

This document is classified as **Clear** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.



DP239

‘Enduring Solution for Resolving SMETS2 Device Certificate Misalignment Issue’

Modification Report

Version 0.2

8 August 2023

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary.....	3
2. Issue.....	3
3. Assessment of the proposal	6
Appendix 1: Progression timetable	8
Appendix 2: Glossary	8

Contact

If you have any questions on this modification, please contact:

Bradley Baker

020 7770 6597

bradley.baker@gemserv.com

1. Summary

This proposal has been raised by Ian Turner from E.ON.

As part of Post Commissioning Obligations, Suppliers and Wide Area Network (WAN) Providers are expected to update the Device certificate. This must be carried out within seven days following installation, via Service Request (SR) 6.17 'Issue Security Credentials' and Service Reference Variant (SRV) 6.15.2 'Update Security Credentials (Device)'. In some instances (estimated to be 120,000 Devices at the time the Data Communications Company (DCC) generated a report (March 2023)), the success response is not processed or not received by the Data Service Provider (DSP), resulting in a certificate misalignment between the Device and the DSP. This renders the Device incommunicable.

The Smart Energy Code (SEC) currently requires the Data Communications Company (DCC) to manually correct errors in the Smart Meter Inventory (SMI) where there is no other available method. Suppliers have indicated they would like an enduring solution to resolve the Device certificate misalignment issue without involving a manual SMI update.

2. Issue

What are the current arrangements?

Updating Device certificates

As part of SEC Post Commissioning Obligations, Suppliers and WAN Providers are expected to update the Device certificate (Electricity Smart Metering Equipment (ESME), Gas Smart Metering Equipment (GSME) and Gas Proxy Function (GPF) for Suppliers, and Communications Hub Function (CHF) for Communication Service Providers (CSPs)). This must be carried out within seven days following installation via SR 6.17 'Issue Security Credentials' and SRV 6.15.2 'Update Security Credentials (Device)'.

The DSP will only update the certificate upon receiving a successful response from the Device before a timeout occurs. This is 1,200 seconds (20 minutes) for ESME and 5,580 seconds (93 minutes) for GSME.

Device Processing of Service Requests

The DSP will transform all Service Requests to the appropriate Great Britain Companion Specification (GBCS) Use Case command, which contains a Message Authentication Code (MAC) generated by the DSP Access Control Broker (ACB) using the 'old' Device key. On receiving the GBCS Use Case command, the Device is expected to validate the MAC (with an exception for GBCS Use Case CS02d) using the "new" Device key.

What is the issue?

Overview

Device certificate misalignment will cause all Service Requests to fail on a Device, except for SRV 6.24.2 'Retrieve Device Security Credentials (Device)'. Therefore, the DCC User will be unable to communicate with that Device.

If the certificate is misaligned, MAC validation will fail and the Device will create a security Alert (for example, 8F3D or 8F1E). Due to this, the DCC User will not receive a Service Request response but will receive a timeout E21 error instead. The DCC User will only be able to send SRV 6.24.2 'Retrieve Device Security Credentials (Device)' to the Device.

It appears that for some of these Devices, the SRV 6.15.2 successfully executes on the Device, however the success response is not processed by the DSP for reasons including:

