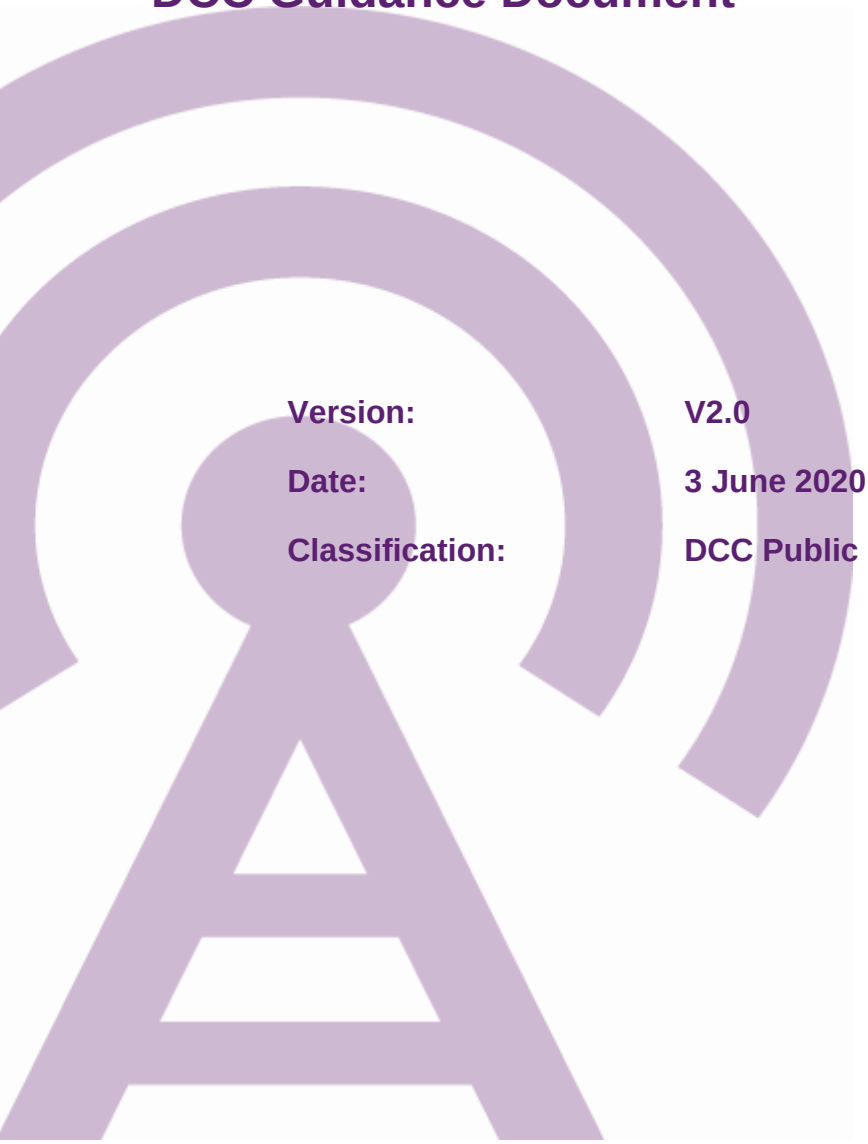
Data Communications Company

Migration Error Handling and Retry Strategy

DCC Guidance Document



Version:	**V2.0**
Date:	**3 June 2020**
Classification:	**DCC Public**

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide guidance regarding how DCC and Users should act when an error occurs, within the DCC Total System or the Systems of a Smart Metering System Operator (SMSO) acting on behalf of the DCC, during the period where a SMETS1 Installation is being prepared for Migration or being Migrated from an existing SMSO to the DCC. It is produced in accordance with Clause 8.8 of the SMETS1 Transition and Migration Approach Document (TMAD) which is Appendix AL of the SEC .

This document is broken down into the phases of Migration and details the types of exceptions/errors that pertain to that phase of Migration (e.g. Demand Commitment, Migration Authorisation, Commissioning etc).

Capitalised terms in this document have the meaning given to them in TMAD or, if not defined in TMAD, in Section A of the SEC.

1.2 Scope

The Migration Error Handling and Retry guidance document:

a) describes the type of exceptions/errors that can occur at each stage in connection with the migration of a SMETS1 Installation;

b) sets out procedures to be followed and actions to be taken by Users and DCC for the purposes of investigating and correcting such error instances;

c) describes the retry and timeout approach when the SMETS1 Service Provider (S1SP) attempts to establish a session with the Communications Hub; and

d) outlines the approach to Dormant Meter error handling.

1.3 Out of Scope

Where an energy supplier wishes to Commission the Devices comprising a SMETS1 Installation itself, it should send the sequence of Service Requests as described in Table 6.3 of the TMAD via the DCC User Interface.

As far as DCC is concerned, where the supplier is doing the Commissioning, Migration is complete for SMETS1 Installations that indicate success in the S1SP Commissioning File. The Migration Control Centre will have oversight of the commissioning activities performed by the supplier. The Error Codes that may be sent during the Commissioning of successfully Migrated devices are detailed in the DCC User Interface Specification (DUIS) v 3.0b and covered by the Error Handling Strategy. As such this is not in scope of this document.

For clarity, where the Commissioning Party is Commissioning Devices on behalf of the supplier, Migration does include the actions of the Commissioning Party and associated systems which is therefore in scope of this document.

1.4 Definitions

1. Migration Control Centre - A DCC function established to control the end to end enrolment and adoption processes, systems and stakeholders to ensure the DCC Total System, Customers and consumers are protected and to meet regulatory obligations.
2. DCC's Service Management System – DCC's Incident Management Solution made up of the BMC Remedy Application, Self-Service Management Interface (SSMI) and the Self-Service Interface (SSI).

1.5 General Provisions

This document should be read in conjunction with the following documents;

1. TMAD v4.0 (which builds on Appendix AL) details additional Error Codes that may be generated in response to Commissioning Requests submitted by the Commissioning Party, where those differ from the Response Codes in DUIS v3.0b, and describes the modifications to Appendix AG (Incident Management Policy) that will be applied during migration;
2. Error Handling Strategy v3.0 draft 1 which classifies error instances and error handling procedures relating to DUIS v3.0b (produced by DCC for users to align with DUIS3);
3. Migration Authorisation Mechanism v2.0 which describes the mechanism by which Responsible Suppliers input into the Migration process;
4. Migration Scaling Methodology v3.0 which describes the mechanism by which Responsible Suppliers submit Daily Migration Demand Requests; and
5. Migration Reporting Regime v2.0 which describes how Responsible Suppliers and others track progress of a SMETS1 Installation through the Migration process.

2 Migration Error Handling

2.1 SharePoint Unavailability

2.1.1 SharePoint Unavailability

Impacted parties are advised to raise an Incident and email the Migration Control Centre (migration@smartdcc.co.uk) where the DCC SharePoint is inaccessible for receiving files or submission of the following files:

- Indicative Migration Forecasts for Active Meters;
- Daily Migration Demand requests for Active Meters;
- Migration Authorisations for Active Meters; and
- Responses to Dormant Meter Migration notifications.

It is possible that such Incidents could relate to an individual party or multiple parties. Only parties affected by the Incident will be notified through the Self-Service Interface as an Interested Party. For clarity, this Incident will not be classified as an Incident relating to Migration.

The DCC will be required to resolve this Incident in accordance with the standard Incident Target Resolution Time described in the Incident Management Policy, whilst providing timely updates to the DCC's Service Management System. The DCC will advise impacted parties about a suitable workaround if appropriate.

