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.

SECMP0037 'Paring Local PPMIDs' and SECMP0038 'Sending Commands via PPMIDs'

Working Group Meeting

26 February 2019, 13:30 – 16:00, Gemserv's Offices

Meeting summary

SECMP0037 'Paring Local PPMIDs'

Results of the SSC SECMP0037 Risk Assessment

The Security Sub-Committee (SSC) advised that going forward it would be beneficial for all of the modifications raised by Utilita to be considered together rather than in isolation as they were all trying, in various ways, to address the same root problem.

SECMP0037 proposes to allow the Prepayment Metering Interface Device (PPMID) to join the Smart Meter Home Area Network (SM HAN), similar to a Hand-Held Terminal (HHT) and to remove the 60-minute time-out currently in place when joining a HHT to the SM HAN. The SSC confirmed the annual SSC risk assessment had stated that the removal of the 60-minute time-out would remove an important risk mitigation and would negatively impact on the security architecture of the Home Area Network (HAN) with potential wider implications, especially when considering the increased range of the HAN with 868 MHz and Alternative Home Area Network (Alt HAN) design proposals.

Considerations of the SSC SECMP0037 Risk Assessment

Despite the outcomes of the SSC risk assessment the SSC acknowledged that there was a genuine business need for a solution to the Proposer's issue that needed to be addressed via alternative solutions and wished to understand what the Proposer's overall business requirement would be. The Proposer confirmed that there had been scenarios where a Smart Meter installation had taken place but due to a loss in Wide Area Network (WAN) coverage following the installation, the PPMID was unable to be joined.

The purpose of the modification was to allow the PPMID to be connected to the Communications Hub without requiring engineer intervention. The Proposer confirmed that before they send an engineer, they would contact the DCC via an incident and then the DCC would attempt to resolve the problem remotely. If this was not possible then an engineer would need to be called out, which would be uneconomical to do every time there was an incident that couldn't be resolved remotely.

The Proposer confirmed there had also been thousands of cases where a replacement PPMID had to be sent out to customers due to the original device being lost or broken. In the case of no-WAN, top-up via the SM network is not possible. However, it is still possible for a consumer to top-up via the keypad of the still-paired PPMID when the user enters the UTRN.

The SSC confirmed the 60-minute time-out in place lowers the risks of rogue devices attempting connection to the ZigBee network and prevents against Denial of Service Attacks (DoS), bringing the threat of these activities down to a level within the risk appetite of the Smart Metering Implementation Programme. Additionally, there were potential risks involved with internet connected devices in general that the SSC confirmed they were aware of. SSC Members stated that removing the time-out would be akin to removing a single control that was acting as part of a wider ZigBee/WAN control centre to protect against rogue devices and this change would weaken the overall protections in place. It was noted that there would always be times threat actors would attempt testing of potential weaknesses via a physical attack, which if successful could affect a large urban area and ultimately the Grid.

The SSC highlighted that PPMIDs in their current technical capacity were not required to undergo Commercial Product Assurance (CPA), and neither were In-Home Displays (IHDs), but changes to these devices to allow them to encompass the same ability of a HHT, for example, would mean they would then be required to undergo CPA – which is time consuming and costly.

DCC obligations under no WAN scenarios

The Working Group discussed the DCC obligations where a No WAN situation was raised to them. Under SEC Section F7.18 it states that the DCC shall within 90 days after having been notified in accordance with the Communications Hub Installation and Maintenance Support Materials, confirm that the SM WAN is now available or provide reasons as to why the SM WAN is not available. In the latter case the DCC must ensure that the SM WAN is made available in the relevant area for at least 99% of instances to allow the Communications Hub to be able to connect to the SM WAN.

SECMP0032 'Prioritising Prepayment Customers in No WAN Situations' proposes to reduce the 90-day period to 30 days. The DCC response to the modification provided an estimated cost of £1billion to reduce the 90-day window to 30 days, as alternative solution the DCC suggested the use of mesh Communications Hub technology. The Proposer pointed out that this alternative solution would only work if all neighbouring Communications Hubs to the affected Communications Hub were under the same Supplier. The DCC suggested if neighbouring Communications Hubs belonged to a different Supplier then the affected Supplier could contact the DCC. In turn the DCC would then be able to contact the neighbouring Communications Hub Supplier owners and suggest the installation of a mesh Communications Hub.

