Data Communications Company

# DCC Performance Measurement Report

## Performance Measurement Period:

## September 2020

| | |
|---|---|
| **Version:** | **V1.0** |
| **Date:** | **03/11/2020** |
| **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** ..... **16**
3.1 Service Levels Attained ..... **16**
3.1.1 CPM1 – PM2 Volumes Data ..... **21**
3.1.2 Service Level below Minimum – CPM1 ..... **21**
3.1.3 Category 1 and 2 Incident Resolution – CPM4 ..... **21**
3.1.4 Category 3, 4 and 5 Incident Resolution - CPM5 ..... **22**
3.1.5 CPM4 and CPM5 – Incidents Re-Opened after Closure ..... **23**
3.1.6 Incident Resolution Information – CPM 4 & 5 ..... **23**
3.2 Performance Level Exemptions ..... **26**
3.2.1 CPM4/5 - Incidents which the DCC is responsible for resolving and are resolved in accordance with the Incident Management Policy within the Target Resolution Time. ..... **26**
**4 Reported List of Service Provider Performance Measures DSP** ..... **28**
4.1 Service Levels Attained ..... **28**
4.1.1 Service Level Below Target Service Level ..... **29**
4.2 Performance Measurement Exceptions ..... **29**
**5 Reported List of Service Provider Performance Measures CSP North** ..... **30**
5.1 Service Levels Attained ..... **30**
5.1.1 Service Level Below Target Service Level ..... **32**
5.2 Performance Measurement Exceptions ..... **32**
5.2.1 In Period Exceptions ..... **33**
5.2.1.1 PM1.4 SMWAN Connectivity Level ..... **33**
5.2.2 Total Estate Exceptions ..... **33**
**6 Reported List of Service Provider Performance Measures CSP Central** ..... **34**
6.1 Service Levels Attained ..... **34**
6.2 Performance Measurement Exceptions ..... **36**
6.2.1 In Period Exceptions ..... **36**

6.2.1.1 PM1.1 First Time SMWAN Connectivity ..... 36
6.2.1.2 PM11 Accuracy of Coverage Database ..... 37
6.2.2 Total Estate Exceptions ..... 38
6.2.2.1 PM1.3 SMWAN Connectivity Level ..... 38
**7 Reported List of Service Provider Performance Measures CSP South ..... 39**
7.1 Service Levels Attained ..... 39
7.2 Performance Measurement Exceptions ..... 41
7.2.1 In Period Exceptions ..... 41
7.2.1.1 PM1.1 First Time SMWAN Connectivity ..... 41
7.2.1.2 PM11 Accuracy of Coverage Database ..... 42
7.2.2 Total Estate Exceptions ..... 43
7.2.2.1 PM1.3 SMWAN Connectivity Level ..... 43
**8 Reported List of Service Provider Performance Measures S1SP SIE ..... 44**
8.1 Service Levels Attained ..... 44
8.2 Performance Measurement Exceptions ..... 44
**9 Reported List of Service Provider Performance Measures S1SP Capgemini 45**
9.1 Service Levels Attained ..... 45
9.2 Performance Measurement Exceptions ..... 45
**10 Reported List of Service Provider Performance Measures S1SP Vodafone . 46**
10.1 Service Levels Attained ..... 46
10.2 Performance Measurement Exceptions ..... 46
**11 Reported List of Service Provider Performance Measures S1SP Critical Software ..... 47**
11.1 Service Levels Attained ..... 47
11.2 Performance Measurement Exceptions ..... 47
**12 Reported List of Service Provider Performance Measures S1SP Morrison Data Services (MDS) ..... 48**
12.1 Service Levels Attained ..... 48
12.2 Performance Measurement Exceptions ..... 48
**13 Service Credits ..... 49**
**14 DCC's Internal Costs and/or External Cost ..... 51**
**15 Appendices ..... 52**
15.1 Appendix A – Open Problem & Incidents relating to Prior Periods ..... 52
15.1.1 PBI000000116812 ..... 52
15.1.2 PBI000000117205 ..... 53
15.1.3 PBI000000117240 ..... 54

15.1.4 PBI000000118930 ..... 54
15.1.5 PBI000000119705 ..... 55
15.1.6 PBI000000120300 ..... 55
15.1.7 PBI000000120414 ..... 56
15.1.8 PBI000000120211 ..... 56
15.1.9 PBI000000120320 ..... 57
15.1.10 PBI000000120410 ..... 57
15.1.11 PBI000000120403 ..... 58
15.1.12 PBI000000120343 ..... 58
15.1.13 PBI000000120245 ..... 59
15.1.14 PBI000000120433 ..... 59
15.1.15 PBI000000120347 ..... 60
15.1.16 PBI000000121007 ..... 60
15.1.17 PBI000000121203 ..... 61
15.1.18 PBI000000121300 ..... 62
15.1.19 PBI000000121210 ..... 62
15.1.20 PBI000000121400 ..... 63
15.1.21 PBI000000121900 ..... 63
15.1.22 PBI000000121704 ..... 64
15.1.23 PBI000000121907 ..... 64
15.2 Appendix B – Performance Measure Exception Definitions ..... 66
15.2.1 CSPN ..... 66
15.2.2 CSPC & CSPS ..... 66
15.3 **Appendix C - Incident Reports Glossary** ..... 68

# Control Sheet

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

| Page/ Section | 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 September 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 95.10% and is below the Minimum Service Level, further details provided in Section 3.1.2.

The Service Levels achieved for CPM2, CPM3, CPM4, CPM5, CPM6, CPM7 and CPM8 are all above the Target Service Level.

### Service Provider Performance Measures Summary

DSP PM2.1 Percentage Service availability – DCC Data Service (Production Services), reported Service Level is 99.76% and is below the Target Service Level.
Further details are provided in Section 4.1.1

CSPN PM6.2 Percentage availability of DCC WAN Gateway Interface, reported Service Level is 99.82% and is below the Target Service Level.
Further details are provided in Section 5.1.1

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 13 of the report.

## Key Incidents

Please see Appendix C Section15.3 for a glossary of the row titles used within the Major Incident reports.

### September Included

| | |
|---|---|
| Incident Reference | INC000000623269 |
| Problem Reference | PBI000000121203 |
| Category | 1 |
| Service(s) Impacted | SMETS1 Service Requests |
| Service impacted date/time | 27/08/2020 15:40 |
| Service restored date/time | 27/08/2020 16:25 |
| Incident raised date/time | 27/08/2020 15:58 |
| Incident resolved date/time | 27/08/2020 18:51 |
| DCC MIM Engagement date/time | 27/08/2020 16:28 |
| Actual Impact Duration | 45 mins |
| Incident Duration | 2 hrs 53 mins |
| Resolved within SLA | Yes |
| Summary of Incident | |

At 15:40 the heartbeat (a periodic signal generated to indicate normal operation) between the NDB cluster within the DCO ProdB (Farnborough) environment failed. This led to the database nodes to indicate communication failures and the nodes began to shut down due to the self-protection process in place. Once the paired nodes 1 and 3 had shut down the entire NDB effectively shut down as per design to protect data integrity.

This resulted in connection failures for all traffic traversing the DCO infrastructure and a 100% outage of SMETS1 SRVs

DCO completed a restart of all database nodes to restore service and resiliency at 16:25. Connections into the NDB was restored as well as the heartbeat process.

Customer Impact

100% of SMETS1 Service Requests were failing between 15:40 and 16:25. This impact would have been seen by all Service Users.

There was no impact to Migration activities (completed for the day by time of outage) or SMETS2 Service Requests

| Actions Completed to Recover Service | | |
|---|---|---|
| Item | Description | Owner |
| 1 | DCO DBA engineers completed a restart of the NDB nodes to restore service | DCO |

| | |
|---|---|
| Incident Reference | INC000000624768 |
| Problem Reference | PBI000000121300 |
| Category | 2 |
| Service(s) Impacted | SMETS1 Service Requests & Migrations |
| Service impacted date/time | 01/09/2020 07:40 |
| Service restored date/time | 01/09/2020 10:19 |
| Incident raised date/time | 01/09/2020 08:45 |
| Incident resolved date/time | 01/09/2020 11:29 |
| Actual Impact Duration | 2 hours 39 minutes |
| Incident Duration | 2 hours 44 minutes |
| Resolved within SLA | Yes |

Summary of Incident

During the MCC Go/No-Go call on 01/09/2020 DCO advised that they were aware of an issue with Viable Master Key Alerts which potentially affected SMETS1 service and they were in the process of investigating. However, it transpired that while this issue was not the cause of major incident, it did mask the actual cause of the impact, resulting in a delay to DCO's identification of the real issue.

At 09:22 CGI Incident Management contacted DCC Incident Management to advise that they had identified a 50%-60% failure rate for Service Requests across the SMETS-1 environment and Remedy Ticket INC000000624768 had been raised by their alerting tool as Category 3 at 08:42.

