# Error Handling Strategy

| Draft DCC Guidance Document |
| --- |
| June 2016 |

## Contents

# 1. Introduction

## 1.1. Purpose

This document is to provide guidance regarding how the DCC and Users should behave when Errors occur within the DCC Systems.

## 1.2. Scope

**1.2.1.** The Error Handling Strategy guidance document:

a. outlines the classification of error instances, within the DCC Systems (where a Service Request or the Commands or Responses related to it fail to provide the result expected from that type or category of Service Request); and

b. sets out procedures to be followed and actions to be taken for the purposes of investigating and correcting such error instances.

**1.2.2.** The Response Codes categorised in this document returned to the User within Service Responses and DCC Alerts are described in the DCC User Interface Specification (DUIS) and are referred to within this document as the common Response Codes.

~~1.2.2.~~1.2.3. The document describes error handling processes for common Response Codes returned through the DCC User Interface resulting from Service Requests or related Commands. It does not cover errors returned from online systems (e.g. SSI or OMS) and does not cover the Registration Data Interface.

## 1.3. General Provisions

**1.3.1.** This document should be read in conjunction with the DUIS and the Incident Management Policy. The DUIS provides the DCC Systems Response to Errors, with the management strategy for handling Errors ~~is~~ provided by this Error Handling Strategy procedure guidance document and the procedure for the resolution of Errors where they generate ~~Incidents is~~Incidents is provided by the Incident Management Policy.

~~**1.3.2.** DCC and each User should each comply with the applicable sections of the Error Handling Strategy guidance.~~

~~1.3.3.~~1.3.2. The Target Response Time relating to the processing of Service Requests and the Commands and Responses related to the Service Requests are listed in ~~SEC~~ Section H3.14 of the SEC. Retry and Back-off Period calculations are defined in ~~the DUIS subsidiary document~~ section 2.10.1 of DUIS (Retry Processing).

~~1.3.4.~~1.3.3. Where an Error occurs a Response Code is returned to the User Systems in a Service Response or DCC Alert. Possible values are defined in DUIS.

~~1.3.5.~~1.3.4. The Incident Management Policy governs any ~~issues~~ Incidents that arise from Service Requests and their constituent parts.

# 2. Error Management

## 2.1. Error Classification

**2.1.1.** Errors will be classified into categories. The purpose of classification is to group individual Errors and their associated Response Codes, as defined in DUIS, into categories that enable the DCC and Users to handle Errors in the correct manner.

**2.1.2.** The Error categories are:

| Error category | Type | Description |
|---|---|---|
| U | Authentication failure | means authentication failures (such as a failure of secure communications channel with an invalid DCCKI Certificate or a failure of a Service Request or Signed Pre-Command which has not been signed with a valid SMKI Certificate); |
| V | Access control authorisation failure | means access control authorisation failures (such as an invalid or non-active SEC Party or the User Role does not have the access rights to perform the Service Request or Signed Pre-Command for the specified device); |
| W | Data validation failure | means data validation failure (such as the Service Request or Signed Pre-Command is not consistent with the DUIS XML schema, or the Service Request or Signed Pre-command is not valid or is not complete); |
| X | Time out | means a time out or communication failure (such as a response is not received within the expected time and/or date) by the User after the defined re-try process has been followed by DCC; |
| Y | Sequencing failure | means sequencing failures; and |
| Z | IMP error | is to be used where an Error has occurred and the Incident Management Policy may be followed. |

Table 1 – Error categories

**2.1.3.** The DCC Systems generated common Response Codes relating to the Error Handling Strategy procedures are shown in the DCC Systems Response Codes (table 30 within section 3.5.10 of DUIS).

**2.1.4.** All common Response Codes and Service Request specific Response Codes are listed within DUIS. ~~Where the User receives a~~A Service Request specific Response Code will be a longer Response Code with an associated message such as E010101 “Too many switching rules defined

(exceeds 200)". ~~that is~~Service Request specific Response Codes are not listed in the DCC Systems Response Codes table (table 30 within section 3.5.10 of DUIS) and therefore ~~has~~ have no related Error Handling Strategy procedure.~~,~~ ~~then~~ Where the user receives a Service Request specific Response Code the User may take action to correct the Service Request with reference to the Response Code and associated ~~description~~ message returned, and may correct and resubmit the Service Request. Where corrective action is not possible or is unsuccessful the User may follow the steps outlined in the Incident Management Policy Section 2.1.

**2.1.5.** The procedure for handling each of the Error categories is described in Section 2.2 of the Error Handling Strategy.

**2.1.6.** The DCC ~~should~~ will, in all cases, attempt to notify the User when an Error occurs, via a Response or DCC Alert, containing the reason for failure as detailed in DUIS.

