|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Reference** | **Category** | **Sub-Category** | **Title** | **Requirement Description** | **Applicable System or Service** | **Included in PIT** | **Included in QT?** | **Included in QAD?** |
| E2E0010 |  |  |  | **End-to-End Architecture Principles** |  |  |  |  |
| E2E0011 | Reliability | Recoverability | Data Loss | There shall be no data loss in the event of a single component failing | All Services | Yes | No | Yes |
| E2E0012 | Security | Accountability | Instance Separation | DIP Participants shall ensure measures are put in place to ensure separation of production and non-production environments | Market Participants | No | No | Yes |
| E2E0013 | Maintainability | Modifiability | Settlement Granularity | All newly developed components of services shall align to the current settlement period of 30 min. This may change in the future and therefore these components should be designed such that any change in this value can be accomodated without the need for fundamental system change, i.e. a reduction to 15 mins | All Services | Yes | No | No |
| E2E0014 | Compatibility | Interoperability | Messaging Interfaces | All services shall send and receive messages for all DIP interfaces and publications via the API defintions in the MHHS Swagger documentation (E2E003) | All Services | Yes | Yes | No |
|  |  |  |  | Message Orchestration |  |  |  |  |
| E2E0100 |  |  |  | **Outgoing Event/Message Handling** |  |  |  |  |
| E2E0101 | Performance Efficiency | Time behaviour | API Message Capacity | All services shall have the capability to control the number of messages that are sent within a single API call | All Services | Yes | No | No |
| E2E0102 | Security | Non-repudiation | Sender Unique Reference | All Services shall generate a Sender Unique Reference (SUR) for each message/event | All Services | Yes | Yes | No |
| E2E0103 | Security | Authenticity | Signing Messages | All Services shall digitially sign messages | All Services | Yes | Yes | No |
| E2E0104 | Security | Non-repudiation | Sender Unique Reference/ Transaction Id | All Services shall use DIP generated Transaction Ids returned in the response body of the API transction to map against messages for audit and tracking purposes | All Services | Yes | No | No |
| E2E0105 | Reliability | Availability | Participant Back Off & Retry | Each service after invoking a DIP API shall implement an exponential backoff and retry with jitter policy in the event of a comms failure with the DIP resulting from a http 429 response | All Services | Yes | No | No |
| E2E0106 | Reliability | Availability | Message/Event Buffering | In the event of a failure to communicate with the DIP, the Service shall be able to buffer messages for a period of at least 72 hours | All Services | Yes | No | No |
| E2E0107 | Security | Non-repudiation | Message Receipt | When sending messages all serivces shall use the http response of the API transaction to establish whether a message has been received by the DIP | All Services | Yes | Yes | No |
| E2E0108 | Compatibility | Interoperability | Message Validation (Level 1) | All services shall interpret the http response code to determine the outcome of DIP validation level 1 for each message sent referenced by Sender Unique Reference & Transaction Id | All Services | Yes | Yes | No |
| E2E0109 | Compatibility | Interoperability | Message Validation (Level 2) | All services shall connect to the Receive Status Messages webhook DIP to establish the outcome of level 2,3,4 validation with messages referenced by Transaction Id | All Services | Yes | Yes | No |
| E2E0200 |  |  |  | **Incoming Event/Message Handling** |  |  |  |  |
| E2E0201 | Compatibility | Interoperability | Schema validation | 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. | All Services | Yes | Yes | No |
| E2E0202 | Security | Authenticity | Signing Messages | All services shall check that messages are digitally signed with the correct certificate from the Sender of the message | All Services | Yes | No | No |
| E2E0203 | Usability | Operability | Error Reporting | When Level 3 validation fails, e.g. when payload contents cannot be reconciled (schema validation), a response with the correponding error code shall be reported back to the DIP via the http response in the webhook callback | All Services | Yes | No | No |
| E2E0204 | Reliability | Fault Tolerance | Participant Idempotency (SUR) | Participant systems shall check for duplicate messages with the same SUR under Level 3 or Level 4 validation | All Services | Yes | No | No |
| E2E0205 | Reliability | Fault Tolerance | Participant Idempotency (Transaction Id) | Participant systems shall check for duplicate messages with the same Transaction Id under Level 3 or Level 4 validation | All Services | Yes | No | No |
| E2E0206 | Reliability | Availability | Message/Event Receipt | In the event of a failure to communicate with the DIP Participant systems shall be able to buffer messages for a period of at least 72 hours | All Services | Yes | No | No |