Additional evidence from CGI and DCC TOC confirmed the SRV failures and DCC IM convened a bridge call with DCC, DCO and CGI.

| |
|---|
| DCO advised on the call that they had identified an issue with memory leaks in the application space and restart of Crypto Pods for both Prod B and Prod A were underway. It was expected that service improvements would be seen immediately following these restarts.<br><br>At 09:56 the restart of Prod B had completed, and improvements could be seen, with response times down to 1-3sec average.<br><br>At 10:19 CGI confirmed that response was back to less than 1 second and the request rate had returned to expected levels. The incident was declared as Resolved. |
| Customer Impact |
| Service users would not have been able to complete scheduled and on-demand Service Requests for SMETS1 devices.<br><br>The resulting delay in migration activity resulted in a "No go" decision for DCC MCC in the Daily Go/No-Go call, effectively halting any new migrations. |

| Actions Completed to Recover Service | | |
|---|---|---|
| Item | Description | Owner |
| 1 | Restarted Crypto Pods on Prod B and Prod A<br>• 09:20 – Prod B restarts started<br>• 09:56 – Prod B restarts finished<br>• 09:57 – Prod A restarts started<br>• 10:12 – Prod A restarts finished | DCO |

| | |
|---|---|
| Incident Reference | INC000000627085 |
| Problem Reference | PBI000000121400 |
| Category | 1 |
| Service(s) Impacted | Total Outage in the Northern Region (outbound) |
| Service impacted date/time | 07/09/2020 15:25 |
| Service restored date/time | 07/09/2020 16:58 |
| Incident raised date/time | 07/09/2020 15:51 |
| Incident resolved date/time | 07/09/2020 18:02 |
| Actual Impact Duration | 1 hour 33 minutes |
| Incident Duration | 2 hours 10 minutes |
| Resolved within SLA | Yes |

| |
|---|
| Summary of Incident |
| CSP North experienced communication issues when attempting to connect to the DSP, in turn this impacted service requests for customers in the northern region, on the SMETS 2 platform. |
| Customer Impact |
| Total loss of service in the Northern Region. |

| Actions Completed to Recover Service | | |
|---|---|---|
| Item | Description | Owner |

| | | |
|---|---|---|
| 1 | Incident resolved at 16:58 by failing back to original F5, all gateways confirmed restored, with confirmation of inbound and outbound traffic returning to Business as usual levels. | CSP/N |

| | |
|---|---|
| Incident Reference | INC000000629108 |
| Problem Reference | PBI000000121900 |
| Category | Category 1 |
| Service(s) Impacted | All Motorway Traffic / SR's / Device generated alerts |
| Service impacted date/time | 11/09/2020 02:00 |
| Service restored date/time | 11/09/2020 03:42 |
| Incident raised date/time | 11/09/2020 02:23 |
| Incident resolved date/time | 11/09/2020 08:26 |
| Actual Impact Duration | 1 hour 42 minutes |
| Incident Duration | 6 hours 3 mins |
| Resolved within SLA | Yes |
| Summary of Incident | |
| DSP have advised that the inbound Motorway access is down due to an issue with the Volt Database experienced during the high impact maintenance window under change reference CRQ000000126234. This will impact all Service requests, install and commission, device generated alerting, CoS, and SMETS1 Estate and Migrations. This is also impacting all scheduled meter reads and reporting.<br><br>To mitigate change overrun in future, DSP have introduced Service Delivery to deployment of change, to minimise impact caused by 'Target Fixation' | |
| Customer Impact | |
| Total service outage. | |

| Actions Completed to Recover Service | | |
|---|---|---|
| Item | Description | Owner |
| 1 | DSP completed a restore of the affected Database. (Request Manager North – a subsection of Volt) | DSP |

| | |
|---|---|
| Incident Reference | INC000000629122 |
| Problem Reference | PBI000000121704 |
| Category | Category 2 |
| Service(s) Impacted | Comms Hub Manager |
| Service impacted date/time | 11/09/2020 02:00 |
| Service restored date/time | 11/09/2020 06:02 |
| Incident raised date/time | 11/09/2020 03:31 |
| Incident resolved date/time | 11/09/2020 08:37 |
| Actual Impact Duration | 4 hours 2 minutes |
| Incident Duration | 5 hours 5 minutes |
| Resolved within SLA | Yes |

| Summary of Incident | | |
|---|---|---|
| CSP North have advised that due to an issue experienced during change request CRQ000000126902, Comms Hub Manager was unavailable.<br><br>This would have impacted some service users install and commission process if not restored by start of business day.<br><br>Comms hub diagnostics were also unavailable.<br><br>This Incident was caused by INC000000629108 | | |
| Customer Impact | | |
| Users would not have been able to complete installs & commissions of new Comms hubs. | | |
| Actions Completed to Recover Service | | |
| Item | Description | Owner |
| 1 | I.P table refresh carried out on CMI Servers.<br>All tests have been completed; services are running as normal | CSP/N |

| | |
|---|---|
| Incident Reference | INC000000632638 |
| Problem Reference | PBI000000121907 |
| Category | Category 2 |
| Service(s) Impacted | SMETS1 Service Requests & migrations |
| Service impacted date/time | 21/09/2020 10:08 |
| Service restored date/time | 21/09/2020 12:31 |
| Incident raised date/time | 21/09/2020 10:15 |
| Incident resolved date/time | 21/09/2020 15:35 |
| Actual Impact Duration | 2 hours 23 minutes |
| Incident Duration | 5 hours 19 minutes |
| Resolved within SLA | Yes |

| Summary of Incident | | |
|---|---|---|
| Approximately 75% of all SMETS1 service requests were failing due to HTTP errors and subsequent timeouts.<br><br>SMETS 1 migrations were also being delayed due to Key rotation timeouts.<br><br>SMETS2 was unaffected by this issue. | | |
| Customer Impact | | |
| 75% of on demand SRVs were failing. Migrations were delayed | | |
| Actions Completed to Recover Service | | |
| Item | Description | Owner |
| 1 | Crypto restarts for Prod A and B | DCO |
| 2 | Forceful close (kill) on MySQL router node | DCO |
| 3 | Restart of affected MySQL Router node | DCO |

## September Excluded

### SMETS1 Migration Related

| | |
|---|---|
| Incident Reference | INC000000625515 |
| Problem Reference | PBI000000121210 |
| Category | 2 |
| Service(s) Impacted | SMETS1 Migrations |
| Service impacted date/time | 02/09/2020 08:18 |
| Service restored date/time | 02/09/2020 16:17 |
| Incident raised date/time | 02/09/2020 10:15 |
| Incident resolved date/time | 03/09/2020 09:38 |
| Actual Impact Duration | 7 hrs 59 mins |
| Incident Duration | 0 days 23 hrs 22 mins |
| Impacted Region | SMETS1 Migrations |
| Was the Incident prioritised correctly? | Categorised as a CAT3 initially but uplifted to a Category2. |
| Resolved within SLA | Yes |
| Summary of Incident | |
| SMETS1 migrations for 17091 total. 10197 Active IOC and 5000 Active MDS migrations were paused due to repackaging (Unable) issue during the migration process within the DCO environment.<br><br>This is not impacting the Core SMETS1 Device Estate. | |
| Customer Impact | |
| A number of SMETS 1 Migrations | |

| Actions Completed to Recover Service | | |
|---|---|---|
| Item | Description | Owner |
| 1 | MCF file removed from Migration process which allowed all other migrations to flow through to completion, all migrations have been completed with the exception of the 2 MCF files | DCO |
| 2 | **Workaround** – MDS to only send 500 migrations per file to ensure migrations process as normal | MDS |
| 3 | Devices impacted rolled back automatically as per process within 48 hours (Service User will need to raise new MA requests). | MDS |

### Duplicate Incidents

INC000000628941 – Category 2 – Within SLA – Duplicate of INC000000629108
INC000000628942 – Category 2 – Within SLA – Duplicate of INC000000629108
INC000000628943 – Category 2 – Within SLA – Duplicate of INC000000629108

### Duplicate of Category 3 Incidents

INC000000632269 – Category 2 – Within SLA – Duplicate of INC000000632334
INC000000632270 – Category 2 – Within SLA – Duplicate of INC000000632334

These incidents were incorrectly categorised as Category 2. 42 Automated DSP Alarm Incidents were generated within a very short period of time, with a variety of different Categories across each Incident. INC000000632334 was used as the primary Incident, with all others related to it. Once an impact assessment was conducted, the Incident was downgraded to a Category 3. Unfortunately, the two Incidents listed above were missed and remained at their original Category. DCC MIM have added additional monitoring and Quality Assurance checks to ensure this issue is not repeated.

# 3 Code Performance Measures

## 3.1 Service Levels Attained

This section reports the Service Levels achieved in September 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.** | | | **95.32%** | **95.10%** | **99.00%** | **96.00%** |
| | PM1.1 | Percentage of DSP Service Request Times within relevant TRT | DSP | 99.88% | 99.79% | 99.00% | 96.00% |
| | PM1.1 | Percentage S1SP Countersigned Service Request Times within relevant Target Response Time | S1SP SIE | 99.24% | 99.02% | 99.00% | 96.00% |
| | PM1.1 | Percentage S1SP Countersigned Service Request Times within relevant Target Response Time | S1SP Capgemini | 97.68% | 99.35% | 99.00% | 96.00% |
| | PM1.4 | Percentage of DCC Service Request Times within relevant TRT | DSP | 99.96% | 99.96% | 99.00% | 96.00% |
| | PM2 | Percentage of Category 1 Firmware Payloads completed within the relevant TRT | CSPN | 60.53% | 54.50% | 99.00% | 96.00% |
| | PM2 | Percentage of Category 1 Firmware Payloads completed within the relevant TRT | CSPC | 98.44% | 99.44% | 99.00% | 96.00% |
| | PM2 | Percentage of Category 1 Firmware Payloads completed within the relevant TRT | CSPS | 97.98% | 99.45% | 99.00% | 96.00% |
| | 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% |

| 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 | CSPC | 99.73% | 99.75% | 96.00% | 90.00% |
| | PM4.3 | Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds | CSPS | 99.73% | 99.73% | 96.00% | 90.00% |
| **CPM2** | **Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time.** | | | **99.89%** | **99.81%** | **99.90%** | **96.00%** |
| | PM1.2 | Percentage of DSP Service Response Times within relevant TRT | DSP | 100.00% | 99.95% | 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 | 99.99% | 99.79% | 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 | 99.33% | 98.44% | 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 | CSPC | 99.80% | 99.96% | 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 | CSPS | 99.80% | 99.92% | 99.00% | 96.00% |
| | PM4.1 | Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours | CSPN | 100.00% | 100.00% | 99.00% | 96.00% |
| | PM4.1 | Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours | CSPC | 100.00% | 100.00% | 99.00% | 96.00% |
| | PM4.1 | Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours | CSPS | 100.00% | 99.99% | 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 | 99.95% | 99.95% | 99.00% | 96.00% |
| | PM4.2 | Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours | CSPS | 99.94% | 99.95% | 99.00% | 96.00% |
| **CPM3** | **Percentage of Alerts delivered within the applicable Target Response Time.** | | | **98.87%** | **99.46%** | **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 | 99.97% | 99.90% | 99.00% | 96.00% |

| Code Performance Measure Number | Performance Measure | | | Previous Service Level | Service Level | Target Service Level | Minimum Service Level |
|---|---|---|---|---|---|---|---|
| | PM1.5 | Percentage of S1SP SMETS1 Alert Response Times within relevant Target Response Time | S1SP SIE | 99.93% | 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 | CSPN | 96.71% | 98.29% | 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 | Performance Measure Not Reported | 99.49% | 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 | Performance Measure Not Reported | 99.65% | 99.00% | 96.00% |
| **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.** | | | **100.00%** | **100.00%** | **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.** | | | **91.73%** | **91.30%** | **90.00%** | **80.00%** |
| **CPM6** | **Percentage Availability – Self Service Interface** | | | **99.63%** | **100.00%** | **99.50%** | **98.00%** |
| | PM2.4 | Percentage Service availability – Self Service Interface (Production Services) | DSP | 96.63% | 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%** |

| Code Performance Measure Number | Performance Measure | | | Previous Service Level | Service Level | Target Service Level | Minimum Service Level |
|---|---|---|---|---|---|---|---|
| | 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%** | **96.00%** |
| | 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% | 100.00% | 99.00% |

