Data Communications Company

SEC Modification Proposal, SECMP0134B, DCC CR4719

Use of SMKI Certificates Relating to a SoLR Event – Part 2

Second Preliminary Impact Assessment (PIA)

Version:	**0.5**
Date:	**26th July, 2022**
Author:	**DCC**
Classification:	**DCC Public**

Data Communications Company

Contents

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to complete the Full Impact Assessment of £39,035
- The timescales to complete the Full Impact Assessment of 30 days
- ROM costs for SECMP0134B, up to the end of Pre-Integration Testing (PIT) of between £650,500 to £1,161,000, an increase of approximately 7% over CR4426

Problem Statement and Solution

The Supplier of Last Resort (SoLR) process was developed by Ofgem to manage the exit of failed Suppliers from the market where no trade sale or commercial agreement is possible. Once Ofgem revokes the supply Licence of a failing Supplier, the DCC are required to revoke the Smart Metering Key Infrastructure (SMKI) Certificates. Whilst SoLRs to date have involved Suppliers exiting the market in an 'orderly' way, there is a concern that a Supplier falling out of the market in a 'disorderly manner' could expose prepayment consumers to the risk of supply continuity.

SoLR events are a significant risk; about 1.8% of domestic energy customers have been impacted over the last two years, and 22 energy suppliers have gone bust. While a smaller percentage were Smart Meter providers, this is still significant.

Whereas the previous PIA CR4426 changed the behaviour of Service Request (SR) 1.6, the Working Group directed that this new PIA should be based on modifying the use of Service Request 2.1 'Update Prepay Configuration'.

Modification Benefit

Changes to the DSP are required for implementing and supporting a new User Role, which will be used to allow Users in this new role, to send Commands to Devices in the event of a Supplier failure. This will ensure continuity of supply to all consumers in the event of a SoLR event.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
12/07/2022	0.1	Initial DCC Review
26/07/2022	0.5	Updated costs in section 7 for all Service Providers

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP134B Modification Report v0.2	SECAS	10/08/2021
2	MP134B Business Requirementsv0.3	SECAS	16/06/2022
3	SECMP0134B CR4426 - PIA - SMKI Certs Relating to SoLR v0.31	DCC	13/04/2022

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is Easton Brown of Smart DCC.

The first Preliminary Impact Assessment was requested of DCC on 11th August 2021, accepted on the 18th August, 2021, and delivered on 11th October, 2021, after a clarification required a pause of 8 Working Days.

The second Preliminary Impact Assessment was accepted on the 20th June, 2022.

3 Context and Requirements

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

The requirements have been provided by SECAS, the Proposer, and the Working Group.

3.1 Context

The Supplier of Last Resort (SoLR) process was developed by Ofgem to manage the exit of failed Suppliers from the market where no trade sale or commercial agreement is possible. Once Ofgem revokes the supply Licence of a failing Supplier, the DCC are required to revoke the Smart Metering Key Infrastructure (SMKI) Certificates. Whilst SoLRs to date have involved Suppliers exiting the market in an 'orderly' way, there is a concern that a Supplier falling out of the market in a 'disorderly manner' could expose their prepayment consumers to the risk of supply continuity.

The SEC Panel requested that the Smart Energy Code Administrator and Secretariat (SECAS) set up a project to examine the risks to consumers from a possible disorderly exit from the market and to propose the solution options available. The project brief was agreed by the Panel in February 2020.

This project concluded in June 2020 when the final update was presented to Panel and the Proposed Solution was taken forward by this modification.

SECMP0134A 'Use of SMKI Certificates relating to a SoLR event' is currently with the Authority for decision. It proposes to allow the SMKI Policy Management Authority (PMA) to delay the revocation of the SMKI Certificates. This would allow a Shared Resource Provider (SRP) to put prepayment customers into a 'safe mode' where they will not lose supply if they run out of credit. SECMP0134A will not require any DCC System changes. SECMP0134B offers an enduring solution to the issue.