| E2E0207 | Compatibility | Interoperability | Content Validation | Level 4 validation of the message content shall be established during processing by the Recipient and reported back to the Sender via the Send Status Messages API using the corresponding status code | All Services | Yes | Yes | No |
| E2E0208 | Performance\_Efficiency | Resource Utilisation | Participant Message/Event Consumption | DIP Participants shall be able to process messages at their own speed, independently to other consumers | All Services | Yes | No | No |
| E2E0209 | Security | Non-repudiation | Message/Event Replay Response | DIP Participants shall put in measures to differentiate the processing of replayed messages c.f. original messages | All Services | Yes | Yes | No |
| E2E0210 | Reliability | Fault Tolerance | Participant Idempotency | In terms of handling messages all participant systems shall be idempotent and have mechanism for handling duplicate messages | All Services | Yes | No | No |
| E2E0211 | Compatibility | Interoperability | Message Receipt | All messages recieved by DIP Participant systems shall be initially acknowledged as received in the http response of the API transaction | All Services | Yes | Yes | No |
| E2E0400 |  |  |  | **Participant Systems** |  |  |  |  |
| E2E0401 | Reliability | Maturity | Participant Software/Systems | Participants shall maintain all DIP facing systems so that all operating system, programming languages and their runtime libraries are at **minimum** supported versions from their respective vendors | All services | No | No | No |
| E2E0402 | Reliability | Availability | Participant Downtime | When participant systems/services are unavailable from both unplanned and planned outages the outage shall be communicated to the DIP via e-mail or via the DIP portal \*\*to be picked up later when DIP governance procedures are written \*\*\* | All Services | No | No | Yes |
| E2E0403 | Reliability | Recoverability | Participant Data Retention | Participant systems shall maintain an archive of all transactional data for 24 months | All services | No | No | Yes |
| E2E0404 | Reliability | Maturity | Participant Software/Systems | Participants shall maintain all DIP facing systems so that all operating system, programming languages and their runtime libraries are at **recommended** supported versions from their respective vendors | All services | No | No | ~~No~~ |
| E2E1000 |  |  |  | **Service Definition** |  |  |  |  |
| E2E1001 | Reliability | Availability | Service Availability | All services (those compnents that physically interface with the DIP, i.e. send and receive messages), unless explicitly defined, shall have an availaibility of 98% outside planned outage periods | All Services | No | No | Yes |
| E2E1002 | Reliability | Recoverability | Service Recovery | In the event of an unplanned outage, each service shall be able to resume operation within 1 hour. | All Services | Yes | No | Yes |
| E2E1003 | Performance\_Efficiency | Time behaviour | Level 3 Processing Times (synchronous) | 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 | All Services | Yes | No | No |
| E2E1004 | Performance\_Efficiency | Capacity | Message Throughput | All Services (see exceptions) shall have capacity to process the following volumes of messages: - average daily volume of 66,000 - peak daily volume of 300,000 - average hourly volume of 2,750 - peak hourly volume of 35,000 - annual volume of 24M | All Services | Yes | No | No |
| E2E1005 | Performance\_Efficiency | Capacity | Message Throughput (Secure Active) | All Services (unless explicitly referenced below) shall have capacity to process the following volumes of messages: - peak daily volume of 2,100,000 \* portfolio coefficient - peak hourly volume of 2,100,000 \* portfolio coefficient - annual volume of 110M \* portfolio coefficient | All Services | Yes | No | No |
| E2E1006 | Performance\_Efficiency | Capacity | Message Channel Scalability | All services shall be designed to cope with an increase in message volumes of 25% over 5 years | All Services | No | No | No |
| E2E1007 | Performance\_Efficiency | Capacity | Message Throughput (Transition) | During transition all meter points (ca. 31M) will be transition between the old and new services. Therefore assuming a linear migration over the year this would result in the load below, hence services shall be capable of processing the following volumes: - average daily volume of 680,000  - peak daily volume of 5.0M - annual volume of 500M | All Services | No | No | No |
| E2E1008 | Performance\_Efficiency | Resource Utilisation | Message Pattern B Payloads | Services sending messages via the 'Pattern B' model shall provide a publicly available (or using a Federated Identity Management (FIM) capability) URI location that other Services/ Market Participants can access and download content | All Services | No | No | No |
| E2E1009 | Performance\_Efficiency | Time behaviour | