This document is classified as **Amber**. Disclosure is limited and restricted to SSC Members and those who have a need to know in order to take action. SSC Members representing a Party Category may share the information with other organisations within that Party Category but only on a 'need-to-know' basis.

Paper Reference:	**SSC_80_2606_12**
Action:	**For Discussion**

SSC Guidance on Device Triage: Resetting the HAN

1. Purpose

To obtain SSC approval to issue guidance for energy Suppliers and Device manufacturers on re-setting the Home Area Network (HAN) for Devices where installation has been aborted for a variety of reasons and the Devices would otherwise be scrapped.

The SSC agreed to sponsor guidance for industry once an agreed method was reached. An agreed method has been developed in a series of Working Groups and has been refined by the BEIS led Technical Specification Issue Resolution Sub-Group (TSIRS) and has been approved by NCSC and BEIS.

2. Background

SEC Modification SECMP0013 aimed to provide a facility for a Supplier (or their appointed sub-contractor) to 'reset' meters that have encountered problems during installation to enable them to be re-used without the cost of replacing them.

At the CPA Industry day on 28 February 2019, Suppliers and Device manufacturers agreed that this was an industry wide problem that can often occur mid-installation and which hinders the ability to complete an installation once started due to e.g. system outages (DCC or energy supplier); intermittent HAN or WAN; long installation time leading to customer refusal; or other faults or issues meaning installation and commissioning can't be completed.

Once the commissioning process on the Device begins, data accumulates on the meter which means that it cannot be reinstalled without work to remove the data. In addition, meters don't have the means to reset HAN information and will therefore not join to a new HAN and so the meter is prevented from being installed and firmware cannot be upgraded via the Service Request via the DCC.

Suppliers have therefore defined a valid business requirement for Device triage to be the equivalent of a "factory reset" to allow meters to be reinstalled.

3. SEC obligations

The SEC places a range of obligations on the SSC in SEC Sections G7.18 to G7.25 that relate to monitoring and addressing security risks and to providing advice on security matters. Of particular relevance in the case of Device triage are G7.19 (c) and (f):

G7.19 The Security Sub-Committee shall:

(c) maintain the Security Requirements to ensure that it is up to date and at all times identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Assessment;

(f) liaise and work with the NCSC to develop and maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs and HCALCs that are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment.

The Security Requirements v0.9 contain eleven specific security controls that relate to Smart Meter Requirements. These security controls are reflected in the CPA Security Characteristics (SCs).

The SSC therefore has a legitimate role arising from the SEC obligations to advise on a secure means of providing Device triage that does not compromise the Security Requirements or the CPA Security Characteristics (SCs).

4. Working Group Consideration

The Working Group considered four use cases that need to be supported:

Use Case 1: The ability for the meter to connect to a new HAN as a new Device;

Use Case 2: The ability to update security credentials (but only those that can be through DCC SRs);

Use Case 3: The ability to update the Firmware; and

Use Case 4: The ability to protect any granular consumption data.

The Working Group output is at Annex 1 and provides clarity the basis for SSC guidance on Use Case 1, setting out a possible process that can be achieved through guidance rather than requiring a regulatory change. It was assumed that Use Cases 2, 3 and 4 will be undertaken on installed meters in consumer premises using the normal DCC Service Request routes and, as such, no guidance is required for these Use Cases.

5. Findings

The findings conclude that it is possible, within the security controls for a Supplier or a manufacturer acting on behalf of the supplier, to re-set a Device into a state that allows installation, following a previous aborted or failed installation and a method has been agreed with industry.

It is considered feasible to modify the data on the meter to enable installation, but these data items must not include the Device's current private keys, SMKI Organisation Certificates or firmware. The

method is to use a non-GBCS command delivered through an external interface, which may or may not be a GBCS-defined one but will have a physical restriction to limit its use to local access only. The method requires access control to protect against unauthorised use of the command and have a high level of protection in line with general good industry security practice, with documented manufacturer rationale to justify why this is the case and to explain why the associated procedural controls cannot be trivially defeated or bypassed which a CPA Evaluation Facility can assess and, if satisfied with the rationale, endorse.