3.2 Problem Statement

In March 2021 Ofgem implemented changes to the Supply Licence Conditions requiring Suppliers to develop and submit a Customer Supply Continuity Plan (CSCP) to set out what will be in place to safeguard the continuity of supply for its customers in the event of its exit from the market.

During the Ofgem process to revoke the Supply Licence of a failing Supplier and the appointment of SoLR, consumers will continue to use energy. Consumers on credit meters will most likely not experience any supply problems but consumers using prepayment meter modes could run out of credit and lose supply. In this situation they would usually call their Supplier to ask for Emergency Credit or purchase a 'top-up'. However, if the Supplier is undergoing a 'disorderly exit' there will not be any answer to their phone calls, and they may have no means to regain their supply until the new Supplier has performed the Change of Supplier (CoS) process. Vulnerable consumers may lose supply, and this would be of particular concern.

The current process whereby Ofgem revoke the Supply Licence of a failing Supplier and the DCC then revoke the SMKI Certificates means that prepayment consumers could lose supply and have no means to regain it until the SoLR has been appointed and the new Supplier has performed the CoS process.

3.3 Business Requirements

There are seven functional requirements for this Modification. Changes to the requirements from the original PIA request for CR4426 to this new request are shown in red text following.

Requirement 1; A new User Role is created with roles as defined in Appendix AD 'DCC User Interface Specification' (DUIS)

Req. 2 Smart Energy Code (SEC) Parties acting in that User Role can subscribe for Extensible Markup Language (XML) Signing Certificates, but not Digital Signing Keys for signing Critical Commands

SEC Parties acting in this new User Role can subscribe for Organisation Certificates with the existing Remote Party Role of xmlSign, but not Digital Signing Keys for signing Critical Commands.

Req. 3 The new User Role will only be able to send Service Request 2.1 'Update Prepay Configuration'. The solution should be configurable to enable other Service Requests to be added to the list of SRVs that this User Role is eligible to use.

The new User Role will be an eligible User of a limited set of Service Requests. The initial list will contain only Service Request 2.1.

Any solution should also allow this list to be easily configured with further or reduced SRVs with limited changes.

Req. 4 Parties acting in this User Role must be able to create Authorised Responsible Officers (AROs) and Senior Responsible Officers (SROs) to enable submission of Anomaly Detection Threshold (ADT) files that will allow the new User Role to send Service Requests to Devices registered to a specific Supplier

Req. 5 The content of the Service Request (for SMETS1 Devices) and Signed Pre-Command (for SMETS2+ Devices) must be checked to accept only messages with an update to the non-disconnect calendar

For Service Request 2.1 'Update Prepay Configuration' whilst parameters other than the non-disablement calendar can be changed, the Business Requirements Working Group suggested a 'fixed format' could be 'matched'. The following is suggested.

'Set to Safe Prepayment' Command

The Commands created and sent would be ECS08a Update Prepayment Configuration on ESME / GCS05 Update Prepayment Configurations on GSME Commands, and so would include the parameters specified in Service Request '2.1 Update Prepay Configuration'

One allowed set of parameters that the DCC would enforce through Anomaly Detection packet inspection. Those parameters would be such that:

- Non-disablement periods would never end, whilst these settings were in force. This means Consumers would not go off supply if already on supply / once supply becomes re-enabled until the SoLR can operate their meter;
- The Emergency Credit Limit would be sufficient to allow the Consumer back on supply, unless they have already been disabled for a very significant period (which would be unrelated to the SoLR event)

- The Emergency Credit Threshold would be sufficient to make Emergency Credit available
- Maximum Credit Threshold would be sufficient to allow available vends to be applied (e.g. £90)
- Maximum Meter Balance would also be sufficient to allow such vends to be added, so more than the vend limit; and
- Debt Recovery Rate Cap could be set to zero, to allow any debts to be address by the new supplier and so not risk debt recovery getting in the way of supply being enabled

For SMETS1 meters, this check will be performed on the Service Request from the SRP, acting in the User Role of SolrContingency.

