Data Communications Company

ECoS Migration Error Handling and Retry Approach V1.0

ECoS DCC Guidance Document

Filename: ECoS Migration Error Handling and Retry Approach v1.0.docx
Version: 1.0
Effective Date: ECoS Service Live Date
Classification: DCC Public

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this document is to provide guidance regarding how The Data Communications Company (DCC) and Supplier Parties should act when an error occurs during ECoS Migration. It is produced in accordance with Section 7 of the ECoS Transition and Migration Approach Document (ETMAD), which is Appendix AS of the Smart Energy Code (SEC).

This document details the types of exceptions/errors that may occur during ECoS Migration and the required remediation activities.

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

1.2. Scope

The ECoS Migration Error Handling and Retry Approach:

a) describes the type of exceptions/errors that can occur during ECoS Migration

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

c) sets out the procedures to be followed with respect to management of the list of Non-Migratable Device Models; and

d) describes the timeout and retry approach when DCC attempts to complete ECoS Migration.

1.3. Out of Scope

DCC's approach to Device selection during ECoS Migration is out of scope for this document. The ECoS Migration Error Handling and Retry Approach will focus on the processes that follow device selection, for attempting ECoS Migration and making further attempts where errors are encountered.

Provision of reports to Supplier Parties in relation to ECoS Migration failures is also out of scope. This is captured through a separate ECoS Migration Reporting Regime, produced in accordance with Section 4 of the ETMAD. The ETMAD places an obligation on Supplier Parties to monitor reports received and endeavour to resolve issues in accordance with this EMEHRA. Therefore, this document assumes that Supplier Parties are aware of Failed Migrations and Non-Migratable Device Models.

Issues associated with SMETS1 devices are out of scope of this document on the basis that this document addresses the process for replacing certificates held in the CoS Certificate slot and SMETS1 devices do not have a CoS Certificate slot. Any error handling relating to transfer of data to the ECoS Party, specific to SMETS1 devices, will be handled by internal DCC processes.

1.4. Document Structure

Section		Purpose
2	ECoS Migration Error Handling	Explains what activities are undertaken in support of ECoS Migration and the errors that might be encountered by during those activities.
3	Migration Batch Submission Retry	Explains how DCC will respond to errors and, where those errors are Device specific, if and when DCC would expect to try migrating the devices again.
4	ECoS Non-Migratable Device Model List	This section provides detail on purpose and handling of the ECoS Non-Migratable Device Model List
5	TCoS Party Timeout and Retry	Explains the elements of retry logic that are built into the Migration Attempt functionality provided by the TCoS Service Provider systems.
6	Responsible Supplier Actions	While section 2,3 and 5 explain what DCC will do to recover from failures, this section focuses on what is expected of a Responsible Supplier.
A	Error Codes	Error codes are referenced throughout the document. In this section, all the errors are listed together for reference, broken down into the relevant processing stages.
B	Format of the ECoS Non-Migratable Device Model List	Recording the structure and file naming convention for the ECoS Non-Migratable Device Model List

1.5. Definitions and Interpretations

Migration Control Centre (MCC)	A DCC function that will control the end to end ECoS Migration processes and systems to ensure the DCC Total System is protected and to meet regulatory obligations. The function will also be responsible for liaising with stakeholders to coordinate ECoS Migration activities.
Migration Batch Submission	Where the MCC instructs the TCoS Service Provider to apply ECoS certificates to a collection of Devices.
Migration Attempt	Where the TCoS Service Provider sends a certificate replacement command to a Device with respect to a particular Migration Batch Submission.
TCoS Service Provider Retry	Where the TCoS Service Provider re-sends the certificate replacement command for the same Migration Attempt, following initial failure, as further described in section 5 of this document.
Cooling Off Period	Where a device is temporarily excluded from future Migration Batch Submissions in response to an error encountered in a previous Migration Batch Submission. The duration of the Cooling Off Period will differ between error codes and some may require no Cooling Off Period at all.

A single device may be included in many Migration Batch Submissions. Not all of those submissions would necessarily be deemed to be a Migration Attempt. For example, it wouldn't deemed to be a Migration Attempt if the device was found to be subject of an imminent CoS or if the batch timed out before the TCoS Service Provider had a chance to send a command for this device.

1.6. General Provisions

This document should be read in conjunction with the latest version of following documents:

1. The ETMAD (SEC Appendix AS) defines the rights and obligations of Supplier Parties and DCC that will be in place over the ECoS Migration Period; and

2. The ECoS Migration Reporting Regime which describes the format and frequency of reporting provided to Supplier Parties in regard to successful and Failed Migrations and also details Non-Migratable Device Models.

2. ECoS Migration Error Handling

This section provides a breakdown of the different types of error that might impact the activity of replacing TCoS Certificates with ECoS Certificates on Devices, and the supporting processes as defined in ETMAD.

The errors will cover a range of topics:

- error codes that are returned by service providers relating to Devices;
- error codes that are returned by service providers relating to systems configuration and system behaviour;
- system errors identified by Supplier Parties; and
- system errors or performance issues identified by DCC.

2.1. Migration Processing Stages

The ETMAD includes, in paragraph 6.1(c), a breakdown of four steps involved in the migration:

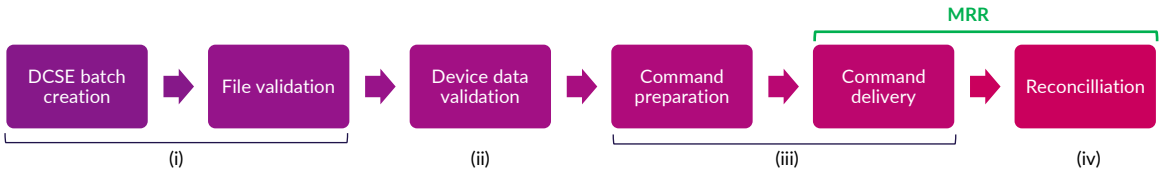
ETMAD 6.1(c)

(i) the instruction to the TCoS Service Provider to initiate ECoS Migration;
(ii) review by the TCoS Service Provider to confirm that ECoS Migration can commence;
(iii) replacement of the Device Security Credentials that pertain to the TCoS Party with those that pertain to the ECoS Party on the relevant Device; and
(iv) confirmation received from both the ECoS Service Provider and TCoS Service Provider that ECoS Migration has completed successfully.

