ELEXON

DIP L3/L4 Validation requirements – DIP Manager Guidance Note

Data Integration Platform (DIP) Manager

Owner/author	**DIP Manager**	Purpose of paper	**Information**
Classification	**Public**	Document version	**1.1**
Date	**4 February 2026**		

Summary **Guidance on formation of L3/L4 validation responses**

Introduction

This file note supplements the details of L3/L4 validation described in the Elexon DIP Rules specifically DS002 Annex 2 – Detailed DIP Operational Requirements (DIP Rules - DSD002 Annex 2). The aim of the file note is to provide guidance on the use of Response codes in L3/L4 validation patterns, previously described in the MHHS-DES138-Interface Catalogue, which is missing from code documents.

The issue of L3/L4 validation and the ownership of the different response codes (RCP codes) was discussed at the MHHS Expert Group. One of the recommendations coming out of the meeting was that the DIP Rules would be the appropriate place to capture the exchange of L3/L4 validation messages and the corresponding response codes. To this end, DCR0014 will be raised by the DIP Manager to ensure the update to the DIP Rules follows the appropriate governance process via DCAB.

This guidance note does NOT cover how any issues that may have been communicated via a status message arising from L3/L4 validation should be resolved, it solely deals with the technical requirements around L3/L4 validation and the different RCP codes. The issue of the method of Participant-to-Participant message resolution, and how that need to be undertaken, is a recognised issue and will be reviewed by the industry code bodies.

Version 1.1 adds a reminder regarding the correct setting of Sender and Recipient Ids within DIP messages.

Requirements

The requirements for Participant L3/L4 validation are taken from the End-to-End requirements and form part of your PIT evidence. All the requirements are rated **MUST** and required for qualification:

E2E0201	Schema validation	M	Services shall undertake Level 3 message validation including structure, and the format of individual data fields/elements shall be performed against the appropriate message schema definition of all interface interactions.

E2E0207	Message Receipt	M	When sending messages all services shall use the http response of the API transaction to establish whether a message has been received by the DIP
E2E0203	Error Reporting	M	When Level 3 validation fails, e.g. when payload contents cannot be reconciled (schema validation), a response with the corresponding error code shall be reported back to the DIP via the http response in the webhook callback

In addition, there are requirements around the performance requirements around the timing for L3 and L4 validations:

E2E1003	Level 3 Processing Times (synchronous)	M	All Services shall provide an initial synchronous response (Level 3 validation) to a message within the following timeframes: - up to average hourly volume, mean response time of 2s or less - up to average hourly volume, 90th percentile response time of 4s or less - from average hourly to peak hourly volume, mean response time of 5s or less - from average hourly to peak hourly volume, 90th percentile response time of 8s or less
E2E0209	Level 4 Processing Times (Asynchronous)	M	All Services with the exception of Helix (VAS,MDS,LSS,ISD) and LDSO Services shall provide an asynchronous response (Level 4 validation) to a message within the following timeframes - up to average hourly volume, mean response time of 6s or less - up to average hourly volume, 90th percentile response time of 12s or less - from average hourly to peak hourly volume, mean response time of 10s or less - from average hourly to peak hourly volume, 90th percentile response time of 16s or less Helix Services (VAS,MDS,LSS,ISD) shall provide an Asynchronous response time of 10 minutes or less. All LDSO (DNO and iDNOs) roles, namely Registration Services, UMSO & LDSO shall provide an asynchronous response (Level 4 validation) to a message within the following timeframes - 60 minutes or less (within normal operating hours) in accordance with the MHHSP_OPC001_Operational_Choreography

Guidance

1. Level 3 - Synchronous Webhook Response

1.1 Issues have arisen with Level 3 validation on the Production system since M10.

1.2 Webhook Time-Outs

1.2.1 During busy periods, particularly during the Secure Active Window, participant webhooks have been timing out and are failing to reach the NFRs (E2E1003 – see above) in terms of response times. When attempting to communicate with a Participant webhook, the DIP will time-out the transaction after 10 secs if no response is received. This has meant that the DIP is having to resend messages, and more than often than not, these messages have already been received and hence getting a duplicate SUR with the second message.

Participants need to scale their systems to cope with the increased load during busy periods.

