SECMP0007 ‘Firmware updates to IHDs and PPMIDs’

Gemserv

What is the issue?

- The Proposer seeks to include the capability to update firmware Over-The-Air (OTA) for mandated HAN devices via the DCC's infrastructure.

- The technical specifications (namely SMETS2, CHTS, GBCS and CPA Security Characteristics) currently capture OTA firmware updates via the DCC to the Comms Hub, ESME and GSME only. Requirements for OTA firmware updates to mandated HAN devices are not captured.

- The Proposer seeks to amend the technical specifications to include the capability to update firmware using OTA for mandated HAN devices (IHD, PPMID, HCALCS).

Working Group consideration of

Solution options and the DCC Preliminary Assessment

Option 1 – Original Approach

- This option involves a mechanism to deliver the firmware images to the PPMID, HCALCS and the IHD HAN devices, using Zigbee OTA delivery.

- The Comms Hub is to manage the activation of firmware and the notification to the Service User upon activation.

- This will require a new Service Request.

Option 2 – Extend Proven OTA Firmware Method

- This approach involves creating a type 1 IHD and extending PPMIDs, HCALCS, and the new type 1 IHD to support firmware distribution in a manner that would be similar to ESME firmware distribution and activation using GBCS critical commands.

- This will require CPA approval of the new IHD/PPMID device which will in turn increase device cost, and was something that Option 1 is designed to avoid.

- A further variation that may need to be considered is a prompt to the user to plug a battery powered device into the mains supply while a firmware image is transferred and activated.

DCC implementation timescales

- Implementation of this change is assumed to follow a waterfall methodology. The DCC assume that this change will be implemented as part of the June 2020 release alongside other change requests and the lifecycle duration is expected to take between 6 and 12 months.

- However this duration will be confirmed as part of an Impact Assessment.

Costs (up to the end of PIT)

- Option 1 – £12.3 million
- Option 2 – £8.5 million
- The fixed price cost for a Full Impact Assessment is £112,434, and is expected to be completed in 40 Working Days.

Working Group views on

Option 1 – Benefits and drawbacks

Option 2 – Benefits and drawbacks

General SEC Objectives

Views against SEC Objectives

- The Proposer believes that this modification better facilitates SEC Objectives (a), (c), (d) and (f) by:

- **a**) Provides a fit for purpose, efficient and effective process for updating firmware on the IHD, PPMID and HCALCS. It would additionally allow Suppliers to avoid unnecessary costs relating to replacement of devices and site visits, thus helping to ensuring the sustainability of devices for the longer term.

- **c**) Allows consumers to better manage their energy usage by having sustainable most-up-to-date devices that provides them with energy related information.

- **d**) Allows Suppliers to use a fit for purpose, efficient and effective process for updating firmware on the IHD, PPMID and HCALCS – this process would be consistent between all Suppliers as well as aligned to the process for updating firmware on the ESME and GSME.

- **f**) The proposed solution would cover any potential security vulnerabilities on the IHD, PPMID or HCALCS that may need be addressed using a fit for purpose, efficient process.

General SEC Objectives

- (a) facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain;
- (b) enable the DCC to comply at all times with the General Objectives of the DCC (as defined in the DCC Licence), and to efficiently discharge the other obligations imposed upon it by the DCC Licence;
- (c) facilitate Energy Consumers' management of their use of electricity and gas through the provision to them of appropriate information by means of Smart Metering Systems;
- (d) facilitate effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy;

General SEC Objectives

- (e) facilitate such innovation in the design and operation of Energy Networks (as defined in the DCC Licence) as will best contribute to the delivery of a secure and sustainable Supply of Energy;
- (f) ensure the protection of Data and the security of Data and Systems in the operation of this Code;
- (g) facilitate the efficient and transparent administration and implementation of this Code; and
- (h) facilitate the establishment and operation of the Alt HAN Arrangements.

Next steps

Thank you for listening

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS

SECMP0024 ‘Enduring Approach to Communication Hub Firmware Management’

Gemserv

What is the issue?

- Due to the lack of a process for Comms Hub firmware update management, that there is currently a significant risk that a Comms Hub firmware update with defects could be deployed and activated to significant numbers of Comms Hubs.

- A range of issues could arise from a DCC deployed firmware update occurring concurrently with:
  - A programmed configuration change to a Supplier's smart metering Device e.g. a CoS event, price change, or tariff change;
  - A Supplier's scheduled firmware deployment to a smart metering Device;
  - Historical consumption data being uploaded to Supplier systems on behalf of the consumer; or
  - A consumer attempting to interface with the Smart Metering System (e.g. a delay in a prepayment top-up).

What is the proposed solution?

- To develop and implement an agreed enduring process for the deployment and activation of Communications Hub firmware updates.

- This would see Suppliers;
  - being informed by the DCC when Communications Hub firmware updates are available; and
  - allow them to specify the date and time, within a period defined by the DCC, when these are deployed.

What are the impacts?

- Suppliers:
  - A coordinated approach to CH firmware upgrades would impact on small and large suppliers.

- DCC:
  - A coordinated approach to Comms Hub firmware upgrades would impact on the DCC and its CSPs.

Working Group feedback on

Business requirements

Business Requirements

Ref.	Requirement
1	The DCC will notify all relevant Users of a Communications Hub firmware update being available
2	The DCC shall trigger the firmware update to a ‘pilot group’ of Communications Hub prior to mass deployment
3	The Supplier(s) can choose to trigger the firmware update at an earlier date than the DCC’s specified deployment date
4	The DCC will update Suppliers regularly at different stages of firmware processing
5	If issues are identified with deployed firmware, the DCC shall investigate and determine whether to proceed with the roll-out

Solution variants

- The use of Service Requests on the DCC User Interface Specification (DUIS) Interface; and
- The use of a DCC operated Web Portal.

- All of the business requirements apply to both solution variants.

Sub-Committee views

TABASC comments

- The requirements follow a ‘happy path’ and don’t account for any exceptions that may arise. For example, if there is a Change of Supplier during deployment.
- A TABASC member advised he would like to see SLA’s in the requirements outlining the rules for Comms Hub firmware management, especially in dual supplier scenarios.
- ‘Responsible Suppliers’ have been referenced, however the requirements don’t account for where a single Party uses two IDs where they are both the electricity and gas supplier.
- TABASC would also like to see more context in regard to the option proposing a DCC operated web portal. TABASC preferred the web portal solution variant as they believed it would be quicker and easier for Parties to implement.

Security Sub-Committee comments

- From a security perspective, the SSC are happy with the requirements as they are and had no comments.

- The SSC requested that the DCC carry out a risk assessment in line with the Preliminary Assessment accounting for any possible exceptions that could occur during firmware deployment and activation scenarios.