For SMETS2+ meters, this check will be performed on the Signed Pre-Command from the SRP, acting in the User Role of SolrContingency.

Note that the above values will be identified and agreed before the FIA is requested from the Service Providers. The values will have no impact on time to implement or cost.

Req. 6 The default position will be that Users in this User Role will only be able to send the Service Requests listed in requirement 3 and will only be able to do so in the event of a Supplier failure and upon specific instruction from the Authority. Additional validation is set out in this requirement.

The default position will be that Users in this User Role:

- will not be able to send Service Requests except those listed in Requirement 3, or subsequently updated through this or a future modification; and
- will only be able to do so upon specific instruction from the Authority (the source of this instruction to be confirmed), which may occur in the event of a Supplier's licence and Certificates being revoked.

In the normal course of events Anomaly Detection Threshold (ADT) values for the SolrContingency User Role will be set to zero for all Service Requests (meaning that Service Requests are not actioned). In the event of this process being required, the SRP will set the ADT values appropriately.

The DCC will validate the following.

A. Prior to processing ADT submissions that:

- It has received an instruction from Ofgem following notification of a SoLR to allow the SolrContingency SRP to set non-zero ADT values; and

B. Prior to countersigning any Service Requests for SMETS1 Devices that:

- the Service Request has been signed with the SRP's xmlSign Certificate relating to the SolrContingency role;
- the Supplier ID identified Service Request xml is for an identity which previously had SMKI Certificates in the Supplier Role (and are now revoked); and
- other existing checks (e.g. DUIS authentication and those set out in Requirement 5 are passed).

C. Prior to adding its Message Authentication Code (MAC) to any Commands for SMETS2+ Devices that:

- the Pre-Command has been signed with the SRP's xmlSign Certificate relating to the SolrContingency role;
- the Business Originator ID identified by the signed GBCS is for an identity which previously had SMKI Certificates in the Supplier Role (and are now revoked); and
- other existing checks (e.g. DUIS authentication and those set out in Requirement 5 above are passed).

Req. 7 The DCC should remain able to send Alerts to the Supplier after the Supplier's Certificates have been revoked (noting that they will be routed to the failed Supplier's SRP).

After the Supplier's Certificates have been revoked the DCC should remain able to send Alerts using the failed Supplier's revoked Certificates, ensuring that safety critical Alerts can be actioned.

The table below provides an initial list of safety critical Alerts.

Alert Code	Alert Name
0x8F1F	Low Battery Capacity
0x8F3F	Unauthorised Physical Access - Tamper Detect
0x8F73	Unauthorised Physical Access - Battery Cover Removed
0x8F74	Unauthorised Physical Access - Meter Cover Removed
0x8F75	Unauthorised Physical Access - Strong Magnetic field
0x8F76	Unauthorised Physical Access - Terminal Cover Removed
0x8F77	Unauthorised Physical Access - Second Terminal Cover Removed
0x8F78	Unauthorised Physical Access - Other
0x8F1D	GSME Power Supply Loss

Table 1: Safety Critical Alerts

3.4 Proposed Solution

The Proposed Solution will include a new SEC Role (e.g. SolrContingency) created for Shared Resource Providers (SRPs) to send Commands to Devices in the event of a Supplier failure (a SoLR situation). The User Role would identify the SRP acting in this capacity and limit its capabilities in that capacity.

Users in this Role could only subscribe for an XMLSigning Certificate such that the associated Private Key could not be used to sign Critical Commands to Smart Metering Equipment Technical Specifications (SMETS) 1 or 2+ Devices, but it could be used to sign certain XML format Service Request(s).

Under normal circumstances an SRP would subscribe to such Certificates, generate associated Keys and offer its Suppliers this service in case of a Supplier failure and revocation of Certificates. It will be a requirement on relevant Suppliers to put such arrangements in place.