When considering the error handling, we must increase the granularity of this process to six steps. The additions being:

- splitting up step (i) into the process that generates the instruction and the process that validates the structure of the instruction.
- splitting up step (iii) into two halves, to differentiate those errors that are internal to the TCoS Service Provider from those that occur when the command is sent to a Device.

The figure below represents those six steps and their association to the four specified in ETMAD.



The following sections provide a high level description of the steps and then addresses the error handling specific to each.

Errors occurring prior to the 'command delivery' step will either reflect a system failure or indicate that the Device wasn't suitable for selection during the batch creation phase. As a result of this, such errors will not be included in reports described in the ECoS Migration Reporting Regime.

2.1.1. DCSE Batch Creation

The Device Candidate Selection Engine (DCSE) is an application that will be used by the MCC to create batches of instructions to have Devices updated, such that their TCoS Certificate is replaced by an ECoS Certificate. The DCSE will support the MCC's processes whereby the MCC

may chose the criteria for a particular batch and the application will select the Devices that fit those criteria, while also applying predefined rules that must be considered.

An example of MCC criteria might be to only select Devices of a specific Device Model. An example of predefined rules would be that there must be evidence that a Device has recently communicated with the Data Service Provider (DSP) ('recent' being a configurable parameter).

Having selected the Devices for a batch, the DCSE will automatically generate files for submission to the TCoS Service Provider and deliver the file(s) to the TCoS Service Provider at the allotted schedule for that batch.

Errors specific to this stage, that are experienced by the MCC either at the user interface or else in the backend processes (such as that which creates batch files), will be logged as an incident. The act of raising an incident allows DCC to manage resolution of the issue and will have no bearing on whether any one Device will be a candidate for migration i.e. a further batch could be progressed including the same Devices whilst the incident remains open. Therefore, Supplier Parties will not receive notification that their Device was in a failed batch.

2.1.2. File Validation

At this stage of migration, the TCoS Service Provider has received batch files from the DCSE. The TCoS Service Provider reviews the files for their validity but there is no review of the accuracy of data pertaining to individual Devices nor the condition of those Devices. Checks on data validity occur in the next step (see section 2.1.3).

The TCoS Service Provider will respond to the MCC with a status of the checks on the file, stating either that they were concluded successfully or, supplying an error code indicating the fault that has been discovered. Where a fault is discovered the TCoS Service Provider will not undertake any action that might have been expected with respect to the content of the file.

Some faults raised by the TCoS Service Provider will be categorised as normal behaviour and, in these circumstances, no incident will be raised. These may occur where TCoS Service Provider is responding to a file sequencing issue, such as a batch cancellation arriving moments before the batch that was intended for cancellation.

Other faults raised by the TCoS Service Provider will be indicative of a genuine failure of some sort. In these circumstances, DCC shall raise an incident. As with the errors detailed in paragraph 2.1.1. the act of raising an incident allows DCC to manage resolution of the issue and will have no bearing on whether any one Device will be a candidate for migration i.e. a further batch could be progressed including the same Devices whilst the incident remains open. Therefore, Supplier Parties will not receive notification that their Device was in a failed batch.

Possible error conditions for this stage and the associated categorisation are indicated in Figure 1, below, and repeated in Table 1 of "Appendix A – File validation errors".

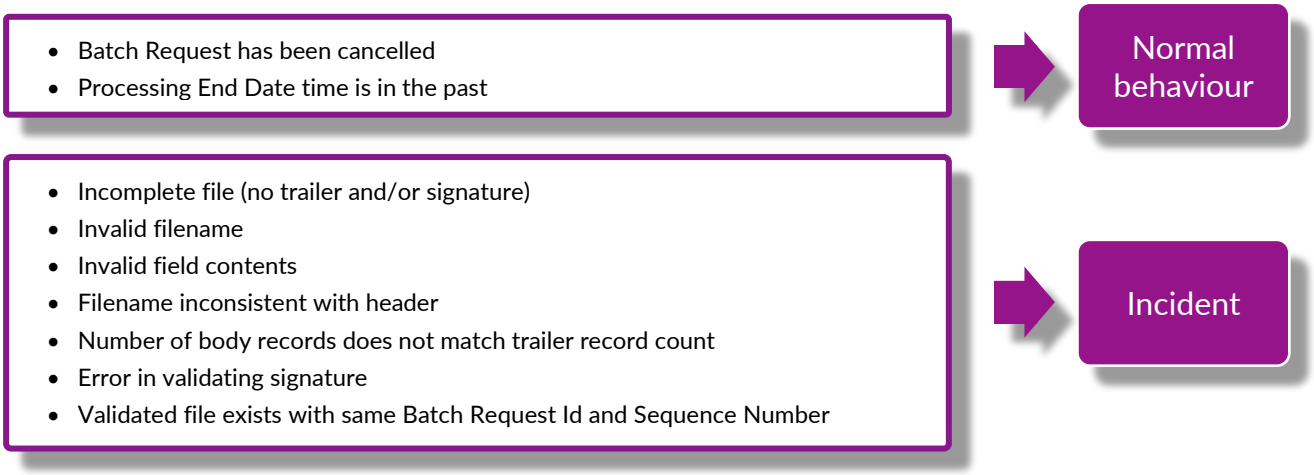


Figure 1 - Categorisation of file validation errors

2.1.3. Device Data Validation

During this stage, the TCoS Service Provider will review an individual Device and the validity of the request to migrate it. Where a Device fails any part of this validation, a certificate replacement command will not be issued to the Device for this Migration Batch Submission.

Possible error codes returned for this stage are shown in Figure 2[1], below, and repeated in Table 2 of "Appendix A – Device migration data validation responses".