Once the Incident has been resolved, the DCC will advise impacted parties to resume the submission and receipt of respective files through the DCC SharePoint.

2.1.2 SharePoint Unavailability (DCC)

The DCC raises an Incident where the DCC SharePoint is inaccessible for receiving files or submission of the following files:

- Migration Demand Commitments;
- Dormant Meter notifications for Device configuration / firmware upgrade;
- Dormant Meter notifications for Migration scheduling; and
- all Migration Reports defined in the Migration Reporting Regime.

Impacted parties affected by any such Incident will be notified through the Self-Service Interface as an Interested Party. For clarity, this Incident will not be classified as an Incident relating to Migration.

The DCC will be required to resolve this Incident in accordance with the standard Incident Target Resolution Time described in the Incident Management Policy, whilst providing timely updates to the DCC's Service Management System. The DCC will advise impacted parties about a suitable workaround if appropriate.

Once the Incident has been resolved the DCC will submit files through the DCC SharePoint.

2.2 Demand Commitment

2.2.1 Demand Commitment not met

Following the demand allocation to each supplier, as defined in the Migration Scaling Methodology, there are several scenarios where the Migration Demand Commitment may not be met. These are outlined below, the details relating to how these scenarios (where relevant) can be handled is detailed in subsequent sections 2.3 and 2.4 of this document:

a) The Responsible Supplier has submitted a number of Migration Authorisations less than the Migration Demand Commitment;

b) DCC systems cannot cope with the demand notwithstanding the fact that the Migration Demand Commitments were given;

c) The Migration Control Centre was not able to verify the supplier signature associated with the Migration Authorisation;

d) The Requesting Party identified errors in the Migration Authorisation file; and

e) The Requesting Party was unable to generate a Migration Common File (e.g. due to system unavailability or the unavailability of data from the SMETS1 SMSO).

The Requesting Party submits daily Migration Summary Reports (one per Party associated with a Migration Authorisation) to the Migration Control Centre. Each week, the Migration Control Centre provides the following report to each Authorising Party on the Migration Authorisations received against the Migration Demand Commitment for the previous four Migration Weeks:

1. Report 8 – 'Summary of Migration Authorisations Received vs DCC Migration Commitment'.

2.3 Migration Authorisation

2.3.1 Migration Authorisation Signature Error

Prior to any Migration Authorisation, for Active Meters only, being transferred from the DCC SharePoint site to the Requesting Party the signature must be checked by the DCC.

Where the supplier signature associated with the Migration Authorisation file is rejected the supplier will, as soon as is reasonably practicable, be contacted by the DCC Migration Control Centre via telephone and email to ensure they are aware of the failure(s).

The suggested action on the supplier is to check the validity of the Certificate and the signature used to sign the file, regenerate the Migration Authorisation and submit to the DCC. These actions will need to be completed in line with the timescales set out in the Migration Authorisation Mechanism document.

2.3.2 Migration Authorisation File Error

On receipt of Migration Authorisations (in relation to Active or Dormant meters), the Requesting Party undertakes the checks (where relevant) described in the table below for the SMETS1 Installations.

Validation Check	Reason Code
Confirm the MPAN provided is a registered MPAN in the SMSO system	MA001
Confirm the MPRN provided is a registered MPRN in the SMSO system	MA002
Confirm the Migration Week provided is a Monday	MA003
Confirm the Migration Week has not ended	MA004
Confirm the Migrate On date is within the specified Migration Week	MA005
Confirm the Migrate On date is a date in the future	MA006
Confirm the Supplier is the Active Supplier for the MPAN as per the SMSO system	MA007

Confirm the Supplier is the Active Supplier for the MPRN as per the SMSO system	MA008
Confirm both the MPAN and MPRN has been provided where the supplier is the Active Supplier for both Devices	MA009
Confirm the Active Supplier has provided the SupplierCertificateIDs for the ESME	MA010
Confirm the Active Supplier has provided the SupplierCertificateIDs for the GSME and GPF	MA011
Confirm the DCC Migration Authorisation contains only Dormant Installations	MA012
Confirm the DCC Migration Authorisation contains the MPAN and MPRN for a dual fuel installation	MA013
Confirm a DCC Migration Authorisation specifies an ESME Supplier ID	MA014
Confirm a DCC Migration Authorisation for a dual fuel installation specifies a GSME Supplier ID	MA015
A certificate serial number has been provided without the corresponding issuer name	MA016
The installation is currently blocked from being migrated.	MA017
If ESME and GSME have same responsible Supplier (Sec Party) then the authorisation should be submitted as 1 MA.	MA018

Where a Reason Code is required, the Requesting Party includes this in the Migration Authorisation Validation Response file sent to the DCC. The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the Reason Code as per the table above:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'; and
2. Report 10 - 'Migration Authorisation Validation Responses in the Reporting Period' (only for Active Installations)

The suggested action on the Responsible Supplier is to review/triage the relevant Reason Code and resubmit the Migration Authorisations for a subsequent Migration Week.

The checks MA012 - MA015 and MA017 are only relevant for Dormant Meter Migrations and the Responsible Supplier will have no action in relation to these Reason Codes.

2.4 Migration Common File (including Validation)

2.4.1 Requesting Party unable to generate Migration Common File

Where the Requesting Party is unable to generate a Migration Common File for any reason (e.g. system unavailability), the Requesting Party will raise an Incident via the Migration Control Centre. The Incident would be assigned to the Requesting Party and managed by the Migration Control Centre.

Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System

Once the Incident has been resolved, the Requesting Party will process the backlog of SMETS1 Installations that have not been included in a Migration Common File if the Migration Authorisations for relevant SMETS1 Installations are still valid. In this scenario, SMETS1 Installations which have been flagged as a 'priority' will be processed first.

The Requesting Party generates a Migration Authorisation Completion Response file which will indicate to the DCC if the Migration Authorisation is no longer valid.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

If the Migration Authorisation is no longer valid, the DCC will not Migrate the relevant SMETS1 Installations and the supplier should reschedule the migration by adding the SMETS1 Installation(s) to a Migration Authorisation for a subsequent Migration Week.

2.4.2 Migration Common File whole file validation error

On receipt of the Migration Common File, which is generated by the Requesting Party, the S1SP and the Dual Control Organisation (DCO) undertake the sequence of checks described in Table 5.9 in the TMAD. Where one of these checks fails, the S1SP/DCO stops processing the file and raises an Incident. This Incident would be assigned to the Requesting Party and managed by the Migration Control Centre.

Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the Requesting Party will regenerate and resubmit the Migration Common File to the S1SP and the DCO.

If the Incident results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation is valid, those SMETS1 Installations will fail at a subsequent step during Migration.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The suggested action on the supplier is to schedule the failed SMETS1 Installation into a subsequent Migration Week.

2.4.3 S1SP unable to generate Migration Common Validation File

Where the S1SP is unable to generate the Migration Common Validation File for any reason (e.g. system unavailability), the S1SP will raise an Incident. This Incident would be assigned to the S1SP and managed by the Migration Control Centre.

Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the S1SP will generate the Migration Common Validation File and process the backlog for SMETS1 Installations. For clarity, the processing/generating of these files will occur in order of receipt.

If the Incident results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation is valid, those SMETS1 Installations will fail at a subsequent step during Migration.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The suggested action on the supplier is to schedule the failed SMETS1 Installation into a subsequent Migration Week.