For **SMETS1 Devices**, the SRP would submit Service Requests to the DCC for any Meters that might be in Prepayment Mode, where:

- the Service Request has been signed with the SRP's XML Signing Certificate relating to the SolrContingency role.

The DCC would countersign the Service Request where:

- the range of checks to verify the XML is authentically from the SRP (e.g. signature etc) are met;
- the Notified Critical Supplier ID is for an identity which previously had SMKI Certificates in the Supplier Role

The Business Originator ID will be for an identity which previously had SMKI Certificates in the Supplier Role.

For SMETS2+ Devices, the SRP would submit Signed Pre-Commands to the DCC for any Meters that might be in Prepayment Mode, where the:

- GBCS Payload has been signed using the former Supplier's Great Britain Companion Specification (GBCS) Digital Signing Keys; and
- Pre-Command has been signed with the SRP's XML Signing Certificate relating to the SolrContingency role.

The DCC would only add its Message Authentication Code (MAC) to such Commands where the:

- range of checks to verify the XML is authentically from the SRP (e.g. signature etc) are met
- Business Originator ID is for an identity which previously had SMKI Certificates in the Supplier Role

Changes from the Solution defined in CR4426 are shown in red in the following sections.

4 Description of Technical Solution

Changes to the DSP, SMETS1 Service Provider (S1SP) CGI IE, S1SP Secure and S1SP Trilliant are required for implementing the new User Role.

4.1 Solution Overview

The DSP and each S1SP will add support for the new User Role called 'SolrContingency', which will be used for the purpose of Users, in this new role, to send Commands to Devices in the event of a Supplier failure (a SoLR situation).

4.2 DSP Solution

The DSP will add support for the new User Role called 'SolrContingency', which will be used for the purpose of Users, in this new role, to send Commands to Devices in the event of a Supplier failure (a SoLR situation).

4.2.1 Managing Failed Suppliers

To allow processing of a Service Request in the SoLR Contingency mode, DSP is required to verify that the corresponding energy supplier has been identified as a failed supplier. This requires SECAS or the DCC to provide the list of Failed Suppliers, for whom the Users can act in the SolrContingency User Role, for use within DCC Total System. DCC will provide a new file upload interface within the Self Service Management Interface (SSMI) for use by DCC to share the Failed Suppliers list with DSP.

Upon receipt of the file via SSMI, the DSP will perform the anti-malware check and following validation checks against the list of Failed Suppliers:

- Identity of the Supplier
- Is the Supplier suspended
- Does the Supplier have any active SMKI certificates

The outcome of the validation checks will be presented as warnings to the SSMI User. The SSMI User will be allowed to ignore the warnings and apply the data after the review. DCC Data Systems will use the applied data for the corresponding validations.

4.2.2 User in SoLR Contingency User Role

A User capable of handling the SoLR processing can be set up as part of an existing Suppliers SEC Party and Corporation. Alternatively, they can be set up to have separate DCCKI and IKI certificates.

New ADT rules are required to be uploaded to allow the Users to send any Service Requests in the SolrContingency User Role. By default, the ADT Thresholds will be set to zero.

The Users in the SolrContingency User Role will only be allowed to submit SRV 2.1 Update Prepay Configuration. This will be managed via configuration so that other Service Requests can be made available to this User Role if needed in the future.

4.2.3 XML Signature Checks

The XML signature checks, code and design pattern introduced via SECMP0104 will be extended to add support for the SoLR processing requirements. When the Service Request has been XML signed by a User who has the SolrContingency User Role then, rather than checking that the XML Signing certificate belongs to the Business Originator identified in the

Service Request (which would fail), the DSP will instead check that the Business Originator is in the 'Failed Suppliers' list.

If this revised check fails, the Service Request will be rejected using the error code E65.

