Data Communications Company

Supplemental consultation

Temporary Maintenance schedule June 2018 review

Consultation opens: 28 June 2018
Consultation closes: 3 July 2018

Date: 28 June 2018

Classification: DCC Public

Table of Contents

1 Background

This consultation is supplemental to the consultation undertaken by DCC on 20 June 2018, 'Temporary Maintenance schedule June 2018 review'. [1]

Responses to the 20 June consultation were broadly supportive of DCC's proposals. However, Parties expressed considerable disappointment that the proposed changes had not been identified and completed before now. In addition to this, the SEC Panel and respondents requested that DCC provides further information regarding its proposals, along with additional clarity around some information already provided. This document is intended to provide that additional information, and seeks the views of Parties.

The key additional information is:

- a revised description of the proposed changes, and the associated benefits (Section 2); and
- a view of the changes proposed for implementation on each day, along with the time and duration of each Maintenance window (Section 3).

DCC received specific feedback from several respondents to the 20 June consultation that the response period allowed for that consultation was not sufficient. Whilst we intend to ensure that Parties are allowed more time to respond to future consultations, the importance of these changes, along with the need to complete them by October 2018 means that this consultation will also need to be undertaken using truncated timescales. DCC Apologises for the inconvenience this will cause, and would like to thank all the respondents to the 20 June consultation for providing feedback so swiftly.

2 Proposed changes

DCC's technical and operational teams have been working closely with the DSP to carry out a low level technical review of DSP systems. This work identified areas where the current design or configuration of DSP systems could result in unnecessary disruption or downtime in the future. DCC's aim is to reduce the number of future outages by addressing these issues prior to the high-volume roll-out of SMETS2 meters which is expected to commence when the deadline for installing SMETS1 meters is reached in the last quarter of 2018.

The improvements identified during the review are essential to ensuring that DCC Systems can operate at scale on an enduring basis. Whilst it may be possible to schedule the work over a longer period, which would reduce the impact on Users in the short-term, DCC considers that it would be more disruptive to allow this work to continue beyond October 2018 due to the expected increase in SMETS2 installations once the deadline for installing SMETS1 meters has been reached.

The individual changes identified during the review total 228 hours of outage time across 25 Maintenance windows during July, August, September and October 2018. They have been grouped into eight work packages, each of which has been allocated to one of four categories, shown in Figure 1 on the following page.

[1] The initial consultation can be found on DCC's SharePoint site at: Information for SEC Parties / Regulatory / Consultations.

