This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0067 'Service Request Traffic Management'

Working Group Meeting 1

4 January 2019, 10:00 – 12:00, Gemserv's Offices

Meeting Summary

Discussions on the proposal

The Working Group meeting began with an overview of the modification by the DCC and outlined the main objectives of the modification. The DCC highlighted that the main objective of the modification was to implement a mechanism for the management of Service Requests within the Data Service Provider (DSP) systems. The DCC stressed that the modification was seeking to manage times of exceptional system usage and was not intended to be a mechanism for managing capacity. It was noted that the solution would allow for priority requests to always go through, and that capping of non-priority requests would only take place when the overall system capacity was nearing maximum.

One member asked why anomaly detection thresholds could not be used here, as exceptional events would surely be in excess of standard thresholds. The DCC noted that a solution involving the anomaly detection thresholds would enforce a cap on each individual User at all times, whereas the proposed approach would only put caps in place for Users when the system was close to maximum capacity.

It was noted that Users would submit forecasts of Service Request usage, which would form an expected load across a period of a week or a month, but there was nothing to stop a User submitting all forecasted requests in the same second through error or miscommunication. It was these spikes that the solution was seeking to address. Such a spike would not breach anomaly detection thresholds but could exceed the system capacity. There was a concern that Users could submit increased forecasts to ensure they get more capacity on the network.

The Working Group discussed the DCC's obligations with regards to the DSP and queried whether the DCC was concerned about the DSP meeting its obligations with the current finite capacity of the DCC Systems. DCC confirmed it was not. Questions were asked included the timeframe that is measured against Service User submissions of Service Requests. The DCC confirmed that the measure would be undertaken in a "by second" basis for assessing heavy Service Request traffic. One member also suggested that, as User gateways would have a finite capacity, the potential maximum volume the DCC could expect would be the sum of this capacity across all Users. It was queried whether Users would be able to physically submit the volumes that would cause capacity issues.

The Working Group also queried a move to a cloud-based system, which the DCC noted was a nice objective. It was highlighted that the DSP uses its own data systems and the architecture is not currently designed to scale up dynamically. The physical limits of a radio network, which both Communication Service Providers (CSPs) use, was also highlighted as a constraint, and the DCC noted that increased capacity takes time to implement. This resulted in an action for the DCC to provide further information in the next Working Group meeting as to its long-term plans around

capacity management and whether the proposed solution for this modification is designed for the long term or as an interim until system capacity can be increased.

It was confirmed that SECMP0067 is a replacement for withdrawn modification SECMP0030 'Demand Management of DCC Systems', and that SECMP0028 'Prioritising Service Requests' has been placed on hold by the Proposer as SECMP0067 could deliver what that proposal seeks; if it does, SECMP0028 would then be withdrawn. SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection' is also looking at traffic management, but in the opposite direction through the system, and the two solutions are independent but complementary of each other. Other initiatives such as TOC and DSP monitoring are also being explored.

One Working Group member raised that the modification presented a potential security risk in the form of fraudulent Service Requests listed as priority requests that could initiate a "Denial of Service" scenario. The other Working Group members agreed to refer this modification to the Security Sub-Committee (SSC) to assess this security risk.

Solution requirements

The Working Group discussed the requirements the modification's solution should be measured against in order to deliver its intent. The draft requirements which were agreed upon were as follows:

- There will be a list of which Service Requests are defined as Priority and Non-Priority when the solution's mechanism is operational, and this list would need to be configurable. The Priority Service Requests need to include all Pre-Payment requests due to the nature of these requests and the increased likelihood that these requests are generated by vulnerable energy consumers. Network Parties requested Service Request 7.4 be included, as they would need information on outages as soon as possible. Another member proposed that the initial list also include Service Request Variants that are not future-dated or scheduled requests and which have a Target Response Time of 30 seconds. SECAS will prepare an initial list of Priority requests based on this for the Working Group to refine.
- There will be a defined formula/calculation which is used to allocate individual Service User capacity in the event of the DSP capacity threshold being breached. The DCC has already prepared a straw man, which will be circulated to the Working Group for consideration. The Working Group requested that allocations be based on portfolio size rather than the number of installations, and that it account for Change of Supplier events. Users would be made aware of their capacity threshold at any given time.
- Service User capacity will be updated monthly, although any reallocation between suppliers as a result of a Supplier of Last Resort event is to happen as soon as the process allows.
- The solution should consider the effects of outages of the DSP, including system maintenance and other unexpected circumstances, on the subsequent traffic through the DCC Systems.
- There will be a transparent reporting process to update Service Users on when throttling has been used by the DCC Systems and which Service User have regularly exceeded their Service User capacity allocations. Members requested this be monthly, covering how often the solution is being used and the Service Requests being affected. There was consideration over whether the reporting should look at the system as a whole or pick up on individual Users affected by any throttling would be identified – one member stressed the purpose of any reporting needs to be clearly defined.

The Working Group discussed whether there should be “503 http//:” obligations included as part of the objective/solution of the modification in the event of resending requests through the DSP. They agreed to consider Service User behaviours and interactions with this, but not to mandate it due to how different Service Users respond and that such obligations could be counter-productive. One member noted an event the previous week where Users were getting this rejection reason and wondered if this would provide any useful information or lessons learnt for consideration.

The Working Group considered whether an alternative approach of queueing messages could be implemented. However, members noted this had been discussed before and rejected on the grounds of cost, as this would require a significant overhaul of the DCC Systems. Members also raised questions of how items in the queue would be prioritised and felt this approach could get complicated. SECAS agreed to gather together all past information on this approach for the Working Group.

One member queried whether it could be the Service Requests sought to be a priority that were the ones that could cause the system to exceed capacity. This will need to be examined further once the list of priority requests is developed. It was acknowledged this was a risk.

The Working Group agreed to refer this modification to the Technical Architecture and Business Architecture Sub-Committee (TABASC) for their input over the short term and long term architecture impacts.

The Working Group discussed what incentives or disincentives would be in place to ensure that Service Users would act responsibly and not exceed their capacity allocations, unless in exceptional circumstances. One Working Group member believed this should be at the centre of the cited modification objectives, but a majority of other members disputed this saying that the modification’s main objective was to introduce a throttling system only in the event of heavy service request traffic and to optimise the existing Service User capacity. These members highlighted that in exceptional events, such as the ‘Beast from the East’ in 2018, they would focus on keeping customers connected, and would ignore all their Service Request forecasts to ensure this was so, even if this was to result in a fine or other penalty. One member noted that during the ‘Beast from the East’ event they had submitted around a million Service Requests in one day to ensure around 100,000 prepayment customers remained connected during this event. Any solution developed would need to cater for such numbers scaled up across all prepayment customers, as well as the requests Network Parties would be submitting during this time to ensure their networks remain operational.

Further actions

Further actions that were agreed to be taken are the following:

- Working Group members will review and provide any further thoughts on the Service Request types that should be prioritised within the modification’s solution.
- The DCC will consider the reporting process that would be used as part of the solution’s requirements and to provide more information on its long term approach to capacity management and whether the solution presented will be a short term or long term measure.
- SECAS will draft the business requirements for the proposed solution with the requirements mentioned earlier in this summary. These are to be prepared for the next Working Group meeting and available for review prior to the meeting. SECAS will also pull together all historical information available regarding discussions on the ‘queueing’ solution.