the RM client, it is within the http timeout so calls actually succeed.

Latest: Target Completion Date 31/03/2020.

13.1.32 PBI000000119007

January Report 2020 - Key Incident **INC000000545509** (Excluded through PMEL)

Multiple reports of E20 and failure to connect to SMWAN

Problem: Multiple reports were received of devices in the CSP Central and South region not connecting to the WAN and E20 errors being received.

The Root Cause was a configuration issue. An unknown feature was introduced into Production within a product upgrade, which implemented a limit to the Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) connections that can be made. This is designed to stop 'denial of service' attacks.

The connection limit has now been set to 10,000 to avoid this issue in the future.

Latest: Target Completion Date 27/03/2020.

13.1.33 PBI000000118924

January Report 2020 - Key Incident **INC000000545619**

SMETS1 Migration - Issue identified with the 5.9.10 check from SecMod.

Problem: Issue identified with the 5.9.10 check from SecMod. Migrations were stalling causing an impact on 995 in flight migrations. Issue occurred following an SIE change on 21/01.

The Root Cause of this Problem is related to an introduction of a change. A change applied involved adding a validation step (5.9.10 check) on the MCF (Migration Common File) that all Supplier certs (if provided) belong to same SEC Party. But it also had a condition that at least one Supplier certificate needs to be present per MCF, otherwise the check fails. It failed to take in to account that supplier certs are not included on MCF files for dormant meters therefore this scenario caused migrations to fail.

A solution has been deployed via a patch to amend the code. Actions on lessons learnt completed.

Latest: Closed

13.1.34 PBI000000118919

January Report 2020 - Key Incident **INC000000545763**

Active and Dormant SMETS1 Migrations Stalled

Problem: Investigations found that the Commissioning party server was unable to communicate with DSP - returning an Error message E204 - Could not connect to DSP. This issue was only appearing on SRVs being sent from this application server. The resolving action taken was to remove the server from the server pool and moving the containers to server another application server, where the issue was not being seen.

The Root Cause has been identified as a configuration issues. Investigations have found a missing routing rule on an application host. This rule was present on all other Application hosts.

The missing routing rule on an application host has been re-added to the server on 29/01/2020 and no further issues have been seen on the server. Improved monitoring remains under investigation.

Latest: Target Completion Date 27/03/2020.