Figure 1

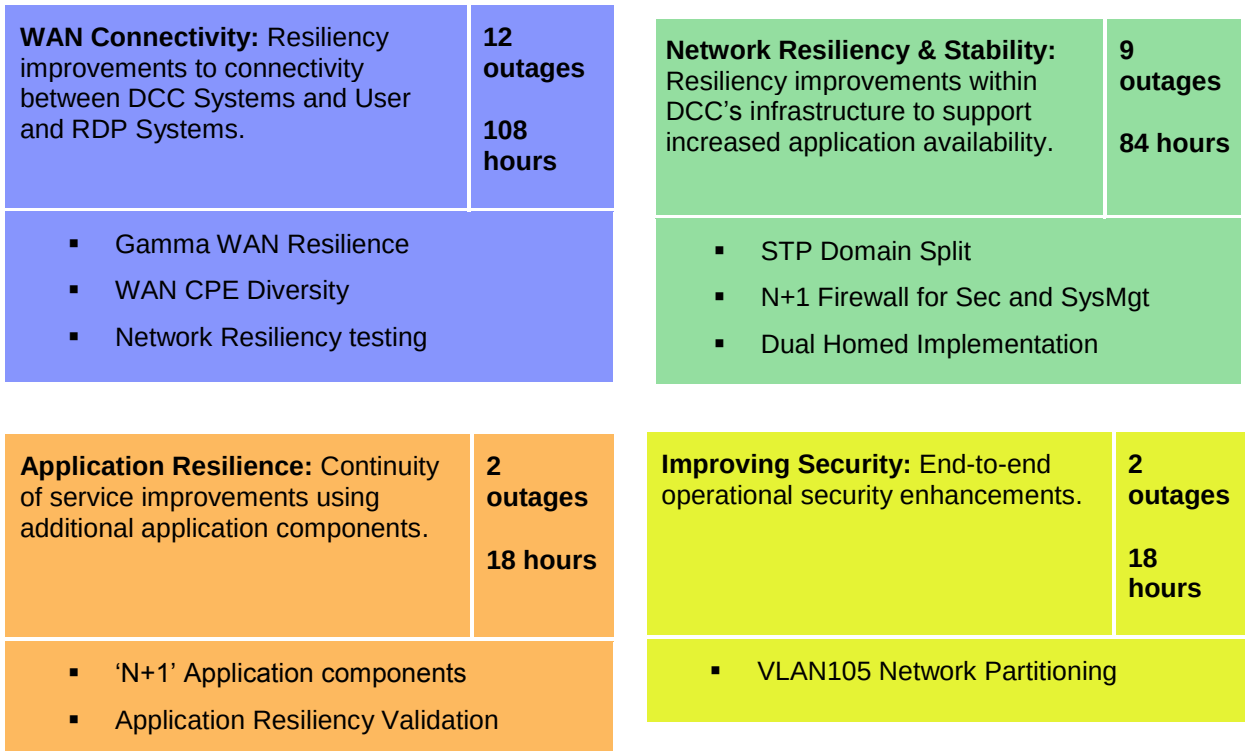

Table 1 on the following page provides an overview of each work package, the number of outages and amount of Planned Maintenance required to implement each package, along with the benefits each work package will deliver.

Table 1

Name: ▪ No. Outages ▪ No. Hours	Context	Problem, solution statement	Benefit to DCC Users
Gamma WAN Resilience: ▪ 4 outages ▪ 36 hours	Connectivity between User and DCC Systems is provided over a network connection provided by Gamma Telecom Ltd (the DCC Gateway Connection). This Gamma connection underpins the provision of: ▪ the DUIS; ▪ the Self-Service Interface; ▪ the SMKI/DCCKI repository; and ▪ the Registration systems.	The current connection between the Gamma connection and the DCC employs a single network switch at each data centre. If that switch fails, the primary means of recovery is to fail-over to the backup (Disaster Recovery) data centre. This change will double the number of switches used to connect the Gamma connection to DCC Systems, allowing the second connection to be used as a local backup if the first switch fails. This will reduce the likelihood of the entire Wide Area Network (WAN) failing-over to the backup data centre. If the WAN does need to failover, this can currently take up to 4 minutes to complete, which exceeds the timeout limit of some User Systems. This change will also help to reduce HAN failover times so that User Systems do not timeout.	Decreased failover times for the Gamma connection will help minimise the risk of User sessions timing-out, or Service Requests failing. The introduction of a second switch adds local resiliency to both the primary and backup systems, reducing the likelihood that a full fail-over to the backup data centre will occur, reducing the risk of User sessions timing-out or Service Requests failing.
WAN CPE Diversity: ▪ 4 outages ▪ 36 hours	The WAN connectivity installed at the DCC data centres underpins the processing of all service messages from the DCC Users to the customer devices.	The physical location of network devices that connect DCC Systems to User and CSP Systems are not optimised within the data centre, resulting in an increased risk of failure in the event of physical disruption at the site. This change will deliver additional resiliency by relocating some network devices within the data centre.	Reduces the impact on Users in case of local datacentre failure event by allowing the failover of specific network components within the same data centre. Reduces the likelihood of invoking a Disaster Recovery event due to the failure of devices.

Network Resiliency testing: ▪ 4 outages ▪ 36 hours	The availability of DCC Services depends on the hierarchy of network, server hosting and application components. Testing is required to prove that the improvements made during the months of July to October meet their objectives.	Resiliency testing will demonstrate the resilience of the services by testing failure or failover of key application, hosting and network components. The difference between implementation testing and this resiliency testing is that this testing has a greater focus on application availability.	Ensures that the enhancements being proposed as part of this activity deliver the resiliency of the end-to-end service across applications, service, hosting and networks.
Application Resiliency testing: ▪ 1 outage ▪ 12 hours	As above (Network Resiliency testing): The availability of DCC Services depends on the hierarchy of network, server hosting and application components. Testing is required to prove that the improvements made during the months of July to October meet their objectives.	As above (Network Resiliency testing): Resiliency testing will demonstrate the resilience of the services by testing failure or failover of key application, hosting and network components. The difference between implementation testing and this resiliency testing is that this testing has a greater focus on application availability.	As above (Network Resiliency testing): Ensures that the enhancements being proposed as part of this activity deliver the resiliency of the end-to-end service across applications, service, hosting and networks.
'N+1' Application components: ▪ 1 outage ▪ 6 hours	DCC Services are provided through the deployment of application components. The resilience of the Services is articulated in terms of the number of installed components, either N or N+1, where N is the number of components to meet a level of capacity, and the +1 refers to the deployment of an additional component to provide resilience. As design has evolved and business priorities changed DCC proposes the implementation of N+1 application components.	Additional nodes are required for the following components to provide N+1 resilience: ▪ CSP Management Gateway; ▪ SSMI Web Server; ▪ SSI Database; ▪ Remedy DSMS Business Object resiliency; ▪ IDP GetAccess; and ▪ LDAP N+1 DCCKI Repo Webserver.	Since December 2017, DCC has had to manage three Incidents which were all related to issues with the IDP GetAccess component, and which could have resulted in authentication issues for SSI Users. N+1 resiliency at the IDP GetAccess component would have mitigated the cause of these Incidents. DCC expects that for each component listed, the additional nodes will: ▪ Improve resilience of the CSP Management Gateway which supports the install and commission of devices and Self-Service Interface (SSI) screens for Communications Hub diagnostics. ▪ Improve the availability of the SSI by increasing resilience