NP001	The device was not processed because it was the subject of an active STOP request[1]
NP002	The device was not processed because it was in a batch that has been cancelled
NP003	The device was not processed because it was too close to a switch date
NP004	The device could not be processed before the batch end date/time
NP005	The device was not processed because it has not communicated with the DCC systems within the last x days
NP006	The device was not processed because it was in the exclusion list
NP007	The device was not processed because the Device ID does not exist in the SMI as a SMETS2 or later device of an appropriate device type which is associated with a CSP
NP008	The device was not processed because it has invalid Device Status
NP009	The device was not processed because the Device ID does not exist in the SMI as a SMETS2 or later device of an appropriate device type
NP010	The device was not processed because the current contents of its CoS Certificate slot cannot be determined or does not belong to the Transitional CoS Party

Figure 2 - Device data validation responses

These responses do not constitute an error within the ECoS Migration Systems but some will still require creation of an incident to investigate the cause. The retry approach for each code is further explained in section 3.2.2.

2.1.4. Command Preparation

Once the TCoS Service Provider has established that a Device is eligible for migration, they will commence activities required to prepare to send a command to the Device and communicating with components of the DCC Total System. Failures that occur during the preparation stage will result from either the intervention of a system control, such as an Anomaly Detection Thresholds (ADT) being breached, or a system failure. These failures are all listed in Figure 3, below, and

[1] An explanation of the purpose of STOP requests is provided in section 2.2.3.

repeated in Table 3 of "Appendix A – Command preparation failures". DCC shall raise an incident where such an error (or group of errors) occurs.

- TCoS Party error in validating DSP request (e.g. replacement certificate error, authentication failed)
- DSP error in validating response from TCoS Party (e.g. format error, certificate error)
- Error in certificate in CoS Certificate replacement request from TCoS Party
- Target in CoS Certificate replacement does not match that of original request
- Anomaly detection failure

Figure 3 - Command preparation errors

Where an error occurs at this stage, DCC can be certain that no command has been sent to the Device.

2.1.5. Command Delivery

In the preceding stage, the TCoS Service Provider will have completed preparation of the replacement command. In this stage, the command is sent to the Device. Failures that occur during or following the delivery of the message are listed in Figure 4, below, and repeated in Table 4 of "Appendix A – Command submission failures". These responses do not constitute an error within the ECoS Migration Systems and will not result in the creation of an ECoS Migration incident.

Where a failure results in an error code of PE103, DE201 or DE202, the Responsible Supplier will be informed of both the error code and the associated failure reason, via the ECOSMIG-002 report. The Responsible Supplier will need to review these failures and fix as appropriate.

PE103-1	No acknowledgement received from CSP
DE201-1	Certificate retrieval timed out
DE202-1	Device failed to execute command
DE202-2	Replacement credentials not on the device
DE202-3	Unknown credentials in CoS Certificate slot
DE202-4	No credentials data received for CoS Certificate slot

Figure 4 - Command delivery responses

2.1.6. Reconciliation

This stage of migration relates to the act of reconciling the migration success between both the TCoS Service Provider activity. This involves checking for the existence of matching reports to confirm that both DSP and ECoS Service Provider agree that the certificate has been replaced. This stage does not result in specific failure or error conditions being logged as part of the migration process.

Where a Device (or cluster of Devices) fails to complete reconciliation within an expected timeframe (e.g. 24 hours), DCC will raise an incident to investigate the cause.

Where a Device successfully concludes migration reconciliation, the Responsible Supplier will be informed via the ECOSMIG-001 report.

2.2. Other instruction types

In addition to the ECoS Migration instructions that the MCC may send to the TCoS Service Provider, there are further instruction types that may be sent. Error handling associated with these additional instruction types is explained in the following sections.

Note that errors associated with these instruction types are not in scope of the reports described in the ECoS Migration Reporting Regime.

2.2.1. Certificate Retrieval

The Certificate Retrieval batch enables the MCC to ask the TCoS Service Provider to interrogate the Device to determine the certificate serial number held in the CoS Certificate slot on a Device.

The MCC may include a Device in a certificate retrieval batch either because the Device has responded to indicate that it was unable to match the TCoS Party's certificate to that which it holds or because the Device failed to respond to the CoS Certificate replacement command (see section 3.2.4).

Possible error conditions for this stage are listed in "Appendix A File validation errors" wherein the relevant error codes are indicated specific to Certificate Retrieval batches.

2.2.2. Batch Cancellation

The MCC may choose to cancel an ECoS Migration batch which has already been created (E.g. the MCC may have determined that a Device Model that is included in the batch may need to undergo investigation). Where the batch instruction has already been issued to the TCoS Service Provider, a Batch Cancellation instruction is sent to the TCoS Service Provider to inform them that the batch is cancelled and to cease commencing any further migration activity with respect to that ECoS Migration batch.

Error handling of Batch Cancellation is limited to file validation errors. For a subset of the possible error conditions, DCC shall raise an incident, either for an individual file or group of files. Error conditions where an incident is not required are those where the error condition indicates that the TCoS Service Provider has correctly responded to a file sequencing issue, which may arise from time to time.

Possible error conditions for this stage are listed in "Appendix A – File validation errors" along with an indication of which conditions would result in an incident.

2.2.3. Stop and End Stop Request

A Stop request may be raised manually by the MCC or automatically by the DCSE system (as described in section 2.5.2) to prevent the TCoS Service Provider from migrating Devices (based on particular criteria such as Device Type, Device Model and CSP). The MCC may subsequently issue an End Stop request to advise the TCoS Service Provider that a previously issued Stop request no longer applies.

Issuing of an End Stop would only occur where the MCC was satisfied that the investigation has concluded that it is appropriate to continue migrations impacted by the Stop that was put in place. There may also be circumstances where an End Stop can only be issued after a more specific Stop has been put in place (e.g. lifting the Stop on an entire Device Model only once a Stop is raised to target a subset of related Devices based on a range of Device IDs).

Possible error conditions for this stage are set out in "Appendix A – File validation errors" along with an indication of which conditions would result in an incident.

2.3. SharePoint Unavailability

Impacted parties are advised to raise an incident and email the MCC (migration@smartdcc.co.uk) where the DCC SharePoint is inaccessible for receiving the reports defined in the ECoS Migration Reporting Regime. DCC may also raise incidents, independent of any observation by Service Users, for the same.