It may be acceptable for the access control mechanism described to be performed via a separate 'unlock' command received beforehand that then allows the "Reset HAN" command and other non-security impacting commands (e.g. requesting diagnostic information) to then be performed over the interface without any need for access control protection to be performed on each of these subsequent commands. However, if such an "unlock" approach is used, the meter must implement a mechanism that automatically ensures that it reverts back to a normal "locked" state (i.e. requiring access control to then be re-performed via the "unlock" command before the "Reset HAN" command can be accepted again), prior to leaving the refurbishment facility and this too will be assessed by a CPA Evaluation Facility.

The meter must only modify a minimal amount of its data to release any previous HAN association. This is to avoid unexpected side-effects on other SC-compliant functionality. If the manufacturer is unclear about the impacts made to their specific implementation to accommodate such functionality, they should discuss the impact of the changes with a CPA Evaluation Facility.

This method is restricted to resetting the Device to remove its link to the previous HAN to enable it to be re-installed. Any other type of triage or refurbishment will need a compelling Use case for further consideration by NCSC, BEIS and SSC. SSC guidance is needed to communicate the method to Suppliers, manufacturers and CPA Evaluation Facilities and others e.g. MAPs.

6. Recommendation

The SSC is now requested to:

- **APPROVE** the method agreed by TSIRS, NCSC, and BEIS to allow Device triage by re-setting the HAN;
- **APPROVE** the production of 'AMBER' SSC guidance to communicate the method to Suppliers, manufacturers, CPA Evaluation Facilities and other parties with a need to know;
- **NOTE** that the method can be implemented without any changes to the Security Requirements or the CPA Security Characteristics or to the SEC.

Gordon Hextall

SSC Chair

19 June 2019

Annex 1: Final paper from TSIRS, approved by NCSC and BEIS

Requirements to re-use SMETS2 meters that have been returned to the supplier during / or following commissioning

Overview

The objective of this paper is to define the requirements on a SMETS2 meter to support an energy supplier re attempting further installations of a previously used meter ('previously used' refers to having been connected to a live comms hub).

Meters which don't have the means to reset HAN information will not join to a new HAN and so the meter is prevented from being installed or firmware upgraded via the SR/ DCC route.

This requirement has been highlighted by several suppliers who have aborted installation or commissioning due to system outage/ consumer issues/ delays during or shortly after installation.

At the current time there are significant numbers of these types of returned meters accumulating in suppliers' facilities which are expected to be capable of reuse.

There are four use cases that were discussed at the recent BEIS/ UKMF/ NCSC meeting that need to be supported:

1. The ability for the meter to connect to a new HAN as a new Device
2. The ability to update security credentials (but only those that can be through DCC SRs)
3. The ability to update the Firmware
4. The ability to protect any granular consumption data

Currently there is no clarity on how/ where 1 can be undertaken, and this paper sets out a possible process that (if approved) would be reflected in some form of guidance rather than any regulatory changes. The working assumption (also reflected below) is that 2, 3 and 4 will be undertaken on installed meters in consumer premises using the normal DCC SR routes. As such no further consideration/ guidance is required for these use cases.

Assumptions

The following assumptions are applicable to these requirements:

1. Any resetting for "re-use" is only undertaken in a supplier or manufacturer facility, rather in at a consumer site – with mechanisms in the product that help to enforce such resetting to only be possible at the aforementioned facilities.
2. Suppliers will be required to send appropriate "decommission" SRs to DCC once the meter has been removed from an installation at a consumer premises
3. Suppliers will be able to reinstall meters without the need to modify the meter's own key material or the organisation certificates retained in the meter memory, when removed from the consumer premises due to aborted installations (as opposed to faulty behaviour identified in the meter).
4. Suppliers will process any firmware upgrades required once the meter has been installed and commissioned to the new premises.
5. This paper will form the basis of NCSC drafted guidance for industry (test houses, manufacturers and energy suppliers) to ensure a consistent CPA approach
6. No changes to SC 1.2 or SC 1.3 envisaged at this point.