2.4.4 Migration Common Validation File whole file validation error

On receipt of the Migration Common Validation File, which is generated by the S1SP, the Requesting Party and DCO undertakes the sequence of checks described in Table 5.9 in the TMAD. Where one of these checks fails, the Requesting Party or DCO stops processing the file and raises an Incident. This Incident would be assigned to the S1SP and managed by the Migration Control Centre.

Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the Requesting Party will regenerate and resubmit a new Migration Common File with affected SMETS1 Installations to the S1SP if the Migration Authorisation is still valid.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The suggested action on the supplier is to schedule the failed SMETS1 Installation into a subsequent Migration Week.

2.4.5 Migration Common File SMETS1 Installation Level Validation Error

Where all the checks and processing at Table 5.9 of the TMAD are successful, the S1SP generates a Migration Common Validation File with the same Migration Header as that of the Migration Common File. The S1SP undertakes the checks described in Table 5.10, should one of those checks fail for a SMETS1 Installation, the S1SP shall append the SMETS1 Installation element in the Migration Common Validation File to detail the FailedStepNumber and the SupportingData. This file is then sent to the Requesting Party and the DCO.

The failure will be included in the next Migration Authorisation Completion Response file which is generated by the Requesting Party based on information in the Migration Common Validation File.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Codes as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The suggested action on the Responsible Supplier is to review the validation failures with the relevant SMSO and correct the data as appropriate. Even though this will be a User led investigation, DCC can provide support (e.g. raise Registration Data Incidents).

Once the data issues have been resolved, the Responsible Supplier will be able to add the affected SMETS1 Installations to a Migration Authorisation for a subsequent week.

2.5 Migration (including SIM cutover, Migration Group Encrypted File & Migration Group File)

2.5.1 Requesting Party unable to trigger Migration of any Installation

Where the Requesting Party has received a Migration Common Validation File from an S1SP, which indicates no errors relating to a particular SMETS1 Installation, the Requesting Party shall attempt to trigger the Migration of those SMETS1 Installations. Should there be a system outage pertaining to the Requesting Party, the Requesting Party will raise an Incident via the Migration Control Centre. This Incident would be assigned to the Requesting Party and managed by the Migration Control Centre.

Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the Requesting Party will process the backlog in order of receipt.

If the Incident results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation remains valid or if the S1SP does not receive the S1SP Required File Set for the SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24, those SMETS1 Installations will fail at a subsequent step during Migration.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The suggested action on the supplier is to schedule the failed SMETS1 Installation into a subsequent Migration Week.

2.5.2 SMSO/CSP unable to Migrate any Installation

Where the SMETS1 SMSO, or any associated systems (e.g. Communications Service Provider (CSP)), is unable to configure the SMETS1 Installation so that it can communicate with the DCC Total System or the CSP is unable to Migrate the SIM on behalf of the SMSO for any reason (e.g. system unavailability), the SMSO will issue a communication to the Migration Control Centre and may also notify the Responsible Suppliers in accordance to the arrangements in place between the SMSO and the Responsible Suppliers.

On receipt of such communication from the SMSO, the Migration Control Centre will issue a communication to all Interested Parties to ensure suppliers who have no arrangements with the SMSO are notified.

For clarity, this is not an Incident within the DCC's Service Management system because the contractual arrangements between the SMETS1 SMSO and the CSP are outside of the DCC contractual framework.

If this results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation remains valid or if the S1SP does not receive the S1SP Required

File Set for the SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24, those SMETS1 Installations will fail at a subsequent step during Migration.

For SMETS1 Installations where GroupID is “CB”:

If the Requesting Party is unable to configure the SIM of the SMETS1 Installations to communicate with the DCC Total Systems as per retries defined in Section 3.2 or within a time duration such that this results in the S1SP not receiving the S1SP Required File Set for those SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24, the Requesting Party will report the failure to migrate these SMETS1 Installations in the next Migration Authorisation Completion Response.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

The suggested action on the supplier is to schedule the failed SMETS1 Installations into a subsequent Migration Week.

2.5.3 Requesting Party unable to Migrate specific Installation(s)

The Requesting Party / SMSO may not be able to Migrate a specific SMETS1 Installation for any of the following reasons:

a) errors were detailed for that SMETS1 Installation in the associated Migration Common Validation File;

b) Wide Area Network communications have not been established within the last 7 days;

c) the Device is not configured in accordance with the requirements of the SMETS1 Supporting Requirements and the SMSO is aware that the device should have been configured as per the SMETS1 Supporting Requirements document;

d) the SMETS1 SMSO, or any associated systems (e.g. CSP), was unable to configure the SMETS1 Installation so that it can communicate with the DCC Total System.

The failure will be included in the next Migration Authorisation Completion Response file generated by the Requesting Party.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The SMSO may choose to liaise with the Active Responsible Supplier directly to notify them of the failure.

The suggested action on the supplier is to liaise with the SMSO to fix the error and reschedule the migration by adding the SMETS1 Installation(s) to a Migration Authorisation for a subsequent Migration Week.

For Dormant Meter Handling, please refer to Section 4.

2.5.4 Requesting Party unable to generate Migration Group File/Migration Group Encrypted File

Where the Requesting Party is unable to generate the Migration Group File/Migration Group Encrypted File for any reason (e.g. system unavailability), the Requesting Party will raise an Incident.

The Incident would be assigned to the Requesting Party and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System.

Once the Incident has been resolved, the Requesting Party will process the backlog in order of receipt.

If the Incident results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation remains valid or if the S1SP does not receive the S1SP Required File Set for the SMETS1 Installations within 24 hours of the Migration Common Validated

File being generated as per TMAD Clause 5.24, those SMETS1 Installations will fail at a subsequent step during Migration.

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The suggested action on the supplier is to schedule the failed SMETS1 Installation into a subsequent Migration Week.

2.5.5 Requesting Party unable to generate Migration Group File/Migration Group Encrypted File (post SIM Handover beyond 24 hours)

There may be a scenario where SMETS1 Installations have been configured so that they can communicate with the DCC Total System in advance of the generation of the Migration Group Encrypted File and the Migration Group File.

Where this scenario occurs, the Requesting Party will investigate and fix as appropriate.

Likely actions include the following:

1. if the problem can be fixed within 24 hours the Requesting Party generates and submits the Migration Group File/Migration Group Encrypted File. In this scenario, the S1SP may not have received the S1SP Required File Set within 24 hours of the Migration Common File being generated pursuant to the TMAD Clause 5.24; or
2. if the resolution time is longer than 24 hours, on instruction from the Migration Control Centre the affected SMETS1 Installations will be reconfigured so that it can communicate with the original SMSO or a new MCF could be regenerated.

For SMETS1 Installations where GroupID = "CB", the Requesting Party will resubmit the affected Installations for migration in a new Migration Common File without carrying out the 7 days communication check as per TMAD check 5.12.(c).

If the resolution time is longer than 24 hours the following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

The suggested action on the supplier is to resubmit the affected SMETS1 Installations in a Migration Authorisation for a subsequent Migration Week.

2.5.6 Migration Group File whole file validation error

On receipt of the Migration Group File, which is generated by the Requesting Party, the S1SP undertakes the sequence of checks described in Table 5.9 in the TMAD.

Where one of these checks fails, the S1SP stops processing the file and raises an Incident. This Incident would be assigned to the Requesting Party and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party. The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the Requesting Party will regenerate and resubmit the Migration Group File to the S1SP if the Migration Authorisation is still valid.