Next steps

Thank you for listening

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS

SECMP0056 Working Group Meeting 3

SECMP0056 IHD/PPMID Zigbee Attributes Available on the HAN

Ali Beard

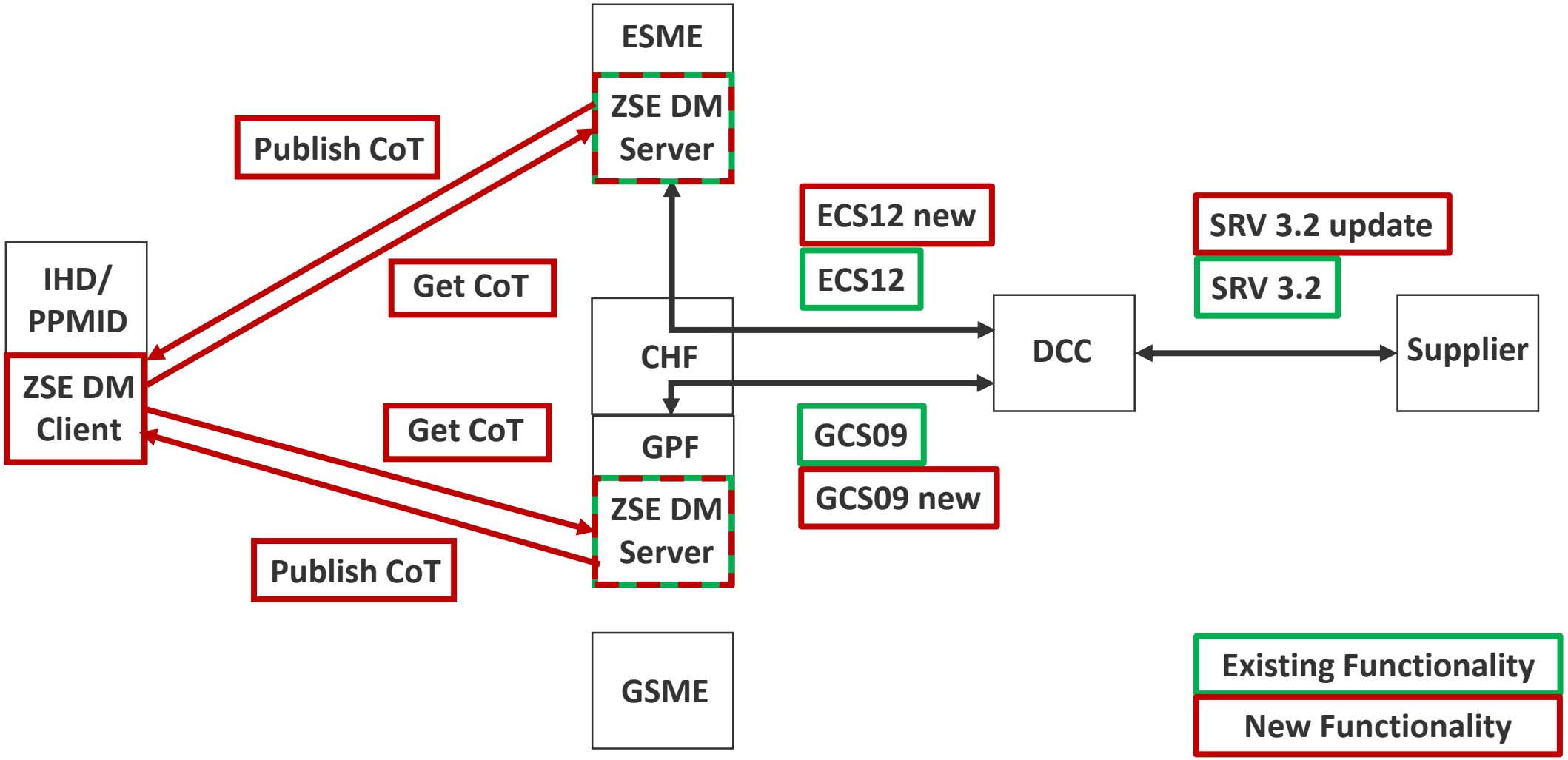
Gemserv

What is the issue?

Currently under the SEC, SMETS2 Type 1 and Type 2 devices specifically In-Home Displays (IHDs) and Prepayment Interface Devices (PPMIDs) are not notified of a Change of Tenancy (COT) or Change of Supplier (COS) event.

This could allow a new tenant to access the previous tenant's personal information and place the Supplier in breach of the General Data Protection Regulation (GDPR).

Proposed solution



Working Group consideration of

DCC Preliminary Assessment

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS

Preliminary Assessment

- DCC estimated timescales - 6-12 months, assumed to be implemented as part of the Jun 2020 Release
- DCC estimated costs - £1.3m (not including SIT and UIT)
- The fixed price cost for a Full Impact Assessment is £92,758 and is expected to be completed in 40 Working Days.

Working Group consideration of

Benefits and Drawbacks of the Modification

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS

Views against the SEC objectives

- a) Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain;
- b) Enable the DCC to comply at all times with the objectives of the DCC and to discharge the other obligations imposed upon it by the DCC License;
- c) Facilitate energy consumers' management of their use of electricity and gas through the provision of appropriate information via smart metering systems;
- d) Facilitate effective competition between persons engaged in, or in commercial activities connected with, the supply of energy;
- e) Facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy;
- f) Ensure the protection of data and the security of data and systems in the operation of the SEC;
- g) Facilitate the efficient and transparent administration and implementation of the SEC;
- h) Facilitate the establishment and operation of the Alt-HAN Arrangements.

Next Steps

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS