SEC
Smart Energy Code

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.

Smart Energy Code

DP134

‘Use of SMKI Certificates relating to a SoLR event’

Modification Report

Version 0.2

12 June 2020

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a draft Modification Report. It currently sets out the background, issue, proposed solution, likely impacts and the 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 4
3. Solution 5
4. Impacts 7
5. Assessment of the proposal 9

Appendix 1: Progression timetable 10

Appendix 2: Glossary 11

Contact

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

Emmanuel Ajayi

020 8132 4134

Emmanuel.ajayi@gemserv.com

1. Summary

This proposal has been raised by Easton Brown from the Data Communications Company (DCC).

When a Supplier fails, the Authority use its Supplier of Last Resort (SoLR) powers to revoke a licence and select and appoint a SoLR. Only the failed Supplier (or its agent) will hold the Smart Metering Key Infrastructure (SMKI) Private Keys that enable Critical Commands to be sent that will be actioned by the meter, until the new Supplier can replace the Certificates. This can take anywhere between two and four weeks.

Consumers with prepayment meters will continue to run down credit during a SoLR process and whilst the new supplier onboards the consumers (knowing enough information about the consumers to populate systems and service them). During a 'disorderly exit' SoLR process there is a risk that a consumer could lose energy supply. It may take a significant amount of time before the new Supplier can issue Critical Commands, such as Emergency Credit, to recommence supply.

The Smart Energy Code Administrator and Secretariat (SECAS) has been working with the industry and Ofgem to identify resolutions to the issues that arise during a SoLR event. This modification has been raised to implement part of that solution.

2. Issue

What are the current arrangements?

Supplier of Last Resort (SoLR) is a process developed by the gas and electricity industry to manage the exit of a failed supply business and to transfer the consumers to a replacement Supplier where a trade sale is not possible. It affects, and is implemented by, several industry codes.

When a Supplier fails, the Authority use its SoLR powers to revoke a licence and select and appoint a new Supplier. Appointing a new Supplier using the SoLR powers will take a few days. Following appointment, it is likely that the new Supplier will require a period of time to onboard and service the new customers.

What is the issue?

Only the relevant Supplier (or its agent) will hold the Private Keys that enable Critical Commands to be sent that will be actioned by the meter. The new Supplier needs to be able to replace the Certificates with its own Certificates on the Device to enable it to service the customers.

Consumers with prepayment meters will continue to run down credit during a SoLR process and whilst the new Supplier onboards the consumers (knowing enough information about the consumers to populate systems and service them). During a ‘disorderly exit’ SoLR process there is a risk that a consumer could lose energy supply.

What is the impact this is having?

In the event of a Supplier failure, consumers with smart meters in prepayment mode may lose supply and it may take a significant amount of time before the new Supplier can issue Critical Commands, such as Emergency Credit, to recommence supply.

3. Solution

Proposed Solution

The Authority monitors Supplier activities and identifies and engages with Suppliers at risk of failure. Suppliers ought to proactively engage with the Authority if they recognise they are at risk of failure. This solution only applies if the failing Supplier uses an Shared Resource Provider (SRP). If the failing Supplier does not use an SRP Ofgem have stated that they would prefer to try to manage the situation as a 'trade sale'.

Various actions are required as part of the solution. These actions are categorised into those taken before, during or after the SRP is required to take action to maintain a consumer's continuity of supply.

- Pre-Make Safe: Determining whether there is a need to instruct the SRP to take action to maintain supply.
- Make-Safe: The actions that an SRP, or other, will take to maintain supply.
- Post-Make Safe: The actions required to revert to normal operation.

These actions required will function as a guidance that need to be taken by the relevant parties.

Pre-Make Safe actions

The Authority monitors Supplier activities and identifies and engages with Suppliers at risk of failure. Suppliers ought to proactively engage with the Authority if they recognise they are at risk of failure.

Make-Safe action by the SRP will not be required if the Supplier in question:

- does not supply consumers using smart meters in Prepayment mode;
- proactively arranges for a "trade sale" of the business or its customer base; or
- engages and commits to continuing to serve the consumer until a SoLR is appointed, or they will take the Make-Safe activities themselves.

In this case, the SRP Make-Safe process is not required and ends.

Make-Safe actions – one time only

These actions need to be taken by the SRP of the failed Supplier and rely on that SRP holding the failed Supplier's private key materials to sign Service Requests. Furthermore, the actions can be completed prior to the SoLR being appointed by the Failing Supplier's SRP, assuming the SRP holds the Supplier's private keys and has the capability to initiate these actions.

Set a 24/7 Non-Disconnect Calendar

The SRP sends Service Request (SR) 2.1 with the existing configuration except that ElectricityNonDisablementCalendar or GasNonDisablementCalendar, as appropriate, would be configured such that the meter will not disable supply when credit is depleted. Once the SoLR is able to service the consumer they will return the configuration as appropriate, taking care that dis-applying the non-disablement period would not disable supply.

Set Payment Mode to Credit

The SRP sends SR1.6 to set a meter's Payment Mode from Prepayment to Credit, thus preventing exhausting meter credit from disabling supply.

Once the SoLR is able to service the consumer it will return the Payment Mode as appropriate, taking care that setting to Prepayment would not disable supply.

Set a large Emergency Credit

The SRP sends SR2.1 with the existing configuration except that a large Emergency Credit value is set, which might delay the point at which the meter will disable supply when credit is depleted.

Once the SoLR is able to service the consumer they will return the Emergency Credit value as appropriate, taking care that this would not disable supply.

Make Safe actions – ongoing

These actions may be required several times between the start of the event (Failing Supplier not servicing the consumer) and end (SoLR servicing the consumer). As such, they may require agreement that the Failing Supplier's credentials can continue to be used for a defined short period after the point at which the SoLR is appointed.

Continue to Vend

The Payment Service Provider (PSP) and SRP maintain the capability for the consumer to procure top-ups via existing channels. Once the SoLR is able to service the consumer it will replace the Certificates on the meter and service them using its own credentials.

Post-Make Safe Actions

The required post-Make Safe actions are determined by whether:

- the SoLR wishes to take on the Failed Supplier's systems, assuming this is possible;
- there is a Change of Supplier (CoS) to the SoLR; or
- whether the Make-Safe action was one-off or ongoing.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
	Electricity Network Operators		Gas Network Operators
✓	Other SEC Parties	✓	DCC

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure'
- Appendix AA 'Threshold Anomaly Detection Procedures'
- Appendix B 'Organisation Certificate Policy'

Usage of Organisation Certificates

Changes to Section L11 'Subscriber Obligations' would be required that would outline the use of certificates and key pairs during SoLR. This change would allow the SoLR to continue to use the failed Supplier's private key materials to continue to make consumers safe immediately after appointment as the SoLR.

This change is required to enable the SoLR to continue to use the existing materials to communicate with meters immediately after appointment, for the purposes of ensuring continuity of supply.

The impacts of not making the changes are on consumers who go off supply, as they are at risk of going off supply as a result of a SoLR event. These consumers will have to wait until the SoLR is in a position to onboard the customers, place its own certificates on the Device and then service the customers.

A recommended control of this situation is the SMKI Policy Management Authority (PMA) should ask for reports from the DCC to check that the Certificates are not used for purposes other than those set out in policy. It is currently assumed that technical constraints are not necessary to prevent other Service Requests from being sent.

Delayed Revocation of Organisation Certificates

A change would be required delay the revocation of the failed Supplier's Organisation Certificates, so they continue to be valid, allowing the SoLR to continue to use the failed Supplier's private key materials to continue to make consumers safe immediately after appointment as the SoLR.

Changes in Appendix B 'Organisation Certificate Policy' section 4.9 to set out circumstances for revocation.

Usage of DCC Key Infrastructure (DCCKI) Certificates

A change would allow the SoLR to use the failed Supplier's User Systems, which would be stopped if the DCCKI Certificates used to authenticate communications were revoked.

SEC Section L13 (DCC Key Infrastructure) and SEC Appendix S (DCCKI Certificate Policy)

This change enables continued use of the failed Supplier's User systems. It may not be necessary if the following are true:

- Where SRPs are used, the SRP does not use DCCKI Certificates issued to Suppliers (and instead it uses the DCCKI Certificates issued to the SRP); and
- SoLRs would never wish to continue to use the failed Supplier's User Systems.

The impact of not making this change is the failed Supplier's User Systems, (including an SRP system if it uses a Supplier-specific DCCKI Key), used to send Commands to prevent the supply being disabled would fail authentication and be unusable.

Expedited Anomaly Detection Threshold Updates

This change would require the DCC to process an ADT submission faster than the current provisions for Fast-Track Notifications.

A change to SEC Appendix AA 'Threshold Anomaly Detection Procedures' section 3 would be required to facilitate this change. However, this change may not be required, given the Fast-Track Notification process does not prevent the DCC from taking less than 24 hours. There may be a delay of up to 24 hours for some consumers to be made safe, as the Threshold Anomaly Detection Procedures may prevent the successful application of non-disablement calendars.

Consumers

This change will have a positive impact on consumers who have a prepayment meter when experiencing a situation of SoLR.

Other industry Codes

This change will have no impact on other industry codes.

Greenhouse gas emissions

This change will have no impact on greenhouse gas emissions.

5. Assessment of the proposal

Observations on the issue

The Change Sub-Committee (CSC) agreed that the issue is understood. Some members of the CSC expressed a desire for greater detail for the provisions around the changes required. Furthermore, the CSC agreed that the change would have a positive impact on consumers and would be an improvement on the current arrangements.

Appendix 1: Progression timetable

SECAS is recommending this modification be submitted to the Refinement Procedure so that the Proposed Solution can be fully developed and clarified. This will be facilitated by a discussion at the Working Group and through a Refinement Consultation.

Timetable	
Event/Action	**Date**
Draft Proposal raised	29 May 2020
Presented to CSC for comment	w/c 1 Jun 2020
Panel converts Draft Proposal to Modification Proposal	19 Jun 2020
Modification discussed with Working Group	1 Jul 2020
Refinement Consultation	6 Jul – 24 Jul 2020
Modification Report presented to Panel	14 Aug 2020

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**
CSC	Change Sub-Committees
DCC	Data Communications Company
DCCKI	Data Communications Company Key Infrastructure
PSP	Payment Service Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administration Services
SMKI	Smart Meter Key Infrastructure
SoLR	Supplier of Last Resort
SR	Service Request
SRP	Shared Request Provider