**Table 1 - DCC Code Performance Measures**

### 3.1.1 CPM1 – PM2 Volumes Data

| | CSPN | CSPC | CSPS |
|---|---|---|---|
| Total number of Communications Hubs with Firmware Payload delivered successfully in Measurement Period | 39,964 | 234,561 | 219,086 |
| Total Number of Connected Communications Hubs identified in Service Requests to have Firmware Payload delivered within Measurement Period | 73,324 | 235,887 | 220,299 |
| Reported Percentage Performance | **54.50%** | **99.44%** | **99.45%** |

**Table 2 - DCC Code Performance Measures**

### 3.1.2 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 95.10% and is below the Minimum Service Level.

CSPN PM2 reported Service Level was 54.50% and is below Minimum Service Level.

Arqiva continued to make firmware download performance a prime area of focus, with a clear path defined to increase stability and overall performance. The timeline to increase the performance by the end of October has been shared with the DCC and Industry.
The measures to boost performance will be implemented during the first two weeks of October 2020 and therefore performance for PM2 in October will continue to be impacted. November performance is expected to be at circa 92.00% with further enhancements to be implemented to improve performance to 99.00%.

### 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 | % Within SLA |
|---|---|---|---|---|
| Category 1 | 3 | 3 | 0 | 100.00% |
| Category 2 | 3 | 3 | 0 | 100.00% |
| **Total** | **6** | **6** | **0** | **100.00%** |

**Table 3 - CPM4 Incident Count**

For Information only: Prior to any Performance Measurement Exclusions Applied

| Category | Total Incident Count | Within SLA | Failed SLA | % Within SLA |
|---|---|---|---|---|
| Category 1 | 3 | 3 | 0 | 100.00% |
| Category 2 | 9 | 9 | 0 | 100.00% |
| **Total** | **12** | **12** | **0** | **100.00%** |

**Table 4 – 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 | % Within SLA |
|---|---|---|---|---|
| Category 3 | 84 | 77 | 7 | 91.67% |
| Category 4 | 70 | 64 | 6 | 91.43% |
| Category 5 | 1,202 | 1,097 | 105 | 91.26% |
| **Total** | **1,356** | **1,238** | **118** | **91.30%** |

**Table 5 - 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 | Total Incident Count | Within SLA | Failed SLA | % Within SLA |
|---|---|---|---|---|
| Category 1 | N/A | N/A | N/A | N/A |
| Category 2 | N/A | N/A | N/A | N/A |
| **Total** | **N/A** | **N/A** | **N/A** | **N/A** |

Table 6 - Incidents Relating to CPM4

| Category | Total Incident Count | Within SLA | Failed SLA | % Within SLA |
|---|---|---|---|---|
| Category 3 | 42 | 37 | 5 | 88.10% |
| Category 4 | 19 | 15 | 4 | 78.95% |
| Category 5 | 330 | 237 | 93 | 71.82% |
| **Total** | **391** | **289** | **102** | **73.91%** |

Table 7 - 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 July | | | | | 2 | 2 |
| 2018 August | | | | | 23 | 23 |
| 2018 September | | | | | 46 | 46 |
| 2018 October | | | | | 73 | 73 |
| 2018 November | | | | | 117 | 117 |
| 2018 December | | | | | 222 | 222 |
| 2019 January | | | | | 412 | 412 |
| 2019 February | | | | 1 | 258 | 259 |

| Category | Cat 1 | Cat 2 | Cat 3 | Cat 4 | Cat 5 | Total Incidents |
|---|---|---|---|---|---|---|
| 2019 March | | | | 1 | 352 | 353 |
| 2019 April | | | | | 381 | 381 |
| 2019 May | | | | | 294 | 294 |
| 2019 June | | | | 1 | 844 | 845 |
| 2019 July | | | | 4 | 909 | 913 |
| 2019 August | | | | | 957 | 957 |
| 2019 September | | | | | 1,365 | 1,365 |
| 2019 October | | | | 2 | 1,524 | 1,526 |
| 2019 November | | | 8 | 1 | 1,342 | 1,351 |
| 2019 December | | | | 1 | 1,990 | 1,991 |
| 2020 January | | | 2 | 1 | 1,188 | 1,191 |
| 2020 February | | | 2 | 1 | 1,677 | 1,680 |
| 2020 March | | | 2 | 9 | 1,680 | 1,691 |
| 2020 April | | | | 3 | 573 | 576 |
| 2020 May | | | 2 | 3 | 450 | 455 |
| 2020 June | | | 4 | 1 | 869 | 874 |
| 2020 July | | | 11 | 1 | 1,323 | 1,335 |
| 2020 August | | | 22 | 4 | 1,803 | 1,829 |
| 2020 September | | | 83 | 4 | 3,311 | 3,398 |
| **Total** | | | **136** | **38** | **23,985** | **24,159** |

**Table 8 - Aged Incidents Assigned to Service Users**

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

Incorrect Credentials Loaded on to Device – 9,807
Incorrect Communications Hub Variant Installed – 7,823
DUIS Service Request 8.14. not received – 1,372

Enhanced attention to “Aged” Incidents has continued to see a decrease in the total. Further to simply resolving these “Aged” Incidents, if a resolution is not possible, actions are being taken to reclassify the specific action required from Service Users to resolve. This additional data quality will provide us with greater insight of what the DCC can influence in these Incidents.

Specific attention has been placed on the Incidents raised prior to 2020. For the third successive month, we have seen a reduction of ~1500 Incidents. The remaining Incidents are predominately related to one of the top three issues.

Discussions have continued and expanded between Operations, Service Management, Service Providers and Service Users to tackle these top issues. Not just to get progression on the “Aged” Incidents, but to improve the manner in which they are currently created. A holistic review has already begun and identified areas for improvement. We are currently

at the point of deciding the best course of action and will require actions from Service Users to progress further.

After extensive analysis on the “Incorrect Communications Hub Variant Installed” Incidents that have been raised, we agreed that we will only raise ‘Incorrect Variant’ Incidents for Gateway hubs. Meaning there is a dependency on the device being a Mesh CH to ensure the connecting properties are able to connect to the network. When comparing these devices to the open Incidents, ~5000 of which are no longer required. Work will continue over the coming weeks to ensure that are closed appropriately.

Workshops have been hosted to understand how “Incorrect Credentials Loaded on to Device” are caused, which has resulted in new DCC reporting that captures all issues with credentials. Rather than just those reported by our Network Operators. Once this reporting is ready for distribution, it should remove the requirement to have Incidents tracking this issue.

Discussions are also ongoing to move the “DUIS Service Request 8.14. not received” Problem (supported by TOC Reporting) and proactive notification to Service Users. Once consistency of data can be attained, Incidents will no longer be used to track the issue.

**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 September | | | | | 1 | 1 |
| 2018 November | | | | | 3 | 3 |
| 2018 December | | | | | 7 | 7 |
| 2019 January | | | | | 14 | 14 |
| 2019 February | | | | | 2 | 2 |
| 2019 March | | | | | 17 | 17 |
| 2019 April | | | | | 26 | 26 |
| 2019 May | | | 1 | | 32 | 33 |
| 2019 June | | | | | 29 | 29 |
| 2019 July | | | | | 65 | 65 |
| 2019 August | | | | | 128 | 128 |
| 2019 September | | | | | 91 | 91 |
| 2019 October | | | | 1 | 199 | 200 |
| 2019 November | | | 1 | 2 | 101 | 104 |
| 2019 December | | | | | 88 | 88 |
| 2020 January | | | 2 | 2 | 114 | 118 |
| 2020 February | | | 5 | 1 | 141 | 147 |
| 2020 March | | | 5 | 1 | 102 | 108 |
| 2020 April | | | 3 | | 119 | 122 |

| Category | Cat 1 | Cat 2 | Cat 3 | Cat 4 | Cat 5 | Total Incidents |
|---|---|---|---|---|---|---|
| 2020 May | | | | 2 | 109 | 111 |
| 2020 June | | | 1 | 3 | 133 | 137 |
| 2020 July | | | 5 | 2 | 254 | 261 |
| 2020 August | | | 3 | 4 | 215 | 222 |
| 2020 September | | | 11 | 20 | 469 | 500 |
| **Total** | | | **37** | **38** | **2,460** | **2,535** |

**Table 9 - 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 daily to bring the number of aged incidents down. The majority of the actions in the previous section are also being applied to the Aged Incidents assigned to DCC and Service Providers.