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 ECoS Migration, as SharePoint unavailability would impact on more business processes that ECoS Migration alone.

DCC will be required to resolve this incident in accordance with standard service management arrangements. DCC will advise impacted parties about a suitable workaround if appropriate.

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

2.4. Migration Reporting Failures

Impacted parties are advised to raise an incident and email the MCC (migration@smartdcc.co.uk) where reports set out in the ECoS Migration Reporting Regime are not delivered as expected, either with respect to schedule or content. DCC may also raise ECoS Migration incidents, independent of any observation by Service Users, for the same.

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.

DCC will be required to resolve this incident in accordance with standard service management arrangements. DCC will advise impacted parties about a suitable workaround if appropriate.

Once the incident has been resolved, DCC will advise impacted parties of the nature of the resolution such that they may resume the receipt of files through the DCC SharePoint.

2.5. Migration application and system failures

2.5.1. Migration performance

The MCC will monitor the performance of migration throughout the stages set out in section 2.1. Where performance is deemed to have broken key indicators, DCC shall raise an incident.

This document does not attempt to record the key indicators to be monitored but the key indicators will include such metrics as; the performance of the TCoS Service Provider consuming and reporting upon new migration batches, the rate by which TCoS Service Provider processes Device records, the level of Device migration failure and the performance of the completion of reconciliation activities.

2.5.2. Auto Stop

The DCSE application will monitor the migration performance 24/7. The DCSE application may initiate an automatic stop (Auto Stop) of migrations fitting specific profiles, where defined metrics have been breached. For example, one profile might be for migration failures relating to one CSP exceeding 30% over a 30 minute period of monitoring. The purpose of this example profile would be to prevent continued ECoS Migrations occurring where there's a sign of a fault within the CSP system. This would ensure the incident could be resolved without continued demand from ECoS Migration.

Auto Stops are sent to the TCoS Service Provider to ensure that the TCoS Service Provider can take account of the command with respect to any migrations already in progress and any that may subsequently be sent by the DCSE.

Where the systems initiate an Auto Stop, DCC shall raise an incident to investigate the cause and will not lift the Stop until such time as the cause has been confirmed and the impact investigated to satisfy re-commencing the scope of stopped migrations.

3. Migration Batch Submission Retry

3.1. Frequency of submissions

There are a number of references within this document to Devices being subjected to a Cooling Off Period following a failed Migration Batch Submission.

These Cooling Off Periods vary in length but their purpose is to provide a reasonable time for the fault that caused the previous failure to be corrected before initiating a further Migration Batch Submission.

For example, in the case of a Device that has failed due to proximity to a CoS event, a Cooling Off Period of 14 days might be enough to avoid the CoS activity on the next Migration Batch Submission.

Another example would be a Device that failed because the Device didn't respond to the certificate replacement command. In this instance a 14 day period between retries will ensure that, over the course of a number of Migration Batch Submissions, DCC and / or the Responsible Supplier will have adequate time to seek a suitable solution to the communications issue, should one be required.

The MCC will be able to tune these Cooling Off Periods. For instance, they may choose to significantly reduce the length of Cooling Off Period as the end of the ECoS Migration Period approaches, in order to allow for more Migration Attempts to be made on Devices installed in those final stages of the ECoS Migration Period.

Cooling Off Periods are intended as a minimum gap between Migration Batch Submissions. Other variables may mean that the gap is longer, such as during the early stages of migration when the MCC would prioritise first Migration Batch Submissions for large volumes of Devices over second or later Migration Batch Submissions.

3.2. Candidates for Retry Migration Batch Submissions

3.2.1. Failures Related to File Level Validation

Where the TCoS Service Provider has rejected a whole instruction file (as detailed in section 2.1.2), all Devices within that file will be considered as a candidate for a future retry with immediate effect.

3.2.2. Responses Related to Device Data Validation

When Device data validation takes place, there is a range of possible error codes and the treatment related to those error codes falls into five high level categories, as shown in Figure 5.

