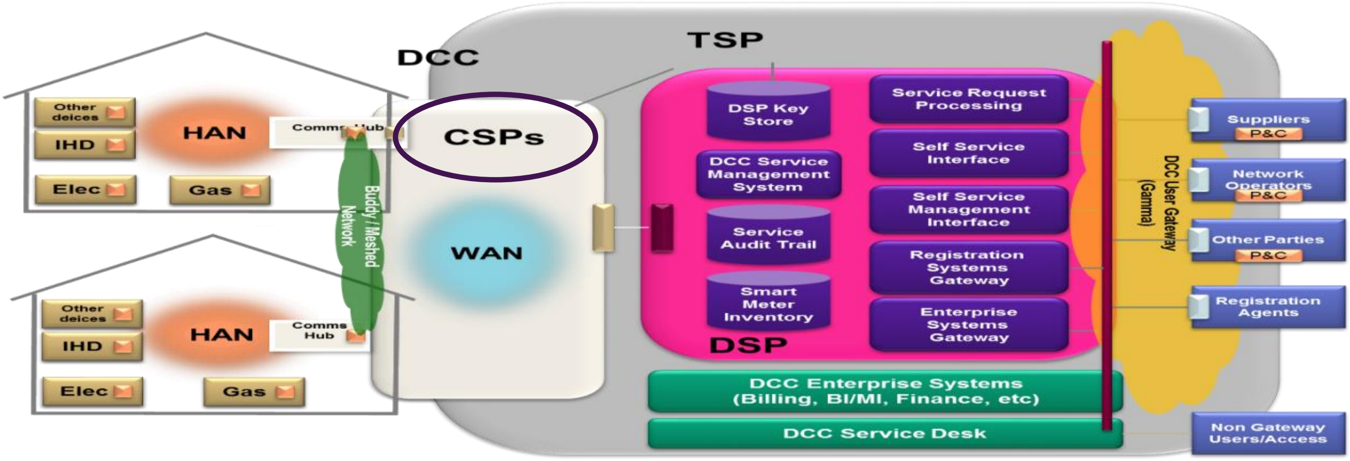
DCC Major Incident Review Report

(Produced in accordance with Section H9 of the SEC)

Date of Incident(s)	02/04/2019
DCC Incident Reference Number	INC000000440855
DCC Problem Reference Number	PBI000000114404
Service Impacted	CSP North core infrastructure related to Install & Commission, on demand Service Request Variants (SRVs) and Meter Firmware downloads
Date/ Time Incident reported	02/04/2019 10:24 (Actual Outage time) 02/04/2019 10:40 (Remedy Incident opened)
Parties involved	• **CSP North** • **DCC**
Date & time incident resolved	02/04/2019 10:48 (Actual Outage/Remedy time)
Time taken to resolve incident (Hours)	24 minutes
Resolution within SLA (Y/N) ***[SEC 9.14(b)]***	Y
Potential SEC Modifications [SEC H9.14(g)]	N
Major Incident summary report *[SEC 9.14(a)]* attached: Y / N	**Y - SEE APPENDIX 1**

Infrastructure Topology View



Summary of Impact [SEC H9.14(c)]

An issue occurred at 10:40 on the 2nd April 2019. This incident was reported by the CSP North informing DCC that they had identified an issue within their core infrastructure. Initial investigations highlighted an issue with their server which processes install and commission of devices, device firmware download requests and on demand Service Requests across the North Region. The impact to Service Users would have been intermittent. CSP North restarted the server and at 10:48 service was restored. At 11:15 DCC Technical Operation confirmed that they could see successful installs and Service Requests processing in the 10:45 – 11:00 reporting interval. This affected all service user's ability to intermittently complete installations of SMETS2 devices In the North region only whilst the Central and South region remain unaffected by this disruption. It is known that approximately 40 birthing events were impacted during this outage, however no impact was reported by the Service Users.