## 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 | 860 |
| User Request | 121 |
| **Total** | **981** |
| **Exclusion Type** | |
| Alert / Event Monitoring (For Information only) | 3,662 |
| Cancelled | 5,303 |
| Duplicate | 72 |
| SMETS1 Migration Related | 30 |
| Internal to DCC – Non DCC Impacting | 14 |
| Testing/Prod Proving | 6 |
| **Total** | **9,087** |
| **Grand Total** | **10,068** |

**Table 10 - PMEL Exclusions Detail**

Further Information on the above exclusions:

**User Responsibility**:

These are predominately Incidents that were caused by CHIPSM non-compliance and required corrective action from Energy Suppliers, including but not limited to; Incorrect Credentials mentioned in Section 3.1.6

**Cancelled:**

Since their creation, both “Incorrect Credentials” raised by the Service Centre and “Incorrect Variant” Incidents have had their validity re-evaluated. These are deemed no longer required and have subsequently been cancelled. The majority of these exclusion would be categorised as one of these two Incident types.

**Alert / Event Monitoring (For Information only)**:

This type of exclusion covers all proactively raised Incidents.

**Duplicate**:

Previously additional Incidents were needed to be created that could manage interactions between multiple Service Users. The second Incident that was created by the DCC Service Centre will be classified as a “Duplicate.”

# 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% | 99.76% | 99.95% | 99.00% |
| | 2.2 | Service availability – DCC User Interface | Monthly | 99.99% | 100.00% | 99.95% | 99.00% |
| | 2.3 | Service availability – DCC Service Management | Monthly | 99.63% | 100.00% | 99.50% | 98.00% |
| | 2.4 | Service availability – Self Service Interface | Monthly | 99.63% | 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 Feb20 – Apr20 | Latest Qtr. Service Level May20 – Jul20 | Target Service Level | Minimum Service Level |
| **Service Management** | 7 | Notification of Planned Maintenance events[5] | Quarterly | 90.91% | 100.00% | 100.00% | 90.00% |

[4] DCC are reviewing the contractual definition of this DSP Performance Measure
[5] Measurement Period is a Calendar Quarter – current reported Quarter is May 2020 – July 2020. Previous Quarter is February 2020 – April 2020

### 4.1.1 Service Level Below Target Service Level

DSP PM2.1 reported Service Level was 99.76% and is below Target Service Level. This was due to an overrunning Planned Maintenance patching activity (under change CRQ000000126234) on 11 September 2020. An issue was experienced during the Planned Maintenance and a decision was taken to restore the database. The database was successfully restored but didn't complete until 102 minutes after the scheduled end of the Maintenance Window. A Category 1 incident (INC000000629108) was raised when it became apparent that service outage would overrun the Window.

Following service restoration, a Problem Investigation (PBI000000121900) was launched to understand why the database didn't start correctly, and to implement improvements to avoid a repeat of the service outage. DSP have identified that the decision to restore the database was taken too late to allow for recovery within the Maintenance Window. Processes have been updated to require a senior DSP Service Delivery Manager to be on-call during Maintenance Windows to ensure any restoration decisions are taken in a timely manner.

DSP has engaged the database vendor to investigate why the database didn't restart following the patching activity. Root cause has determined a file became corrupted during the restart. The vendor has identified a workaround to ensure the database will restart if the situation reoccurs. This has been added to the DSP change processes.

## 4.2 Performance Measurement Exceptions

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

# 5 Reported List of Service Provider Performance Measures CSP North

## 5.1 Service Levels Attained

*Performance Measures are reported monthly unless otherwise specified.

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

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

| 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 | 99.23% | 99.39% | 80.00% | 70.00% |
| | 1.2 | First time SMWAN connectivity within 30 days | Monthly | 99.77% | 99.82% | 90.00% | 80.00% |
| | 1.4 | SMWAN connectivity Level | Monthly | 99.98% | 99.98% | 99.90% | 99.00% |
| Availability | 6.2 | Percentage availability of DCC WAN Gateway Interface | Monthly | 99.61% | 99.82% | 99.98% | 98.25% |
| Service Management | 11 | Accuracy of Coverage Database provided to DCC Service Users | Monthly | 99.69% | 99.22% | 99.00% | 95.00% |
| Power Outage Events | 12.1 | Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer | Monthly | 99.07% | 99.35% | 99.00% | 96.00% |

| Performance Area | Performance Measure Number | Performance Measure Name | Measurement Period | Previous Service Level | Service Level | Target Service Level | Minimum Service Level |
|---|---|---|---|---|---|---|---|
| | 12.2 | Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs | Monthly | 392.76% | 387.85% | 99.00% | 96.00% |
| Communications Hub delivery | 1.1 | Percentage of Communications Hubs delivered on time | Monthly | No Events | 100.00% | 99.00% | 95.00% |
| | 1.2 | Percentage of Communications Hubs accepted by DCC Service Users | Monthly | No Events | 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 2020 Q2** | **Previous Qtr. Service Level 2020 Q3** | **Target Service Level** | **Minimum Service Level** |
| Communications Hub Connectivity | 1.3 | First time SMWAN connectivity within 90 days | Quarterly | 100.00% | 99.98% | 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 12 - CSPN Reportable Performance Measures**

[6] Measurement Period is a Calendar Quarter

PM12.2 - The calculation results for PM 12.2 comes as 387.85%. CSPN had a total of 6,929 CH power outages reported, in September, of which 6,864 were sent to DSP within SLA (99.06%)

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 * (6929/ ((6864 – 50) * 0.25) + 50) = 387.85%

### 5.1.1 Service Level Below Target Service Level

CSPN PM6.2 reported Service Level was 99.82% and is below Target Service Level

This was due to an F5 failure on 7th September, out of memory errors and resilience failed. Key Incident INC000000627085 in Executive Summary, the investigation remains open with vendor support (PBI000000121400 applies).

## 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.

[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

### 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) | 14,435 | Failure to follow maintenance as per CHIMSM | These figures are for the reporting period (not cumulative) |

**Table 13 - CSPN PM1.4 Exclusions**

14,435 x CH excluded for September 2020 due to several reasons^, covering: -

***^CSPN Performance Measures Exceptions Classification Definitions can be found in Section 15.2 Appendix B, Sub-section 15.2.1***

- Communications Hubs where no incident has been raised for outage – 8,749
- Incomplete Communication Hub Install – 5,441
- Communication Hub in Low Coverage database – 233
- Comms Hubs where the Operational Status in the CSPN system is not set to Active – 9
- Communication Hub installed on non-consumer premises e.g. Live Lab – 3

### 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% | 99.98% | 90.00% | 80.00% |
| | 1.3 | SMWAN connectivity Level | Monthly | 99.98% | 99.98% | 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 | 99.39% | 99.14% | 95.00% | 90.00% |
| Power Outage Events | 12.1 | Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer | Monthly | 100.00% | 99.95% | 98.00% | 96.00% |
| | 12.2 | Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs | Monthly | 396.52% | 396.00% | 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 2020 Q2** | **Latest Qtr. Service Level 2020 Q3** | **Target Service Level** | **Minimum Service Level** |
| Communications Hub Connectivity | 1.2 | First time SMWAN connectivity within 90 days | Quarterly | 100.00% | No Events | 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 14 - CSPC Reportable Performance Measures**

PM12.2 - The calculation results for PM 12.2 comes as 396.00% CSPC had a total of 14,838 CH power outages reported in September, 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 * (14838/ ((14838– 50) * 0.25) + 50)) = 396.00%

[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) | 12,736 | Failure to follow installations as per CHIMSM | SU has not submitted the appropriate Service Requests post Installation.<br>These figures are for the reporting period (not cumulative) |

**Table 15 - CSPC PM1.1 Exclusions**

12,736 CH excluded for September 2020 due to a number of reasons^, covering: -

***^CSPC Performance Measures Exceptions Classification Definitions can be found in Section 15.2 Appendix B, Sub-section 15.2.2***

- There were no, or incomplete address details provided by the Service User – 7,516*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 2,971
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,242
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 468
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 416
- Installed outside of region – 99
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 21
- CHIMSM Not Followed - 8.14.2 on Cellular – 3

*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) | 12,736 | Failure to follow installations as per CHIMSM | SU has not submitted the appropriate Service Requests post Installation.<br>These figures are for the reporting period (not cumulative) |

**Table 16 - CSPC PM11 Exclusions**

12,736 CH excluded for September 2020 due to a number of reasons^, covering: -

***^CSPC Performance Measures Exceptions Classification Definitions can be found in Section 15.2 Appendix B, Sub-section 15.2.2***

- There were no, or incomplete address details provided by the Service User – 7,516*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 2,971
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,242
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 468
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 416
- Installed outside of region – 99
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 21
- CHIMSM Not Followed - 8.14.2 on Cellular – 3

*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) | 124,650 | Failure to follow installations as per CHIMSM | SU has not submitted the appropriate Service Requests post Installation.<br>These figures are for the reporting period (not cumulative) |

**Table 17 - CSPC PM1.3 Exclusions**

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

124,650 x CH excluded for September 2020 due to a number of reasons^, covering: -

***^CSPC Performance Measures Exceptions Classification Definitions can be found in Section 15.2 Appendix B, Sub-section 15.2.2***

- There were no, or incomplete address details provided by the Service User – 83,595 *
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 24,926
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 6,259
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 3,578
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 3,481
- Installed outside of region – 2,173
- Aborted Installation – 638

*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 | 99.96% | 99.96% | 90.00% | 80.00% |
| | 1.3 | SMWAN connectivity Level | Monthly | 99.99% | 99.98% | 99.90% | 99.00% |
| Availability | 6.2 | Percentage availability of DCC WAN Gateway Interface | Monthly | 100.00% | 100.00% | 99.98% | 98.25% |
| Service Management | 11 | Accuracy of Coverage Database provided to DCC Service Users | Monthly | 98.81% | 98.58% | 95.00% | 90.00% |
| Power Outage Events | 12.1 | Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer | Monthly | 100.00% | 99.93% | 98.00% | 96.00% |
| | 12.2 | Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs | Monthly | 395.96% | 395.42% | 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% |
| 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 2020 Q2 | Latest Qtr. Service Level 2020 Q3 | 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 18 - CSPS Reportable Performance Measures**

PM12.2 - The calculation results for PM 12.2 comes as 395.42%. CSPS had a total of 12,957 CH power outages reported in September, 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:

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

Using the calculation above PM12.2 = 100 * (12957 / ((12957 – 50) * 0.25) + 50)) = 395.42%

[10] Measurement Period is a Calendar Quarter

## 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) | 12,346 | 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 PM1.1 Exclusions**

12,346 CH excluded for September 2020 due to a number of reasons^, covering: -

***^CSPS Performance Measures Exceptions Classification Definitions can be found in Section 15.2 Appendix B, Sub-section 15.2.2***

- There were no, or incomplete address details provided by the Service User – 5,727 *
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 4,291
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,021
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 678
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 486
- Installed outside of region – 103
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 25
- Aborted Installation – 10
- CHIMSM Not Followed – 8.14.2 on Cellular – 5

[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

*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.

