DIP Onboarding and Connection Supporting Information

The following slides will provide guidance on:

- Relevant documentation to support connection and testing
- Potential Early Onboarding Steps for Production
- Connection Smoke Testing
- Certificates Overview
- Webhook setup overview and methods
- Errors codes for triaging of issues
- Schema Validation API use

Relevant Documentation

Useful Documentation to support message troubleshooting

Resource	Description	How to use it?	Link
DES-138 Interface Catalog	Original design artifact showing message structures of IF messages. Contains information about the MSGXXXX error codes that maybe received with a HTTP 400 response. Note this is superseded by Swagger for the IF message contents	Understand what blocks make up the message and data items. Has a list of message code that extend beyond DIP including REGS.	MHHS Programme Link
Swagger	API description for the all the message interfaces for DIP	Use the information in SWAGGER to configure messages correctly.	SubmitEvents | 2.0.1 | MHHSPROGRAMME | SwaggerHub
End-to End Architecture Document	Contains information about the API, Message Structure and Orchestration and HTTP Response Codes	Use the information in this document to understand DIP architecture how it deals with common scenarios etc	MHHS Programme Link
Code of Connection Document	Contains the detailed security related information for DIP connecting parties	Use the information to understand how to manage certificates.	MHHS Programme Link
REC EMDS	Energy Market Data Specification has been developed to create a common set of standards for all industry data represented within the Energy Market Architecture Repository	An up to date catalogue of data items for each interface. REC Portal account required.	REC Link

Early DIP Onboarding Steps

This shows the DIP Onboarding steps that can be completed prior to receiving the DIP Production Invitation

Onboarding Activity	Detail	Production Onboarding Note
GlobalSign Vetting	One time activity completed in for SIT/UIT	Not required as completed in test environment
Production GlobalSign API Key/Secret	API Key/Secret and Certificate pfx file created assigned to identity profile	This can be completed within the Atlas portal prior to invitation to Production DIP. These will then be uploaded into DIP Production Portal when access granted
Domain Verification	Domain verification for certificate	This can be completed early in Atlas Portal
DIP Production Certs	Production DIP Certificate used for TLS connection and/or Signing	Requires previous steps to be completed
Webhooks Registration	PUB Webhooks registration for receiving messages from DIP	Requires previous steps to be completed

Connection Smoke Testing

Guidance that can be used to verify the connection to and out of the **Production DIP** before the Effective From Date of a DIP ID

Validate DIP to Org Endpoint
When the webhook is registered the DIP initiates a TLS connection to validate the certificate on the endpoint so this will verify the outbound path.

Validate Endpoint to DIP
To validate the inbound path you can send a status message into the DIP with the following body to https://api.energydataintegrationplatform.co.uk/v1/statusMessage


```
{
   "transactionID": "T-999-123456abc-SUP-20260101-123456",
   "senderUniqueReference": "S-999-1234567abc-SUP-20260101-12345687A",
   "correlationID": null,
   "sentTimestamp": "2099-12-31T06:05:45+00:00",
   "senderID": "[YOUR DIP ID]",
   "recipientID": "0000000000",
   "DIPConnectionProviderID": null,
   "message": "RCP9999 - Smoke Test Status Message",
   "help": null,
   "serviceTicketURL": null
}
```


You should receive a HTTP 201 Created response if working.

DIP Certificates Overview

Certificates Overview and Use

There are two types of certificates available, TLS and Signing Certificates. A combined certificate is also possible to perform the functions of both types of certificate.

- TLS Certificate
  - Mutual TLS (mTLS) is a method for mutual authentication where both the client (Service User) and the DIP confirm they trust each other by verifying certificates sent as part of establishing the connection. mTLS will be used on both the ingress data API and egress webhook.
  - The TLS connection ensures all data is encrypted between the two points the TLS certificates are installed.
  - The TLS Certificate is typically installed on a PEP (Policy Enforcement Point) which could be a network firewall, this may also be handled by an endpoint management module in a cloud solution (Application Gateway in Azure).
- Signing Certificate
  - Authentication of individual messages which is achieved through the application of a digital signature. Applying a digital signature to a message also adds a layer of data integrity assurance.
  - Digital signatures are applied to hashes of JSON messages (sometimes called message digests) and are used to detect unauthorised modifications to data, as well as to authenticate the identity of the signatory. In addition, the recipient of signed data can use the digital signature as evidence in demonstrating to a third-party that the signature was, in fact, generated by the claimed signatory.
  - The signing certificate will be used to generate the message signature at the point of sending the message.