Incident Mitigation [SEC H9.14(c)]

- DCC requested the CSP North to treat any failure related to the CSP North Flex IP Server as a Severity 1 Service affecting incident until the RCA is completed and a hot fix is deployed (Date to be confirmed).
- CSP North implemented 2 tactical fixes to restore service.

1. CSP North restarted the server which was experiencing degraded service.
2. Amended the Cron job to remove child processes every hour. Furthermore if a 10,000 process limit (1/3rd of capacity) is reached during the hour the cron job will activate and remove child processes immediately.

Preventative Measures [SEC H9.14(d)]

Preventative Measures:

- Increased automation of the Cron job (A scheduled task to run every hour which will clear down any processes that have not closed effectively within the Gateway Schedular process.

- CSP North have implemented more manual monitoring to prioritise any alerts received for this service.

Root Cause Summary [SEC H9.14(d)]

The Root Cause has been found by CSP North through provision of their logs and working with their vendor. UIT and SIT had failed over successfully, Production system defect resulted in the production server not failing over. If the failover had occurred successfully there would have been no capacity issues as alternate servers would have been able to manage the number of requests. In summary system defect exasperated by volume.

Root Cause Actions

(Actions tracked under Problem investigation ticket - PBI000000114404)

Action	Open	Closed	Owner
Investigations are ongoing by CSP North surrounding a failover from the primary to the secondary server. Failover only occurs if the server hardware fails. CSP North investigating and implementing options for application failover. This action will include monitoring of channels and concluding when failovers should occur.		✓	CSP North
CSP North were running a Severity 3 (INC000000441204) with the DCC and DSP relating to an identified increase to RTT (Round Trip Time). (Service restored following a restart of the CSP North ActiveMQ application).		✓	CSP North
CSP North to treat any Flex IP server incidents as Severity 1 until Problem Management complete a full investigation. **Implemented 02/04/2019**		✓	CSP North
Implement a cron job to remove child processes every hour. Furthermore, if a 10,000-process limit (1/3rd of the capacity) is reached during the hour the cron job will activate and remove child processes immediately. **Implemented 02/04/2019**		✓	CSP North
CSP North to provided captured logs to vendor to aid them with determining the full root cause. **Implemented 02/04/2019**		✓	CSP North
CSP North to Determine what steps can be implemented to ensure the master Flex IP server utilises the slave server to avoid outages of this nature whereby server hardware hasn't failed.		✓	CSP North

Identified Risks:

(Actions tracked under Problem investigation ticket - PBI000000114404)

Action	Open	Closed	Owner
There is a risk that if the automation fails then this could re-occur. This risk will remain until the hot fix is deployed by CSP North. This is being tracked under the Problem investigation ticket.	✓		CSP North

Details of the review of the response to the Major Incident and its effectiveness [SEC H9.14(e)]

🟩	No Area for Improvement
🟥	Improvement Identified

Incident Process Steps	Summary Outcome	R/G
Identification	CSP North created a ticket (INC000000440855) at 10:40 on 02/04/2019. This was for a single birth event failure managed as a Sev3.	🟥
Classification/Prioritisation	Following further checks completed by CSP North it was identified this was impacting more than just a single birth event and the incident was upgraded to a Sev1.	🟥
Investigation/Diagnosis	Investigations and diagnosis were completed in a timely manner including engagement of CSP North	🟩
Resolution/closure	Once a fix had been found, restoration approval was managed via the Incident Management Procedure. With no delays.	🟩
Customer Communications	DCC provided regular updates via the Incident Management communications process, providing an accurate update of current status. Some customer-facing communications were delayed. DCC have been working to enhance their customer communication timings to address the improvement required.	🟥

Any failures by Incident Parties to comply with their obligations under Energy Licences and/or this Code [SEC H9.14(f)]

None

The likelihood there will be a reduction in the DCC's External Costs arising as a consequence of the DCC Service Providers failing to achieve a restoration of any Services within the Target Resolution Time [SEC H9.14(g)]

None