If this results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation remains valid or if the S1SP does not receive the S1SP Required File Set for the SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24, those SMETS1 Installations will fail at a subsequent step during Migration.

For SMETS1 Installations where GroupID is "CB":

The Requesting Party will fix the issue, regenerate and resubmit the Migration Group File to S1SP to process the affected SMETS1 Installations. However, if the Incident will result in the affected SMETS1 Installations not being processed since the time taken for incident resolution would result in the S1SP not receiving the S1SP Required File Set for those SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24, the Requesting Party will resubmit the affected SMETS1 Installations in a new Migration Common File without carrying out the 7 days communication check as per TMAD check 5.12.(c).

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

If the Migration Authorisation is no longer valid, the SMETS1 Installations will need to be rescheduled by the supplier in a subsequent Migration Week.

2.5.7 Migration Group Encrypted File whole file validation error

On receipt of the Migration Group Encrypted File, which is generated by the Requesting Party, the S1SP and the DCO undertakes the sequence of checks described in Table 5.9 in the TMAD.

Where one of these checks fails, the S1SP/DCO stops processing the file and raises an Incident. This Incident would be assigned to the Requesting Party and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the Requesting Party will regenerate and resubmit the Migration Group Encrypted File to the S1SP/DCO if the Migration Authorisation is still valid.

If this results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation remains valid or if the S1SP/DCO does not receive the S1SP/DCO Required File Set for the SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24 and Clause 5.18, those SMETS1 Installations will fail at a subsequent step during Migration.

For SMETS1 Installations where GroupID is "CB":

The Requesting Party will fix the issue, regenerate and resubmit the Migration Group Encrypted File to S1SP to process the affected SMETS1 Installations. However, if the Incident will result in the affected SMETS1 Installations not being processed since the time taken for incident resolution would result in the S1SP/DCO not receiving the S1SP/DCO Required File Set for those SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24 and Clause 5.18, the Requesting Party will resubmit the affected SMETS1 Installations in a new Migration Common File without carrying out the 7 days communication check as per TMAD check 5.12.(c).

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the Migration Authorisation is no longer valid, the SMETS1 Installations will need to be rescheduled by the supplier in a subsequent Migration Week.

2.5.8 S1SP Required File Set SMETS1 Installation level validation error

Where a SMETS1 Installation fails any of the checks described in Table 5.25 of the TMAD, the S1SP undertakes no further processing in relation to such SMETS1 Installation and includes the FailedStepNumber in the associated S1SP Commissioning File.

For SMETS1 Installations where GroupID = “CB”,

Where any of the SMETS1 Installation fails these checks, the Migration Control Centre will raise a Service Request on the Requesting Party. The Requesting Party will be required to resolve the Service Request in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates. Once the Request has been resolved, the Requesting Party will resubmit the affected Installations for migration in a new Migration Common File without carrying out the 7 days communication check as per TMAD check 5.12.(c).

The failure will be included in the next Migration Authorisation Completion Response file generated by the Requesting Party based on information in the S1SP Commissioning File.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the:

1. FailedStepNumber in Report 2 – ‘Migration Failures Occurring in the Reporting Period’; and
2. Reason Code as per Appendix A.1 in Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the ToBeCommissionedByDCC flag is set to ‘False’, then a S1SP Commissioning File will be sent to the both the Supplier and the Requesting Party. This will include details of the failure(s). The Requesting Party will correct the data as appropriate and liaise with Suppliers if so required.

2.5.9 Migration Group Encrypted File validation error (S1SP)

Where a SMETS1 Installation fails any of the checks described in Clause 5.23 of the TMAD, the S1SP stops processing the file and raises an Incident.

This Incident would be assigned to the Requesting Party and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD.

Once the Incident has been resolved, the Requesting Party will regenerate and resubmit the Migration Group Encrypted File to the S1SP if the Migration Authorisation is still valid.

If this results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation remains valid or if the S1SP does not receive the S1SP Required File Set for the SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24, those SMETS1 Installations will fail at a subsequent step during Migration.

For SMETS1 Installations where GroupID is “CB”:

The Requesting Party will fix the issue, regenerate and resubmit the Migration Group Encrypted File to S1SP to process the affected SMETS1 Installations. However, if the Incident results in the affected SMETS1 Installations not being processed since the time taken for incident resolution would result in the S1SP not receiving the S1SP Required File Set for those SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.24, the Requesting Party will resubmit the affected SMETS1 Installations in a new Migration Common File without carrying out the 7 days communication check as per TMAD check 5.12.(c).

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the Migration Authorisation is no longer valid, the SMETS1 Installations will need to be rescheduled by the supplier in a subsequent Migration Week.

2.5.10 Migration Group Encrypted File SMETS1 Installation level validation error (DCO)

Where a SMETS1 Installation fails any of the checks described in Clause 5.15 (a) of the TMAD, the DCO stops processing the file and raises an Incident.

This Incident would be assigned to the Requesting Party and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Requesting Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD.

Once the Incident has been resolved, the Requesting Party will regenerate and resubmit the Migration Group Encrypted File to the DCO if the Migration Authorisation is still valid.

If this incident results in the affected SMETS1 Installations not being processed whilst the Migration Authorisation remains valid or if the DCO does not receive the DCO Required File Set for the SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.18 those SMETS1 Installations will fail at a subsequent step during Migration.

For SMETS1 Installations where GroupID is “CB”:

The Requesting Party will fix the issue, regenerate and resubmit the Migration Group Encrypted File to S1SP to process the affected SMETS1 Installations. However, if the Incident will result in the affected SMETS1 Installations not being processed since the time taken for incident resolution would result in the DCO not receiving the DCO Required File Set for those SMETS1 Installations within 24 hours of the Migration Common Validated File being generated as per TMAD Clause 5.18, the Requesting Party will resubmit the affected SMETS1 Installations in a new Migration Common File without carrying out the 7 days communication check as per TMAD check 5.12.(c).

The following supplier facing report, detailed in the Migration Reporting Regime, confirms the Reason Code as per Appendix A.1:

1. Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the Migration Authorisation is no longer valid, the SMETS1 Installations will need to be rescheduled by the supplier in a subsequent Migration Week.

The following sections 2.6 and 2.7 of the document describe the error handling and resolution steps for SMETS1 Installations that have failed Migration and cannot be communicated with by the supplier either through the SMSO or DCC and will require some intervention.

2.6 Migration (including Device validation and key rotation)

The scenarios covered within section 2.6 are related to error handling and resolution of failures in processing of SMETS1 installations by S1SP or DCO prior to commissioning.

2.6.1 S1SP unable to process any S1SP/DCO Viable Installation

Where the S1SP or DCO is unable to process any S1SP/DCO Viable Installation for any reason (e.g. system unavailability) the S1SP or DCO will raise an Incident.

This Incident would be assigned to the S1SP and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP or DCO will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the S1SP or DCO will process the backlog.

2.6.2 Device connectivity failure and timeouts

Where the S1SP fails to communicate with the Communications Hub, in advance of the checks for the specified Group IDs, as detailed in the Group Specific Requirements of the TMAD, the S1SP will perform a series of retries as described in Section 3.1 of this document.

Once the timeout period has been reached, the following activities will occur:

1. the SIM profile will be changed so that the SMSO can communicate with the Communications Hub;
2. the S1SP will indicate WAN testing has failed in the S1SP Migration Audit Files; and
3. Error Code 12.9.1.ET01 will be included in the S1SP Commissioning File.

