SECMP0007 Streamlining Meeting, 29th November

Attendees

[SECAS]; Joe Hehir, Alison Beard, Rainer Lischetzki

[Arqiva]; Tim Carey, Hannah Daniels, Sudnyesh Itraj, Andrew Woodcock

[CGI]; Steve Bull

[Telefonica]; Lydia Chung, Kevin Condliffe, Rich Hanks, Gary Oates, Vivek Ramani, Duncan Tytler

[DCC]; Vince Rawle, David Walsh

Agenda

SEC Panel Feedback

Review SECMP0007, CR211 Design (briefly)

Identify Items Causing Significant Cost and Duration – Why is this so hard?

Propose Design Changes for Review

DCC List of options

Expected Change Requests

Requirements That Expand Scope, Cost and Duration

Summary of all options is provided at the end of this document.

This section considers options to remove requirements that will impact design, development, and test.

Fragmented Firmware Images

Remove the requirement for fragmented Images by limiting firmware updates to 750KB only. Make 750K image update size an upper limit - if special screen features do it as a standalone OTA, or do multiple updates under 750K.

Limiting update size would reduce costs and effort in development (less error messages, less coding, reducing expected impact on suppliers), with significantly reduced costs in defining test cases and test execution. Risks go up as the number of blocks are increased, such as image corruption, requiring repeated image sending, and overwrites. As there is no retry mechanism for image transmission, there is reliance on the Service Users managing the image dispatch.

Note development is in the Comms Hubs to handle the two or more updates, not the CSPs.

Using ESME or GSME Blocks (Memory Slots) for Holding Updates

All the SPs prefer the use of a single block.

Telefonica noted that the use of both blocks will impact the technical architecture, but this isn't the driver of costs, it is the testing. The number of test cases will increase, and the behaviour when a new update arrives is more complicated.

There are also concerns about sleepy GSMEs. The availability of the slots is a minor concern, because ESME updates are relatively quick, and while GSMEs can take up to 4 days, they are available the rest of the time.

Future Dated Update Activation

Requirements for SECMP0007 state that a firmware update can be sent with an attribute to future date the firmware activation up to 30 days in the future.

Limiting the updates to immediate activation would minimally reduce costs and effort in DSP and CSP development (less error messages, less coding, reducing expected impact on suppliers), with significantly reduced costs in defining test cases and test execution over future activation. Risks go up as the activation date goes further into the future, with concerns such as image corruption, repeated image sending, and overwrites.

Comms Hub Logging of Updates

The requirements for SECMP0007 specifies the logging of up to 15 entries of actions on the Comms Hub relating to firmware updates.

The CSPs don't currently do any such updates so this will increase development and testing cost for them.

Note that the firmware versions can be read from the OTA header.

Remove IHDs from Scope

IHDs have no firmware version. CGI believe 95% of all deployed displays are PPMIDs - some of the remaining 5% are wrongly logged as IHDs and are in fact PPMIDs.

Note that the SMETS1 programme are only including PPMIDs in their updates.

Service Requests

We have been progressing the Full Impact Assessment with a design of using the existing Service Request 11.1 to manage PPMID / IHD / HCALCS firmware updates. However the SSC have introduced a new requirement to implement and run separate achieving separate ADTs for PPMID/IHD. We believe this is best achieved by a new Service Request 11.4; could use 11.1 but the cost to do this would outweigh 11.4. However both the cost and duration associated with creating a new Service Request is significant.

This change would be introduced as a Change Request on the Modification, as we have been working with assumption of re-using and updating SR11.1 since 26/9. Telefonica belive introducing a new SR would require a new API and would introduce new cost.

Reduce Alerts and Notifications

Suggestion that the Modification should be used as a transport mechanism only, rather than a way to deliver, monitor, and confirm the update. One SP had requested adding Alerts when a Comms Hub was "nearly" full

However there have been requests from Suppliers and Service Users that they want more information, such as diagnostics around firmware updates, so that the alerts can help improve systems and reliability.

Phased Delivery

To deliver an initial release as a transport mechanism with a subsequent later phase to deliver full functionality was not viewed favourably, because:

- Overall costs and duration would increase
- Time savings in developing a first phase are not expected to be that great
- Testing would have to be repeated

Arqiva have requested a new alert when FW image for any HAN device is deleted from CH without being activated.

Testing Approach

In general SIT is the longest time, but PIT and retests are the biggest cost for CSPs.

Limitation of only one firware version (one Release CR) in CSP Testing, but that firmware release could include multiple Change Requests or Modifications.

DCC recommended approach is to take these recommendations to TAG for their direction and clarification

More than Two Activities (e.g. variants) in Parallel

CSPs have stated that they can only test two firmware variants in the PIT environment at the same time. This extends the testing time for the expected number of device variants (16).

Current Test Sets, Dual Band and Single Band

Is there an option to create Test Sets that are feature rich and real meters in PIT; test in PIT with real devices and meters there - device isn't being changed.