Meter functionality to support supplier reuse

The meter may incorporate a mechanism that enables the supplier or manufacturer (on behalf of the supplier), to set it into a state that allows installation, following an aborted or failed installation. It is anticipated that one or more persistent data items in the meter will need to be modified (e.g. reset) to achieve this however, but these data items are not expected to include the device's current private keys, organisational certificates or firmware. To achieve this there could be a non-GBCS command (other approaches may be possible too, e.g. use of the meter's user interface, but these are beyond the scope of this paper), which:

- Gets delivered through an external interface, which may or may not be a GBCS-defined one but will have some sort of physical restriction to limit its use to local access only
- Requires, as a first step, some form of access control check to have been successfully performed in order to protect against unauthorised use of the command. The following must be considered:
    1. The level of protection should be in line with general good industry security practice, with manufacturer rationale to justify why this is the case and why, for instance, the access control mechanism, and associated procedural controls, cannot be trivially defeated or bypassed (which a CPA Evaluation Facility can assess and, if satisfied with the rationale, endorse). Where manufacturers are unclear as to whether their planned solution meets the guidance in this document, this can be discussed with a CPA Evaluation Facility, with NCSC also being involved in such discussions if necessary.
    2. The "authentication value" used to authenticate the command either with the command or shortly prior to the command being provided, (see Note: below) must vary from meter to meter i.e. it must not be possible to re-use the authentication value for one meter in other meters or modify the value in a trivial manner to enable the same outcome (such as by changing part of the value that relates to a unique identifier value that is printed on the device). Note: This does not necessarily mean the meter has to have its own unique key material.
    3. Possible approaches for such an access control mechanism may include use of manufacturer key material (asymmetric or symmetric) with existing GBCS-defined cryptographic mechanisms. Other approaches may be possible too and could for instance include the use of non-GBCS defined cryptography. In all cases, the CPA Evaluation Facility (in coordination with NCSC) will need to be satisfied that the properties of the access control mechanism meet the general requirements of this paper.
       Note: As alluded to above (in point 2), it may be acceptable for the access control mechanism described to be performed via a separate command received beforehand (some type of "unlock" command) that then allows the "Reset HAN" command and other non-security impacting commands (e.g. requesting diagnostic information) to then be performed over the interface without any need for access control protection to be performed on each of these subsequent commands. If such an "unlock" approach is used, the meter must implement a mechanism that automatically ensures that it reverts back to a normal "locked" state (i.e. requiring access control to then be re-performed via the "unlock" command before the "Reset HAN" command can be accepted again), prior to leaving the refurbishment facility.
- If the access control checks in the preceding point are successful, the meter can then proceed to perform the "Reset HAN" functionality with the following result:

1. The meter is left in a condition whereby any ‘join network’ functionality in the meter application will be re-enabled or allows the normal join procedures to be activated. Either way its resultant state will be compliant with GBCS expectations, in which one such state could be that defined by the ZigBee Stack Specification “05-3474” (e.g. revision 22), section 3.6.1.4.1.
2. This reset can be performed regardless of whether or not the meter had been decommissioned with the DCC before it was removed (to allow for instances where the meter was removed in an uncontrolled manner).

Note: The meter should only modify a minimal amount of its data to release any previous HAN association. This is to avoid unexpected side-effects on other SC-compliant functionality. If the manufacturer is unclear about the impacts made to their specific implementation to accommodate such functionality, they should discuss the impact of the changes with a CPA Evaluation Facility.

- Regardless of whether the above process succeeds, the attempt to perform a “Reset HAN” operation shall be treated by the meter as a tamper breach, with a security log entry being written and an attempt being made to send an alert.