1.3 Incorrect Response Codes and messages

1.3.1 Participant systems are not responding with the HTTP response codes as defined in the DIP swagger – see appendix 1.

1.3.2 E.g. Incorrect response codes 207 instead of 400 for duplicate Sender Unique Reference have been used.

1.3.3 It has been noted that these codes are not currently in the DIP rules – as part of DCR0014 this omission will be fixed.

Participants need to return the correct HTTP response codes in webhook responses.

2. Level 4 – Asynchronous Responses

2.1 Participants have not been following the guidance for the formatting of the Status Messages being sent due to L4 validation and this consequentially has an impact on downstream systems as they are unable to interpret the messages sent. See section 3 below on Status Message Guidance.

Participants need to return a fully formed Status Message.

2.2 Also, Participants need to remember that they have an obligation to undertake the validation checks on each message channel. Validation can either take place at either Level 3 or Level 4; however, all checks **MUST** be undertaken. The expectation is that these will be a mixture of L3 and L4 as it is very unlikely, especially if your architecture contains a DIP adaptor, that all checks can be undertaken at the adaptor level. Table 1 in appendix 1 below outlines the L3/L4 checks that need to be undertaken

Participants need to perform all validation checks either at L3 or L4.

3. Status Message Guidance

3.1 The guidance for populating Status Messages is described MHHS-E2E001 End-to-End Solution Architecture document. The Status Message is either sent in the response as L3, or as a Status Message for L4, the format is the same for both:

Field	Description	Mandatory/ Optional
Transaction Id	Transaction Id of the original message the DIP	M
Sender Unique Reference	Sender Unique Reference of the original message	O
Correlation Id	Correlation Id of the original messages (where available)	O
Sent Timestamp	Sent timestamp of the Status Message	M
Sender Id	Logical Sender of the Status message	M

Field	Description	Mandatory/ Optional
Recipient Id	Recipient of the Status message, which will in most cases be the Sender of the original message. It the message is directed at the DIP then DIP Id '00000000000' should be used	M
DIP Connection Provider Id	Physical sender of message (where different to Sender id)	O
Message	Information regarding subject of message	M
Service Ticket URL	URL to create/view appropriate service ticket – not implemented at present	N/A
Help	Help text	O

3.2 The following fields need to be included as a **minimum** when sending back an L4 response. Without these fields messages cannot be correctly identified against the correct message and relayed to the relevant party:

i Transaction Id

ii Sender Unique Reference

iii Sender Id

iv Recipient Id

v Message

3.3 The "Message" text is taken from the messages that were defined in the MHHSP- DES138 Interface Catalogue and included in Table 1 of Appendix 1.

3.4 The "Message" is a concatenation of both the Error Code and the Generic Text taken the from the message list in Table 1, e.g. "REG0000 - MPAN Invalid or does not exist".

3.5 When the "Message" is formed, the guidance is that the Error Code and the text need to be separated by a space – hyphen – space, i.e. " – ".

3.6 The "Help" text is freeform and should convey other information about the error condition, e.g. specific MPAN details.

3.7 **Reminder – the Sender Id reported in the Status Message needs to be set to DIP Id of the sender of the Status Message and NOT the sender of the original message that the status message is in response to. Similarly, the Recipient Id needs to be set to the Recipient of the Status Message and NOT the recipient of the original message. Any message, sent/received to/from the DIP, the context of the Sender/Recipient roles within the message is ALWAYS within the context of the specific message be it an IF-xxx or a Status message.**

Appendix 1. MHHS Response Codes

Table 1 below details all the Response Codes that are within the current scope of L3/L4 validation. The Mandatory/Conditional (M/C) column denotes whether the check is mandatory or conditional. Some of the codes are marked as conditional because the checks referenced can be accomplished within swagger validation and therefore would not need to be explicitly checked as this check have already been undertaken.

M/C Column	
M	Mandatory
C	Conditional, the check could be covered by a schema validation check
C*	Conditional, the check could be covered by a new schema validation check to add a regex expression
M**	Mandatory, but dependent on back-office architecture
Rem	Remove

As part of DCAB CR0014 both tables 1 & 2 will be incorporated into the DIP rules.

