SEC Modification Proposal, SECMP0107, DCC CR1352

SMETS1 Validation of SRV 6.15.1

Preliminary Impact Assessment (PIA)

Version:	**0.5**
Date:	**25th June 2020**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Data Communications Company

Contents

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
03/06/2020	0.1	Initial version, for DCC internal review
04/06/2020	0.2	Updated following DCC internal review
15/06/2020	0.3	Updated following information from Service Providers
19/06/2020	0.4	Updated after further DCC internal review
25/06/2020	0.5	Released following DCC internal review

1.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	DP107 Modification Report	SECAS	13/01/2020

References are shown in this format, [1].

1.3 Document Information

The Proposer for this Modification is Gemma Slaney of Western Power Distribution. The original proposal was submitted in January 2020.

The Preliminary Impact Assessment was requested of DCC on 20 April 2020.

2 Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The SEC Definitions, issue statement, and requirements following have been provided by SECAS and the Proposer.

2.1 Current Arrangements

Critical Commands in Smart Metering Equipment Technical Specifications 2 (SMETS2) do not have any Registered Data Provider (RDP) validation and therefore in order to send Service Reference Variant (SRV) 6.15.1 - 'Update Security Credentials (KRP)' to update certificates on a device, the only requirement is that the Service Request (SR) sender is the owner of the certificate.

For SMETS1 devices, the Network Operator certificates are held by the SMETS1 Service Providers (S1SP). There is an additional RDP validation step to Service Requests including the SRV 6.15.1 used to update the Network Operator certificates. The DSP and S1SPs will validate these Critical Commands against the RDP data. If the user of the Service Request is not the owner of the Meter Point Administration Number (MPAN) for ESME or Meter Point Registration Number (MPRN) for GSME, that Service Request is rejected.

2.2 What is the issue?

During the enrolment phase of a SMETS1 Installation, a Network Operator Smart Meter Key Infrastructure (SMKI) Organisation certificate can be provided by:

- the Supplier via Migration Authorisation or via the response of Dormant Meter Migration Notification
- the DCC's Migration Control Centre Team for the SMETS1 Electricity Smart Metering Equipment (ESME) where the Supplier has not provided the Network Operator certificate
- the Supplier using SRV 6.21 where Network Operator certificate is not provided by any of the above methods.

If an incorrect Network Operator certificate is placed (stored at S1SP) in error, no Network Operator can send a Critical SR including SRV 6.15.1 to the SMETS1 Device. This is currently enforced by the following validations:

#1 DSP performs RDP validation adhering to clause 6.1(f) of SEC Appendix AB - Service Request Processing Document (SRPD).

#2 S1SP performs RDP validation adhering to clause 16.1 of SRPD.

#3 S1SP validates the certificate owner with the Business Originator ID as per clause 4.2 of SEC Appendix AM - SMETS1 Supporting Requirements (S1SR).

This means that a SRV 6.15.1 sent from the current Network Operator to update the incorrect certificate is rejected due to validation number # 3 because Business Originator ID of the SR does not match with the Entity Identifier of the certificate associated with the device.

Also, SRV 6.15.1 from the Network Operator whose certificate was incorrectly associated with the device is rejected because they fail the RDP checks as per validation #1 and #2.

In the equivalent situation on SMETS2 devices, the issue can be overcome by the Network Operator that has certificates on the device sending an SRV 6.15.1 because validation #1 is not applied. This is not blocked by the DSP since it is a Critical request and the device will accept matching certificates. This means that the “wrong” Network Operator can place the correct Network Operator’s certificates on the device.

This is not possible for SMETS1 because RDP checks are required for all SRVs, including Critical SRs.

2.3 Impact of the issue

2.3.1 Network Operators

This section contains the impact of the issue on the Network Operator as provided by the Proposer and SECAS. In this context Network Operator means both the Electricity and Gas Network Operators.

The impact is currently low due to the way that SMETS1 Devices are migrated and the Network Operator certificates validated on migration, coupled with the fact that not all Network Operators are currently using Appendix AD ‘DCC User Interface Specification’ version 3.0/3.1 (DUIS 3). However, there is the potential that in the future the problem could become much larger.

2.3.2 DCC

This section contains the impact of the issue on the Supplier and the Network Operator as assessed by the DCC.