### 7.2.1.2 PM11 Accuracy of Coverage Database

| Performance Area | Performance Measure Number | Number of Exception Events | Exception Scenario | Further Information |
|---|---|---|---|---|
| **Service Management** | PM11 (CSPS) | 12,346 | Failure to follow installations as per CHIMSM | SU's have not submitted the appropriate Service Requests post<br>Installation.<br>These figures are for the reporting period (not cumulative) |

**Table 20 - CSPS PM11 Exclusions**

12,346 CH excluded for September 2020 due to a number of reasons^, covering: -

***^CSPS Performance Measures Exceptions Classification Definitions can be found in Section 15.2 Appendix B, Sub-section 15.2.2***

- There were no, or incomplete address details provided by the Service User – 5,727 *
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 4,291
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,021
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 678
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 486
- Installed outside of region – 103
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 25
- Aborted Installation – 10
- CHIMSM Not Followed – 8.14.2 on Cellular – 5

*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) | 117,049 | Failure to follow installations as per CHIMSM | SU has not submitted the appropriate Service Requests post<br>Installation.<br>These figures are for the reporting period (not cumulative) |

*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.

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

117,049 x CH excluded for September 2020 due to a number of reasons^, covering: -

***^CSPS Performance Measures Exceptions Classification Definitions can be found in Section 15.2 Appendix B, Sub-section 15.2.2***

- There were no, or incomplete address details provided by the Service User – 74,294 *
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 28,362
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 7,017
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 2,985
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 2,198
- Installed outside of region – 1,122
- Aborted Installation – 1,071

*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 | 0 | 0 | 1 |
| | 3.2 | Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release | Monthly | 0 | 0 | 0 | 5 |
| Performance Area | Performance Measure Number | Performance Measure Name | Measurement Period | Previous Qtr. Service Level 2020 Q2 | Latest Qtr. Service Level 2020 Q3 | Target Service Level | Minimum Service Level |
| **Service Management** | 7 | Planned Maintenance events | Quarterly | 100.00% | 100.00% | 100.00% | 90.00% |

**Table 21 – S1SP SIE Reportable Performance Measures**

## 8.2 Performance Measurement Exceptions

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

# 9 Reported List of Service Provider Performance Measures S1SP Capgemini

## 9.1 Service Levels Attained

| Performance Area | Performance Measure Number | Performance Measure Name | Measurement Period | Previous Service Level | Service Level | Target Service Level | Minimum Service Level |
|---|---|---|---|---|---|---|---|
| **Availability** | 2.1 | Service Availability – S1SP Data Service (Production Services) | Monthly | 99.90% | 100.00% | 99.99% | 99.59% |
| | 2.2 | Percentage Service availability – CP Service (Production Environment) | Monthly | 100.00% | 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 |

**Table 22 – S1SP Capgemini Reportable Performance Measures**

## 9.2 Performance Measurement Exceptions

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

# 10 Reported List of Service Provider Performance Measures S1SP Vodafone

## 10.1 Service Levels Attained

| Performance Area | Performance Measure Number | Performance Measure Name | Measurement Period | Previous Service Level | Service Level | Target Service Level | Minimum Service Level |
|---|---|---|---|---|---|---|---|
| **Availability** | | Monthly availability of the Radio Network across VF-UK network | Monthly | 99.45% | 99.58% | 99.00% | 99.00% |
| | | Combined monthly IoT Core and Management Service Availability | Monthly | 99.92% | 99.85% | 99.70% | 99.70% |
| | | Monthly IoT Core availability (Voice/Data/SMS) | Monthly | 99.98% | 99.98% | 99.90% | 99.90% |
| | | Monthly Management Service Availability (API, Reporting, Provisioning, GUI, Portal) | Monthly | 99.95% | 99.95% | 99.70% | 99.70% |
| | | Monthly Availability of DCC dedicated fixed links | Monthly | No Events | No Events | 99.95% | 99.95% |

**Table 23 – S1SP Vodafone Reportable Performance Measures**

*Back-haul solution “dedicated fixed links” is not currently live therefore no data is available*

## 10.2 Performance Measurement Exceptions

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

# 11 Reported List of Service Provider Performance Measures S1SP Critical Software

## 11.1 Service Levels Attained

| Performance Area | Performance Measure Number | Performance Measure Name | Measurement Period | Previous Service Level | Service Level | Target Service Level | Minimum Service Level |
|---|---|---|---|---|---|---|---|
| **Application Management** | 3.1 | Category 1 or 2 Incidents directly related to a change release within 30 days of release | Monthly | No Events | No Events | 0 | 1 |
| | 3.2 | Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release | Monthly | No Events | No Events | 0 | 5 |

**Table 24 – S1SP Critical Software Reportable Performance Measures**

## 11.2 Performance Measurement Exceptions

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

# 12 Reported List of Service Provider Performance Measures S1SP Morrison Data Services (MDS)

## 12.1 Service Levels Attained

| Performance Area | Performance Measure Number | Performance Measure Name | Measurement Period | Previous Qtr. Service Level 2020 Q1 | Latest Qtr. Service Level 2020 Q2 | Target Service Level | Minimum Service Level |
|---|---|---|---|---|---|---|---|
| **Service Management** | 7 | Notification of Planned Maintenance events within required target | Quarterly | No Events | No Events | 100.00% | 90.00% |

**Table 25 – S1SP Morrison Data Services Reportable Performance Measures**

## 12.2 Performance Measurement Exceptions

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

# 13 Service Credits

The Service Credits accrued for this measurement period are as follows:

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

CSP (N) 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 54.50%. This failure resulted in the accrual of 175 Service Points which equate to Service Credits of £45,377. (This Performance Measure contributes to DCC Performance Measure 1.)

CSP (N) PM3.1 – Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time. The Target Service Level for this PM is 99.0% and the Actual Service Level achieved was 98.44%. This failure resulted in the accrual of 14 Service Points which equate to Service Credits of £3,630. (This Performance Measure contributes to DCC Performance Measure 2.)

CSP (N) 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 98.29%. This failure resulted in the accrual of 60 Service Points which equate to Service Credits of £16,076. (This Performance Measure contributes to Code Performance Measure 3.)

CSP (N) PM6.2 – Percentage availability of DCC WAN Gateway Interface. The Target Service Level for this PM is 99.98% and the Actual Service Level achieved was 99.82%. This failure resulted in the accrual of 21 Service Points which equate to Service Credits of £5,445. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP (N) PM6.3 – Percentage Access Node availability. The Target Service Level for this PM is 99.80% and the Actual Service Level achieved was 99.16%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP (N) PM7.1 – Percentage of Incident Responses provided to DCC Service Desk within requirement based on Severity Level. The Target Service level for this PM is 99% and the Actual Service Level achieved was 97.43%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP (N) PM7.2 – Percentage of Incident Notification provided to DCC Service Desk within requirement based on Severity Level. The Target Service level for this PM is 99% and the Actual Service Level achieved was 92.86%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP (N) PM7.4 – Percentage of Incident Resolution of Category 3, Category 4 and Category 5 incidents within requirement based on Category Level. The Target Service level for this PM is 90% and the Actual Service Level achieved was 62.50%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP (N) PM9 – Delivery of Change Requests Impact Assessments within required target. The Target Service level for this PM is 100% and the Actual Service Level achieved was 75.0%. 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 £70,528.

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

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

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

DSP PM2.1 - Percentage Service availability – DCC Data Service (Production Services). The Target Service level for this PM is 99.95% and the Actual Service Level achieved was 99.76%. This failure resulted in the accrual of 20 Service Points which equate to Service Credits of £3,014.75.

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

SIE PM10.2 - Percentage of RCA provided to DCC via DSMS for High, Medium and Low Problem records, within requirement. The Target Service Level for this PM is 90.00% and the Actual Service Level achieved was 0.00%. This is a KPI and therefore has not associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

SIE PM10.6 - Percentage Problem Resolution of Medium and Low problems based on Severity Level, within requirement. The Target Service Level for this PM is 90.00% and the Actual Service Level achieved was 66.66%. This is a KPI and therefore has not associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

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

**A summary of last 12 months Service Credits is provided in the table below:**
NB. This table has now been updated to reflect the amendments to Service Credits applied due to the Arqiva updates to PM2 Performance for March 2018 to June 2020.
Please see the accompanying 202009 Service Credits Tracker Report for full details of each impacted period.