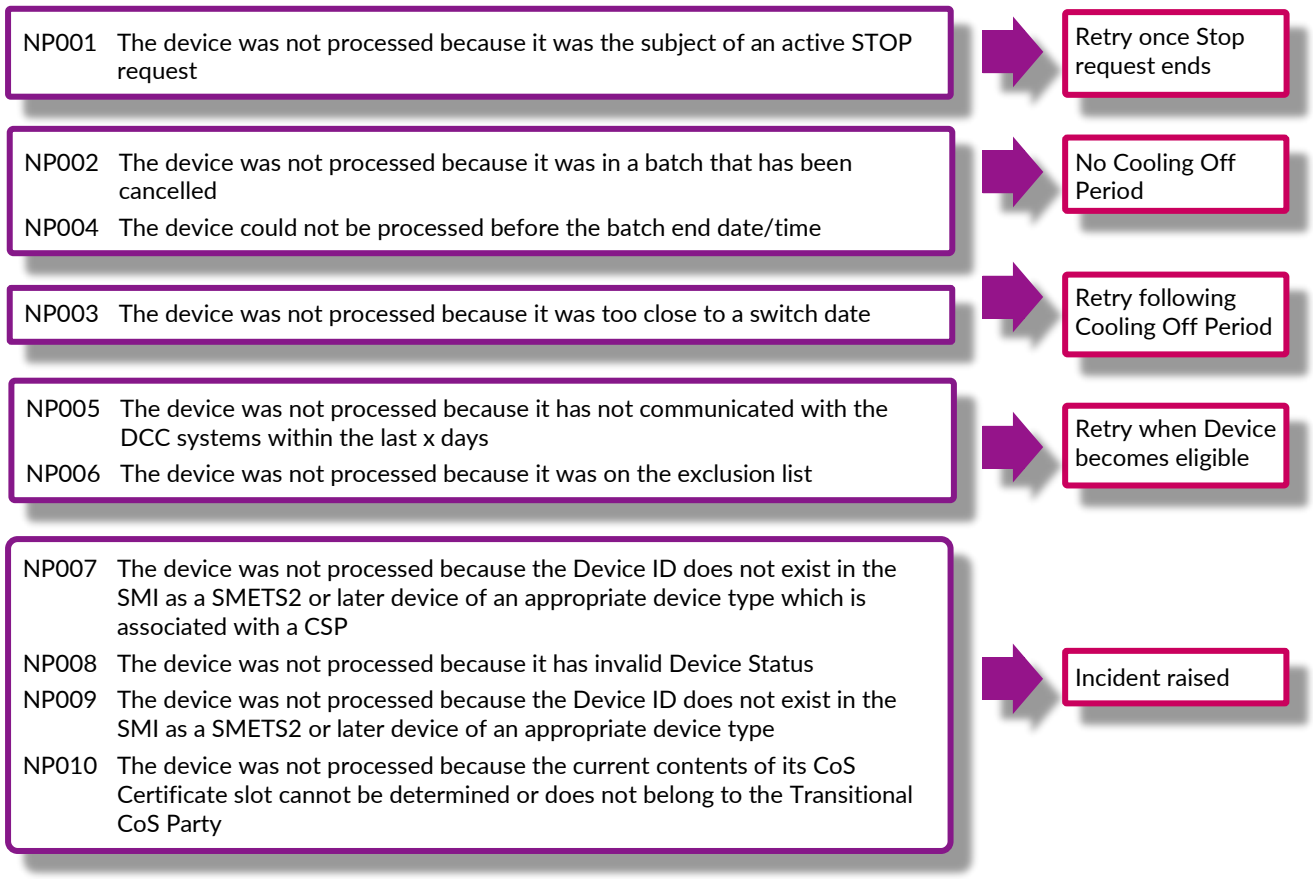


Figure 5 – Error handling for device data validation responses

Retry once Stop request ends

When the TCoS Service Provider performs data validation on a Device that cannot be progressed owing to the existence of an active Stop (or Auto Stop) request, the response relating that Device shall be NP001. A Device failing a Migration Batch Submission for this reason won't become a candidate again until the associated Stop (or Auto Stop) request has ended. At this point the Device will become a candidate for another Migration Batch Submission immediately, there will be no additional Cooling Off Period required in these cases.

No Cooling Off Period

Where a Migration Batch Submission fails with an error code of NP002, this will indicate that the MCC chose to cancel the batch. As this decision was taken by the MCC and is not necessarily a decision specific to that Device, no Cooling Off Period will be applied for that Device becoming a candidate for future migration once the issue that resulted in the batch cancellation has been resolved.

Where a Migration Batch Submission fails with an error code of NP004, this will indicate that the TCoS Service Provider didn't process the migration request for the Device before the batch end date was reached. As this has no bearing on the validity of the request to migrate the Device, no Cooling Off Period will be applied for that Device becoming a candidate for future migration once the issue that resulted in the batch cancellation has been resolved.

Retry following Cooling Off Period

Where a Device Migration Batch Submission concludes with an error code of NP003, this indicates that request to migrate the Device was too close to a change of supplier event. The Device will be subject to a Cooling Off Period (e.g. 14 days) before it becomes a candidate for a subsequent Migration Batch Submission to account for this error.

Retry when Device becomes eligible

Where a Device Migration Batch Submission concludes with an error code of NP005 or NP006, the Device will be deemed to be ineligible for migration. These Devices will only become a candidate for migration again if they are found to be eligible again.

Devices that are the subject of an NP005 will only become a candidate if communications are re-established with the Device.

Devices that are the subject of an NP006 only become a candidate if the Device and/or Device Model associated the Device is removed from the replacement exclusion list.

Incident raised

Error codes NP007 to NP010 are indicative of a fault with the Device which questions whether the Device is eligible for migration. In these circumstances, an incident will be raised for each Device or a group of Devices, for further investigation.

In the case of a NP010 error code, the Device would likely be the subject of a Certificate Retrieval batch to confirm the content of the CoS Certificate slot on the Device.

Where the investigation is concluded with a resolution that corrects the issue that resulted in the error code, the Device will become a candidate for migration.

Where the investigation concludes that the issue cannot be resolved, the Device will no longer be considered eligible for migration on the basis that there is a technical issue impacting the functionality of the Device.

3.2.3. Failure during Command Preparation

Where the TCoS Service Provider has rejected a Device during its preparation to send the certificate replacement message, the Device will be considered as a candidate for a future retry following a Cooling Off Period (e.g. 14 days). Issues that arise at this stage will result in an incident and, while the incident is unlikely to relate the Device in question, the Cooling Off Period will allow initial stages of investigation to be carried out to confirm that.

3.2.4. Responses related to Command Delivery

When ECoS Migration fails during the command delivery phase, treatment falls into three high level categories, as shown in Figure 6.

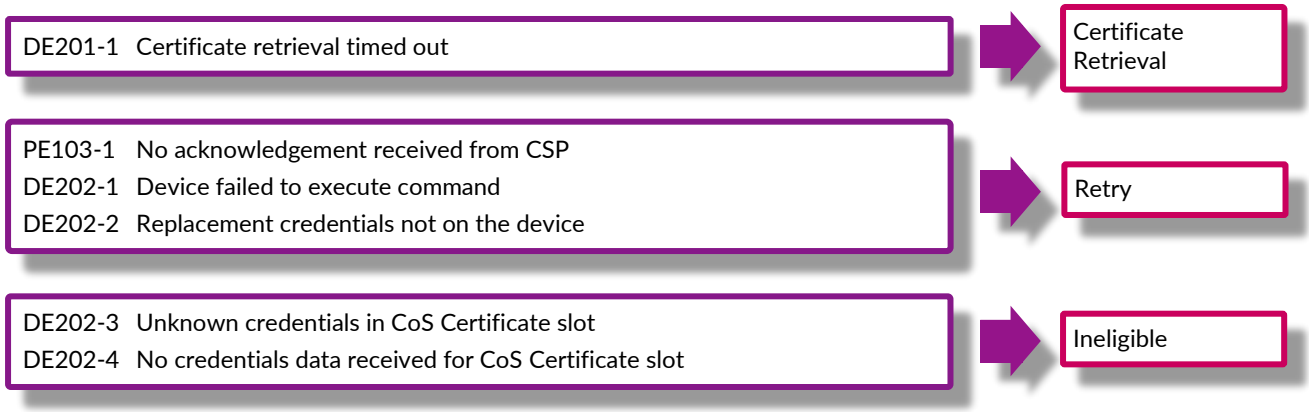


Figure 6 – Error handling for command delivery

Certificate Retrieval

Where a Migration Batch Submission results in an error code indicating no response from a Device (Error code = DE201), it is still possible that the Device did replace the TCoS Certificate

with the ECoS Certificate. To account for this possibility, DCC will instruct the TCoS Service Provider to perform a Certificate Retrieval command for the affected Device.