	▪ This improvement will deal with, for example, improvements when performing Installation and Commissioning work, since the CSP Management Gateway is now on a critical path and must deliver resiliency.		in the user authentication service. ▪ Provide a faster recovery time of the SSI database. ▪ Provide increased resilience of the DCCKI repository service that provides DCCKI certificates to users and service providers.
N+1 Firewall for Security Services and Systems Management: ▪ 2 outages ▪ 24 hours	The DCC solution utilises network firewalls as part of its security architecture. These firewalls restrict access between zones of the network to specifically permitted traffic. This change relates to specific firewalls which limit access to the Security Services and Systems Management zones. These zones contain authentication services required for SSI and operational tooling respectively.	Currently the Security Services and Systems Management firewalls use a pair of devices split between the primary and backup data centres. Whilst the current approach offers a highly available solution across data centres, the implementation of N+1 firewalls in the primary datacentre will increase resiliency.	Increasing resilience within the primary data centre for key network security components should reduce the need to fail-over to the Disaster Recovery systems, resulting in less system down-time.
STP domain split: ▪ 2 outages ▪ 18 hours	The DCC solution provides hosting infrastructure at primary and back-up data centre locations. These locations are connected via diverse communications circuits.	Currently, network components located at each data centre are connected to each other in a loop. To prevent traffic from flowing infinitely around the loop the switches utilise the Spanning Tree Protocol (STP) to detect and block one of the links in the loop. This change makes enhancements to the STP design so that the two data centres can be managed independently, ensuring that changes at one site do not impact the other site.	Reduces service interruptions by improving the stability and recovery times of the network. Minimises the risk of an outage through the containment of local network changes.

Dual Homed Implementation: ▪ 5 outages ▪ 42 hours	DCC Systems use resilient network components in the primary data centre to increase service availability. These components include switches, firewalls and other network appliances e.g. load balancers.	The network firewalls are connected to each switch layer with a single connection. These switches have a limited number of ports allowing specific number of connections. In case of port malfunction, for example, the issue can potentially cascade through the network causing application instability.	Improves the resiliency of the network to avoid outage of the service user facing applications in the event of a network switch failure. Minimises the actions Users need to take to recover in the event of a single component failure.
VLAN 105 network partitioning: ▪ 2 outages ▪ 18 hours	The DCC solution data centre networks utilise virtual local area networks (VLANs) to isolate network traffic. Network routers are used to enable traffic flows between each VLAN. A specific use of VLANs is to provide the “glue” between routing devices. These are known as “transit VLANs”.	Currently, a single transit VLAN (VLAN105) is used to conjoin multiple network security devices. Enhancements are required to segregate VLAN105 to align it with an improved security separation design.	Increases security of DCC Systems by adopting the latest network security design.

3 Schedule of change

The monthly calendars below provide a daily schedule of the proposed changes by work package. This schedule has been produced using DCC’s detailed plan and considers other change initiatives taking place at DCC, for example the deployment of Release 2.0 functionality at the end of September 2018, along with functional defect fixes and security patches.

By setting out the fixed schedule of change in advance in this way, DCC is aiming to minimise disruption to Users by providing clarity around the dates and maximum duration of Planned Maintenance activities well in advance.

DCC’s desire is to commence this activity as soon as possible. Having a forward schedule of change through to October means that DCC will ensure that almost all of the Maintenance windows will be notified 20 Working Days in advance. We will request that the Panel considers granting a shorter Notice period for the Maintenance proposed to take place during July.

There may be instances where it is more practical, or more beneficial for Users, to amend the sequencing of changes within this schedule. If DCC needs to make any amendments to the schedule, our proposal is to inform Parties of any such amendments at least five Working Days in advance. We welcome specific views on this aspect of our proposal.

Consideration has been given to ensuring that any impact on the operational activities of SEC Parties is minimised. Because of this, we propose that the longer outages should be scheduled to take place on Sundays, when we have historically seen lower usage of DCC Systems.