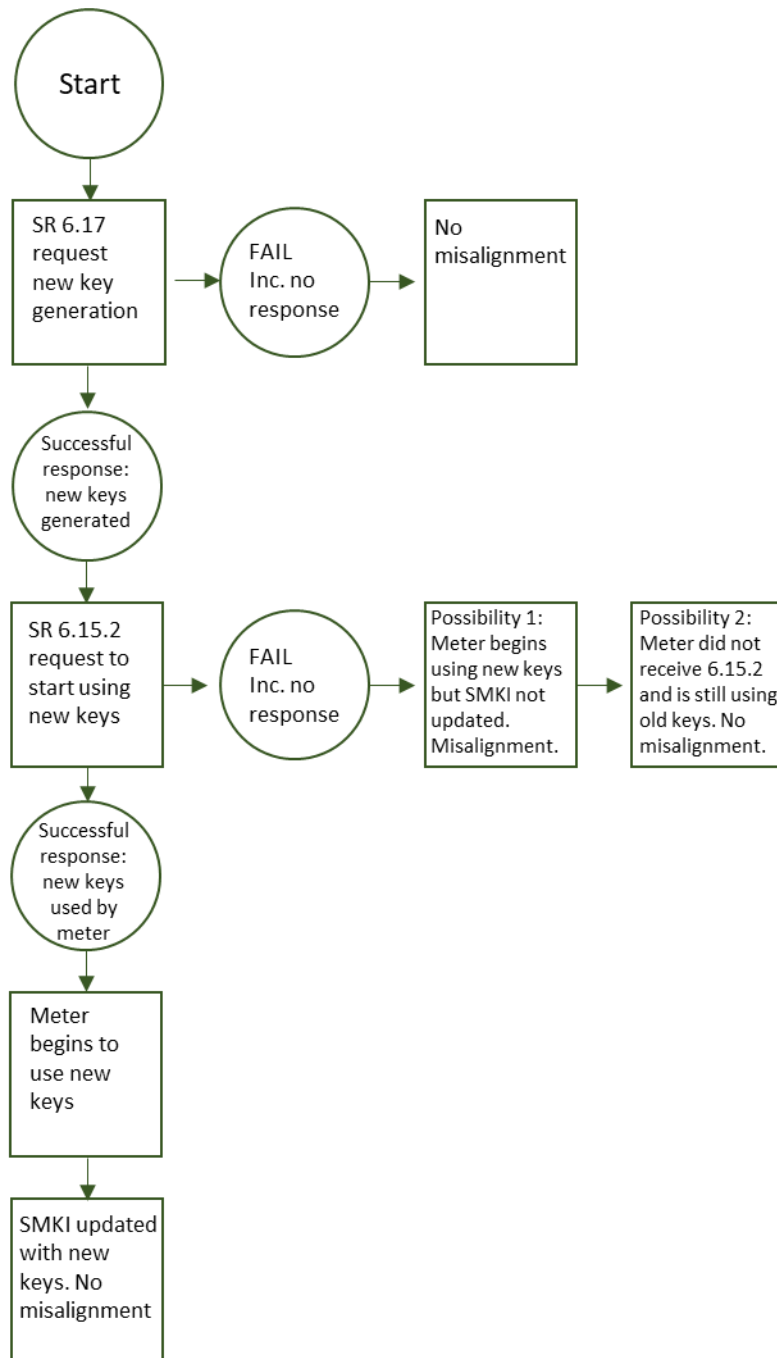
1. the response is never generated by the Device;
2. the response is lost in transit; or
3. the response reaches the DSP after timeout.

There are some Devices that become non-communicable after this process. Root cause analysis has identified that due to the reasons above, the Device certificate (Device Signature (DS) or Key Agreement Key (KAK)) is misaligned with what is held within the DSP Master Key Store.

The Proposer advises that Device certificate misalignment can also occur when attempting to address the issue of an incommunicable Device by cycling certificates, where the issue may persist due to intermittent Home Area Network (HAN) or WAN connectivity.

Suppliers have indicated they would like an enduring solution to resolve the Device certificate misalignment issue without involving a manual SMI update.

The Proposer has provided the below diagram, setting out the current scenario:



Older firmware versions

Some Devices utilising specific old firmware versions reject SRV 6.24.2 'Retrieve Device Security Credentials (Device)' and GBCS Use Case CS02e, as they take a prolonged period to validate the MAC. It is not possible to perform a firmware update to fix the issue, as SR 11.3 'Activate Firmware' will fail (due to the Device being incommunicable).

Scale of the issue

A DCC Data Science and Analytics (DSA) report was produced to identify the potential Devices that may suffer from this Device certificate misalignment issue. There is approximately a combined 120,000 ESME and GSME Devices identified to date which could increase.

What is the impact this is having?

Parties are unable to communicate with any Device that has a certificate that is misaligned with the DSP Master Key Store. Without an enduring solution there is a reliance on manual correction of each individual Device. The Proposer has advised that this is a time-consuming process, which has associated costs and can be prone to errors in relation to incorrect information provided to the DSP for manual correction. The process of producing the information require to complete manual corrections may lead to security risks.

Impact on consumers

Without an enduring solution in place, Suppliers must rely on manual corrections for each Device impacted, otherwise the Devices will not be able to receive Service Requests or the relevant responses or Alerts cannot be validated by the receiving SEC Party. An example of this is where Suppliers are unable to support a CoS, and the consumer will therefore not benefit from improved tariffs from the gaining Supplier.

Additionally, prepayment customers would be unable to perform top-up operations until the Device certificate misalignment issue is resolved.

