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.

DP072 'Change of Supplier process' Problem statement – version 0.5

About this document

This document provides a summary of this Draft Proposal, including the issue or problem identified, the impacts this is having, and the context of this issue within the Smart Energy Code (SEC).

Proposer

This Draft Proposal has been raised by Kieran Williams from SmartestEnergy.

What is the issue or problem identified?

Change of Supplier testing scenario

A potential General Data Protection Regulation (GDPR) issue has been found following Change of Supplier (CoS) testing with a Supplier, in which a data change request was submitted for the Supplier to regain their meter back following testing carried out by SmartestEnergy, with effect from 18 September 2018. For reasons unknown to SmartestEnergy, the gaining Supplier in question did not action their CoS Service Requests. It was not until trying to resolve an issue with a meter manufacturer that SmartestEnergy noticed they had been receiving daily reads from a device that they were no longer the Supplier for.

SmartestEnergy were advised by the Triage team at the Data Communications Company (DCC) that for them to stop receiving these alerts, the gaining Supplier needed to issue Service Request 6.23 'Update Security Credentials (CoS)'. Despite numerous attempts requesting this, it took the gaining Supplier 50 days to properly acknowledge the request and to issue the Service Request. This resulted in SmartestEnergy receiving three to four alerts per day (only one of these alerts would contain the customer read, the rest contained DCC E4[1] response codes). With no official process or escalation point to stop receiving unwanted alerts SmartestEnergy received a total of 234 alerts, with roughly 78 of these messages containing specific readings with the date and time of a customer SmartestEnergy were no longer the Supplier for.

What may have caused this issue?

This issue has been raised with the DCC, and at several industry groups including the Smart Metering Design Group (SMDG), the Security Sub-Committee (SSC) and the Common Issues and Pilot groups. The DCC have identified two root causes:

1. Gaining Supplier is not registered in DCC Systems and is therefore unable to send Service Request 6.23 to update their security credentials; and
2. Gaining Supplier is registered in DCC Systems, but due to their system/process maturity or other issues, they have failed to send Service Request 6.23.

SmartestEnergy have made the DCC aware of a third cause, Erroneous Transfers.

How does this issue relate to the SEC?

The Proposer expects this issue to impact Section H 'DCC Services' as this section hosts the obligation on enrolment and exchange of certification after installation and would be a suitable section for any CoS related definitions.

[1] Verify that the User, in the User Role defined in the Service Request is an Eligible User for the Device.

What is the impact this is having?

What are the impacts of doing nothing?

The Proposer believes that this issue could potentially become more serious as rollout continues. The December 2018 SMDG DCC update confirmed a total of 1,046 Service Request 6.23 requests were not initiated (an increase of 288 since November 2018) with numbers expected to continue to rise. Should the same scenario experienced in testing happen in Production, and using the figures provided by the DCC, the DCC and SmartestEnergy, as a Supplier, would receive roughly 244,764 alerts, with 81,588 containing reads belonging to customers SmartestEnergy are no longer responsible for.

There is currently no process that SmartestEnergy have been made aware of when it comes to this scenario. The DCC are already aware of the amount of Service Request 6.23s that have not been initiated and they have informed SmartestEnergy that they receive regular emails on issues with installs and sending/receiving Service Requests.

By doing nothing the DCC will need to ensure their systems can tolerate this additional traffic, on top of traffic from sending or receiving other Service Requests. It also means that Suppliers will need to dedicate time and resources to sift through the alerts and make up their own minds with what they should do with information that they should not be holding.

How could this issue impact SEC Parties?

This issue would impact Large and Small Suppliers as they may receive alerts for supply points they are no longer responsible for. It will also test data retention plans that Suppliers should have in place, confirming what actions need to be taken when dealing with data they should not be receiving.

Other SEC Parties, like the DCC, will be affected by an increase in alert traffic (inbound and outbound alerts) they will receive.

What are the views of the industry?

Views of the DCC

The DCC have advised that this issue could be addressed by the Proposer raising a defect and provided advice as to how the Proposer could do this. However, the Proposer highlighted that they raised a defect, but it was subsequently closed with them still unclear on what the solution should be.

The DCC also noted that this issue resulted from a failure to follow the CoS process rather than a technical issue in the first instance. They added that this Draft Proposal needs to answer the question as to whether DCC operational guidance covers the resolution on what Service Users need to do, or if a Modification Proposal is required in order to put technical safeguards into place.

Views of SEC Parties

Prior to this Draft Proposal being raised, the gaining Supplier in question investigated the scenario further and understood why it had occurred. They advised that the scenario in question could occur in the 'live' environment depending on how Suppliers have designed their read processes and that there will always be occasions when a gaining Supplier doesn't issue CoS Service Requests in a timely manner (or is unable to do so). It was the gaining Supplier's view that this Draft Proposal should not result in a Modification Proposal as the scenario in question relies upon specific Supplier processes being in place.