**SMETS2 Service Providers**

| Month | Arqiva | BT | CGI | Telefonica | Total |
|---|---|---|---|---|---|
| Aug – 19 | £42,265 | £0 | £29,758 | £86,321 | **£158,344** |
| Sep – 19 | £115,387 | £0 | £17,005 | £6,188 | **£138,580** |
| Oct – 19 | £113,572 | £0 | £20,201 | £0 | **£133,773** |
| Nov – 19 | £113,572 | £0 | £0 | £44,523 | **£158,095** |
| Dec – 19 | £139,502 | £0 | £0 | £49,694 | **£189,196** |
| Jan – 20 | £113,572 | £0 | £0 | £69,954 | **£183,526** |
| Feb – 20 | £74,159 | £0 | £9,110 | £0 | **£83,269** |
| Mar – 20 | £60,157 | £0 | £0 | £13,112 | **£73,269** |
| Apr – 20 | £60,935 | £0 | £3,949 | £0 | **£64,884** |
| May – 20 | £60,935 | £0 | £0 | £0 | **£60,935** |
| June – 20 | £72,084 | £0 | £0 | TBC | **£72,084** |
| July – 20 | £51,859 | £0 | £0 | £0 | **£51,859** |
| Aug – 20 | £105,533 | £0 | £0 | £8,111 | **£113,644** |
| Sept -20 | £70,528 | £0 | £3,015 | £0 | **£73,543** |

**Table 26 – SMETS2 Service Providers Service Credits**

**SMETS1 Service Providers**

| Month | SIE | Capgemini | Vodafone | Critical | Total |
|---|---|---|---|---|---|
| Mar - 20 | £254 | £0 | £0 | £0 | **£254** |
| Apr – 20 | £11.29 | £0 | £0 | £0 | **£11** |
| May – 20 | £316.16 | £9,896 | £0 | £0 | **£10,212** |
| June – 20 | £4,539 | TBC | £0 | £0 | **£4,539** |
| July – 20 | £6,704 | £0 | £0 | £0 | **£6,704** |
| Aug – 20 | £0 | £0 | £0 | £0 | **£0** |
| Sept -20 | £0 | £0 | £0 | £0 | **£0** |

**Table 27 – SMETS1 Service Providers Service Credits**

# 14 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 £73,543.

# 15 Appendices

## 15.1 Appendix A – Open Problem & Incidents relating to Prior Periods

| Performance Measurement Report | Volume of Related Problems on Current Report | Volume Closed in Current Performance Reporting Period | Volume Remaining Open at End of Reporting Period |
|---|---|---|---|
| 2019 August | 1 | 0 | **1** |
| 2019 September | 1 | 0 | **1** |
| 2019 October | 1 | 0 | **1** |
| 2020 February | 1 | 0 | **1** |
| 2020 April | 1 | 0 | **1** |
| 2020 June | 6 | 2 | **4** |
| 2020 July | 1 | 1 | **0** |
| 2020 August | 4 | 0 | **4** |
| 2020 September | 7 | 2 | **5** |

**Table 28 – Problem Record Summary**

**(Correct as of 26/10/2020)**

### 15.1.1 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.

Due to the DCC change freeze and a data centre lockdown due to the Covid-19 restrictions, the sniffer/fluke analyser test will have to be rescheduled. DCC are working with DSP to now reschedule change work post lockdown. A switch upgrade Change will be completed1 st September following this, DSP will plan the implementation of the sniffer on the switch, to capture baseline performance prior to firewall failover. Change Planning is ongoing.

The Problem is still pending firewall failover and sniffer implementation and once again has been impacted by Covid-19 restrictions.

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

### 15.1.2 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:

Phase 1 is complete and all Smart Meter Key Infrastructure (SMKI) ADN hosts are successfully upgraded.
Phase 2 progress continues. SIT-A and SIT-B memory upgrade increases from 4Gb to 8Gb continue to be progressed via Changes; once complete, the ADN host upgrades can

commence. Performance testing of the ADN hosts is complete. In Production, Smart Metering Key Infrastructure (SMKI), DCC Key Infrastructure (DCCKI), Management System and Security Services ADN host Changes have successfully completed. Phase 3 ADN upgrades are being scheduled independently of Phase 2 and are ongoing.

Vulnerability upgrades completed 10/07/2020, Key ceremony completed 18/07/2020. DSP have obtained revised change info/target timeframe for completion of their Project work to upgrade load balancers. There is a significant amount of Change activity to complete before closing this Problem, but the work is ongoing.

**Latest: Target Completion Date for this Problem is 30/11/2020**

### 15.1.3 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.

Production deployment of the required HSM firmware progressing in parallel with application delivery networking (ADN) host upgrades, the estimated completion date for this work is November 2020.

**Latest: Target Completion Date 30/11/2020**

### 15.1.4 PBI000000118930

February Report 2020 - Key Incident **INC000000549963 & INC000000550023**

Multiple Service Users unable to communicate with DSP

Problem: Multiple Service Users reported an inability to commission installs, perform diagnostics and submit Service Requests. The issue was traced to a physical fibre cable issue (a fibre break) in network carrier equipment. Once replaced, service was restored.

The Root Cause is known, a physical fibre cable issue (a fibre break) in the network carrier equipment created this Problem.

The affected fibre cable was replaced. Co-ordinated failover of circuits is needed but progress has been delayed by COVID-19. Work is ongoing to arrange the resiliency/failover work.

A possible LAN issue has put a hold on completing a failover, work is ongoing to clarify and complete the remaining tasks on the Problem.

**Latest: Target Completion Date 30/10/2020**

### 15.1.5 PBI000000119705

April Report 2020 - Key Incident **INC000000580851**

DCC SMS and SSMI - Degradation of services

Problem: DCC Service Management System (SMS) and Self-Service Management Interface (SSI) services were degraded. Service Users and DCC colleagues were reporting issues with accessing the system, pages loading slower than usual or not displaying.

The Root Cause is a configuration issue. The incident was caused via TOC Python script taking up too much resource. The actions performed by the script was found not to be suited in terms of capability with the application interface design (such as extracting SAT data).

A CR (Change Request) has been created to formalise DCC use of the monitoring interface and enable utilisation of a new set of load balancers to handle the SAT volume required and to remove impact from other services (e.g. the Motorway). CR reference is CR1333 and the scope of the improvements are being developed. DSP have also supported the DCC with script improvements to limit the amount of data pulled.

**Latest: Target Completion Date 31/01/2021**

### 15.1.6 PBI000000120300

June Report 2020 - Key Incident **INC000000594100**

SMETS1 Increase in failed Service Requests & Migration delays 27/05

Problem: At 16:32 on 27/05 DCC received reports of failed SMETS SRVs since 15:00. Analysis completed by TOC (technical operations centre) and ELS (early life support) confirmed that the vast majority of SMETS1 SRVS (service requests) of all types were failing for all SUs (service users). Service was restored following restarts of the DBs (databases) at both DCO (Dual Control Organisation) and a restart of the S1SP application servers connecting into the DCO.

The Root Cause was a Capacity which was created by a configured database job not working. The Primary Database became overloaded and this was caused by a database clean up job not completing properly. The clean-up job continued to fail and roll back each time, this caused an increase in workload and the data & error log files to fill. This eventually caused the database to overload and remove itself from the cluster. The Database attempted to failover to a secondary node, but it was in a read only state. The Database cluster behaviour is to synchronise the currently live database and the other non-live databases in the cluster. During a failover event, expected behaviour is that the Secondary Database will become live and enter read-write mode once synchronisation is complete. During this specific event, the Secondary node was in a permanent state of 'catch up' with the previously live database due to the failing clean up job and subsequent rollbacks and as a result, was unable to complete the synchronisation process.

Permanent Enhanced monitoring has been completed by S1SP; this is specifically around throughput as this is where the issue was seen to emanate from. Enhanced monitoring / health checks of Primary DB and secondary DB is underway by the DCO Operator. Enhanced monitoring from S1CSP to identify delays is also underway. A fix is being devised to ensure the database clean-up job is completing its work and this will avoid a repeat build up. Database cleardown and optimization change was completed successfully. Database cleardown activities will remain in place until the standard BAU cleardown job has been developed and enabled. Monitoring for the new cleardown job has been developed and implemented.

**Latest: Problem Closed.**

### 15.1.7 PBI000000120414

June Report 2020 - Key Incident **INC000000599486**

SMETS1 Critical Degradation of core infrastructure 17/06

Problem: There was a Critical Degradation of core infrastructure 17/06. For the duration of this incident the SMETS1 core estate was in effect down for service users, no service requests could be delivered, and device heartbeats were not available.

The Root Cause is under review. There was the belief that the issue could be related to a memory leak but that has now been ruled out and it was not a factor. The Docker vendor have recommended to update the version of the Docker software in use. Work has begun in the Development environment to upgrade and will be rolled out to other environments via the agreed "path to live" process. This would be a mitigation action as Root Cause analysis continues.

The Docker update will be completed by the end of October. DCO advise the full Root Cause will be difficult to obtain and the update will provide strong mitigation.

**Latest: Target Root Cause Date Expired 02/07/2019**

### 15.1.8 PBI000000120211

June Report 2020 - Key Incident **INC000000596467 & INC000000598205** (Excluded from PMEL)

SMETS1 Core Infrastructure Degraded

Problem: Service Requests were failing on the SMETS1 core estate (above 90% on 06/06 and repeat issues seen 13/06), returning E21 errors. Service restored following the restart of DCO's (Dual Control Organisation) Application servers.

The Root Cause is an Application Issue. There is a memory leak in the software API (Application Programming Interface) that the HSMs (Hardware Security Modules) use that is causing the DCO (Dual Control Organisation) Crypto Application components to run out of memory.

There is a mitigation in place to restart the Crypto containers every few days to prevent the memory leak impacting service.

A release/hotfix for the memory issue has been delivered. The final mitigation activity is an upgrade to an application.

**Latest: Target Completion Date 27/11/2020**

### 15.1.9 PBI000000120320

June Report 2020 - Key Incident **INC000000598753** (Excluded from PMEL)

SMETS1 Migrations Paused

Problem: SMETS1 Migrations Are Paused Due to SFTP Connectivity Errors

The Root Cause was a Design Issue. Following a major incident on 13/06/2020 whereby restoration was achieved by routing all traffic to the providers secondary site it was established during investigation of the observed migrations failures on 15/06/2020 that the file transfer link was not configured to route via the secondary site as it had not been deployed into live service for secure file transfer services.

Residual activities post incident review will be progressed to ensure the services resiliency is instigated. In order to restore service, re-enablement of the file transfer link at the primary site was restored and migrations were re-commenced successfully.

Design review tasks have been completed and they are focussed on interaction between the Primary and Secondary sites which have been tested and confirmed working as expected via a fail over test.

**Latest: Problem Closed**

### 15.1.10 PBI000000120410

June Report 2020 - Key Incident **INC000000597373**(Excluded from PMEL)

SMETS1 SFTP issue Middle Operating Capability (MOC)

Problem: SMETS1 Migrations Are Paused Due To secure file transfer protocol (SFTP) Connectivity Errors.