If the Device responds to this request with an indication that it now holds the ECoS Certificate, the TCoS Service Provider will complete the final stages of migration, that being the update to inventory. DCC will expect the ECoS Party to do the same and would then indicate the successful migration of the Device in migration report ECOSMIG-001.

If the Device fails to respond or responds with an indication that it still holds a TCoS Certificate, the Device will be considered for inclusion in a future Migration retry following a Cooling Off Period (e.g. 14 days).

Retry

Where a Migration Batch Submission results in an error code of DE202 with sub code of either 1 or 2, the Device will be considered for inclusion in a future Migration Batch Submission following a Cooling Off Period (e.g. 14 days). This Cooling Off Period is intended to spread future Migration Batch Submissions such that the Responsible Supplier has an opportunity to review the status of this Device and take action that might permit future Migration Attempts to be successful.

Where a Migration Batch Submission results in an error code of PE103, no Cooling Off Period will be applied for that Device. The reason why this error doesn't require a Cooling Off Period is that, while the error suggests that the Device isn't chatty, when we include the Device in a subsequent Migration Batch Submission, DCSE will still check that there has been recent communication with the Device to ensure it is still eligible.

Ineligible

Where a Migration Batch Submission results in an error code of DE202 with sub code of either 3 or 4, the Device will be deemed ineligible for migration and no further Migration Batch Submissions will be made. This is because, where the Device does not hold a valid TCoS Certificate, DCC will be unable to sign the command required to apply the ECoS Certificate to the Device. This is therefore categorised as having a technical issue impacting the functionality of the Device. Note that this is not a condition we expect to encounter. We are merely documenting what would happen were we to find a Device in this state.

3.3. Migration Retry Limitations

Where ECoS Migration fails for a Device, DCC will aim to carry out at least five Migration Attempts. After this point, DCC will consider that the Device has an unresolved technical issue and the Device will no longer be considered eligible for migration, as defined under ETMAD 1.4(c).

ETMAD 1.4(c)

1.4 The DCC shall not attempt to migrate a particular Device that is deemed to be Ineligible for ECoS Migration. Devices may be Ineligible for ECoS Migration where:

(a) the Device is of a Device Model that has been classified as Non-Migratable;

(b) there is a transient issue which may impact the effectiveness of ECoS Migration such as recent or pending change of supplier, or recent Commissioning; or

(c) there is a technical issue impacting the functionality of the Device.

If the issue which made the Device Ineligible for ECoS Migration is subsequently resolved and / or no longer applies, the relevant Device shall no longer be Ineligible for ECoS Migration and the DCC shall attempt ECoS Migration for the Device in accordance with Clause 1.3.

DCC's ability to carry out multiple Migration Attempts will be influenced by a number of factors. At a high level these are:

- the likelihood of the Device being considered eligible at any one time
- the date of installation of the Device compared with the time remaining to carry out migrations.

4. ECoS Non-Migratable Device Model List

The list of Non-Migratable Device Models is provided as the "ECOSMIG-004 - Summary Report: Devices Count by Non Migratable Device Model" report with the purpose of informing Supplier Parties that DCC has determined that particular Device Model(s) have been classified to be Non-Migratable, as defined in ETMAD.

ETMAD 1.12

The DCC shall publish a list of Non-Migratable Device Models, to be updated regularly and as soon as practicable to reflect any changes identified.

ETMAD 1.14

Where an appeal has been made pursuant to Clause 1.13, the determination by the Secretary of State shall be final and binding for the purposes of this Code, provided that where a Device Model is categorised as Non-Migratable, the DCC may subsequently re-categorise the Device Model as being capable of ECoS Migration.

The list of Non-Migratable Device Models will also be made available. The format of the report is presented in Appendix B of this document.

The issuing of updated versions of the list of Non-Migratable Device Models may occur either to add new Device Models, remove Device Models or to revise existing entries as may be required to support the conditions set out in ETMAD.

Where DCC determines that a new entry should be added to the list of Non-Migratable Device Models, DCC will ensure that the creation of the entry is supported by rationale for its creation. DCC anticipates that this rationale will be formed of statements that express a need to cease migration and the reason. DCC will seek these statements, with the support of the Responsible Supplier, from the manufacturer of the Device.

Where DCC is required to remove an entry from the list of Non-Migratable Device Models, the entire row shall be removed from the list and a record of the associated entry numbers will be made in the version control of the updated version.

5. TCoS Party Timeout and Retry

Where there is no response from the Device after sending a command to swap the TCoS certificate with an ECoS certificate, the TCoS Service Provider will perform a series of retries using the strategies defined below:

1. Short and long retry

   a) The TCoS Service Provider attempts to resend the command a configurable number of times at configurable intervals (e.g. 3 times every 40 seconds). This will be attempted for a configurable retry time period (e.g. for 320 seconds). This is known as a 'short retry'.

   For a GSME (which has a 'sleep' time – it may take up to 30 minutes to respond) a different short retry strategy may be defined (e.g. once after 1840 seconds for a retry period of 3780 seconds).

   b) If the short retry fails, the TCoS Service Provider attempts a long retry: this consists of requeuing the command and making a new short retry attempt (i.e. the short retry intervals are repeated) after a configurable long retry wait period (e.g. 2 hours).

   c) If this attempt fails, the TCoS Service Provider repeats the long retry (i.e. requeues the command and makes a new short retry attempt after the configurable long retry wait period) until it succeeds or a maximum redelivery attempt time (e.g. 24 hours) is reached. At this point, the system will move to the Certificate Confirmation Scheme strategy described below.