**2.1.7.** Where DCC is unable to deliver a response or alert to the User, the DCC shall raise a Service Management Event and retry delivery as defined in DUIS.~~There are instances where the DCC may raise an Incident in accordance with the Incident Management Policy where an Error has returned as defined in DUIS. DUIS details the instances where the DCC should automatically raise an Incident.~~

## 2.2. Error Handling Strategy procedures

**2.2.1.** The procedures to be followed and actions to be taken for the purposes of investigating and correcting Errors are detailed in the table below.

**2.2.2.** The 'Error Handling Strategy procedure' identifier consists of a letter prefix (defining the Error category) followed by a unique number. The table below details the step(s) to be undertaken by the User.

**2.2.3.** For all common Response Codes (those covered by this document) which are raised as the result of an Error~~s~~ and where the User requires a resolution to the issue, the User ~~should~~ may first reference the Response Code in DUIS Section 3.5.10 to confirm the specific failure reason attributable to that Response Code ~~and identify the applicable 'Error Handling Strategy procedure'~~. The User should then follow the steps outlined under 'Details' in the table below.

| Error Handling Strategy procedure | Response Codes | Details |
|---|---|---|
| U1 | E100 | Prior to sending any Service Request the User must ensure the User Certificate is in accordance with the DUIS and will pass the checks set out in section DUIS 3.2.3 Message Authentication. The User must have successfully completed the relevant procedures and satisfied the criteria set out in the Organisation Certificate Policy and the SMKI RAPP.<br><br>Where the User receives an E100 Response Code, they should validate the status of their Organisation Certificate by checking the Organisation Certificate Revocation List (CRL). If it is an invalid status the User will need to follow the process in the SMKI Registration Authority Policies and Procedures (RAPP~~,~~). Both documents are available through the SMKI Repository. ~~i~~If the status is valid then the User should follow the process in Z1 to raise an Incident and include the Service Request certificate information held in Key Info and Organisation ID. |
| V1 | E4 | Where the User receives an E4 Response Code the User should check that they have access permission to read the Service Audit Trail for the relevant Device via the SSI for the period relevant to the submitted Service Request. Where the User does not have permission to read the Service Audit Trail they will need to check whether the Device is correctly registered to themselves within Industry Registration Data for the relevant period and should follow existing industry processes to correct the Registration Data where it is not accurate.<br><br>Where the Registration Data has recently changed (since the end of the last working day) the User may resubmit the Service Request after waiting at least one working day after the original submission to allow for daily Registration update files to be received from Industry registration ~~sytems~~systems and processed by the DCC.<br><br>Where the User does have permission to see the Service Audit Trail ~~the User may retry submission of the Service Request or~~or determines from the Registration Data that they should have permission to see the Service Audit Trail, they may follow the process in Z1 to raise an Incident providing the information from the Business Target ID and User ID. |
| V2 | E1 | Where the User receives an ~~E2~~ E1 Response Code the sending organisation should check the Business Originator ID and the associated User Role and confirm it is a valid SEC party / User Role combination. Where the User determines that the combination is incorrect, the information should be corrected and the Service Request resubmitted. Where the User determines that the combination is correct, they should follow the process outlined in Z1 to raise an Incident and include the detail of the Service Request, Business Originator ID and the associated User Role. |

| Error Handling Strategy procedure | Response Codes | Details |
|---|---|---|
| V3 | E3 | Where the User receives an E3 Response Code indicating that the User has had its rights suspended with respect to one or more Services; the User should check that the Service Request is subject to the suspension of rights. Where an individual within a User organisation is unaware of the suspension of rights, they should raise the issue within their own organisation to check that the Suspension has been notified.<br><br>Where the User acknowledges that its rights are suspended but determines that the Service Request should not be subject to the suspension then the User should follow the process in Z1 to raise an Incident and include the detail of the Service Request and a statement of the Users understanding of the extent of the suspension of rights with reference to M8.6 of the SEC.<br><br>Where the User's organisation does not acknowledge that its rights are suspended, the User should validate its status with the SEC Panel. If the SEC Panel confirms that the User status held by the DCC is incorrect the User may then follow the process in Z1 to raise an Incident~~the steps outlined in the Incident Management Policy Section 2.1~~. |
| V4 | E2 | Where the User receives an E2 Response Code the User should check DUIS to ensure that the User Role that is being used is allowed to carry out that Service Request.<br><br>The mapping between Service Requests and User Roles is provided in DUIS Section 3.1.1 - Service Request Matrix. The User must check that the User Role is an Eligible User Role for the Service Request being submitted. If appropriate the User should then make the appropriate amendments and re-submit the Service Request to the DCC.<br><br>Where the User determines that the User Role is an Eligible User Role but receives an E2 Response Code, they should follow the process in Z1 to raise an Incident and include details of the Service Request and User Role. |