Root cause was found to be twofold:

1. A software bug in the vendor firewall which triggered traffic to fill over to an available secondary link.
2. The availability of a secondary link for traffic which had been removed from the original design however not prevented from advertising availability.

Measures have been taken to avoid the service from failing over to the secondary redundant link. For the identified software bug the vendor is developing a fix.

**Latest: Target Completion Date 31/12/2020**

### 15.1.11 PBI000000120403

June Report 2020 - Key Incident **INC000000595042** (Excluded from PMEL)

SMETS1 Migrations Paused Due to a Network issue between S1SP and the Core Network

Problem: On the 01/06 investigation revealed that a network link from S1SP to the core infrastructure was being over utilised. This was due to an alert storm that occurs every 1st of the month caused by asynchronous billing reads. This has not previously affected migrations as the estate was smaller. Additional traffic for the DCO from S1SP, due to 197,000 key rotations also contributed to the alert storm. All though commissioning service request were being received following retries. The decision to halt SMETS1 migrations until the alert storm passed was taken, as the risk to devices being migrated was high. Once the alert storm passed migrations progressed as usual.

The Root Cause was a capacity issue. Asynchronous billing reads that happen on the 1st of every month have grown due to the SMETS1 estate having grown. The storm now utilises S1SPs network link (average 200% utilisation) into the core infrastructure causing migrations and other service requests to fail.

A fix to devices pre migration has been completed. A Change to block the alerts at the DSP push gateway has been completed. The devices will still be alerting to the DSP until a Contract Change is completed, but the alert volume will not grow.

**Latest: Target Completion Date 31/12/2020**

### 15.1.12 PBI000000120343

July Report 2020 - Key Incident **INC000000610783**

Monitoring Alert received from S1SP indicating failure of SMETS1 service requests

Problem: Proactive monitoring alert from S1SP indicating potential failure of SMETS 1 service requests as 50% of heartbeat requests to SMETS1 devices were failing.

The Root Cause was a Memory utilisation threshold management processes issue. The Network database (NDB) database is currently running without resilience in the providers Production ‘B’ data centre. On the evening of Thursday 23rd July one of the two NDB database nodes experienced a high memory usage event. This triggered the Out of Memory (OOM) service to take action, resulting in a full database shutdown and associated Dual Control Organisation outage. OOM’s purpose is to free up memory when the server is under high memory pressure. OOM sent a kill command to the NDB

database process to release memory for the Operating System, which resulted in all NDB instances shutting down. The fact that all NDB database nodes shutdown at once is an expected and correct behaviour, to maintain the integrity of the database. The OOM process was disabled permanently whilst the NDB service was restored.

Out of Memory (OOM) service was disabled permanently as part of the incident. Mitigation tasks were also completed, and they included enhancements to monitoring to pick up any future issues before there is a service impact.

**Latest: Problem Closed.**

### 15.1.13 PBI000000120245

August Report 2020 - Key Incident **INC000000607981**

Degradation in SMETS1 Service Requests identified by S1SP.

Problem: Monitoring by S1SP identified an increase in failures for SMETS1 Service requests at 12:30 on 15/07/2020. A further significant increase in failures of SMETS1 Service requests of all types was see at 14:50 on 15/07.2020 with the number of failures fluctuating between 30% to 60%.

The Root Cause is memory utilisation following a planned change:
Following the implementation of the network database (NDB) rollout change the time taken to process each service request (SRV) increased significantly leading to latency and an increase in time outs and errors. Investigations found high execution times for the structured query language (SQL) queries from the Request Manager into the smart metering key infrastructure (SMKI) tables within the database (DB). Each request generated by every SRV was completing a full scan of the tables within the DB which is resource expensive.

Investigations found high execution times for the structured query language (SQL) queries from the Request Manager into the smart metering key infrastructure (SMKI) tables within the database (DB). Each request generated by every SRV was completing a full scan of the tables within the DB which is resource expensive and led to the increased latency and errors since deployment of the network database (NDB). the S1SP and their vendor are working towards making changes to the application so that a different field is looked up on queries. The new field will be indexed which will eliminate the need for a full table scan and significantly improve performance times.

**Latest: Target Completion Date 01/12/2020**

### 15.1.14 PBI000000120433

August Report 2020 - Key Incident **INC000000611822**

SMETS1 - Migrations Paused

Problem: On 27/07 S1SP raised an incident for issues with migrations not passing out of device testing. There was an error: “The key was not found in the migration database” DCO investigations identified that required migration files were not being populated into a key database table. This was due to another database job long running and causing the required table population process to time out. Following a configuration change to extend

the time allowed for an associated table deletion job on the database the key database table started to populate, and migrations could be seen to be completing as expected.

SMETS1 migrations for 731 dormant and 5 active migrations were paused at the 'device testing' phase due to a Master Key not available error being received when trying to process migrations. The migrations were completed the next day.

The Root Cause was a data issue that caused configuration issues. The database housekeeping and migration data population job within the DCO migration component had failed because it was attempting to delete a large amount of data, failing then rolling back the database. The script was attempting to delete expired installations over 60 days old. This deletion transaction has a limit of 5 minutes and 143 MB of data to be deleted, and the delete transaction was exceeding the 5 minutes timeout. As a result, the portion of the job that populated the new installs migration data was not run. The "expired-installation-clean-up" value was set from 60 to 90 days and the job rerun. This prevented the data being deleted by the job and allowed the job to complete and populate the required tables for new installs.

DCO and DCOSW implemented database indexing on key fields to reduce the time the application takes to scan the relevant database fields and DCOSW have implemented further optimized clean-up scripts in Core 1.2 release to prevent future re-occurrences of this issue. A change to values is to be completed as the final mitigation.

**Latest: Target Completion Date 20/11/2020**

### 15.1.15 PBI000000120347

August Report 2020 - Key Incident **INC000000614119**

Security issue

Problem: This Problem Record is with DCC and is related to a Security issue.

The underlying Root Cause for this issue was confirmed during the course of Incident investigations.

Remediation actions being undertaken.

**Latest: Target Closure Date 30/11/2020**

### 15.1.16 PBI000000121007

August Report 2020 - Key Incident **INC000000621486**

Gateway server certificate expiration

Problem: CSP North Investigations identified failures on the Firewall servers handling inbound traffic from the DSP preventing message communication. Communication between the Firewall and the gateway servers was failing due to the certificates on the gateway servers expiring resulting in server authentication failure. The certificate requirement was bypassed in order to restore service. This was seen to be of minimal security risk and ratified by DCC and CSP North Security.

The Root Cause was a Process issue. The related incident was a consequence of a knowledge/training/capability issue which is fundamentally aligned with ineffective knowledge transfer between organisations. This failing was combined with a lack of due diligence during the resolution of internal work orders requesting certificate renewal. The failure to ensure necessary renewal was compounded further by the failure of key internal stakeholders to react to weekly proactive notification messaging advising certification expiry.

As part of the incident process, new gateway certificates were created and deployed with expiry date of 23rd August 2022. Work is ongoing to mitigate against further issues.

**Latest: Target Closure Date 30/10/2020**

## 15.1.17 PBI000000121203

September Report 2020 - Key Incident **INC000000623269**

SMETS1 - Failure of Service requests

Problem: This Problem Record is with DCO. There was a 100% service request failure of SMETS1 SRVs from 28/08/2020 15:40 until 28/08/2020 16:25. This issue was caused by a full outage to the DCO (Dual Control Organisation) database caused by both the primary and secondary NDB (Network Databases) becoming unavailable. Service was restored by DCO by restarting one of the primary NDB database servers (the NDB servers work in a shared pair) which was in a hung state. Following that action, it was confirmed that DCO was processing service requests. Resilience was restored by DCO at 16:30 by restarting one of the secondary NDB database servers (the NDB servers work in a shared pair) which was in a hung state.

The Root Cause was primarily Configuration related Issues and from review design improvements could be made. There were two root cause factors in this incident, the Memory ballooning event of and the network reset "oops" event. 1 -The Ballooning event can occur as per design but resulted in out of memory / Operating system hang. The Virtual Memory ballooning event requested memory from database, no swap space was available for paging out and Out Of Memory manager attempted to free RAM (Random Access Memory but was unable to satisfy the request. Around this time the live mitigation of the running virtual machines from one server to another as per design occurred, and the server was then found in a hung state post the motion. 2 - Network Reset at the time of the Network Database event, a kernel ‘oops’ message was experienced which ultimately restarted the networking stack on. Two databases where on the same data group (group 0), resulting in 50% of the Network Database cluster being unavailable and therefore a Network Database automated shutdown to protect data integrity occurred.

The Solutions implemented:
1- For the memory ballooning additional RAM (Random Access Memory) to avoid performance impact and swapping whilst ballooning, noting “If the virtual machine has plenty of free guest physical memory, inflating the balloon will induce no paging and will not impact guest performance”. The action will be to enable swap (2GB) and extend swap space (replace 2GB with 20GB) to support ballooning activity.
2- To avoid the Network Database shutdown Migration from the current driver to a para-virtualised network driver was completed.

**Latest: Problem Closed.**

### 15.1.18 PBI000000121300

September Report 2020 - Key Incident **INC000000624768**

High Service Request Variant Failure Rate in SMETS1 Environment

Problem: This Problem Record is with DCO (Dual Control Organisation). Service Requests were failing on the SMETS1 core estate (50% to 60% on 01/09/20. Service restored following the restart of DCO's (Dual Control Organisation) Application servers.

The Root Cause is an Application Issue. There is a memory leak in the software API (Application Programming Interface) that the HSMs (Hardware Security Modules) use that is causing the DCO (Dual Control Organisation) Crypto Application components to run out of memory.

A release/hotfix for the memory issue has been deployed as part of the September release.