The gaining Supplier advised that the given scenario could only occur whereby a losing Supplier had their daily reads set up in a way using the credentials on the meter, rather than the data held by the DCC Registration Data Provider. If the losing Supplier has set up a meter to send daily billing calendar reads, these are not validated by the DCC. In this scenario, meter readings will be sent to the Supplier whose Certificate is in the meter and will not stop until the CoS process is complete and the gaining Supplier has their Certificates on the meter. Therefore, if there is any delay in the sending of Service Request 6.23 the losing Supplier will continue to receive the meter readings.

The gaining Supplier in question raised an alternate approach to this scenario which they currently utilise themselves. Rather than setting up a daily read schedule with the meter, the schedule is set up directly with the DCC. This means that during the CoS process any reads that are generated to the losing Supplier are rejected by the DCC as they are not the Supplier for the meter on or after the Supply Start Date (SSD). Unlike DCC schedules, there is no ability for the meter to know who the Supplier is for the MPxN on any date, so it just sends reads to the Supplier whose Certificate is on the meter. When the meter churns to the new Supplier, the meter will still send the encrypted reads to the losing Supplier even after the SSD. This can only be rectified once the gaining Supplier has sent Service Request 6.23 and puts their Certificates on the meter. The method of using DCC read schedules which validate against registration data would prevent this from occurring.

An Other SEC Party queried whether there is a way that the DCC could prevent any responses/alerts which are not included in the Critical Alerts list from being sent to a non-registered Supplier. The DCC consider this to be feasible but advised that a solution would not be considered until the Refinement Stage, if this proposal were to progress that far. The DCC advised the Proposer of possible ways of handling the issue now:

- Currently, the losing Supplier can cancel any and all requests to receive regular information prior to the CoS date. Following the CoS date, they can't cancel these requests and will

continue to receive them. However, the DCC's service providers block all Critical Commands from going to the losing Supplier once the registration data states that a CoS has occurred.

- The losing Supplier can also 'black hole' any data relating to a customer they are no longer the Responsible Supplier for so that they do not store it if it is received.

Views of Panel Sub-Committees

Views of the TABASC

The Technical Architecture and Business Architecture Sub-Committee (TABASC) agreed that the CoS issue raised under this Draft Proposal needed to be addressed. However, they believed that this is an issue with an operational process rather than the SEC, and that a modification was not necessarily the most suitable way to address the matter.

The TABASC also advised that there is a service provided by the DCC whereby Suppliers can manage their alerts, which may help the Proposer in the scenario they have highlighted in their problem statement. However, this service does not prevent the Supplier from being notified on critical alerts.

Views of the Operations Group

The Operations Group could see the issue raised by the Proposer being an enduring issue as new Suppliers enter the market. However, it was their view that any solution should be based on guidance rather than raising a Modification Proposal.

Views of the SSC

The SSC noted the GDPR aspect raised by the Proposer and advised that this is a data privacy issue rather than a security issue. They noted that the issue had been discussed previously, and that the view is Supplier Parties shouldn't be storing information they shouldn't have. It is the Supplier's responsibility to discard this data and meet their GDPR obligations, including the losing Supplier in the scenario raised by the Proposer. The SSC's view was that any solution should be based around guidance rather than raising a Modification Proposal.

Views of the Change Sub-Committee

A Small Supplier on the Change Sub-Committee advised that anomalies in test scenarios aren't always replicated in the live environment. It was also their opinion on the Proposer's view of this issue potentially breaching GDPR that, if this is true, it should be addressed under the GDPR rather than the SEC.

The Change Sub-Committee stressed the importance of the CoS process being one of the key elements to the consumer experience, yet neither the SEC nor the Design Notes advise how personal data should be process as part of GDPR and that some guidance is needed to make Suppliers aware of their obligations. A Large Supplier also highlighted the fact that the sending of Service Request 6.23 by the gaining Supplier in a CoS scenario is implied in the SEC but not explicitly stated in the SEC. They did however note that the sending of Service Request 6.23 upon CoS is referenced in the TBDG Design Notes which are available on the SEC website.

The DCC suggested that there could be an obligation for the CoS process in the Retail Energy Code (REC) that Suppliers can abide by. In addition, SECAS noted that the DCC already has steps in place to monitor Suppliers for sending Service Request 6.23 in their Supplier of Last Resort (SoLR) process map.

The Change Sub-Committee agreed that the issue needed to be addressed but that further investigation is required to establish whether further guidance on the CoS process is required or if a modification to the SEC will be necessary.