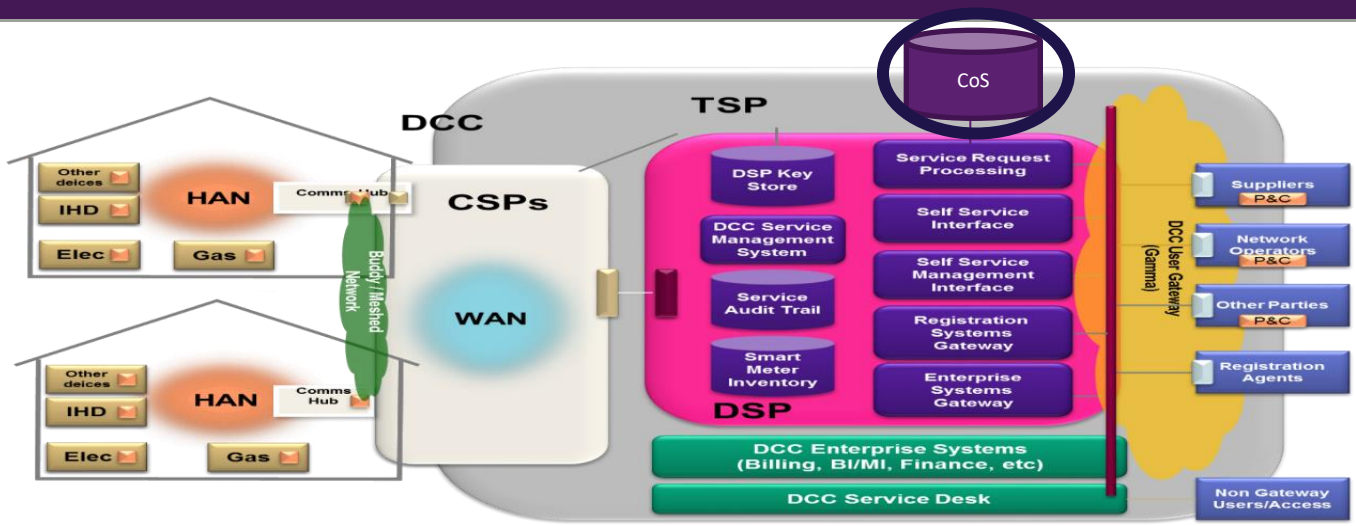
DCC Major Incident Summary Report

(Produced in accordance with Section H9 of the SEC)

Date of Incident	07/08/2019
DCC Incident Reference Number	INC000000478818 PBI000000116808
Service Impacted	DSP Change of Supplier (CoS) Environment
Date/ Time Incident reported	07/08/2019 10:22 (Severity 5 Incident Raised) 07/08/2019 11:25 (Severity increased to a 3) 07/08/2019 12:06 (Severity increased to a 2) 07/08/2019 21:00 (Severity increased to a 1)
Date & time incident resolved	07/08/2019 21:51
Time taken to restore Service(s) (Hours)	11 hours 29 minutes
Resolution within SLA (Y/N) ***[SEC 9.14(b)]***	N

Nature of the Major Incident / Short Description



At 10:22 on Wednesday 07th August, A single Service User raised a Severity 5 incident relating to Change of Supplier (CoS) Service Request 6.23 not completing.

At 11:25 this incident was raised to a Severity 3 as further incidents had been raised by other Service Users.

At 12:06 the incident was further escalated to a Severity 2 as the Data Service Provider (DSP) found that the Change of Supplier (CoS) environment was inaccessible.

At 12:23 DSP opened an internal technical bridge to investigate this failure.

Between 12:23 and 21:20 the DSP engineering teams carried out a process of elimination on the complex CoS environment checking connectivity. The engineers traced the communication through the network step by step, device by device until full service was restored at 21:20.

At 21:00 DCC Major Incident Management escalated this incident to a Severity 1 due to the length of time the service was unavailable and the adverse impact this could have on the DCC and its Users.

From 21:20 DSP carried out sanity checks on the CoS environment to ensure full end to end connectivity was restored. They could see 6.23 Service Requests progressing with successful responses.

Region / Location impacted

This incident affected all regions (North, Central and South)

Summary of impact / Likely future impact of the Major incident

The impact was that the 6.23 Service Request was not completing.

This meant that the gaining supplier was not able to place their certificates on the Devices they had gained via Change of Supplier (CoS). This also impacted the gaining Service Users ability to send any critical commands to that Device. This did not affect other Service Request Variants (SRVs).

An estimated 900 6.23 Service Requests were impacted and Service Users received a genuine response of E4 or HTTP500, which means they would have to resubmit the 6.23 Service Request the following day.

Immediate mitigation steps have also implemented:

- Immediate change freeze from the DSP whilst a review takes place;
- All DSP open changes being re-reviewed; and
- Suppliers engaged for Root cause analysis

Resolving actions taken

DSP carried out a series of restoration activities with full service being restored when the DSP removed and re-added the routing protocol on the secure element of the CoS environment.

Root Cause, if known

Root Cause is currently unknown. Further investigations are in progress under Problem Management ticket PBI000000116808.