The failure will be included in the next Migration Authorisation Completion Response file generated by the Requesting Party based on information in the S1SP Commissioning File.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the:

1. FailedStepNumber in Report 2 – 'Migration Failures Occurring in the Reporting Period'; and
2. Reason Code as per Appendix A.1 in Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'.

If the ToBeCommissionedByDCC flag is set to 'False', then the S1SP Commissioning File will be sent to the both the Supplier and the Requesting Party. This will include details of the failure(s).

The Responsible Supplier can either:

a) Liaise with the relevant SMSO to review the failures, fix as appropriate and add the affected SMETS1 Installations to a Migration Authorisation for a subsequent week; or

b) Replace the SMETS1 Installation with SMETS2+ in due course.

2.6.3 S1SP / DCO Commissioning of a SMETS1 Installation Failure

Where one of the checks required by the 'S1SP / DCO Commissioning of SMETS1 Installation' section of the TMAD for the associated GroupID fails at a check marked as 'Critical', the checking in relation to that SMETS1 Installation stops and the following activities will occur:

1. the SIM profile will be changed so that the SMSO can communicate with the Communications Hub; and
2. include the FailedStepNumber relating to the SMETS1 Installation in an S1SP Commissioning File.

The failure will be included in the next Migration Authorisation Completion Response file generated by the Requesting Party based on information in the S1SP Commissioning File.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the:

1. FailedStepNumber in Report 2 – ‘Migration Failures Occurring in the Reporting Period’; and
2. Reason Code as per Appendix A.1in Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the ToBeCommissionedByDCC flag is set to ‘False’, then the S1SP Commissioning File will be sent to the both the Supplier and the Requesting Party. This will include details of the failure(s).

The Responsible Supplier can either:

a) Liaise with the relevant SMSO to review the failures, fix as appropriate and add the affected SMETS1 Installations to a Migration Authorisation for a subsequent week; or

b) Replace the SMETS1 Installation with SMETS2+ in due course.

2.6.4 DCO Migration Group Encrypted File Timeout

Once the DCO has authenticated a Migration Group Encrypted File it will start a timer. If the timer reaches 48 hours and the S1SP has not requested to use details the DCO will discard the file pursuant to the TMAD Clause 5.16.

When the S1SP then requests to use details from the DCO where the file has been discarded, the S1SP will indicate the processing failure by populating the FailedStepNumber in the S1SP Commissioning File.

The failure will be included in the next Migration Authorisation Completion Response file generated by the Requesting Party based on information in the S1SP Commissioning File.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the:

1. FailedStepNumber in Report 2 – ‘Migration Failures Occurring in the Reporting Period’; and
2. Reason Code as per Appendix A.1 in Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the ToBeCommissionedByDCC flag is set to ‘False’, then the S1SP Commissioning File will be sent to the both the Supplier and the Requesting Party. This will include details of the failure(s).

The SMETS1 Installations will need to be rescheduled by the supplier in a subsequent Migration Week.

2.6.5 Rollback

Where it has been identified that a SMETS1 Installation needs to be rolled back, the following errors could occur during this process:

1. the DCO was unable to delete any keys and/or related information it has stored during the 'S1SP / DCO Commissioning of SMETS1 Installation';
2. the S1SP was unable to delete any keys and/or related information it has stored during the 'S1SP / DCO Commissioning of SMETS1 Installation'; or
3. the S1SP was unable to restore WAN communication between SMETS1 Installation and the relevant SMETS1 SMSO.

If the S1SP/DCO is unable to delete the information mentioned above, the S1SP/DCO (as appropriate) party will raise an Incident. The Incident would be assigned to the S1SP/DCO and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party. The S1SP/DCO will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System.

If the S1SP was unable to restore WAN communication between SMETS1 Installation and the relevant SMETS1 SMSO, the S1SP will take reasonable steps to restore WAN communications between the SMETS1 Installations and the SMETS1 SMSO. Once the WAN communications has been restored or the problem is not able to be resolved after investigation, the S1SP will report the appropriate Error Code(s) in the S1SP Commissioning File.

Where the SMSO is unable to establish WAN communication with SMETS1 Installation, the supplier should liaise with SMSO to establish if they may need to replace SMETS1 Installation with a SMETS2+.

The outcome of this manual processing will be included in the next Migration Authorisation Completion Response file generated by the Requesting Party based on information in the S1SP Commissioning File.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the:

1. FailedStepNumber in Report 2 – ‘Migration Failures Occurring in the Reporting Period’; and
2. Reason Code as per Appendix A.1 in Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the ToBeCommissionedByDCC flag is set to ‘False’, then the S1SP Commissioning File will be sent to the both the Supplier and the Requesting Party. This will include details of the failure(s).

2.6.6 Commission Device (CHF) failure

Where the S1SP fails to add the Communications Hub Function (CHF) details to the Smart Metering Inventory (SMI) and set the SMI Status to ‘Commissioned’, then Error Code ‘**12.9.5.DP01**’ will be included in the S1SP Commissioning File.

An Incident will be raised when a CHF has not successfully been Commissioned. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC’s Service Management System. Once the Incident has been resolved, the S1SP will process the backlog.

The outcome will be included in the next Migration Authorisation Completion Response file generated by the Requesting Party based on information in the S1SP Commissioning File.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the:

1. FailedStepNumber in Report 2 – ‘Migration Failures Occurring in the Reporting Period’; and
2. Reason Code as per Appendix A.1 in Report 6 – ‘Migration Authorisation Outcomes for the Previous Migration Day’.

If the ToBeCommissionedByDCC flag is set to ‘False’, then the S1SP Commissioning File will be sent to the both the Supplier and the Requesting Party. This will include details of the failure(s).

If the Incident can't be resolved, 'Installation Rollback' will be carried out as per TMAD for the respective Group ID. Despite the rollback, if the SMSO cannot resume the service with the SMETS1 Installation, the supplier should liaise with the SMSO to establish if they may need to replace the SMETS1 Installation with a SMETS2+.

2.6.7 S1SP unable to generate S1SP Commissioning File

Where the S1SP is unable to generate the S1SP Commissioning File for any reason (e.g. system unavailability), the S1SP will raise an Incident.

The Incident would be assigned to the S1SP and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the S1SP will take the necessary actions so that the Device is successfully Commissioned with in the SMI.

2.7 Commissioning (by DCC)

In line with Clause 4.36 of the TMAD, the DCC Commissions all Devices from SMETS1 Installations that include a Dormant Meter. The act of Commissioning successfully validated Devices, apart from the CHF, will be undertaken by the Commissioning Party as defined in the TMAD.

The Commissioning Party Commissions Devices from Active SMETS1 Installations where there is more than one Responsible Supplier and where the DCC has received Migration Authorisations from both such Responsible Suppliers which authorise the Migration of that SMETS1 Installation in the same Migration Week.

Responsible Suppliers, for SMETS1 Installations comprising only Active Meters, have the option to Commission successfully validated Devices (excluding the CHF) themselves using Service Requests described in the DUIS 3.0b.

The following section describes error scenarios that could occur during the Commissioning process by the Commissioning Party, including associated systems, only.

2.7.1 Commissioning Party unable to process any Installation

Where the Commissioning Party has received a S1SP Commissioning File indicating no errors relating to a particular SMETS1 Installation the Commissioning Party will attempt to Commission devices comprising that same SMETS1 Installation. Should there be a system outage pertaining to the Commissioning Party, the Commissioning Party will raise an Incident.