The Network Operator certificate for a SMETS1 Device is used to:

A. validate the Business Originator ID for Critical SRs. However, only SMETS1 Critical SR is available to Network Operator is SRV 6.15.1- Update Security Credentials (KRP). So even if the certificate is incorrect, Network Operator can issue Non Critical SR to SMETS1 Devices.

B. identify the Business Target ID for Alerts from SMETS1 ESME1. So, if the Non-Critical Network Operator certificate is incorrect, Alert can go to the incorrect party.

This means the impact of incorrect Network Operator certificate is limited to SMETS1 ESME for alert routing. There is no alert from SMETS1 GSME for Network Operator.

Secondly, Network Operator certificate can be associated with SMETS1 Device at S1SP (as shown in Figure 1) in the following way:

① During SMETS1 Enrolment - when a certificate is provided by the Supplier or in absence of that, by the DCC. DCC’s Commissioning party issues SRV 6.21 to associate certificates with the SMETS1 Device (at S1SP).

② By the Supplier using SRV 6.21- when Supplier chooses to commission SMETS1 Device themselves or DCC has not issued SRV 6.21 for any reason (such as mixed Installation with Dormant ESME and Active GSME).

③ By the Network Operator using SRV 6.15.1.

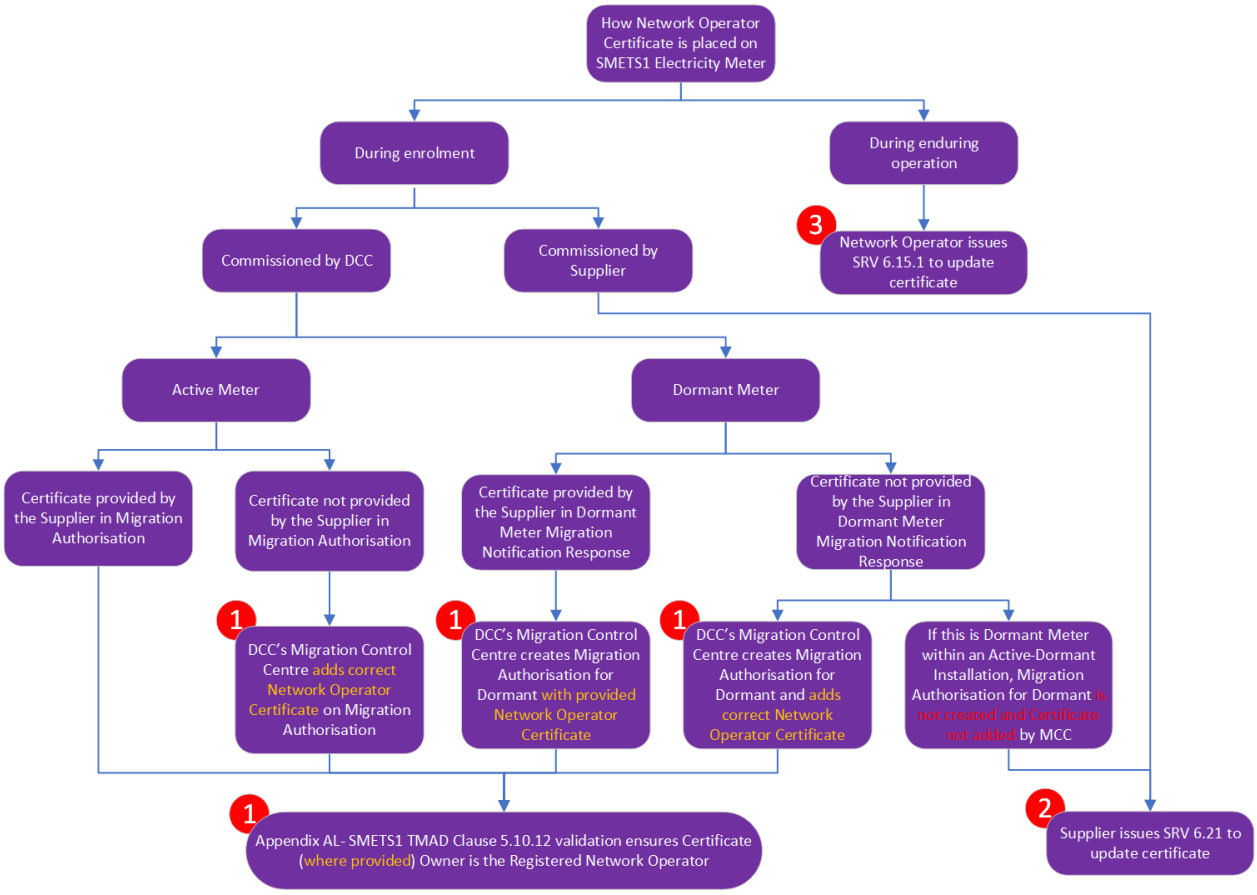

Figure 1: ESME Network Operator certificate update process

Additional measures for Process ① such as

i. population of ESME Network Operator certificate by the DCC when the Supplier has not provided certificates in the pre-enrolment process (as per SEC Appendix AL - SMETS1 Transition and Migration Approach Document (TMAD) clause 4.42)

ii. validation of Network Operator certificate during enrolment (as per TMAD clause 5.10.12 and 5.10.17)

ensures the provided certificates are correct during enrolment. Also, non-availability of Network Operator certificate during enrolment will default ACB certificate in corresponding Trust Anchor at S1SP.

This leads to the fact that the Supplier needs to apply a Network Operator certificate using SRV 6.21 where

- Network Operator certificate is not applied during enrolment due to any issue in the process ① ; or
- Supplier commissioning the SMETS1 Meter during enrolment (Process ②) however no Supplier has shown interest yet to commission themselves during SMETS1 enrolment; or

- Supplier applying the Network Operator certificate post-commissioning by the DCC for mixed SMETS1 Installations with Active GSME and Dormant ESME (because no provision for capturing ESME Network Operator certificate in current enrolment process for such mixed Installation)

The Network Operator may also apply another party's certificate in error using SRV 6.15.1 during enduring operation.