Errors within the SMI

The SEC currently requires the DCC to manually correct errors in the SMI where there is no other available method. In the case of a Device certificate becoming misaligned between the Device and the DSP Master Key Store or Smart Metering Key Infrastructure (SMKI), it is not possible for the Supplier to fix the issue after a Change of Supplier (CoS) event. The only way to resolve the issue is with a manual DSP SMI correction.

The DCC has advised that it has a process (script-based) to update the SMI based on the information energy Suppliers provide (for example, the Global Unique Identifier (GUID) of the Device, certificate serial number of the to-be-replaced certificate, and the certificate serial number of the new certificate). The Proposer has commented that it is a labour-intensive exercise to gather this information.

3. Assessment of the proposal

Areas for assessment

SECAS has engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC) and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums. The key points can be found below:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	Does this issue have any operational impact on the smart metering infrastructure?
SMKI PMA	Does this issue impact the Smart Metering Key Infrastructure?
SSC	Does this issue or potential solution have any security impacts?
TABASC	Does this issue or potential solution have any technical or business architecture impacts?

During the Chair Triage meeting, the SSC / SMKI PMA Chair noted the potential link with [DP232 'ACB Certs on I&C'](#). This is part of a wider concern that relates to several issues with certificates. They stated that the DCC has been asked to provide a plan of how all the issues relate and will be resolved. SECAS will keep the OPSG, SMKI PMA and SSC updated as this modification progresses.

The DCC has undertaken the project looking to resolve certificate-related issues, however it has stated that this modification is still necessary. The Proposer has confirmed that the issue identified under this modification relates specifically to Device certificates.

Observations on the issue

Are Devices physically removed?

SECAS presented the Draft Proposal to the Change Sub-Committee (CSC) for initial comments in April 2023. A CSC member asked if it can be investigated how many meters are physically removed prior to the resolution. They commented that they had seen many meters being physically removed shortly after installation due to a failed commission, and queried if this could be related to the issue being considered under this modification. SECAS raised this with the DCC who stated it is not aware of any Devices that have been physically removed due to this issue. The DCC advised that the issue may result in Devices losing smart capability but they should not be physically removed.

Scale of the issue

During the Development Stage the Proposer expressed concern with the lack of reporting on Device certificates. They advised that they were faced with a large quantity of certificate issues in differing forms. They added that a common area of concern is the CoS (Gain) scenario where visibility of Device certificate misalignment is especially opaque. The Proposer added that identifying misalignments is only beneficial if they can also remediate the issue. They commented that they have many customers where the CoS (Gain) cannot progress beyond SR 6.23 'Update Security Credentials (CoS)' due to either DSP or Device certificate misalignment. Raising an incident to request Device certificate misalignment is pointless at present as Parties are asked to provide information that they do not have access to.

The Proposer stated that the DCC had provided some useful data that would be advantageous if turned into a regular report. The Proposer and the DCC have agreed to consider this when building the Proposed Solution

Appendix 1: Progression timetable

Timetable	
Event/Action	Date
Draft Proposal raised	3 Apr 2023
Presented to CSC for initial comment	18 Apr 2023
Draft Proposal discussed with Sub-Committee Chairs	19 Apr 2023
Presented to Sub-Committees for initial comment	Apr – May 2023
DCC certificate issue project	May – Jul 2023
<i>Business requirements developed</i>	<i>Aug 2023</i>
<i>CSC converts Draft Proposal to Modification Proposal</i>	<i>15 Aug 2023</i>
<i>Business requirements workshop</i>	<i>Aug 2023</i>
<i>Modification discussed with the Working Group</i>	<i>6 Sep 2023</i>
<i>DCC Preliminary Assessment requested</i>	<i>11 Sep 2023</i>
<i>Update provided to CSC</i>	<i>21 Nov 2023</i>

Italics denote planned events that could be subject to change

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	Full term
ACB	Access Control Broker
CHF	Communications Hub Function
CoS	Change of Supplier
CSC	Change Sub-Committee
CSP	Communication Service Provider
DCC	Data Communications Company
DS	Device Signature
DSA	Data Science and Analytics
DSP	Data Service Provider
ESME	Electricity Smart Metering Equipment
GBCS	GB Companion Specification
GSME	Gas Smart Metering Equipment
GPF	Gas Proxy Function
GUID	Global Unique Identifier
HAN	Home Area Network
I&C	Install & Commission

Glossary	
Acronym	Full term
KAK	Key Agreement Key
MAC	Message Authentication Code
OPSG	Operations Group
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMI	Smart Metering Inventory
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SR	Service Request
SRV	Service Reference Variant
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
WAN	Wide Area Network