2. Certificate Confirmation Scheme (CCS)

   If the outcome of the certificate swap is still unknown following the strategy above, then the TCoS Service Provider attempts to retrieve the certificate details from the device in order to resolve the uncertainty as to whether the certificate has been replaced:

   a) The TCoS Service Provider sends a certificate retrieval request to the device.

   b) If the retrieval request fails (i.e. no response is returned), then the TCoS Service provider performs a short retry by attempting to send the commands at configurable intervals (e.g. 3 times every 40 seconds) for a configurable retry time period (e.g. for 320 seconds).

   Note that the short retry strategy for the certificate retrieval request may differ from that used for the certificate swap request. A different strategy may also be defined for the retrieval request for the GSME to accommodate the 'sleep time'.

   c) If the short retry fails, then the TCoS Service Provider waits for a CCS configurable wait period (e.g. 24 hours) and reattempts to send the retrieval request, with a new short retry attempt if that request fails.

   d) The TCoS Service Provider repeats the sending of the retrieval request after the CCS configurable wait period, performing short retries on no response, until a response is retrieved or until the maximum CCS attempts (e.g. 7) is reached. If the retrieval was not successful at this point, then an outcome of 'Failed' (Error Code DE201-1, indicating 'Certificate retrieval timed out') is recorded.

   If the Certificate Confirmation Scheme succeeded in returning a response from the device, then the TCoS Service Provider processes the response as follows:

a) If the certificate returned is that of the target ECoS Certificate, then the TCoS Service Provider updates the Smart Metering Inventory with the ECoS certificate details, records a successful outcome and informs the ECoS Service Provider.

b) If the certificate returned is not that of the target ECoS Certificate, then the TCoS Service Provider updates the Smart Metering Inventory with the certificate details and records an outcome of 'Failed' (Error Code DE202-2 indicating 'Replacement credentials not on the device').

c) If there is some other error, then the TCoS Service Provider updates the Smart Metering Inventory and records an outcome of 'Failed'. The result here will either be that the device returned unknown credentials (Error code DE202-3) or the failed to return credentials data (Error code DE202-4).

6. Responsible Supplier Actions

This section provides a summary of the aspects of error handling that Responsible Suppliers are expected to monitor and take action on and further expands other aspects of the ETMAD that may require action by Responsible Suppliers.

6.1. Monitoring of Migration Failures

Sections 2 and 3 of this document provide an explanation of error handling processes and how DCC will react with regards to retrying Migration Batch Submissions.

Responsible Suppliers are expected to monitor reports issued by DCC, as detailed in the ECoS Migration Reporting Regime. In particular, Responsible Suppliers should be observing failures documented either in "ECOSMIG-002 - Detail Report: ECoS Migrations Completed Unsuccessfully" or "ECOSMIG-003 - Detail Report: Gaining Supplier Devices History".

The following sections will list each of the error codes that might be included in these reports, grouped by the similar meaning for the Responsible Suppliers.

6.1.1. Devices having Invalid Certificate in the TCoS Slot which Prevents Migration

When the TCoS Service Provider reports that a Device has an invalid certificate, in the CoS Certificate slot the Device will be considered ineligible for migration (see section 3.2.4). The only viable option remaining in this circumstance would be for the Responsible Supplier to replace the Device in question. In this scenario, DCC believes replacing the Device is required as the errors identified would also prevent the TCoS Party or ECoS Party from successfully processing a CoS command (SRV 6.23).

Error Code	Error Sub Code	Meaning
DE202	3	Unknown credentials in CoS Certificate slot
DE202	4	No credentials data received for CoS Certificate slot

6.1.2. Failures where the Device reports that it failed to execute the command

Where the TCoS Service Provider reports that a Device failed to execute the CoS Certificate replacement command, the Responsible Supplier should consult with the Device manufacturer to understand the background to this fault and seek advice on the cause and possible corrective actions available.

Note that the MCC will also review failures of this nature to ensure that, where there is a pattern of behaviour of a particular Device Model, this will inform the selection of Devices for migration and will feed into the processes associated with the Non-Migratable Device Models list.

Error Code	Error Sub Code	Meaning
DE202	1	Device failed to execute command

6.1.3. Failures Indicating a Communications Issue

The following errors relate to Devices suffering communication issues. The Responsible Supplier should consider whether they have also observed communication issues with this Device in the past and whether action is required to improve communications to this Device to improve the chance of successful ECoS Migration.

Error Code	Error Sub Code	Meaning
PE103	1	No acknowledgement received from CSP
DE201	1	Certificate retrieval timed out

6.2. Non-Migratable Device Models

DCC will maintain the list of Non-Migratable Device Models, as described in Section 4. Service Users are advised to monitor updates to this list and any bearing that the entries would have on the Devices for which they are responsible.

Responsible Suppliers are also advised to monitor the ECoS Migration Report "ECOSMIG-004 - Summary Report: Devices Count by Non Migratable Device Model" which is intended to summarise how many Devices will not be eligible for ECoS Migration as they are of a Device Model categorised as Non Migratable.

Responsible Suppliers may need to upgrade the firmware on Devices (with the exception of Gas Proxy Functions, where DCC is responsible for applying firmware upgrades) that are of a Device Model included in the list of Non-Migratable Device Models and should seek advice from manufacturers on the appropriate action.

Appendix A - Error Codes

File validation errors

The errors listed in Table 1 relate to file handling of instructions sent from the DCC Migration Control Centre to the TCoS Service Provider. Those indicated with a tick in the column titled 'Migration' relate to the error handling described in section 2.1.2. Those indicated with a tick in the columns titled 'Retrieval' – 'End Stop' relate to the error handling described in section 2.2. Those indicated with a tick in the column titled 'Incident' would warrant raising an incident.