Table 1 – List of Level 3/4 Response Codes

MHHS Response Code	**Message**	**Description**	**Usage Guidance**	M/C
RCP0000	Message Success		Used in response body of a 201 L3 response	M
RCP1000	Message Processing Failed	Generic / Catch All	Used when unspecified error trapped	M**
RCP1001	Schema Failure	Message is malformed and failed to complete schema Validation	Validation failure against the swagger.	M

RCP1002	Interface ID Invalid	Interface ID (..CommonBlock.S0.interfaceID) provided in the message is not valid / recognised	Would expect this to be captured by generic schema failure (RCP1001)	C
RCP1003	Event Code Invalid, Unexpected or Missing	Event Code (..CommonBlock.S0.eventCode) provided in the message is not valid or does not link to IF ID provided	Would expect this to be captured by generic schema failure (RCP1001)	C
RCP1004	Environment Code Invalid, Unexpected or Missing	Environment code (..CommonBlock.S1.environmentTag) contained in the message does not match the environment the message was presented to	Only the list of valid enumerations is presented in the Swagger hence Participants need to undertake the check. They can edit the swagger to set the enumeration to a single value hence it could be trapped by a generic schema failure	C
RCP1005	Schema Version Invalid or Not Compatible	Schema version (..CommonBlock.S0.schemaVersion) provided in the message is not compatible with the current schema in use	Again, would expect this to be captured by generic schema failure (RCP1001)	C
RCP1006	Sender Unique Reference Missing or Duplicated	Sender Unique Reference (..CommonBlock.S1.senderUniqueReference) is not populated or has already be processed by the DIP for that Participant ID	DIP Manager backlog to add regex pattern to Sender Unique Reference to implement	M*
RCP1007	Sender Sent Date/Time Invalid or Missing	Sent Date/Time (..CommonBlock.S1.senderTimestamp) provided in the message is not a valid format or not populated	Would expect this to be captured by generic schema failure (RCP1001)	C
RCP1008	Sender Sent Date/Time is in the Future	Sent Date/Time (..CommonBlock.S1.senderTimestamp) provided in the message is in future	Not checked by DIP	M
RCP1009	Sender DIP ID Invalid, Unexpected or Missing	Sender ID (..CommonBlock.S1.senderRoleID) is Invalid or Sender is not approved to send the message type stated	Missing value also be trapped by generic schema failure (RCP1001). Unexpected or invalid would be an incorrect value hence not a schema failure	C
RCP1010	Sender Role Invalid, Unexpected or Missing	Sender Role (..CommonBlock.S1.senderRoleID) provided is invalid or Role does not apply for Sender ID	Check not undertaken in Swagger (however it could be added)	M
RCP1021	Msg Mandatory Data Item Missing		Missing value also be trapped by generic schema failure (RCP1001).	C
RCP1022	Msg Contains Invalid Value for Value Restricted Field	Value of data item provided is not in the list of valid values/ISD for that data item	Enumerations exist in swagger hence these can be trapped via a RCP1001, however those defined external to the swagger, e.g. ISD.	M**
RCP1023	Msg Contains Invalid Valid Value Combination(s)	Can also be used for instances where Date/Time fields are not populated/formatted per the design guidance.	Would expect this type of error to be trapped via a schema failure RCP1001	C