The DCC added that progress was being made to reduce the Radio Frequency noise problem which, once resolved could mean that the 1% of WAN coverage that cannot be remedied may be reduced further.

The Proposer advised there were network improvement plans in place, but no deadlines attached when there was a requirement for an immediate resolution. Working Group members advised that the take up of prepayment was expected to increase with time and there was a significant concern that the customer could be building up an unsurmountable level of debt.

Members of the Working Group pointed out that improvements and re-assurance of the SM-WAN coverage to Suppliers will greatly reduce the need for the measures proposed in SECMP0032,37 and 38.

SECMP0038 'Sending Commands via PPMIDs'

Considerations of the Gemserv Ltd Risk Assessment

The SSC had requested a risk assessment to be carried out by an external company in order to evaluate the risks posed by different solutions. Gemserv Ltd presented the risk assessment results to the Working Group confirming that the assessment was based solely off the proposed solutions and deliverables provided to them.

Gemserv Ltd confirmed they had identified 98 risks, of which 46 were Unique Risks, 8 were considered High Risks, 13 Moderate Risks and 24 Low Risks. This risk score is a factor of threat capability and cumulative scores for the likelihood and impacts of the risk materialising. A critical risk was deemed to impact the whole smart metering infrastructure or end-to-end operation and a High risk is deemed to impact significant components of the infrastructure or its sub services due to risks arising from the breach of multiple Smart Metering Home Area Networks.

Whilst the Gemserv Ltd risk assessment highlighted that 'Deliverable 3' posed the highest risks, there was debate amongst the Working Group whether this was accurate. However, the majority of the Working Group agreed that 'Deliverable 3' and 'Deliverable 4' were not relevant as they were already in existence and posed the lowest threats out of the four.

The SSC raised concerns over the level of security risks the assessment had captured as they thought these mainly focused on availability rather than security. The Working Group agreed that the emphasis of the risk assessment, and subsequent meeting in which it would be reviewed, should be placed on understanding the feasibility of achieving 'Deliverable 1', with 'Deliverable 2' being considered a 'nice to have'.

Alternative Solutions to no WAN scenarios for PPMIDs

The Working Group discussed various methods of resolving the issue via alternative means:

Change to Communications Hub	Change to the ESME/GSME	Firmware/App	Changes to WAN infrastructure
Add a button onto the Communications Hub that will allow connection to the PPMID at any time.	Add Bluetooth to the ESME or GSME to allow connection to a mobile telephone removing the need for a separate interface (PPMID).	Without changing hardware, which could be timely and costly a firmware upgrade could be undertaken that allows the Communications Hub and PPMID to connect remotely.	Use Repeaters to amplify the WAN signal to and from target devices.
Remove the 60-minute window and add a five-minute access window at alternating times in a 24-hour period to allow connection when the WAN does come back.	Add Near Field Communication (NFC) capability to the ESME or GSME to allow connection to a mobile telephone removing the need for a separate interface (PPMID).		Use mini base stations to provide WAN-connections in hard to reach areas in the Telefonica Central and South regions.

Actions

- SSC Members to review the SECMP0038 'Sending Commands via PPMIDs' Gemserv Ltd risk assessment and provide feedback at the next joint Working Group meeting.
- Gemserv Ltd to reissue updated slides detailing the Gemserv Ltd risk assessment and present to the SSC in a separate meeting.
- SECAS to begin work on developing a 'Problem Statement' to encompass the reasoning behind why modifications SECMP0031 'Adding UTRN Functionality to SMETS', SECMP0032 'Prioritising Prepayment Customers in No-WAN Situations', SECMP0037 'Pairing Local PPMIDs' and SECMP0038 'Sending Commands via PPMIDs' were raised.