Certificates Rules

GlobalSign and DIP Certificates

Both of the Private Keys used for the GlobalSign API TLS connection and the DIP connection/signing must use the following parameters:

- Encryption: RSA
- Key Size: 4096

DIP Certificate

When defining your organisations "hostname" and "domain" for the DIP Certificate - there is a limit of **35 characters** to be used between those two fields. This is to keep the CN (Common Name) field within the X.509 certificate specification.

Note: the characters can be split between the two fields in any combination as long as neither are zero-length.

Webhook Registration

The following rules apply to the webhook registration:

- Each message channel will use a standard RESTful architecture for both the inbound Interface and the outgoing publication: a Send Message API (https://api.{environmment}.energydataintegrationplatform.co.uk/{version}/dipchannel/{IF-xxx}) for incoming messages and a Receive Messages webhook for outgoing messages. **NOTE: {environment} is blank for Production**
- Each message channel has both synchronous and asynchronous methods for reporting status/error messages back to the Sender.
- No custom ports can be used for the webhook – the DIP will always use the standard HTTPS port (**Port 443**).
- Parties should send **HTTP 201** response code back for successful message (more details on next slide) **NOTE: DIP will count HTTP 200 as delivery failure**

DIP Portal

- Webhooks can be registered for a DIP and IF through the DIP Portal.
- After entering the webhook URL, Max Message Quantity, Max Message Size and clicking “Confirm” – DIP will attempt to establish a TLS Connection to the endpoint and Fail if this connection cannot be established.

Webhook Registration API

- Swagger page on the webhook registration : Swagger Webhook Registration

HTTP 201 Response

As per End-to End Architecture Document - Section 4.6.6, HTTP 201 response should contain the following information (example response):

```
HTTP/1.1 201 Created
Content-Type: application/sendEvent.api+json
{ "dipchannel": { "version": "1.0" },
{
"messageArray": [
{
"transactionId": "T-IF-006-1234567890-SUP-20220401-1234CC0123456789",
"senderUniqueReference": "S-IF-005-0345890082-SUP-20222313-12345687A",
"correlationId": "CI-20220401-1234567890123abce123092",
"sentTimestamp": "2025-03-21T19:05:00+00:00",
"senderId": "10000000",
"recipientId": "1009012345",
"DIPConnectionProviderId": null,
"message": "RCP0000 Message OK",
"help": null,
"serviceTicketURL": null
}
```

Please review the document for all information and other HTTP response details.

Error Codes

This section will provide a reference to the error codes that may be received back from the DIP during testing to support the triage of any issues. This will cover:

- HTTP Response Codes – these are the synchronous response codes sent back to the sender when a message is sent into the DIP. Anything that is not a HTTP201 response indicates an issue.
- MSGxxxx Codes – Some of the HTTP Responses will have a MSGxxxx error code embedded into the response body data.

HTTP Response Codes – 2xx

DIP Egress; i.e. webhook ("Level 3" validation)						
Code	**Messages**	**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			

HTTP Response Codes - 4xx

DIP Egress; i.e. webhook ("Level 3" validation)						
Code	**Messages**	**Retry**	**Reason**	**Action**	**Retry Behaviour**	**Notify Sender via a status Message**
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		

HTTP Response Codes – 5xx

DIP Egress; i.e. webhook ("Level 3" validation)						
Code	**Messages**	**Retry**	**Reason**	**Action**	**Retry Behaviour**	**Notify Sender via a status Message**
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			

