SECMP0063 'Ensuring correct Network Operator Certificates are placed on Electricity Smart Meters'

September 2019 Working Group Meeting summary

SECMP0063 'Ensuring correct Network Operator Certificates are placed on Electricity Smart Meters' proposes to prevent incorrect Network Operator Certificates from being loaded on Smart Meters. The proposed solution would enable this by placing a validation check in place with the Data Communications Company (DCC), which will check the Network Operator listed in the Certificate matches the Network Operator held in the Data Service Provider's (DSP) registration data. The Working Group discussed the issue and the DCC's Preliminary Assessment of the proposed solution.

The DCC's Preliminary Assessment

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the business requirements on which the DCC based their Preliminary Assessment.

SECAS clarified that requirement 2 'the DCC will block the Certificate from going on the Electricity Smart Metering Equipment (ESME) if it fails DCC validation' would not be enforced where Service Request (SR) 6.15.1 'Update Security Credentials (KRP)' is submitted by a Network Operator. This would still allow for the current workaround in place whereby a Network Operator can exchange their Certificate for the correct Network Operator Certificate, where it had been incorrectly loaded on a Device outside of their region.

How would the DCC deliver the solution?

The DCC Data System will validate against the following SRs submitted by Energy Suppliers:

- SR 6.15.1 'Update Security Credentials (KRP)': required only when it is targeted at an ESME; and
- SR 6.21 'Request Handover of DCC Controlled Device': required for the target device types ESME and Gas Proxy Function (GPF).

The validation check on SR 6.15.1 'Update Security Credentials (KRP)' is on required on ESME due to Devices that are manufactured with Supplier Certificates in the Network Operator Trust Anchor Cell. These Certificates can only be replaced by the Supplier using SR 6.15.1.

How can GPF Devices be validated?

DCC propose that the validation checks for both SRs will be carried out against the DSP's copy of Registration data. This provides a common and standard solution for both ESME and GPF devices. If validation fails, the Service Request will be rejected, and the Service Users will be notified using a specific error code.

A Supplier noted that this approach would be dependent on the accuracy of the DSPs registration data, adding in the past they've had to notify the DCC to update it.

Working Group discussions on the scale and cause of the issue

Types of incidences

A Network Operator advised that their organisation have seen incidences where there their Certificates are not on their Devices. However, the number of times either:

- Their Certificates have been incorrectly loaded on a Device not in their region; or
- another Network Operator's Certificates have been incorrectly loaded on their own Devices

is a very small number.

This is in comparison to Suppliers that haven't yet put the Network Operator Certificates on the Device, post-commissioning. This causes the Network Operator slots to continue with the Supplier's Certificates or the DCC ACB Certificates present.

The Network Operator estimated that the solution put forward by this modification would only prevent incidences in 0.005% of their meter population. Taking this into account the Network Operator asked for clarity and statistics on the number of incorrect Network Certificates on Devices, as well as where Suppliers hadn't updated their pre-loaded Certificates in the Network Operators slot. This could then be used to assess the business case.

Cause of the issue

A Supplier noted that the issue put forward in this modification had only arisen in their early pilots of post-commissioning Devices and were sure that they are not one of organisations causing this issue now. They added that some Independent Distribution Network Operators (IDNOs) haven't created SMKI credentials, making it impossible for Suppliers to fulfil their post-commissioning obligations. This was noted as an opportunity to improve the information available to Suppliers on SMKI Certificates as a preventative measure.

An Other SEC Party believed this modification should focus on preventing the issue from happening in the first instance. However, a Network Operator advised the solution proposed by this modification is the earliest point in the post-commissioning process that could stop incorrect Network Operator Certificates from being loaded on Devices.

Rectifying Certificates already incorrectly loaded on Devices

Some Network Operators' systems have the capacity to allow them to replace Certificates when their Certificates have been incorrectly loaded on a Device outside of their region. However, not all Network Operators' can do this, and the Proposer of this modification confirmed they are one of those organisations. Another Network Operator confirmed that they themselves are using the workaround and that at least one other Network Operator is using it as well.

The Proposer is opposed to view that all Network Operators should be able to facilitate the workaround as they shouldn't have the authority, not should they be expected to, change Certificates on a Device in a region of another Network Operator.

A Supplier advised that the Department for Business, Energy and Industrial Strategy (BEIS) had designed the Smart Meter Implementation to programme to facilitate the workaround and questioned why SEC Parties should be expected to pay for a modification if there is already a workaround in place.

Taking this into account, the Working Group suggested the Refinement Consultation ask:

- If SEC Parties should be required to pay the DCC to update their systems to validate Network Operator Certificates; or
- If Network Operators should pay to upgrade their own systems in order to accommodate the workaround already in place.

Next steps

The Working Group agreed that this modification is not yet ready to progress to a Refinement Consultation. Statistics on incorrect Network Operator Certificates are needed for Parties to assess the scale of the issue and ultimately, the business case for the modification.

Actions

- DCC to investigate and provide statistics on the number of incidences of incorrect Network Operator Certificates being placed on Devices.