Description	Migration	Retrieval	Cancel	Stop	End Stop	Incident
Incomplete file (no trailer and/or signature)	✓	✓	✓	✓	✓	✓
Invalid filename	✓	✓	✓	✓	✓	✓
Invalid field contents	✓	✓	✓	✓	✓	✓
Filename inconsistent with header	✓	✓	✓	✓	✓	✓
Number of body records does not match trailer record count	✓	✓	✓	✓	✓	✓
Inconsistent use of "ALL" in STOP Request criteria				✓		✓
Error in validating signature	✓	✓	✓	✓	✓	✓
Batch Request has been cancelled	✓	✓				
Processing End Date time is in the past	✓	✓				
Have already received cancellation for this batch			✓			
Stop Request has already been ended				✓		
Have already received End Stop for this Stop request					✓	
Validated file exists with same Batch Request Id and Sequence Number	✓	✓				✓
Validated file exists with same Stop Request Id and Sequence Number				✓		✓
Firmware criteria in STOP Request is not present on the Central Products List				✓		✓
MPID supplied does not exist				✓		✓
CSP supplied is not ARQ or VMO2				✓		✓

Table 1 - File validation errors

Device migration data validation responses

Table 2 lists the validation responses that may be returned by the TCoS Service Provider in response to the request to migrate a Device.

Error Code	Meaning	Incident
NP001	The device was not processed because it was the subject of an active STOP request	
NP002	The device was not processed because it was in a batch that has been cancelled	
NP003	The device was not processed because it was too close to a switch date	
NP004	The device could not be processed before the batch end date/time.	
NP005	The device was not processed because it has not communicated with the DCC systems within the last x days	
NP006	The device was not processed because it was in the exclusion list	
NP007	The device was not processed because the Device ID does not exist in the SMI as a SMETS2 or later device of an appropriate device type which is associated with a CSP	✓
NP008	the device was not processed because it has invalid Device Status	✓
NP009	the device was not processed because the Device ID does not exist in the SMI as a SMETS2 or later device of an appropriate device type	✓
NP010	The device was not processed because the current contents of its CoS Certificate slot cannot be determined or does not belong to the Transitional CoS Party.	✓

Table 2 - Device migration data validation error codes

Command preparation failures

Table 3 lists the failures that may occur during the activity of preparing to submit a migration (as described in section 2.1.4) or certificate retrieval command.

Request Type	Error Code	Error Sub Code	Meaning
Replacement	PE101	1	TCoS Party error in validating DSP request (e.g. replacement certificate error, authentication failed)
Replacement	PE101	2	DSP error in validating response from TCoS Party (e.g. format error, certificate error)
Replacement	PE101	3	Error in certificate in CoS Certificate replacement request from TCoS Party
Replacement	PE101	4	Target in CoS Certificate replacement does not match that of original request
Replacement	PE102	1	Anomaly detection failure
Retrieval	PE102	2	Anomaly detection failure
Retrieval	PE103	2	No acknowledgement received from CSP

Table 3 - Command preparation failure reasons

Command submission failures

Table 4 lists the errors that might arise from migration and certificate retrieval requests.

In summary, the errors fall into three categories:

- PE103 and DE201 – No response was received from the Device
- DE202 – The Device reported that the certificate replacement failed
- DE203 – The certificate retrieval command failed or resulted in an erroneous state

and are then supplemented with an optional failure reason comment.

Request Type	Error Code	Error Sub Code	Failure Reason Comment	Failure meaning
Replacement	PE103	1	No acknowledgement received from CSP	No response
Replacement	DE201	1	Certificate retrieval timed out	No response
Retrieval	DE201	2	No response received from device	No response
Replacement	DE202	1	Device failed to execute command	Replacement failed
Replacement	DE202	2	Replacement credentials not on the device	Replacement failed
Replacement	DE202	3	Unknown credentials in CoS Certificate slot	Replacement failed
Replacement	DE202	4	No credentials data received for CoS Certificate slot	Replacement failed
Retrieval	DE203	1	Unknown credentials returned	Retrieval failed
Retrieval	DE203	2	Credentials not returned from device	Retrieval failed

Table 4 – Command submission failure codes

Appendix B – Format of the ECoS Non-Migratable Device Model List

The ECoS Non-Migratable Device Model List shall be issued as a spreadsheet in Office Open XML format (.xslx)

Filename

The filename will identify the unique release version of the file as well as the date of issue:

ECoS-Non-Migratable-Device-Model-List-v[release version]-[release date].xlsx

Where:

- [release version] – is a unique integer counter indicting the version of the report
- [release date] – is the date of issue of this version of the report in the form ddmmyyyyy

Structure

The Spreadsheet will consist of two tabs:

1. Version Control tab
2. Non-Migratable List tab

Version Control tab

Version Control will contain a table list all previous issues of this report including the version number, issue date and a summary of changes incorporated in those releases.

Non-Migratable List tab

Non-Migratable List will contain a table listing a row for each Device Model that has been determined to be Non-Migratable. Each row will consist of the following fields

Data element	Mandatory/ Optional	Field Type and format	Max Length	Notes
Entry	M	Integer	6	Unique identifier for this entry
Version Of Entry	M	Integer	6	Version of report when this entry was added
Version Of Last Edit	O	Integer	6	Version of report when this entry was last edited. Blank if never before edited.
Device Type	M	Text	6	Equivalent to “Device_Type” field from CPL
Device Manufacturer	M	Text	30	A unique identifier for the manufacturer. For example: 1057

Data element	Mandatory/ Optional	Field Type and format	Max Length	Notes
Device Model	M	Text	30	A unique identifier comprised of the Device Model Identifier, the Device Model Hardware Version and Device Model Revision as supplied by the CPL. For example: 54342152 where 5434 is a Device Model Identifier, 21 is Device Model Hardware Version and 52 is Device Model Revision
Firmware Version	M	Text	8	an identifier of the firmware version. For example: 00123402
Supporting Rationale	M	Long Text	-	An unstructured field containing DCC's rationale for including this entry in the report
Notes	O	Long Text	-	An unstructured field containing explanation for any changes made to this entry.

Note that the field "Entry" will contain a unique identifier which will be unique across all versions of the ECoS Non-Migratable Device Model List. Therefore, when a record is deleted from the list, the "Entry" value from that deleted record cannot be reused on future records for any other purpose.