It should be noted that this Modification uses the re-purposing of Anomaly Detection checks to enforce a standard set of safe Prepayment mode configuration values. For SMETS1 Critical Service Requests, it is the S1SPs who carry out the Anomaly Detection for attributes contained in the XML[1] while the DSP carries out those checks on GBCS messages for SMETS2. There is no GBCS message relating to a SMETS1 Service Request. So now we're getting CGI to also check attributes in the XML. This new functionality means the attribute values are checked at both the DSP and the S1SPs. There might be limited consequences of attribute anomaly detection being applied twice for SR 2.1 (and any other future SMETS1 Critical Service Requests) with potentially different attribute value thresholds. This is a risk that will need to be managed by DCC Security.

4.2.4 Service Request Processing

When Service Request 2.1 is received from a Service User in the SolrContingency User Role, the following validation checks will apply.

A. Check the data included in the request (XML or Pre-command) matches the agreed rules with DCC. The values in the fields of interest will be agreed before the FIA as follows:
    1. Non-disablement calendar
    2. Emergency Credit Limit
    3. Emergency Credit Threshold
    4. Maximum Credit Threshold
    5. Maximum Meter Balance
    6. Debt Recovery Rate Cap
B. Check that the Message Code within the Signed Pre-Command indicates Update prepayment configuration (00DE for Electricity and 006F for Gas) for the Command Variants CV=5, CV=6 and CV=7..

Note: To carry out the validations, the required data will be extracted from the signed pre-command (new transform-parse use case) or from the XML, as applicable. This validation requires SR-specific processing for SR2.1, which is more than would be required for SR1.6. In the case of SR2.1, it is necessary to extract data from the body of the binary signed pre-command.

If the above checks fail then the Service Request will be rejected using a new error code E020101. This new error code will be introduced in a new version of DUIS. If the Service User uses an earlier version of DUIS, the Service Request will be rejected using the error code E2.

The SAT log entries in the SoLR processing scenario will use the ID of sender of the request rather than the ID of the Business Originator.

[1] This is referred to as Threshold Anomaly Detection of the type referred to in (b)(ii) of the definition of an Anomaly Detection Threshold.

The responses to the Service Requests will be delivered to the sender of the request instead of the Business Originator. Similarly, any DCC Alerts arising out of failed Commands will also be delivered to the sender of the relevant Service Request.

4.2.5 Device Alerts

Requirement 7 notes that a number of Safety Critical Alerts originating from the Device will need to be delivered to the Failed Supplier. In some situations, these Device Alerts are expected to be routed to the Failed Supplier's SRP. It is expected that any such routing will be managed outside of DCC Total System and DSP will continue to deliver these Alerts to the Business Target (Failed Supplier) at the existing end point.

4.2.6 Requirements Traceability

#	DSP Impact
1	DSP will add support for the new User Role 'SolrContingency'.
2	None
3	Service Request 2.1 'Update Prepay Configuration' will be configured as the only Service Request allowed for a User in the SoLR Contingency User Role. Other Service Requests can be added by way of configuration for use by this User Role.
4	None
5	The processing of Service Request 2.1 'Update Prepay Configuration' will be amended to allow only one set of parameters if submitted by a User using the SolrContingency User Role.
6	DSP will make use of the Failed Suppliers list to ensure that the Users in the SolrContingency User Role will only be able to send the Service Request listed in requirement 3 and will only be able to do so in the event of a Supplier failure and upon specific instruction from the Authority.
7	None

4.3 S1SP CGI IE Solution

IE S1SP will support the new SEC User Role of SolrContingency in line with existing processing where IE S1SP will receive the required reference data from files sent by DSP via the Management Interface.

In order to process Service Requests from an SRP, where requests are received from a Service User in the SolrContingency User Role, the 'S1VE100' validation rule that checks the Business Originator ID in the request matches the ID in the signing certificate will be removed from the Check Cryptographic Protection validation. All other existing validation rules for the 'S1VE100' will remain and any failure will result in the S1SP Alert 'S1VE100' being returned to users indicating the Service User signature has failed authentication.