Along with the Maintenance windows to accommodate the non-functional changes above, the calendars also include an additional six hours of Planned Maintenance each month during July, August and October. These Maintenance windows are required to allow functional defect-fixes and security patches to implemented.

3.1 July 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2	3	4	5	6	7
8 VLAN105 Network Partitioning: 12 hours from 8am to 8pm	9	10	11	12 VLAN105 Network Partitioning: 6 hours from 8pm to 2am	13	14
15 STP Domain Split: 12 hours from 8am to 8pm	16	17	18	19 Network Resiliency Validation: 6 hours from 8pm to 2am	20	21
22 Gamma WAN Resilience: 12 hours from 8am to 8pm	23	24 Defect fixes or patching: 6 hours from 8pm and 2 am[2]	25	26 STP Domain Split: 6 hours from 8pm to 2am	27	28
29 Dual Homed Implementation: 12 hours from 8am to 8pm	30	31				

[2] This Planned Maintenance window may take place on 31 July instead. DCC will provide confirmation at least five Working Days in advance of the window being used.

3.2 August 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	2 Gamma WAN Resilience: 6 hours from 8pm to 2am	3	4
5 Gamma WAN Resilience: 12 hours from 8am to 8pm	6	7	8	9 Network Resiliency Validation: 6 hours from 8pm to 2am	10	11
12 Dual Homed Implementation: 12 hours from 8am to 8pm	13	14	15	16 WAN CPE Diversity: 6 hours from 8pm to 2am	17	18
19 WAN CPE Diversity: 12 hours from 8am to 8pm	20	21	22	23 Gamma WAN Resilience: 6 hours from 8pm to 2am	24	25
26 N+1 Firewall for Sec and SysMgt: 12 hours from 8am to 8pm	27	28 Defect fixes or patching: 6 hours from 8pm and 2am	29	30 Dual Homed Implementation: 6 hours from 8pm to 2am	31	

3.3 September 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1
2 WAN CPE Diversity: 12 hours from 8am to 8pm	3	4	5	6 Dual Homed Implementation: 6 hours from 8pm to 2am	7	8
9 N+1 Firewall for Sec and SysMgt: 12 hours from 8am to 8pm	10	11	12	13 Dual Homed Implementation: 6 hours from 8pm to 2am	14	15
16 Network Resiliency Validation: 12 hours from 8am to 8pm	17 R2.0 Change restriction	18 R2.0 Change restriction	19 R2.0 Change restriction	20 R2.0 Change restriction	21 R2.0 Change restriction	22 R2.0 Change restriction
23 R2.0 Change restriction	24 R2.0 Change restriction	25 R2.0 Change restriction	26 R2.0 Change restriction	27 R2.0 Change restriction	28 R2.0 Change restriction	29 R2.0 Change restriction
30 R2.0 Change restriction						

3.4 October 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1 R2.0 Change restriction	2 R2.0 Change restriction	3 R2.0 Change restriction	4 WAN CPE Diversity: 6 hours from 8pm to 2am	5 R2.0 Change restriction	6
7 Network Resiliency Validation: 12 hours from 8am to 8pm	8	9	10	11 'N+1' Application components: 6 hours from 8pm to 2am	12	13
14 Application Resiliency Validation: 12 hours from 8am to 8pm	15	16 Defect fixes or patching: 6 hours between 8pm and 2am	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

4 Impact on Users

Implementing these changes will require the full suspension of DCC Services, which will be unavailable during each Maintenance period. The impact on Users during the outage will be as follows:

- The DUIS will be closed and no new Service Requests will be accepted. No Alerts or responses will be delivered;
- All DSP Future Dated and Scheduled events that are due to be executed during each Maintenance window will be suspended and restarted after the window ends;
- Future Dated, Schedule and other events originating from the HAN during the outage period will be queued and delivered after the upgrade;
- The SSI will be unavailable;
- The Service Desk will remain open and contactable via email and telephone during all outages;
- The SMKI Service will remain available for CSR processing, but the publishing and SMKI/DCCKI Repository features will not be available; and
- The daily file transfers of Registration updates from the DSP will be disabled, although inbound Registration files will still be received from the RDPs and the data applied at the end of each Maintenance window.

5 Next steps and how to respond

DCC will be seeking a decision on our proposals from the SEC Panel at an ex-committee meeting on 3 July. We encourage SEC Parties to provide views on our proposals prior to DCC requesting a decision.

In recognition of the potential impact of our proposals, along with the short timescales available for Parties to provide views, we welcome feedback across several channels, including:

- Email
- Bilateral meetings or teleconferences

Please contact DCC at contact@smartdcc.co.uk if you would like to discuss any aspect of these proposals.