| Error Handling Strategy procedure | Response Codes | Details |
|---|---|---|
| W1 | E12 | Where the User receives an E12 Response Code the User should check DUIS to ensure that the Service Request is applicable to that Command Variant.<br><br>The mapping of Command Variant to Service Request or Signed Pre-Command is shown in DUIS clause 3.1.1 - Service Request Matrix. When required the User should resolve the underlying cause of the Error occurring prior to submitting a new Service Request to the DCC.<br><br>Where the User determines that the combination is valid but receives the E12 Response Code, they should follow the process in Z1 to raise an Incident and include details of the Service Request and Command Variant. |
| W2 | E13 | Where the User receives an E13 Response Code the User should check DUIS to ensure that the Service Request is applicable to that URL (Web Service).<br><br>Check DUIS clause 2.4 - Web Services that the Service Request or Signed Pre-Command has been sent to the correct Web Service. The URL for the Web Service should be checked to match that published by DCC. When required the User should resolve the underlying cause of the Error occurring prior to submitting a new Service Request to the DCC.<br><br>Where the User determines that the Service Request or Signed Pre-Command has been posted to the correct URL they should follow the process in Z1 to raise an Incident and include details of the Service Request and URL. |
| W3 | E19 | Where the User receives an ~~E13~~ E19 Response Code the User should confirm the Device ID on the Self-Service Interface, if the Device ID is incorrect the user should make amendments to the Service Request and then re-submit the Service Request to the DCC. If the Device ID is showing as correct on the Self-Service Interface the User may follow the process in Z1 to raise an Incident and include details of the Service Request and Device ID.<br><br>Note that for Non-Device Service Requests the Response Code E19 is returned if the Business Target ID is not the DCC Access Control Broker ID. |

| Error Handling Strategy procedure | Response Codes | Details |
|---|---|---|
| W4 | E48 | Where the User receives an E48 Response Code the User should check within DUIS that the Service Reference is applicable to that Service Reference Variant.<br><br>The DUIS clause 3.1.1 - Service Request Matrix defines the valid combinations of Service Reference and Service Reference Variant. When required the User should resolve the underlying cause of the Error occurring prior to submitting a new Service Request to the DCC.<br><br>Where the User determines that the combination is valid they should follow the process in Z1 to raise an Incident with details of the Service Request including the Service Reference and Service Reference Variant as submitted. |
| W5 | E49<br>E51<br>E55 | Where the User receives an E49, E51, or E55 Response Code, the User should validate the format within DUIS. For each code specifically the User should perform the following validation:<br><br>E49 – The User should verify that the Service Request format matches the Service Reference Variant in the message header. This check is in addition to the XML format checks defined in DUIS clause 3.2.2, and therefore very few Service Responses are expected with this code as the majority will be identified and reported as HTTP Response Code 400.<br><br>E51 - For Signed Pre-Commands the User should check the Message Code contained within the Command matches the Service Reference Variant in the message header.<br><br>E55 - The ~~User should check that the Request ID is not the duplicate of another Request being processed by the~~ DCC Systems recognise the Request ID as a duplicate of one that had not been sent a response at the time the error was generated. The User will need to decide what action to take dependent on the status of their processes.<br><br>Where having completed the appropriate checks the User determines that the Service Request format is valid the User should follow the process in Z1 to raise an Incident and include the full details of the Service Request or Signed Pre-Command. |

| Error Handling Strategy procedure | Response Codes | Details |
|---|---|---|
| W6 | E5<br>E17 | Where the User receives an E5 or E17 Response Code, the User should use the Smart Metering Inventory query within the SSI to determine the SMI Status of the Device and then reference DUIS clause 3.2.4 to determine that the combination of SMI Status and Service Request or Signed Pre-Command is valid, referencing the combinations for Response Code E5 or E17 as appropriate.<br><br>Where having completed the appropriate checks the User determines that the Service Request and SMI Status combination is valid the User should follow the process in Z1 to ~~they should~~ raise an Incident and include the details of the Service Request and Device Id. |
| W7 | E11 | Where the User receives an E11 Response Code, the User should check the Device Type on the Self Service Interface (SSI) and then check in DUIS to ensure that the Service Request is applicable to that Device Type.<br><br>Where having completed the appropriate checks the User determines the Service Request and Device Type combination to be valid they should follow the process in Z1 to raise an Incident and include the details of the Service Request and Device Id. |
| W8 | E50 | The E50 error response from a request for a Command for Local Delivery indicates the Service Request has been quarantined. The User should follow the required steps on receipt of ~~this~~ the out of band notification as detailed in the Threshold Anomaly Detection document, prior to resubmitting the Service Request.<br><br>The normal and expected process following threshold anomaly events is that the User will receive an out of band notification and an Incident will be raised, therefore an Incident will exist prior to the E50 Response Code being received. Where the User has either not received an out of band notification or there is no pre-existing Incident the User should follow the steps outlined in the Incident Management Policy Section 2.1 to determine whether an Incident needs to be raised. |
| X1 | E20<br>E21 | Where the User receives an E20 or E21 Response Code indicating a 'communications failure' the User may follow the steps outlined in the Incident Management Policy Section 2.1, checking for the existence of any existing Incident regarding the communications failure, raised by another User or by the DCC. Where no pre-existing Incident exists the User should include details of the Service Request and Device and the installation location of the Device in the Incident. |