This Incident would be assigned to the Commissioning Party and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Commissioning Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the Commissioning Party will process the backlog.

2.7.2 S1SP Commissioning File whole file validation error

On receipt of the S1SP Commissioning File, which is generated by the S1SP, the Commissioning Party undertakes the sequence of checks described in Table 5.9 in the TMAD.

Where one of these checks fails, or the Commissioning Party does not hold a Migration Common File with the same Migration Header as the S1SP Commissioning File, the Commissioning Party stops processing the file and raises an Incident. This Incident would be assigned to the S1SP and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the S1SP will regenerate and resubmit the S1SP Commissioning File to the Commissioning Party. Once the Incident has been resolved, the Commissioning Party will process the backlog.

2.7.3 S1SP Commissioning File SMETS1 Installation level validation error

For each SMETS1 Installation specified as being successful in the S1SP Commissioning File, the Commissioning Party confirms that there is a corresponding SMETS1 Installation in the Migration Common File in line with Clause 6.3 of the TMAD. Should this check fail for any SMETS1 Installation, the Commissioning Party stops processing the file and raises an Incident.

This Incident would be assigned to the S1SP and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the S1SP will regenerate and resubmit the S1SP Commissioning File to the Commissioning Party.

2.7.4 DSP unable to process any Installation

Should there be a system outage pertaining to the DSP on receipt of a Commissioning Request from the Commissioning Party, the DCC will raise an Incident.

This Incident would be assigned to the DSP and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The DSP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the DSP will then process the backlog.

2.7.5 Commissioning Request SMETS1 Installation level validation error (DSP)

Where the DSP has received a Commissioning Request from the Commissioning Party, it attempts to perform checks in Table 8.7-1 in the TMAD for that same SMETS1 Installation. Only if all checks in Table 8.7-1 are successful the DSP performs checks Table 8.7-3 in the TMAD, as well as the validation checks in the DUIS (as modified by TMAD).

If one of the checks required by the DUIS or Clause 8.7 of the TMAD fails, the DSP sends a Service Response to the Commissioning Party detailing the relevant Response Code described in the DUIS or in the TMAD.

Where the Commissioning Party receives a Service Response from the DSP indicating an error or failure, in relation to checks performed in Tables 8.7-1/8.7-3 of the TMAD or the DUIS, it will raise an Incident and not continue processing subsequent Commissioning Requests for that SMETS1 Installation. For clarity, where the Commissioning Party receives an error Response Code in relation to a 'Request Handover Of DCC Controlled Device', an Incident will not be raised and it shall continue processing subsequent Commissioning Requests for that SMETS1 Installation.

This Incident would be assigned to the Commissioning Party and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The Commissioning Party will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the Commissioning Party will then process the backlog.

The Commissioning Party will also append the SMETS1Installation element in the Commissioning Outcome File to include the FailedStepNumber, as per Table 6.3 of the TMAD, which details the point at which an error occurred during the Commissioning phase. The recipients of the Commissioning Outcome File are the Requesting Party and the Responsible Supplier. For clarity, DCC would have concluded all attempts to recover and Commission the relevant SMETS1 devices successfully.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the FailedStepNumber:

1. Report 2 – 'Migration Failures Occurring in the Reporting Period'.

For the failed SMETS1 Installations that have been reported in the Commissioning Outcome File, the suppliers should consider replacing the SMETS1 Installations with SMETS2+.

Table 8.7-1 of the TMAD

Validation Check	Response Code	Response Code Name	Suggested Action
The combination of values in the Service Reference and Service Reference Variant fields, with their DUIS meanings, is a combination detailed in one of the rows in Table 8.7 2 of the TMAD.	E48	Commissioning Party is not allowed to use such Service Requests	Commissioning Party should resubmit Commissioning Request (including Service Reference and Service Reference Variants) in line with Table 8.7-2 of the TMAD
The Remote Party Role in the Certificate used to verify the Digital Signature on the Commissioning Request is that required by Table 5.5 of the TMAD.	C2	Wrong Remote Party Role for Commissioning Request	Commissioning Party should sign the Commissioning Request using a key which is associated with their SMKI Certificate with the role commissioningPartyXmlSigning
The Business Originator ID in the RequestID (with their DUIS meanings) has the same value as the Entity Identifier in the Certificate used to verify the Digital Signature on the Commissioning Request.	E100	Commissioning Party identifier mismatch in Commissioning Request	Commissioning Party should resubmit the Service Request with the same Business Originator ID and Entity Identifier
Where Business Target ID in the RequestID (with their DUIS meanings) refers to a Device, the Device is, according to the SMI, a SMETS1 Device or a CAD. For clarity, CADs are not specified in any version of SMETS, and so cannot have an associated SMETS version, where CAD has its DUIS meaning.	C4	Target is not a SMETS1 Device	Commissioning Party should resubmit the Commissioning Request and ensure the Business Target ID is a SMETS1 Device or a CAD
Where the Body part of a Commissioning Request, which is not a 'Device Pre-notification', contains a Device ID (with their DUIS meanings), that Device ID is for a SMETS1 Device according to the Smart Metering Inventory.	C5	Other Device is not a SMETS1 Device	Commissioning Party should resubmit the Commissioning Request and ensure the Business Target ID is a SMETS1 Device

Table 8.7-3 of the TMAD

Commissioning Request name	Validation Check (With terms having their DUIS meaning, where not defined otherwise)	Response Code	Response Code Name	Suggested Action
Request Handover Of	If RemotePartyRole is 'supplier' in the Commissioning Request, confirm that	C062199	Remote Party Role in Certificates	Commissioning Party should resubmit Commissioning

DCC Controlled Device	the Remote Party Role in all Certificates in ReplacementCertificates is 'supplier'. If RemotePartyRole is 'NetworkOperator' in the request, confirm that the Remote Party Role in all Certificates in ReplacementCertificates is 'networkOperator'.		different than in request	Request so that the Remote Party Role is the same as that in the Certificate.
Request Handover Of DCC Controlled Device	Confirm that the Entity Identifiers in all Certificates contained within ReplacementCertificates are identifiers for the same Party.	C062197	Not all identifiers are for the same Party	Commissioning Party should resubmit the Commissioning Request so that the Entity Identifiers are consistent.
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'Supplier' in the request, confirm that according to: • the Registration Data linking MPxN to current Import Supplier or Gas Supplier, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates, that the Party identified is the current Import Supplier or Gas Supplier for the Device identified.	C062196	Asserted Supplier is not the Supplier	Commissioning Party should resubmit the Commissioning Request identifying the correct Supplier.
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'NetworkOperator' in the request, confirm that according to: • the Registration Data linking MPxN to current Electricity Distributor or Gas Transporter, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates, that the Party identified is the current Electricity Distributor or Gas Transporter for the Device identified.	C062195	Asserted Network Operator is not the Network Operator	Commissioning Party should resubmit the Commissioning Request identifying the correct Network Operator.

2.7.6 S1SP unable to process any Installation

Where the S1SP has received a Countersigned Commissioning Request from the DSP, it attempts to perform checks detailed in Section 2.7.7 for that same SMETS1 Installation. Should there be a system outage pertaining to the S1SP, the S1SP will raise an Incident.

This Incident would be assigned to the S1SP and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the S1SP will process the backlog.

2.7.7 Commissioning Request SMETS1 Installation level validation error (S1SP)

Where the S1SP has received a Countersigned Commissioning Request from the DSP, it shall attempt to perform the subset of the checks in Table 8.7-1 in the TMAD (detailed in this Section) for that same SMETS1 Installation. Only if all of the checks detailed below are successful, the S1SP will perform the subset of the checks in Table 8.7-3 in the TMAD (detailed in this Section).

