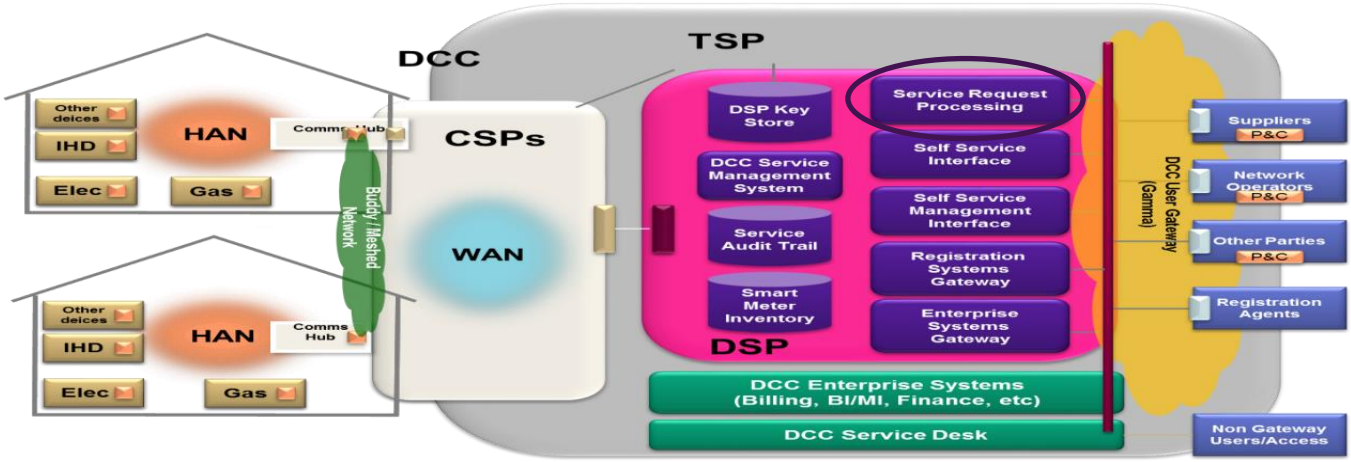
DCC Major Incident Summary Report

(Produced in accordance with Section H9 of the SEC)

Date of Incident	26/04/2021
DCC Incident Reference Number	INC000000719287
DCC Problem Reference Number	PBI000000122600
Service Impacted	Delivery of SMETS1 and SMETS2 Service Requests responses and device generated alerts to Service Users
Date/ Time Incident reported	26/04/2021 02:11 (service impact start time)
Date &time incident resolved	26/04/2021 04:56 (Service restoration time)
Time taken to restore Service(s) (Hours)	2 Hour 45 Minutes
Resolution within SLA (Y/N) ***[SEC 9.14(b)]***	Yes

Nature of the Major Incident / Short Description



At 03:00 on 26/04/2021, TOC monitoring identified that the delivery of responses to on-demand and scheduled Service Requests were failing. This was impacting both SMETS1 and SMETS2 traffic. Increased failures were also detected by DSP automated alerting.

The volumes of Service Request traffic increased shortly after 02:00, when the daily scheduled meter reads commenced.

As the volumes increased, DSP analysis identified a high number of failures in the delivery of traffic to Service Users, via the North facing servers. This led to the implementation of the automated self-protection circuit breaker at 03:15. As a failsafe, the Message Gateway Application will stop sending messages to specific service users if there are 200 or more consecutive failures to the same end point. This effectively stopped the flow of Northbound traffic.

The impact was mitigated by the temporary pausing of the scheduled meter read retries and therefore reduced the volumes of Service Request responses sent through the Northbound route.

The failure of delivery of Service Requests and alerts to Service Users occurred between 02:11 and 04:56. The backlog of Northbound Service Requests responses and alerts cleared through the retry schedule by 17:00 the same day.

Region / Location impacted

All regions. SMETS1 and SMETS2 Northbound traffic impacted.

Summary of impact / Likely future impact of the Major incident

This incident impacted the delivery to Service Users of:

- Responses to on-demand and scheduled Service Requests
- Device alerts including AD1 Power Alerts

After restoration was achieved there remained a backlog of alerts and scheduled meter reads in the Northbound message queue. This cleared throughout the day until normal levels were seen at 17:00 (26/04).

Resolving actions taken

The impact was mitigated at 04:55 by DSP pausing the polling of scheduled reads retries, which accounted for the increased volume of traffic in the early hours of the morning. The Message Gateway Application will try to re-send messages every 5 minutes until a successful response is received. As the delivery attempts, and therefore failure rate was reduced, the application started sending messages at increased volumes again, as there was a reduced likelihood of 200 consecutive failures being reached.

Investigations identified that the internal errors, indicating a delivery failure, were being returned by one of the two network appliances that were used to validate the requests processed en route to the North facing servers and delivery to Service Users.

The network appliance was removed from the load balanced pool at 06:06 and the throughput of message delivery to Service Users was restored to expected levels. Service Request and alert Northbound delivery returned to BAU levels.

Root Cause, if known

Following the BCDR DSP failover to the secondary data centre, there was a connection failure from a Network appliance to the North facing servers. This was due to a missing configuration on the virtual switch ports and resulted in the appliance to return HTTP500 errors.

There was no initial impact as retries pushed traffic through an alternate route. However, when the scheduled reads began and the traffic volumes increased, the number of failures also increased. This led to the Message Gateway Application to implement self-protection and limit the volumes of traffic sent through the Northbound route.

Investigations into the cause of the missing configuration are ongoing.

Table of linked incidents

Incident	Linked incident	Nature of link
INC000000719287	INC000000718832	Related
	INC000000719223	Related
	INC000000719235	Related
	INC000000719241	Related
	INC000000719267	Related
	INC000000719272	Related
	INC000000719277	Related
	INC000000719278	Related
	INC000000719283	Related
	INC000000719288	Related
	INC000000719291	Related
	INC000000719292	Related
	INC000000719294	Related
	INC000000719306	Related
	INC000000719353	Related
	INC000000719376	Original of
	INC000000719378	Related
	INC000000719379	Related
	INC000000719385	Related
	INC000000719388	Related
	INC000000719393	Original of
	INC000000719398	Related
	INC000000719404	Related
	INC000000719433	Related
	INC000000719435	Related
	INC000000719436	Related
	INC000000719441	Related
	INC000000719442	Original of
	INC000000719447	Related
	INC000000719471	Related
	INC000000719505	Related
	INC000000719506	Related

Incident	Linked incident	Nature of link
	INC000000719508	Related