DCC is currently analysing how many enrolled SMETS1 ESMEs are there with default ACB certificate and incorrect Network Operator certificate. Details of this analysis will be provided in Full Impact Assessment(FIA).

3 Description of Solution

DCC considered the following solutions:

A) Remove RDP validation at the DSP (Validation #1) and S1SP (#2) for the SRV 6.15.1 where the sender is a Network Operator.

B) Keep the SRV 6.15.1 RDP check and avoid the certificate check(#3); this was rejected by the DCC and Service Providers because it introduces a higher security risk.

C) Relax the anti-replay checks on SRV 6.21; this was rejected by the DCC and Service Providers because that would require the Supplier to initiate the change of certificates, which they would be reluctant to do because of the additional effort required.

3.1 SEC Changes

The DCC and Service Providers have reviewed the solution and agree with the change in the SEC Appendix AB - Service Request Processing Document. Clause 6.1(f) of the SRPD requires DCC (which, through clause 16.1, includes S1SP as well as DSP) shall check Registration Data for incoming SRVs. However, it says that the check is "subject to Clause 6.2" which lists exceptions. Suggested changes to Clause 6.2 are highlighted below:

SRPD Clause 6.2

The step set out at Clause 6.1(f) shall not apply in the following circumstances (and, where it is necessary to identify a Responsible Supplier, the DCC shall do so using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory):

(a) an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Smart Meter sends a 'Join Service' Service Request to join that Gas Smart Meter to a Gas Proxy Function;
(b) an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Proxy Function sends a 'Restore GPF Device Log' Service Request to restore the Device Log of that Gas Proxy Function; or
(c) the Service Request has been sent by a User acting in the User Role of 'Other User'.
(d) a SMETS1 Service Request with Service Reference Variant 6.15.1 (Update Security Credentials) received from an Electricity Distributor or Gas Transporter.

3.2 DSP Solution Overview

The DCC Data System will be updated to remove the RDP check for SRV 6.15.1 where the sender is a Network Operator. RDP checks will remain for a SMETS1 6.15.1 from a supplier or any other type of service user in future. This is a SMETS1-only SRV and is not carried out for SMETS2 Critical Service Requests.

DSP will implement a single feature switch to enable the functionality, i.e. the change will not be enabled separately for different S1SPs. This means, if there is a period when one or more S1SPs has not enabled the change, then a request could be allowed by the DSP but rejected by an S1SP (using the standard S1SP Alert mechanism).