| Error Handling Strategy procedure | Response Codes | Details |
|---|---|---|
| X2 | E30<br>E31 | Where the User receives an E30 or E31 Response Code indicating a 'time out' the User may follow the steps outlined in the Incident Management Policy Section 2.1, checking for the existence of any existing Incident regarding the 'time out' communications failure, raised by another User or by the DCC. Where no pre-existing Incident exists the User should include details of the Service Request and Device including the installation location of the Device.<br><br>For both E30 and E31 Response Codes the User may follow procedure X3 once the Incident is resolved. |
| X3 | E30<br>E31 | Where desired and only when the communications have been confirmed as operational through the resolution of the related Incident, the User may submit a new Service Request to the DCC. |
| Y1 | E40<br>E41<br>E42<br>E52 | Where the User receives an E40, E41 or E42 Response Code the sequenced Request has been submitted incorrectly. Where the User identifies the issue the Service Request can be resubmitted and where the User cannot identify an error in the sequenced Service Request the User may raise an Incident and include the full details of the sequenced Request.<br><br>Where the User receives an E52 Response Code indicating a failure to cancel a Future Dated (DSP) Service Request of the same type, the User should check the details of the Service Request match those of the Future Dated (DSP) Service Request to be deleted and where any inconsistency is found, amend and resubmit the Service Request. Where the User determines the details to be correct, the User should follow the process in Z1 to ~~they should~~ raise an Incident and include the details of the Service Request. |
| Y2 | E43<br>E44<br>E45<br>E46<br>E47<br>E53 | Where the User receives an E43, E44, E45, E46, E47, E53 or E54 Response Code the sequenced Request has failed during execution and the User should refer to DUIS 3.5.10 for the description of the error and to DUIS 2.6.4 for the detail of Sequenced Services. Where the User identifies the issue the Service Request that has failed can be resubmitted and where the User cannot identify an error in the sequenced Service Request the User may raise an Incident as described in Z1 and include the full details of the sequenced Service Request. |
| Z1 | | Should the User continue to receive Error notifications once the issue has been corrected as directed, it may then, and not otherwise, follow the steps outlined in the Incident Management Policy Section 2.1 to determine whether an Incident needs to be raised. |

Table 2 – Error Handling Strategy procedures

## 2.3. HTTP Response Code handling procedures

**2.3.1.** In addition to the Error categories identified in the table above DUIS identifies HTTP Response Codes that are returned to Users in certain circumstances. The procedures to be followed for each of these are described in the table below:

| HTTP Response Codes | Procedure |
|---|---|
| 300: The recipient requires that the client redirects its request to an alternative URL | 1. The User should check all the connection information provided by the DCC with respect to URLs provided for the Service.<br>2. When required the User should resolve the underlying cause of the Error occurring prior to submitting a new Service Request to the DCC. |
| 400: Bad request | 1. The User should confirm that the failed Service Request is in the format as defined in the DUIS.<br>2. When required the User should resolve the underlying cause of the Error occurring prior to submitting a new Service Request to the DCC. |
| 500: Internal Server Error | 1. The User may follow the steps outlined in the Incident Management Policy Section 2.1.<br>2. Where having followed the IMP the User determines that an Incident should be raised the details of the web service instigation, Service Request and Device should be included within the Incident. |
| 503 Service Unavailable | 1. The User may follow the steps outlined in the Incident Management Policy Section 2.1.<br>2. Where having followed the IMP the User determines that an Incident should be raised the details of the web service instigation, the Service Request and Device should be included within the Incident. |
| Any other HTTP Response Code (excluding 200 the 'success' code) | 1. The User should assess the error based on the error response received and where the User decides it to be necessary they may follow the steps outlined in the Incident Management Policy Section 2.1.<br>2. Where having followed the IMP the User determines that an Incident should be raised the details of the web service instigation, the Service Request and Device should be included within the Incident. |

Table 3 – HTTP Response Code Handling procedures