**Latest: Problem Closed.**

### 15.1.19 PBI000000121210

September Report 2020 - Key Incident **INC000000625515**

SMETS1 - Migrations paused due to DCO Re-Packaging issues

Problem: This Problem Record is with DCO (Dual Control Organisation) Software Provider. On 02/09 SMETS1 migrations off 17091 total were paused due to repackaging (Unable) issue during the migration process within the DCO environment. This did not impact the Core SMETS1 Device Estate. The issue was resolved when MCF (Multimedia Container Format) files were removed from the Migration process which allowed all other migrations to flow through to completion. All migrations have been completed with the exception of 2 MCF files. The devices impacted rolled back automatically as per process within 48 hours.

The workaround until an enduring fix is delivered is that the Data Provider will only send 500 migrations per file to ensure migrations process as normal.

The Root Cause is a Configuration Issue. Investigations have found the Data Provider of the MCF (Multimedia Container Format) files are packaged with 2000 migrations. This volume causes a blockage within the DCO (Dual Control Organisation) software migration flow due to every element in the migration file defining a new namespace. This issue resulted in a constant retry and ultimately stops any further migrations from processing.

The DCO software Provider have identified that a long term will be needed via a common code fix. The current plan is to deliver this in the October maintenance release window

**Latest: Target Completion Date for this Problem is 30/10/2020**

## 15.1.20 PBI000000121400

September Report 2020 - Key Incident **INC000000627085**

Failure of primary Firewall device

Problem: This Problem record is with CSP North. Failure of primary Data Centre device and subsequent unsuccessful failover caused outbound communication loss across all Production CSP North gateways - these include Wide Area Network (WAN) gateway, CSP North Management gateway and Service Management gateway.

Root Cause has been confirmed as configuration issue. Application Visibility Reporting parameter was larger than required causing stability issues.

This Problem Record is related to PBI000000113813 which was closed with the Mitigation of periodic reboot of network management devices put in place along with the permanent solution coming at the end of Q4 2020 in form of Firewall Technical Refresh that will exchange the devices on the Firewall to ones that do not have the bug causing memory leak that attributed to the issue that occurred (This is being managed as a Risk that has been raised in DCC Central Risk Register).

Mitigation in form of periodic reboot of network management devices has changed its frequency to be executed monthly with next one scheduled for 28th October 2020 for Production environment. Additional mitigation in form of internal CSP North change to amend the Application Visibility Reporting parameter based on Vendor recommendation has been raised.

**Latest: Target Completion Date for this Problem is 30/11/2020**

## 15.1.21 PBI000000121900

September Report 2020 - Key Incident **INC000000629108 (Exclusions 628941, 628942 & 628943)**

Inbound motorway availability issue

Problem: This Problem Record is with DSP. During planned Change work, the inbound motorway access was down due to an issue with a database; the database crashed during motorway restart.

A database restore along with a restart of the northbound motorway restored service, taking DSP outside of the allotted Change window.

Root Cause was confirmed as a database crash during the motorway restart, which resulted in the requirement to rebuild the database during the Change window. Two factors led to the restoration activity not being completed within the Change window:

1. The decision to undertake database restores should have been made earlier.

2. Limited timeframes to undertake patching activity outside of high-risk maintenance windows.

Preventative actions being reviewed to ensure no reoccurrence.

To mitigate against a reoccurrence of this issue:

Short Term: A DSP Service Delivery Manager is to be available during Changes to support/ensure that target fixation is achieved.

Long Term: A process is to be developed to ensure that support outside of DSP Service Delivery Manager is available during Changes being implemented Out of Hours for High Risk Change Windows.

**Latest: Target Completion Date for this Problem is 30/10/2020**

### 15.1.22 PBI000000121704

September Report 2020 - Key Incident **INC000000629122**

Unavailability of Communication Hub Manager (CHM)

Problem: This Problem Record is with CSP North. Communication Hub Manager (CHM) unavailability was determined during post change checks for a related change. The change couldn't be successfully tested as there were issues noted with CHM routing connectivity. Service was restored by refreshing the IP routing tables by CSP North.

The Root Cause was Unidentified. Due to the network connectivity problem between CHM nodes and CMI, a connection could not be established between clustered environments (nodes). This was due to a port being blocked. The reasoning for the routing connectivity issue is undetermined at this time, and key logs for investigation are no longer available due to an existing log rotation policy (1.5 days).

CSP North are increasing the log retention to enable RCA analysis in case of future occurrence. Additional Monitoring is also being explored.

**Latest: Target Completion Date for this Problem is 30/11/2020**

### 15.1.23 PBI000000121907

September Report 2020 - Key Incident **INC000000632638**

SMETS1 - 75% of on demand SRVs were failing 21/09

Problem: This Problem Record is with DCO Operator (Duel Control Organisation). Approximately 75% of all SMETS1 service requests were failing due to HTTP errors and subsequent timeouts. SMETS 1 migrations were also being delayed due to Key rotation timeouts. Service was restored following a forceful close (kill) of a router node and then the subsequent restart of it.

The Root Cause was a data issue caused by capacity load. A DCO (Dual Control Organisation) database application node became unresponsive, and as a result, the DCO application was unable to communicate as expected with the database. The database vendor has advised the issue was caused by an overall connectivity issue, or cluster undergoing a severe load which compromises communication capabilities. because of this, the application node was not capable to reach the cluster and logs.

Mitigation has been completed and a restart of the Application Node will occur if the issue reoccurs. Database servers RAM (Random Access Memory), update virtual network cards and improve swapfile configuration has been completed.

A number of recommendations were provided by the database vendor to mitigate this issue going forward and will be completed before closure of the Problem.

**Latest: Target Completion Date for this Problem is 27/11/2020**

## 15.2 Appendix B – Performance Measure Exception Definitions

### 15.2.1 CSPN

**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.

**Incomplete Communication Hub Install**
Installations that have been aborted by the service user, but no service requests submitted. If the installation results in an install and leave, then the SU should be submitting and 8.14.2 service request. If the install is fully aborted, then an 8.14.3 service request should be submitted. This is being investigated as part of problem ticket.

**Data 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.

**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.

**Communication Hub in Low Coverage database**
Comms Hub is installed in a low coverage area.

**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

**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.

### 15.2.2 CSPC & CSPS

**No Address/Postcode in JSR**
Missing address/postcode in received CHSU, so unable to determine CHIMSM compliance

**CHIMSM Not Followed - No aerial is attached for installed SKU2 Device**
Aerial not installed for a Cellular & Mesh Comms Hub as per BE. CHIMSM not followed

**CHIMSM Not Followed - SKU1 Device installed when SKU2 Device is recommended**
Service User Installed Cellular instead of Cellular & Mesh (CSPC/CSPS Coverage Recommendation – Cellular & Mesh). CHIMSM not followed

**CHIMSM Not Followed - Comms Hub Never connected but received 8.14.1**
CSPC/CSPS have never received Birth event to support 8.14.1. These should be 8.14.2 with Cellular & Mesh Installed.

**Aborted Installation**
Service User confirmed as Aborted as part of one of the incidents raised for these Comms Hubs

**CHIMSM Not Followed - Outside CSPC/CSPS Committed Coverage Area**
Comms Hub installed outside CSPC/CSPS Committed Coverage Area. CHIMSM not followed.
CSP Automation also returns CHIMSM Not Followed – Postcode not available in CCDB

**CHIMSM Not Followed - Associated with NEP**
As per CSPC/CSPS, coverage is not available yet and the given postcode in CHSU is associated with Network Enhancement Plan (NEP). CHIMSM not followed

**CHIMSM Not Followed - 8.14.2 on Cellular**
Service User submitted 8.14.2 for Cellular Hub. Service User should have attempted with Cellular & Mesh if no connectivity. CHIMSM not followed

**CHIMSM Not Followed - Install and Leave Incident raised for Cellular Hub**
Service User raised Install and Leave Incident (Category 6) for a Cellular Hub and received 8.14.1 instead of 8.14.2. Service User should have attempted with Cellular & Mesh if no connectivity at the time of installation. CHIMSM not followed

**CHIMSM Not Followed - Given UPRN is not available**
UPRN received in CHSU is not available in CSPC/CSPS Coverage Database, so unable to determine CHIMSM compliance

**Partial Address Match**
Partial address received in CHSU, unable to determine CHIMSM compliance based on given partial address.
CSP Automation also returns CHIMSM Not Followed - Postcode available in CCDB but given address is not in CCDB

**Installed Out of Region**
Service User installed CSPC/CSPS Comms Hubs in CSPN Region. CHIMSM not followed

**Test Lab Installations**
Comms Hubs installed in Test Labs

**CHIMSM Non-Compliant - No Comms Hub Install on Cellular**
Service User submitted 8.14.2 for Cellular Hub. Service User should have attempted with Cellular & Mesh if no connectivity. CHIMSM not followed

## 15.3 Appendix C - Incident Reports Glossary

| Report Title | Description |
|---|---|
| Incident Reference | Incident ID from DSMS |
| Problem Reference | Problem ID from DSMS |
| Category | Incident Category |
| Service(s) Impacted | E.g. Installs, Service Requests, DSMS |
| Service impacted date/time | Time the outage started confirmed by logs, alerts (Confirmed via Supplier(s)) |
| Service restored date/time | Time the outage was confirmed as resolved |
| Incident raised date/time | Taken from “Reported Date+” field in DSMS |
| Incident resolved date/time | Time incident was marked as resolved in DSMS |
| DCC MIM Engagement date/time | Time the issue was escalated to the DCC MIM team for management as a high category incident |
| Actual Impact Duration | Duration of impact to service |
| Incident Duration | From logged to resolved in the DSMS ticket |
| Impacted Region | CSP Region: North, Central and South or all |
| Was the Incident prioritised correctly? | Outcome of the Post Incident Review, with a brief explanation why. |
| Resolved within SLA | Reference to the performance measure |
| Relevant Logs Captured | Evidence of the impact to service to determine root cause |
| Date Completed | Post Incident Review Completion Date |
| Summary of Incident | High level summary of the incident, the investigations and resolution activities |
| Customer Impact | The consequences of the service outage.<br>Example: Users were unable to complete birthing events, affecting installs & commissions. |
| Actions Completed to Recover Service | Details of restorative work<br>Example: DSP removed the failed application server from the pool which allowed traffic to flow through the alternate servers |