~~RCP1041~~	~~Recipient ID Invalid, Unexpected or Missing~~	~~Recipient ID (..CommonBlock.S1.senderRoleID) is Invalid or Sender is not approved to send the message type stated~~	~~Missing value also be trapped by generic schema failure (RCP1001). Unexpected or invalid would be an incorrect value hence not a schema failure~~	Rem
RCP1042	Publication ID Invalid, Unexpected or Missing	Schema version (..CommonBlock.D0.publicationID) provided in the message is not a valid format or not populated	Missing value also be trapped by generic schema failure (RCP1001). Unexpected or invalid would be an incorrect value hence not a schema failure. Not sure what unexpected is.	C
RCP1043	DIP Txn ID Invalid, Unexpected or Missing	Schema version (..CommonBlock.D0.transactionID) provided in the message is not a valid format or not populated	Missing value also be trapped by generic schema failure (RCP1001). Invalid value - DIP Manager backlog to add regex pattern	C*
RCP1044	DIP Txn Timestamp Invalid or Missing	Schema version (..CommonBlock.D0.transactionTimestamp) provided in the message is not a valid format or not populated	Invalid/missing value could also be trapped by RCP1001.	C
RCP1045	DIP Txn Timestamp is in the Future	Schema version (..CommonBlock.D0.transactionTimestamp) provided in the message is in the future	Condition not trapped by DIP	M
RCP1046	DIP Correlation ID Invalid, Unexpected or Missing	Schema version (..CommonBlock.D0.correlationID) provided in the message is not a valid format or not populated	If a correlation ID was unexpected then would be ignored. Invalid value - DIP Manager backlog to add regex pattern	C*
~~RCP1047~~	~~Replay Indicator Invalid or Unexpected~~	-	~~Unsure under what conditions this would be trapped. Invalid value would be trapped by generic schema failure (RCP1001)~~	Rem
~~RCP1051~~	~~R0 Response Code Invalid~~	-	~~Unsure how this is used, swagger only Accept or Reject. Would be covered by generic schema failure (RCP1001)~~	Rem
RCP1052	R0 Response Code Inconsistent with Error Condition(s)	Response Code is 'Accepted' but error conditions also provided, Response code is 'Rejected' but no error conditions exist		M
RCP1061	MPAN Invalid or Unknown	This error message should be issued by the recipient in any circumstances where the MPAN is unknown or has a status (Migrated/Reverse Migrated) at which the IF type is not expected.		M
RCP1062	PUB Unexpected given MPAN Process Status/Condition	Unexpected message within context of business process		M
RCP1063	Message Data Content Differs from that Issued or Expected	Used to allow Registration Service to reject IF-034 containing inconsistent data from that issued in PUB-033		M

RCP1064	MDR provided not valid	Used to allow Registration Service to reject IF-034 containing invalid MDR		M
RCP9999	Message Signature Invalid	Signature provided in message is invalid	Can be reported by a 403 response	C

If the check is accomplished at L3 then the HTTP response code comes into scope (Table 2), only the RCP0000 is associated with a 201 (success), all other codes are seen as errors. All codes can be either L3 or L4 (except RCP0000 as success at L4 is not published). The choice of L3 or L4 is at the discretion of the system implementor.

Level 3 Validation

The callback response contains the outcome of the Level 3 validation undertaken by the recipient, the return code the result of the overall transaction and the response body details of the individual messages/events.
Each connection will result in a HTTP return code that will indicate the success or otherwise of the complete transaction. The list of response codes is also available in the swagger definition. The DIP retry and retry behaviour columns presents the pattern of behaviour that the DIP will undertake in the event of an error code.
The current DIP retry behaviour is under review between DIP Manager and Avanade.

Table 2

DIP Egress; i.e. webhook ("Level 3" validation)						
Code	**Messages**	**DIP Retry**	**Reason**	**Action**	**Retry Behaviour**	**Notify Sender via a status Message**
2xx	**Successful**					
201	Messages Created		Messages successfully received by Recipient and passed L3 validation.			
207	Some Messages Created	No	Some messages successfully received by Recipient and passed L3 validation.	The DIP will automatically send status messages for those messages failing validation		Yes; those messages failing validation
2xx	**Other 200 messages**		Participant systems should only send 201 or 207 messages			

4xx	**Client Errors**					
400	Bad Request	no	Malformed messages or HTTP Header content.	The DIP will automatically send status messages for those messages failing validation		Yes
401	Unauthorised Error	no	Issues related to Message Signing Certificates, Header problems or Account Issue (this includes any errors related to the X-API Key).	Ensure certificate validity; check cert has not expired. If problem persists contact DIP 1st line support	If participant believes issue is fixed then request messages to be resent via DIP replay	No
403	Forbidden	no	Issues related to TLS Certificates (including authentication failures), alongside other general 403 related issues i.e., could be IP blocking	Contact DIP 1st line support	If participant believes issue is fixed then request messages to be resent via DIP replay	No
404	Not Found	no	Resource not found	Resource could be temporarily unavailable, hence assume a periodic retry. If problem persists contact DIP 1st line support	If participant believes issue is fixed then request messages to be resent via DIP replay	No
405	Method Not Allowed	no	Requested method unsupported	Assume significant issue with participant system. Contact DIP 1st line support	If participant believes issue is fixed then request messages to be resent via DIP replay	Yes
406	Not Acceptable	no	Requested method unsupported	Assume significant issue with participant system. Contact DIP 1st line support	If participant believes issue is fixed then request messages to be resent via DIP replay	Yes
408	Request Timeout	yes	System timeout waiting for resource		The DIP will adopt a retry with an exponential back-off whilst attempts to rectify the issue are made	No