To ensure any SRP acting in the SolrContingency Role is an eligible user, the validation rule for the 'S1VE2' access control check will be modified explicitly for Service Requests where the User Role is SolrContingency. When a request is signed with a "SolrContingency" signing certificate, IE S1SP will take the User Role of the User ID from the signing certificate and get the SEC User Role from the inventory held in the Management Interface data to check that the retrieved role is allowed to use that Service Reference Variant. If this check fails, S1SP Alert 'S1VE2' will be returned to the user indicating that the User Role and Service Request Combination failed verification

The new SolrContingency User Role will be configured against SRV 2.1 only in the CGI IE S1SP database with the option to add additional SRVs in future via the same configuration. If Service Users in the SolrContingency User Role submit a Service Reference Variant outside of the authorised list an S1SP Alert 'S1VE2' will be returned to the user indicating that the User Role and Service Request Combination failed verification.

Updates to the CGI IE S1SP Security Module component High Level Design document will be made to reflect the modification of validation rules set out above.

4.4 S1SP Secure Solution

Requirement 3 states SRV 2.1 is a Critical Service Request, plus the other SRVs that may be added to the configurable list could be Critical Service Requests. As such, the full set of DUIS validations at the S1SP for Critical Service Requests has been considered as part of this initial assessment.

The technical areas for change can be considered in the following two main parts:

Updates to existing DUIS validations in the Secure S1SP system:

This section lists required changes to existing DUIS validations that are currently performed by the Secure S1SP system.

- S1VE100 confirms that the entity identifier in the signing certificate matches the business originator in the request. This validation would need to be updated/suppressed, otherwise the request would be rejected for this reason.

- S1VE3 validation checks the user sending the request has the status 'A' (Active). This would need to be updated if the user status of the revoked supplier is no longer expected to be 'A' (Active) at the time of sending the request.

Continuing to return device alerts for revoked supplier:

Regarding the following statement from the business requirements:

"The DCC should remain able to send Alerts to the Supplier after the Supplier's Certificates have been revoked (noting that they will be routed to the failed Supplier's SRP)"

There should be no change required provided the trust anchor cells in the Secure S1SP system are left as they are after the supplier is revoked. This assessment assumes that the original supplier certificates will be left in the trust anchor cells in the Secure S1SP system until an SRV 6.23 (Change of Supplier) is received at the Secure S1SP system for the device.

Secure S1SP will continue to notify all the alerts being received from the device.

4.5 S1SP Trilliant Solution

The development of this solution based on the information currently available will require:

- Changes to the S1SP to load new file values, including checks to ensure that the user new role does not trigger any file loading failures

- Any other S1SP requirements to be confirmed at the Full Impact Assessment stage

5 Impact on Systems, Processes and People

This section describes the impact of SECMP0134B on Services and Interfaces that impact Users and/or Parties.

5.1 DSP Components

5.1.1 Security Impact

The implementation will be security assured throughout. Assurance includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

A schema update will be required on Datapower appliances to validate the new DUIS schema which needs to be applied across each environment.

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

5.1.2 Technical Specifications, DUIS and DUGIDS

DUIS and DUGIDS requires changes to add support for the new User Role and the new error code. The DUIS schema also needs changes to support this.

Given the extent and nature of this change, it is expected this Modification would be part of a SEC Release featuring a DUIS uplift. Charges associated with the DUIS uplift would be shared across other Modifications and Change Requests with DUIS changes resulting in a decrease in Design, Build and PIT costs.

5.1.3 Request Management

Request Management needs to be updated to handle the processing changes to Service Request 2.1 as described above.

5.1.4 Transform

Transform Parse needs to be updated to extract data required for validation from the signed pre-command of the Service Request 2.1.

5.1.5 Data Management

Configuration changes are required to Data Management to support the new User Role SolrContingency.

Data Management will need to store the list of Failed Suppliers for whom the SoLR processing by another Service User is permitted. Data Management will also need to provide an API to carry out the validation of the data contained in the Failed Suppliers file uploaded to SSMI.

5.1.6 Self Service Management Interface

SSMI will provide a new file upload interface for DCC to upload the Failed Suppliers file.