If one of the relevant checks required by Clause 8.7 of the TMAD fails, the S1SP shall send a S1SP Alert to the Commissioning Party detailing the relevant S1SP Alert Code described in this section.

Where the Commissioning Party receives a S1SP Alert from the S1SP indicating an error, in relation to checks mentioned in this Section and the standard checks defined in the Service Request Processing Document and the DUIS, the Commissioning Party raises an Incident and does not continue processing/submitting subsequent Commissioning Requests to the DSP for that SMETS1 Installation. For clarity, where the Commissioning Party receives a S1SP Alert from the S1SP in relation to a 'Request Handover Of DCC Controlled Device', the Commissioning Party shall not raise an Incident and it shall continue processing/submitting subsequent Commissioning Requests to the DSP for that SMETS1 Installation.

This Incident would be assigned to the S1SP and managed by the Migration Control Centre. Users affected by any such Incident will be notified through the Self-Service Interface as an Interested Party.

The S1SP will be required to resolve the Incident in accordance with the Incident Target Resolution Time described in the TMAD, whilst providing timely updates to DCC's Service Management System. Once the Incident has been resolved, the S1SP will process the backlog.

The Commissioning Party will also append the SMETS1Installation element in the Commissioning Outcome File to include the FailedStepNumber, as per Table 6.3 of the TMAD, which details the point at which an error occurred during the Commissioning phase. The recipients of the Commissioning Outcome File are the Requesting Party and the Responsible Supplier. For clarity, DCC would have concluded all attempts to recover and Commission the relevant SMETS1 devices successfully.

The following supplier facing reports, detailed in the Migration Reporting Regime, will confirm the FailedStepNumber:

1. Report 2 – 'Migration Failures Occurring in the Reporting Period'.

For the failed SMETS Installations that have been reported in the Commissioning Outcome File, the suppliers should consider replacing the SMETS1 Installations with SMETS2+.

Table 8.7-1 of the TMAD (applicable to the S1SP)

Validation Check	S1SP Alert Code	S1SP Alert Name	Suggested Action
The combination of values in the Service Reference and Service Reference Variant fields, with their DUIS meanings, is a combination detailed in one of the rows in Table 8.7.2 of the TMAD.	S1VE48	Commissioning Party is not allowed to use such Service Requests	Commissioning Party should resubmit Commissioning Request (including Service Reference and Service Reference Variants) in line with Table 8.7-2 of the TMAD
The Remote Party Role in the Certificate used to verify the Digital Signature on the Commissioning Request is that required by Table 5.5 of the TMAD.	S1C2	Wrong Remote Party Role for Commissioning Request	Commissioning Party should sign the Commissioning Request using a key which is associated with their SMKI Certificate with the role commissioningPartyXmlSigning
The Business Originator ID in the RequestID (with their DUIS meanings) has the same value as the Entity Identifier in the Certificate used to verify the Digital Signature on the Commissioning Request.	S1VE100	Commissioning Party identifier mismatch in Commissioning Request	Commissioning Party should resubmit the Service Request with the same Business Originator ID and Entity Identifier

Where Business Target ID in the RequestID (with their DUIS meanings) refers to a Device, the Devices is, according to the SMI, a SMETS1 Device or a CAD. For clarity, CADs are not specified in any version of SMETS, and so cannot have an associated SMETS version, where CAD has its DUIS meaning.	S1C4	Target is not a SMETS1 Device	Commissioning Party should resubmit the Commissioning Request and ensure the Business Target ID is a SMETS1 Device or a CAD
Where the Body part of a Commissioning Request, which is not a 'Device Pre-notification', contains a Device ID (with their DUIS meanings) , that Device ID is for a SMETS1 Device according to the Smart Metering Inventory	S1C5	Other Device is not a SMETS1 Device	Commissioning Party should resubmit the Commissioning Request and ensure the Business Target ID is a SMETS1 Device

Table 8.7-3 of the TMAD (applicable to the S1SP)

Commissioning Request name	**Validation Check** (With terms having their DUIS meaning, where not defined otherwise)	**S1SP Alert Code**	**S1SP Alert name**	**Suggested Actions**
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'supplier' in the Commissioning Request, confirm that the Remote Party Role in all Certificates in ReplacementCertificates is 'supplier'. If RemotePartyRole is 'NetworkOperator' in the request, confirm that the Remote Party Role in all Certificates in ReplacementCertificates is 'networkOperator'.	S1C062199	Remote Party Role in Certificates different than in request	Commissioning Party should resubmit Commissioning Request so that the Remote Party Role is the same as that in the Certificate.
Request Handover Of DCC Controlled Device	Confirm that ExecutionDateTime is not present	S1C062198	Cannot future date Commissioning Requests	Commissioning Party should resubmit an On Demand Commissioning Request.
Request Handover Of DCC Controlled Device	Confirm that the Entity Identifiers in all Certificates contained within ReplacementCertificates are identifiers for the same Party.	S1C062197	Not all identifiers are for the same Party	Commissioning Party should resubmit the Commissioning Request so that the Entity Identifiers are consistent.
Request Handover Of	If RemotePartyRole is 'Supplier' in the request, confirm that according to:	S1C062196	Asserted Supplier is	Commissioning Party should resubmit the

DCC Controlled Device	• the Registration Data linking MPxN to current Import Supplier or Gas Supplier, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates that the Party identified is the current Import Supplier or Gas Supplier for the Device identified.		not the Supplier	Commissioning Request identifying the correct supplier.
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'NetworkOperator' in the request, confirm that according to: • the Registration Data linking MPxN to current Electricity Distributor or Gas Transporter, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates that the Party identified is the current Electricity Distributor or Gas Transporter for the Device identified.	S1C062195	Asserted Network Operator is not the Network Operator	Commissioning Party should resubmit the Commissioning Request identifying the correct Network Operator.
Update HAN Device Log	Confirm that RequestType is 'Add'.	S1C081199	Commissioning Party cannot remove Devices	Commissioning Party should resubmit the Commissioning Request indicating 'Add'.
Update HAN Device Log	Confirm that InstallCode is '00000000000000000000000000000000'	S1C081198	Commissioning Party cannot install new Devices	Commissioning Party should resubmit the Commissioning Request with InstallCode '00000000000000000000000000000000'

3 Retry and Timeout Strategy

The following section relates to Migration only, the SMETS1 enduring retry and timeout strategy is detailed in the following document:

- General guidance on SMETS1 DCC Retry and Timeouts for Service Request Processing.

3.1 Device Connectivity Retry and Timeout Strategy

Where the S1SP attempts to establish a session with the Communications Hub in advance of the checks for the specified Group IDs, as detailed in the Group Specific Requirements the TMAD, the S1SP will perform a series of retries using the strategy described below:

1. the S1SP attempts to communicate with the Communications Hub 3 times at five-minute intervals ('short retry'); and then
2. repeats the 'short retry' every 2 hours for a period up to 24 hours.

For example, if the test started at exactly midnight, and all attempts to contact the device failed, these would be made at (hh:mm): 00:00, 00:05, 00:10, 02:00, 02:05, 02:10, 04:00, 04:05, 04:10, 06:00, 06:05, 06:10, 08:00, 08:05, 08:10, 10:00, 10:05, 10:10, 12:00, 12:05, 12:10, 14:00, 14:05, 14:10, 16:00, 16:05, 16:10, 18:00, 18:05, 18:10, 20:00, 20:05, 20:10, 22:00, 22:05, and 22:10.