413	Payload Too Large	no	Request is too large for firewall/gateway	Participant can reduce size of webhook callback via API/portal. If still unsuccessful contact 1st line DIP support	If participant believes issue is fixed then request messages to be resent via DIP replay	No
429	Too Many Requests	yes	Rate limiting in force.	Assumption is that the participant system has implemented some rate limiting on their gateway	The DIP will adopt a retry with an exponential back-off	No
4xx	Other 400 messages		The DIP is not expecting to receive any other 400 message	Contact DIP 1st line support		
5xx	**Server Errors**					
500	Internal Server Error	yes	The DIP is aware that it has encountered an error with the Participant system.	Contact DIP 1st line support	The DIP will adopt a retry with an exponential back-off whilst attempts to rectify the issue are made	No
502	Bad Gateway	yes				
503	Service Unavailable	yes				
504	Gateway Timeout	yes				
505	HTTP Version Not Supported	no	Contact support			
5xx	Other 500 messages		The DIP is not expecting to receive any other 500 message			

Table 2 has been lifted from the MHHS-E2E001- End -to End Solution Architecture v3.8.

Response Body

The response uses the common Standard Response body (the same is used for the Status Message)

Field	Description
Transaction Id	Unique DIP transaction Id
Sent timestamp	DIP Receipt timestamp
Sender Unique Reference	The original Sender Unique Reference
Sender ID	The Sender of ***this*** message, i.e. the recipient of the incoming message.
Correlation Id	Correlation ID relayed back (optional)
Recipient Id	Recipient of the message, i.e. Recipient of this message most likely to be the Sender of the corresponding incoming message. If a DIP issue, then the recipient is the DIP and use DIP Id '0000000000'
DCP Id	DCP (optional – used if the Sender uses a DCP)
Message	Information on the message status
Help	Extra help information
Service Ticket URL	Not implemented

Where a field is not written/available/optional, then a null value needs to be written.

3. *Response Body Examples*

The response body of the HTTP call will deliver a response back to DIP indicating the success or otherwise of processing each message received.
In the first example below, one messages is successfully received: the first accepted and the second rejected:

Accepted message response:

HTTP/1.1 201 Messages Created

```
Content-Type: application/recieveEventCallback+json
{ "recieveEventCallback": { "version": "1.0" },
{
    "messageArray": [
        {
            "transactionID": "T-IF-004-2399990036-SUP-20251016-667B277A6C95B000",
            "senderUniqueReference": "S-IF-004-2399990036-SUP-20251009-123456811",
            "correlationID": null,
            "sentTimestamp": "2025-10-09T14:43:45+00:00",
```

```
            "senderID": "2399990036",
            "recipientID": "0000000000",
            "DIPConnectionProviderID": null,
            "message": "RCP0000 - Success",
            "help": null,
            "serviceTicketURL": null
        }
    ],
    "timestamp": "2025-10-16T10:43:16+00:00"
}
```


Rejected message response:

HTTP/1.1 400 Bad Request

Content-Type: application/recieveEventCallback+json

{ "recieveEventCallback": { "version": "1.0" },

```
{
    "messageArray": [
      {
          "transactionId": "T-IF-005-1234567890-SUPP-20220313-1234CC",
          "senderUniqueReference": "S-IF-005-1234567890-SUP-20220313-12345687a1234567a",
          "correlationID": "CI-20220313-1234567890123abce123092",
          "sentTimestamp": "2022-03-13T19:05:00+00:00",
          "senderId": "1009012345",
          "recipientId": "1009012346",
          "DIPConnectionProviderId": null,
          "message": "RCP1008 - Sender Sent Date/Time is in the Future"
          "help": "Sender date/time is beyond the current date/time",
          "serviceTicketURL": null

       }
    ],
    "timestamp": "2022-03-13T19:05:05+00:00"
}
```