Put All Devices in the Single Test Environment

Carry out device testing with fullest possible set of devices delivered to SEC Operations.

For Testing Devices, the SPs have only been able to use emulators. These aren’t as good and therefore require more testing than a real Device would. Also an issue if you start testing on an emulator and then the real device becomes available – do you take the risk and not test the real device or test it as well and increase cost/time?

Reduce Number of Test Cases (e.g., SKU1 and 2)

Could Regression be Planned and Reduced Based on New Capabilities?

CSPs are currently required to run full regression tests. Rather than regression testing all functionality, could regression be limited to only the new areas of functionality introduced by this Modification?

Value of this could be reduced if other Modifications and Change Requests are included in a SEC Release, and further functionality regression is required.

Reduce Device Variants, Reduce DUIS Versions

See the SECMP0080 proposal to remove support for DUIS 1 and DUIS 2 and to force users to move to DUIS 3 or later.

Discarded Options

Scrap Supplier-Specific Updates

One CSP suggested scrapping Supplier specific updates to make more efficient use of the WAN. This is not feasible as some Devices have Supplier specific branding

Allow Local Updates

As well as the previously discussed security concern, there is a real danger that updating the firmware locally will not update the DSP and will leave the device inventory out of sync with the devices on site.

Concerns with Local Updates to PPMIDs

1. How does the local firmware update of PPMIDs/IHDs get communicated back to the DSP? How does the local update get communicated to the Service User?
2. The Supplier is the only DCC User role allowed to read the firmware version of the device. A successful read of the PPMID/IHD firmware will allow to update the SMI exactly as it is done currently for meters. There is however no obligation on the Supplier to issue a Service Request to read the firmware version and this can lead to extended periods of mismatches between the active firmware on the PPMID/IHD and the firmware version recorded in SMI.
3. The SMI inventory will not have the correct Firmware version matching what is now on the device. We could implement "Read Firmware Version via the Comms Hub" where the Comms Hub will have to request the firmware version from the PPMID/IHD in intervals. Unless the Comms Hub keeps a record of the PPMID/IHD firmware this will result in an Alert each time the PPMID/IHD firmware is read. Local updates had been discussed (and rejected) at Working Group meetings and a daily check had been proposed. [Food for thought: Assuming one (1) firmware update per IHD/PPMID per year this means 364 unnecessary Alerts and one (1) meaningful Alert per year for every PPMID and IHD. Or assuming every premise in the UK has one PPMID or one IHD this equates to roughly 25 million of non-meaningful Alerts per day]
4. How is the update secured – how do we verify the person doing the local update is the correct person?
5. How can it be ensured that local firmware upgrades are restricted only to firmware versions listed on CPL?
6. How will the DSP handle a firmware read which contains a firmware version not listed on CPL?

Expected Change Requests

Change Requests for the following functionality are expected as part of this Modification.

1. Use new SR11.4 instead of 11.1. (SSC will accept 11.1 usage so long as PPMID update distribution can be distinguished)
2. ESME and GSME blocks
3. Volumetrics (numbers of PPMIDs and IHDs, profile over time, expected transactions per second, number of days storage for update images); CSPs would like to see these figures in terms of expected transactions per second, and numbers of days of storage for update images.

4. Working Group had requested the removal of the option to delete an update image from the Comms Hub if it had been there for 2 days.

Supporting Notes

Service Management needs more information provided as part of an incident response. Alerts will improve diagnostics, improve systems with better reliability. Suppliers have indicated they want more information regarding problems.

Summary

Table shows relative impacts of each scope change option, e.g., adding Comms Hub logging will add development, build, and test, while removing IHDs from scope will reduce development, build, and test

Requirements Impacting Scope, Cost and Duration			
Impact on Application Phase	Development	PIT	SIT and UIT
Fragmented Firmware Images	Medium	High	High
Using ESME or GSME Blocks (Memory Slots) for Updates	Medium	High	High
Future Dated Update Activation	Low to Nil	High	High
Comms Hub Logging of Updates	Medium	Medium	Medium
Remove IHDs from Scope	High	High	High
Service Requests	High-DSP only	Low	Medium
Reduce Alerts and Notifications	Medium	Low	Low
Testing Approach			
More than Two Activities (e.g, variants) in Parallel			Medium
Current Test Sets, Dual Band and Single Band			High
Put All Devices in a Single Test Environment		Medium	High
Reduce number of Test Cases (e.g., SKU1 and 2)		Medium	High
Regression Based on New Capabilities?		High	High
Reduce Device Variants, Reduce DUIS Versions		Low	High
Change Requests			
Use new SR11.4 instead of 11.1.	High-DSP only	Low	Medium
ESME and GSME blocks	Medium	High	High
Volumetrics		Low	Low
Remove option to delete an update image	Medium	Medium	Medium