MSG Error Codes

Error Code	Generic Text	Description
Level 1 DIP 'Synchronous' response		
-	-	-
MSG0000	Success	Message is successful
MSG1001	Schema Failure	Message is malformed and failed to complete schema Validation. Review message content, format and structure. You can use the DIP API validation end-point to review failures
MSG1006	Sender Unique Reference Duplicated	Sender Unique Reference is not populated or has already been processed by the DIP for that Participant ID. Investigate why duplicated. Update message with a different Sender Unique Reference.
MSG1009	Sender DIP ID Invalid	Sender ID is Invalid or Sender is not approved to send the message type stated or sender is not responsible for the given DIP ID. Check the DIP ID is allowed to send these type of messages. Update message with a corrected Sender DIP ID - refer to ISD M16 for valid DIP IDs. Ensure egress and status URLs are set up for the interface id
MSG1010	Sender Role Invalid	Sender Role provided is invalid or Role does not apply for Sender ID. Check the role is relevant for the message being sent and is valid for that participant. Update message with a corrected Sender Role - refer to ISD M16 for valid DIP Roles
MSG1011	Connection Provider ID Invalid	Connection Provider ID is invalid or is not Authorised to issue transactions for the stated Sender ID-Role Combination. Check Connection Provider ID has been authorised and is valid - refer to Market Participant Organisation screens on the DIP portal for valid Connection Providers
MSG1017	Mtls Certificate doesn't match the Organisation	Check you are using the correct Mtls Certificate
MSG1018	Signing Certificate doesn't match the Organisation	Check you are using the correct Signing Certificate
MSG5001	Internal server error	Processing error in the DIP. Contact Elexon Service Desk.
MSG5002	No data contained in request body	Empty message received. Update with required content - refer to valid message format in DES138
MSG5003	Unable to determine correlationId requirement. Server configuration error or sender request error	Correlation ID has not been set correctly. Refer to DES138 routing tables for Correlation ID requirements
MSG5005	SDS~MDR Pairing not established/confirmed by SDS	Check SDS MDR Pairings have been established by the SDS in the Market Participant Organisation DIP portal screens
MSG5006	Role is not enabled for DIP Comms	Contact Elexon Service Desk

MSG Error Codes

Level -2 - DIP 'Asynchronous' Errors ~ Returned using the MsgStatus Transaction		
MSG2002	Missing Primary Routing Information	Check DES138 routing rules and add the missing Primary participant if required. If participant is not yet known, no further action required.
MSG2003	Secondary / Always Recipient Unknown or Unexpected	The DIP will add these participants where available. Ensure none of these participants are included in the original message - check DES138 routing rules and, if required, remove any participants that should be Secondary or Always routed. Contact Elexon Service Desk if Participant should be known, but have not been added by the DIP (This can be investigated in the DIP portal). Note if a Secondary participant is not yet known, no further action is required.
MSG1039	Invalid MPAN	The MPAN is not recognised in the DIP. Check the format is correct and whether the MPAN has migrated. Contact Elexon Service Desk if MPAN should be valid in the DIP.
MSG1040	Not currently appointed	Only the current Data Service can send an IF-015. Contact Elexon Service Desk if you have a confirmed appointment as the current Data Service
MSG1041	MPAN not known	The MPAN requested in the IF-015 is not recognised in the DIP. Check whether MPAN is migrated. Contact Elexon Service Desk if MPAN should be valid in the DIP.
MSG1042	{0} DIP Id not known in DIP	The DIP was unable to route the IF-040 Annual Consumption as the participant* DIP ID is not set up to receive IF-040's * - Data Service on receipt of IF-036 [DSAppActive]; or * - Supplier on receipt of IF-001
MSG1043	{0} Api Subscription ID incorrect	The DIP ID is not registered to the message sender. Check API key matches data in ISD M16 and #45 (ie DIP ID is the responsibility of the sending organisation)
MSG1044	No Data Available	No data is available in the DIP to share on the IF-016 for this MPAN.
MSG5004	Internal server error. Payload not processed	Level 2 processing error in the DIP. Contact Elexon Service Desk.

Schema Validation API

If you receive a HTTP 400:MSG1001 Schema validation error - the Validate Schema API can be used in Postman to check the message.

The address is (example in UIT):

https://api.uit.energydataintegrationplatform.co.uk/v1/validate/IF-034/MSAppSPResponse

This is an example for the IF-034 and MSAppSPResponse Validation – the IF and Event Code should be updated in the URL for the message being validated.

An example response showing a field in B070 has string rather than null:

{

"SchemaIssue": "Path:[0].payload.CustomBlock.B070.contractReferenceMeteringService Message: Invalid type. Expected Null but got String. Line: 33, Position: 58 SchemaId: #/components/schemas/NullString"

}