After 24 hours of retries, the S1SP will timeout for that SMETS1 Installation and as such will stop attempting to establish a session with the Communications Hub. The following activities will then occur:

1. the SIM profile will be changed so that the SMSO can communicate with the Communications Hub;
2. the S1SP will indicate WAN testing has failed in the S1SP Migration Audit Files; and
3. Error Code 12.9.1.ET01 will be included in the S1SP Commissioning File.

3.2 Retry strategy for SIM swap for GroupID 'CB'

Where the Requesting Party attempts to amend the SIM configuration on the Communication Hub of the SMETS1 Installation to use the DCC "elster" APN prior to generation of the MGF/MEF migration files, the Requesting Party will perform a series of retries using the strategy described below:

1. the Requesting Party attempts to amend the SIM configuration on the Communication Hub of the SMETS1 Installation [3] times in a configurable interval and
2. for upto a configurable number of hours.

The configurable interval referenced in point 1 will be initially set to 60 minutes and will be adjusted based on performance of the production system.

The total duration referenced in point 2 will be initially set to 5 hours and will be adjusted based on performance of the production system.

After the retry attempts have completed, the Requesting Party will timeout and will stop attempting to migrate the SIM for that SMETS1 Installation. The following activities will then occur:

1. MA120 reason code will be included in the Migration Authorisation Completion Response file.

4 Dormant Meter Error Handling

4.1 Dormant/Dormant SMETS1 Installation

Where a SMETS1 Installation, which comprises only Dormant Meters, fails during the Migration process the Migration Control Centre will consider whether the installation can be scheduled for Migration at a later date. The Migration Control Centre will take into account the following:

- the failure reason recorded from the last attempt;
- the number of times Migration has been attempted for that SMETS1 Installation; and
- the actions that may be taken by the SMETS1 SMSO to enable Migration to proceed successfully.

Should the SMETS1 Installation be identified as a suitable installation to be rescheduled, the Migration Control Centre will triage the error and include the SMEST1 Installation in a subsequent Migration Week.

When the Migration of a SMETS1 Installation comprising only Dormant Meters fails, the Responsible Supplier(s) will be informed of the SMETS1 Installations that failed the Migration and the relevant failed migration process step as per the error handling process defined in this document.

4.2 Active/Dormant SMETS1 Installation

Where a SMETS1 Installation, which comprises Active and Dormant Meters, fails during the Migration process the Migration Control Centre will liaise with the Active Meter supplier and consider whether the installation can be scheduled for Migration at a later date. The Migration Control Centre will take into account the following:

- the failure reason recorded from the last attempt;
- the number of times Migration has been attempted for that SMETS1 Installation; and
- the actions that may be taken by the SMETS1 SMSO to enable Migration to proceed successfully.

Should the SMETS1 Installation be identified as a suitable installation to be rescheduled, the Migration Control Centre will undertake the following activities:

- triage the Dormant Meter error; and then
- liaise with the Active Meter supplier to include that SMETS1 Installation in a subsequent Migration Week.

When the Migration of a SMETS1 Installation comprising Active and Dormant Meters fail, the Responsible Supplier(s) will be informed of the SMETS1 Installations that failed the Migration and the relevant failed migration process step as per the error handling process defined in this document.

Appendix A – Additional Error Codes

A.1 Requesting Party Reason Codes

The TMAD details the checks and processing which are undertaken by the following DCC systems:

1. the Requesting Parties;
2. the S1SPs;
3. the DSP;
4. the DCOs; and
5. the Commissioning Party.

As described in earlier Sections of this document, where a SMETS1 Installation fails a step described in the TMAD that Failed Step Number will be recorded in Report 2 as defined in the Migration Reporting Regime.

There are validation steps undertaken by the Requesting Party that are not described in detail in the TMAD, as such these can be found in Table A.1 below. The Reason Codes below may be included in the following supplier facing reports detailed in the Migration Deporting Regime:

1. Report 6 – 'Migration Authorisation Outcomes for the Previous Migration Day'; and
2. Report 10 – 'Migration Authorisation Validation Responses in the Reporting Period'.

Table A.1 - Additional Reason Codes

Reason Code	Description	GroupID applicable	
		"AA", "BA", "CA"	"CB"
MA001	Required meter type not registered at MPAN	X	X
MA002	Required meter type not registered at MPRN	X	X
MA003	Migration Week date provided is not a Monday.	X	X

MA004	The Migration Week has already ended.	X	X
MA005	The Migrate On date is not within the specified Migration Week	X	X
MA006	The Migrate On date is on or earlier than today.	X	X
MA007	Supplier is not the current Active Supplier for MPAN.	X	X
MA008	Supplier is not the current Active Supplier for MPRN.	X	X
MA009	Both the MPAN and MPRN need to be provided where the requesting supplier is operating both the MPAN and the MPRN at the installation.	X	X
MA010	Supplier has not provided the SupplierCertificateIDs for the ESME.	X	X
MA011	Supplier has not provided the SupplierCertificateIDs for the GPF and GSME.	X	X
MA012	DCC authorisation received for an installation which has an Active meter.	X	X
MA013	Migration Authorisation received from DCC does not specify the MPAN or the MPRN for a dual fuel installation.	X	X
MA014	A Migration Authorisation received from DCC does not specify an ESME Supplier Id.	X	X
MA015	A Migration Authorisation received from DCC for a dual fuel installation does not specify an GSME Supplier Id.	X	X
MA016	A certificate serial number has been provided without the corresponding issuer name.	X	n/a
MA017	The installation is currently blocked from being migrated.	X	n/a

MA018	If ESME and GSME have same responsible Supplier (Sec Party) then the authorisation should be submitted as 1 MA.	X	n/a
MA101	Authorisation Expired	X	X
MA102	Required meter type no longer registered at MPAN	X	X
MA103	Required meter type no longer registered at MPRN	X	X
MA104	Supplier is no longer the operating supplier for MPAN.	X	X
MA105	Supplier is no longer the operating supplier for MPRN.	X	X
MA106	Where the meter is part of an split site then no MA has been received for the other Active meter.	X	n/a
MA107	DCC authorisation received for an installation which now has an Active meter. i.e. an MPxN for which a MAD file was accepted from the DCC now has an Active supplier in Instant Energy due to a cos gain.	X	n/a
MA108	For a dual fuel site where both MPAN and MPRN are dormant, the MA from the DCC does not include the MPRN.	X	X
MA109	Device does not have CPL entry	X	X
MA110	The installation does not have an entry on the Eligible Product Combinations List	X	X
MA111	The installation configuration does not meet the SMETS1 pre-migration requirements.	X	X
MA112	There has been no WAN comms with the installation in the last 7 days	X	X

MA113	Failure MVF Received.	X	X
MA114	Installation is currently being updated / configured by SMSO.	X	X
MA115	Failure SCF Received	X	X
MA116	No MVF received within processing day	X	n/a
MA117	The installation is currently blocked from being migrated.	X	n/a
MA118	Vodafone CSP move failed.	X	n/a
MA119	Configuration of hub on migration failed (Honeywell Only)	X	n/a
MA120	The APN account switch attempts have failed and the installation cannot be migrated.	n/a	X
MA121	The SMSO could not communicate with the Installation after the rollback was attempted.	n/a	X
MA999	Other Failure	X	n/a