Firmware Updates on Other HAN Devices

Options Paper

Comments in red throughout the document capture DECC input as per the Energy UK and DECC bilateral meeting on 24th June 2015. Comments in blue capture input from the TSEG meeting on 26th June, specific to local firmware updates only.

1. Background

Energy UK has carried out work to understand the supplier requirements for the management of firmware updates. This is a key area where there still remains a number of unanswered questions, including how the end to end updates process will work and be governed as described in SEC and the Programme's Technical Specifications[1]. Energy UK is working with DECC to produce a firmware management Design Note to help its members (and Programme stakeholders) understand the detail and expectations of how this process will work.

A key facet of the process is the ability to update firmware on other HAN devices, which are not currently covered by the Programme's Technical Specifications – notwithstanding the point that the Technical Specifications are minimum requirements. Section 3 below covers the scope of the HAN devices referred to in this options paper, and section 4 captures a summary of the current Technical Specifications coverage.

It is important to understand the drivers: faults vs. enhancements. Are issues in the metering devices or is it an issue on the HAN devices (e.g. IHD). Is it an issue for interoperability? An update could be fixing an issue but may affect the interoperability going forward e.g. may break the certification (and will impact SMDA).

Need governance / control around updating firmware to other HAN devices, especially where for example there are 2 Suppliers on 1 IHD. Additionally, if the firmware update is required to be done via DCC then access control will be needed for these devices. Will also need to be explicit around supplier provided devices only and mandated ones.

The way forward (scope) should only cover:

- *mandated devices as per the Technical Specifications (i.e. it does not include CADs); and*
- *Supplier provided devices (i.e. it does not include consumer bought devices or devices not provided by the Supplier).*

2. Purpose

Energy UK and its members discussed these areas above in a firmware management workshop on 27th April 2015 and it was agreed that an options paper will need to be developed.

The purpose of this options paper is for:

a) Energy UK to share with DECC what suppliers believe are the potential options for ways of updating firmware on other HAN devices – these options are captured in section 5 below.

b) DECC to review these potential options to assess:

- their content and validity in terms of technical feasibility – this would include reasons for why the options would not work in terms of technical feasibility; and
- that they would work within the context of the current Technical Specifications, i.e. there is nothing that prohibits them for being used and/or they do not break any security model – this would include reasons for why they would not work within the

[1] This refers to Programme documents such as: SMETS2, CHTS and GBCS.

context of the current Technical Specifications and what changes are required to the options and/or the Technical Specifications to make them work.

The expectation is that this will involve DECC engagement with Energy UK and its members.

The output from the above will drive the next steps for Energy UK and its members with regards to defining the process and where that process should be covered (e.g. within the existing Technical Specifications) – section 6 captures the next steps.

3. Other HAN Devices in Scope

SMETS2 (v1.58) currently captures requirements for firmware updates to ESME and GSME. CHTS (v1.46) covers the CH firmware updates (including logical devices CHF and GPF). This options paper deals with other HAN devices – the scope for these is as follows:

- IHD;
- PPMID;
- HAN Connected (HC) ALCS; and
- CAD.

4. Technical Specifications Coverage Summary

In summary, firmware coverage in SMETS2 (v1.58) is as follows:

SMETS2 Section	SMETS2 Section Reference				
	GSME	ESME	PPMID	HCALCS	IHD and CAD
Physical Requirements	4.3	5.4/5.10/5.16	7.3	8.3	No coverage
Security	4.4.10	5.5.11	7.4.7	8.4.4	No coverage
Activate Firmware	4.5.3.2	5.6.3.2	No coverage	No coverage	No coverage
Receive Firmware	4.5.3.15	5.6.3.18	No coverage	No coverage	No coverage

Additionally, CHTS (v1.46) covers buffering (4.4.4), security (4.4.6) and the commands for activating CH Firmware (4.5.1.1) and receipt of CH Firmware (4.5.1.8). The GBCS and DCC documentation are aligned to SMETS2 and CHTS.

5. Potential Options for Firmware Updates on other HAN Devices

This section cover the potential options for updating firmware on other HAN devices, the subsections below cover each device type separately and the potential options associated with it.

5.1. IHD

The following table captures the potential options for updating firmware on an IHD:

Option	Description
1	This aims to align to the Technical Specifications and has the following steps: a) Supplier uses the Distribute Firmware command to direct the firmware image to the IHD GUID (the IHD would need to have the ZSE OTA Client). b) Supplier receives response from IHD confirming receipt of firmware – this would require the IHD to be designed and built with communications functionality similar to PPMIDs. c) Supplier sends the Activate Firmware command to the IHD GUID. d) Upon receipt of the Activate Firmware command, the IHD performs the activation.