5.1.7 Key Management System

Key Management System will need updates to check if there are active SMKI Certificates for the Supplier as part of the Failed Suppliers file validation.

5.1.8 Infrastructure Impact

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

Additional processing and storage will be required; however, they are not sufficiently large to warrant the procurement of additional compute power or storage. The change does not impact the DSP resilience or DR implementation.

It will be necessary to deploy the revised DUIS schema to Data Power devices.

5.1.9 Service Impact

It is anticipated this Modification will require some pre-go live service preparation to update support documentation and some early life support for a short period after go live. However, it is not thought that there will be a material impact on the ongoing service. A more detailed service impact will be completed as part of the Full Impact Assessment.

No changes to Service Level Agreements or reporting are expected as a result of this change.

5.2 DCC Security

As noted in section 4.2.3 above, this Modification uses the re-purposing of Anomaly Detection checks to enforce a standard set of safe Prepayment mode configuration values. There might be limited consequences of attribute anomaly detection being applied twice for SR 2.1 (and any other future SMETS1 Critical Service Requests) with potentially different attribute value thresholds. This is a risk that will need to be managed by DCC Security.

5.3 SEC Party Impacts

The XML signature checks introduced in SECMP0104 will be extended to add support for the SoLR processing requirements. When the Service Request has been XML signed by a User who has the SolrContingency User Role then, rather than checking that the XML Signing certificate belongs to the Business Originator identified in the Service Request (which would fail), the DSP will instead check that the Business Originator is in the ‘Failed Suppliers’ list.

If this revised check fails, the Service Request will be rejected using the error code E65. SEC Parties will need to ensure they use the XML Signing certificate belonging to the Business Originator identified in the Service Request for a successful completion.

6 Implementation Timescales and Approach

This change is expected to be included in a future SEC Release. Design, Build, and PIT is expected to take between three and six months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA.

6.1 Testing and Acceptance

There will be an impact to Systems Integration Testing (SIT) as a result of this change. SIT activities will include test preparation, execution and reporting as required, as well as Service Reference Variant (SRV) testing to verify the use of critical commands on selected devices. The tests will also include:

- Users in the new SolrContingency role can obtain just XML Signing certificates
- ADT files for new SolrContingency role and the list of failed suppliers can be uploaded via SSMI
- SolrContingency Users are able to submit ADT files for SR2.1
- SolrContingency Users are only able to submit SR2.1 (using each valid Command Variant) to set a meter (ESME and GSME) into safe Prepayment mode for a Failed Supplier, otherwise getting an error
- SolrContingency Users are able to update SMETS1 (for each S1SP) and SMETS2 (for each CSP) meters from Prepayment mode into safe Prepayment mode
- Device Alerts are still delivered to the failed Supplier while they remain the Responsible Supplier for the meter
- Negative testing of the security model for SolrContingency Users and for the failed Supplier

The business process relating to SolrContingency Users creating ARO and SRO will not be tested by SIT.

User Integration Testing (UIT) will test the SoLR functionality by creating a new Service User for use as a failed supplier and a new SRP Service User will be created along with the relevant SMKI certificates. During test execution, SSMI will be tested to ensure that an existing Service User can be marked as a failed supplier. SR2.1 will be sent to an ESME and GSME on one SMETS1 and one SMETS2 meter set by the new SRP Service User.

The System Integrator will be required to manage SIT and UIT. These costs will be included in the FIA.

7 Costs and Charges

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

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional requirements. 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.

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	Days to Create FIA	Cost to Create FIA
DSP & all S1SPs	£650,500 to £1,161,000	30	£39,035

Table 2: SECMP0134B CR4719 Cost

These charges represent an increase of approximately 7% over CR4426.

The phases included are as follows.

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.

It should be noted that these costs are similar to, but slightly higher, than the previous submission, CR4426.

Based on the existing requirements, the fixed price cost for a Full Impact Assessment is **£39,035** and would be expected to be completed in 30 days.