There will be no impact on the DCC Service Management System.

3.3 S1SP Solution Overview

The S1SP system will be updated to remove the RDP check for SRV 6.15.1 specifically where it targets Network Operator certificates.

The existing RDP checks will remain for all other SRVs; and will remain for an SRV 6.15.1 that targets supplier certificates.

3.4 Other Solution Impacts

Apart from DSP and S1SPs, no other SMETS1 Components are impacted by this change.

4 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0107 on DCC Services and Interfaces that impact Users and/or Parties.

4.1 System Components

Only SRV 6.15.1 RDP validation from Network Operators are impacted at DSP and all S1SP systems.

4.2 Security Impact

The implementation will be security assured during the implementation phase. This includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

A more detailed security impact will be carried out as part of the Full Impact Assessment.

At this stage, a penetration test and updates to protective monitoring are not thought to be required.

4.3 Technical Specifications

No changes to DUIS, GBCS, or any other Technical Specification are expected apart from proposed changes to SRPD.

4.4 Integration Impact

An appropriate level of Systems Integration and User Integration Testing (SIT and UIT) will be carried out prior to progressing the release of this change to the Production environment, but this is not included in the PIA.

4.5 Infrastructure Impact

There will be no change to the infrastructure design as a result of this change.

The Modification does not impact the DSP or S1SP's resilience or Disaster Recovery implementation.

4.6 Application Support

No changes to Application Support are expected.

4.7 Service Impact

No material impact is expected for the Operations team and no changes to SLAs are expected.

4.8 Safety Impact

No impact is expected, but a full Safety Impact Assessment will be carried out as part of the production of the Full Impact Assessment (FIA).

4.9 Contract Schedules

No changes to contracts are expected, but this will be re-evaluated for the FIA.

5 Implementation Timescales and Approach

As this change affects DSP and all the S1SPs, it will need to be implemented as part of a scheduled release. Notwithstanding in which release this change is implemented, based on the current response from Service Providers, the elapsed time for implementation from project initiation through to PIT completion will be:

- 3 months for DSP
- 3 months for S1SP1s

The release lifecycle duration will be confirmed as part of the FIA. As currently planned, the standard ongoing major release model will provide drops to the production environment in November 2021.

5.1 Implementation Approach

Implementation of this change is assumed to follow a hybrid of agile and waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

5.2 Testing and Acceptance

It is assumed that the change will be implemented and tested as part of a major release and will include release based regression testing in SIT and UIT.

6 Costs and Charges

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

The scope of supply under this PIA includes design, development (build), system testing, and performance testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional requirements as assumed above. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change during discussions with the DCC. As a result, the final offer price may result in a variation.

6.1 Design, Build and Testing Cost Impact

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

£	Design, Build and PIT
For DSP and 3 S1SPs	193,125

Based on the existing requirements, the total fixed price cost for a Full Impact Assessment by all Service Providers is **£22596.58** and would be expected to be completed in 30 days.

7 Risk, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified. Two clarifications are also requested.

Further RAID may be established as part of the Working Group reviews and the FIA.

7.1 Risks

None at this time.

7.2 Assumptions

None at this time.

7.3 Issues

None at this time.

7.4 Dependencies

Ref.	Area	Dependency	Impact
MP107-DD01	IA	To provide a Full Impact Assessment, DCC will need to confirm that all S1SPs will deliver the change as part of a single release alongside the DSP change.	Low

7.5 Clarification

None at this time.

Appendix A: Glossary

The table below provides definitions of the terms used in this document.

.Acronym	Definition
CR	DCC Change Request
DCC	Data Communications Company
DSP	Data Service Provider
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
IHD	In Home Display
KRP	Known Remote Party
MPAN	Meter Point Administration Number
MPRN	Meter Point Registration Number
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
RDP	Registration Data Provider
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
S1SP	SMETS1 Service Provider
SMETS	Smart Metering Equipment Technical Specification
SMI	Smart Metering Inventory
SMKI	Smart Meter Key Infrastructure
SP	Service Provider
SR	Service Request
SRPD	Service Request Processing Document
SRV	Service Request Variant
SSI	Self Service Interface
UIT	User Integration Testing