	The IHD would need to become a Client to receive the command and would need to have keys to verify the commands. IHDs would need to have business processes to cover the E2E process. Would need a DCC change and Tech Spec change (CHTS / SMETS2).
2	This aims to align to the Technical Specifications and has the following steps: a) Supplier uses the Distribute Firmware command to direct the firmware image to the IHD GUID (the IHD would need to have the ZSE OTA Client). b) Supplier receives response from IHD confirming receipt of firmware – this would require the IHD to be designed and built with communications functionality similar to PPMIDs. c) Supplier uses the Display Message command to the ESME to send the text ''*activate firmware hash*'' which will include the value of the hash for the IHD[2] – this assumes 1 IHD at the customer's premises. d) Upon receipt of the Display Message command, the IHD performs the activation – the ESME would be a trusted source for the IHD. *This would break the security model as it proposes the use of a non-critical command.*
3	IHDs to be designed and built with hardware for security chips (covering up to 2 supplier certificates) that allow the standard firmware process as defined in the Technical Specifications – this is expected to be a commercial process. *This is needed to enable option 1 – not an option on its own right. If you need access control through DCC then you need this.*
4	IHDs to be designed and built with communications functionality similar to PPMIDs. *This is needed to enable option 1 – not an option on its own right. If you need access control through DCC then you need this.*
5	Use of Wi-Fi to enable an internet connection to download and activate the firmware image – this would require a Wi-Fi chip and/or a physical interface to allow the internet connection and assumes that the customer has an internet connection and Wi-Fi Router. *Need detail / process around this; steps need to be articulated. 2 potential options for non-DCC comms:* • *Proactive: device looks after itself and periodically checks a URL for new updates.* • *Reactive: someone triggers the update to the device.* *Questions: how is the device connected to internet? Is it connected?* *Smartphones (e.g. Samsung) are proactive in their approach. Consumer consent needs coverage – the customer may be content with the existing functionality, and the supplier is providing the device to the customer – so shouldn't the customer have a choice as to update the firmware or not?*
6	Attend a site visit to the customer's premises to either locally update the firmware or swap the device – this is a costly approach as it is a strain on logistics and field resource. *Derivative of option 5 – firmware being delivered by non-DCC route. Or return device to manufacturer.* *Discussions at TSEG 25th June meeting concluded that there does not appear to be any security implications by allowing local upgrades via local means such as a premise visit or asking tech-savvy customers to connect a device to a computer etc…. . This appeared to be the best stop-gap solution until OTA upgrades could be made available via the DCC.*

Others points for consideration within the context of this IHD section:

- The SEC obligation for IHD firmware is on the installing supplier; the current supplier will need to ensure interoperability. Additionally, as there will be scenarios where 1 IHD can have 2 suppliers connecting to it, a lead supplier may require definition for the process – governance around this will be required. *Potentially could be via a Supplier to Supplier agreement.*

[2] This is to ensure the IHD is activating the right firmware image.

- There is a view that IHD manufacturers are often more agile in their development of firmware compared to meter manufacturers. When issues with IHDs were identified in the Foundation stage of the roll-out, it appeared quicker / more efficient to get the IHD manufacturer to change its device firmware than it was to try to get the meter manufacturer to do the same process for its meters. The current requirements in SMETS2 result in this benefit not being there. *We need to make sure we are not deviating from the standards.*
- Dealing with third party provided IHDs, i.e. IHDs not provided by the supplier of electricity and/or gas at the customer's premises – an example of a third party could be an independent energy management organisation or where an IHD may have been bought by the customer directly from a retail shop. *Must be out of scope for the DCC option*
- The IA benefits in relation to the impacts of consumer behaviour if the industry does not have a fit for purpose firmware update process.
- The Firmware Version will need to be held on the DCC Inventory and mapped to this device type – it may also need to be held on the device. *Dependent on the chosen option*

5.2. PPMID

The following table captures the potential options for updating firmware on a PPMID:

Option	Description
1	This aims to align to the Technical Specifications and has the following steps: a) Supplier uses the Distribute Firmware command to direct the firmware image to the PPMID GUID (the PPMID would need to have the ZSE OTA Client). b) Supplier receives response from PPMID confirming receipt of firmware. c) Supplier sends the Activate Firmware command to the PPMID GUID – this would be a Non-Critical command as the PPMID does not have the supplier certificate. d) Upon receipt of the Activate Firmware command, the PPMID performs the activation. *This is slightly different to the IHD in that it is always a Supplier owned device. PPMID would need to become a Client to receive the command and would need to have keys to verify the commands. PPMIDs would need to have business processes to cover the E2E process. Would need a DCC change and Tech Spec change (CHTS / SMETS2).*
2	PPMIDs to be designed and built with hardware for security chips (covering up to 2 supplier certificates) that allow the standard firmware process as defined in the Technical Specifications – this is expected to be a commercial process. *This is needed to enable option 1 – not an option on its own right. If you need access control through DCC then you need this.*
3	Use of Wi-Fi to enable an internet connection to download and activate the firmware image – this would require a Wi-Fi chip and/or a physical interface to allow the internet connection and assumes that the customer has an internet connection and Wi-Fi Router[3]. *Need detail / process around this; steps need to be articulated. 2 potential options for non-DCC comms:* • *Proactive: device looks after itself and periodically checks a URL for new updates.* • *Reactive: someone triggers the update to the device.* *Questions: how is the device connected to internet? Is it connected?* *Smartphones (e.g. Samsung) are proactive in their approach. Unlike the IHD, consumer consent may not need coverage for a PPMID as it is a Supplier owned device.*
4	Attend a site visit to the customer's premises to either locally update the firmware or swap the device – this is a costly approach as it is a strain on logistics and field resource.