Appendix A: Risks, Assumptions, Issues, and Dependencies

The tables below provide a summary of any Risks, Assumptions, Issues, and Dependencies (RAID) observed during the production of this PIA. DCC requests that the Working Group considers this section and considers any material matters that have been identified. Changes may impact the proposed solution, implementation costs and/or implementation timescales.

Risks

Ref	Description	Status/Mitigation
MP134B-R1	For Requirement 3, what would be the mechanism / process to inform Service Providers and Service Users that additional SRVs are to be enabled?	Open, should be included as part of a FIA request
MP134B-R2	For Requirement 6, what is the process that allows Users with the SolrContingency User Role to send Service Requests in the authorised list?	Open, should be included as part of a FIA request
MP134B-R3	If SRV 2.1 fails due to HAN or WAN connectivity or any other reason, then there could be a risk that consumers are going off supply in a NO CREDIT condition.	Open
MP134B-R4	There might be consequences of attribute anomaly detection being applied twice for SR 2.1 (and any other future SMETS1 Critical Service Requests) with potentially different attribute value thresholds. This risk will need to be managed by DCC Security.	Open

Assumptions

These assumptions have been used in the creation of this PIA. Any changes to the assumptions may require DCC to undertake further assessment, prior to the contracting and implementation of this change.

Ref	Description	Status/Mitigation
MP134B-A1	The Business Originator ID in a Service Request submitted by an SRP acting in the SolrContingency role will be that of the failing Supplier.	Open
MP134B-A2	The DCC Service User status of a failing Supplier will be ‘Active’ throughout the period during which an SRP acting in the SolrContingency role is submitting Service Requests on behalf of that Supplier.	Open
MP134B-A3	An SRP acting in the SolrContingency role will have knowledge of the failing Supplier’s Originator Counter value(s).	Open
MP134B-A4	A Service Request arriving from a SRP acting in the SolrContingency role will appear in all respects as if it had arrived from an Energy Supplier with the exception of the	Open
MP134B-A5	Future additions to the list of Service Requests for which SolrContingency is an Eligible User Role will be subject to Change Request.	Open

MP134B-A6	Submission of Update Payment Mode requests by an SRP acting in the SolrContingency role will be done in such a manner as not to overload DCC Systems.	Open
MP134B-A7	The will be no change to S1SP Service Request processing required by Clauses 4.2 and 12.1 of SEC Appendix AM SMETS1 Supporting Requirements.	Open
MP134-A8	The arrival of SRV 2.1 (and further SRVs that may be added to the configurable list) will be the same as if it had arrived from the supplier, with the exception of a different Service User signature.	Open
MP134B-A9	The failed supplier will remain 'active' in the Registration data received via the Management Interface	Open
MP134B-A10	Assume that the business originator ID sent from the SRP in the SRV requests shall always match: o The business originator ID actively associated with the MPxN of the target device in the SMI data (with the date range of this association still being valid/current even though the supplier may no longer be considered active). o The business originator ID that is the notified critical supplier in the trust anchor cell for the target device.	

Appendix B: Glossary

Acronym	Definition
ADT	Anomaly Detection Threshold
ARO	Authorised Responsible Officers
CAN	Contract Amendment Note
CoS	Change of Supplier
CR	DCC Change Request
CSCP	Customer Supply Continuity Plan
CSP	Communication Service Provider
DCC	Data Communications Company
DCCKI	DCC Key Infrastructure
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
IKI	Infrastructure Key Infrastructure
MAC	Message Authentication Code
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
ROM	Rough Order of Magnitude (cost)
SAT	Service Audit Trail
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SoLR	Supplier of Last Resort
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specification
SMKI	Smart Meter Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SoLR, SOLR	Supplier of Last Resort
SRO	Senior Responsible Officers
SRP	Shared Resource Provider
SRV	Service Reference Variant
SSMI	Self Service Management Interface
S1SP	SMETS1 Service Provider
UIT	User Integration Testing
XML	eXtensible Markup Language