[3] It is possible that this introduce an additional security vector that needs consideration, particularly as the PPMID has elevated command privileges on the HAN when compared to a type 2 device.

	Derivative of option 3 – firmware being delivered by non-DCC route. Or return device to manufacturer. *Discussions at TSEG 25th June meeting concluded that there does not appear to be any security implications by allowing local upgrades via local means such as a premise visit or asking tech-savvy customers to connect a device to a computer etc…. . This appeared to be the best stop-gap solution until OTA upgrades could be made available via the DCC.*

Others points for consideration within the context of this PPMID section:

- The SEC obligation for PPMID firmware is on the installing supplier; the current supplier will need to ensure interoperability. Additionally, as there will be scenarios where 1 PPMID can have 2 suppliers connecting to it, a lead supplier may require definition for the process – governance around this will be required. *Potentially could be via a Supplier to Supplier agreement*
- Dealing with third party provided PPMIDs, i.e. PPMIDs not provided by the supplier of electricity and/or gas at the customer's premises – an example of a third party could be an independent energy management organisation or where a PPMID may have been bought by the customer directly from a retail shop. *Out of scope for the DCC option*
- The IA benefits in relation to the impacts of consumer behaviour if the industry does not have a fit for purpose firmware update process.
- The Firmware Version will need to be held on the DCC Inventory and mapped to this device type – it may also need to be held on the device. *Dependent on the chosen option*

5.3. HC ALCS

The following table captures the potential options for updating firmware on a HCALCS:

Option	Description
1	This aims to align to the Technical Specifications and has the following steps: a) Supplier uses the Distribute Firmware command to direct the firmware image to the HCALCS GUID (the HCALCS would need to have the ZSE OTA Client). b) Supplier receives response from HCALCS confirming receipt of firmware. c) Supplier sends the Activate Firmware command to the HCALCS GUID – this would be a Critical command as the HCALCS has the supplier certificates. d) Upon receipt of the Activate Firmware command, the HCALCS performs the activation. *HC ALCS has security credentials that allows it to validate GBCS commands from its Supplier (this point TBC by DECC).*
2	Attend a site visit to the customer's premises to either locally update the firmware or swap the device – this is a costly approach as it is a strain on logistics and field resource. *Or return device to manufacturer.*

Others points for consideration within the context of this HC ALCS section:

- The ability to update firmware on a HCALCS will be material to load / heat control at customers' premises. This is further amplified into a critical process depending on the customer's geographical location. The consequences of not having this functionality relates to both the impact on the customer experience as well as electricity grid. *Simple device; can turn on or off. It is ZigBee certified and it is always based on what the ESME tells it (on or off; or for a period based on the ESME calendar). Unclear why it would need a firmware update.*
- The IA benefits in relation to the impacts of consumer behaviour if the industry does not have a fit for purpose firmware update process. *Not relevant based on the above comments.*
- The Firmware Version will need to be held on the DCC Inventory and mapped to this device type – it may also need to be held on the device. *Only relevant if DCC is doing something with it if a CR is proposed. Unclear why HC ALCS would need a firmware update as it is a*

simple device that just turns on or off. As above, it is works based on what the ESME tells it (on or off; or for a period based on the ESME calendar).

5.4. CAD

This is a placeholder for when the requirements are defined by DECC – this assumes DECC will define the requirements.

Currently work-in-progress within DECC to provide for CADs. There is a distinction between Supplier provided devices and other devices. Unlikely that there will be explicit requirements defined for CADs but more likely to be a tweaking to the IHD requirements to cover CADs functionality – DECC's work is around the presentation of information to the customer rather than the method to present the information.

6. Next Steps

As captured in section 2, the finalised options paper will need socialising with DECC so that it reviews the options to assess their content and validity in terms of technical feasibility; and that they would work within the context of the current Technical Specifications. The DECC assessment / review would include reasons for why the options would not work in terms of technical feasibility or within the context of the current Technical Specifications and what changes are required to the options and/or the Technical Specifications to make them work. The expectation is that this will involve DECC engagement with Energy UK and its members.

Energy UK and its members' consideration of the outcome of the above, in conjunction with DECC, will define the approach going forward. This may include one or more of the following items to ensure the appropriate coverage of firmware updates to other HAN devices:

- Raising a defect with the Technical Specifications.
- Raising a change request to the Technical Specifications.
- Updating the Design Note for Firmware Management to reflect an agreed (guidance) process.

Expectation is that a CR would be raised to cover IHDs and PPMIDs aligned to option 1 for both – this would cover Supplier provided devices only.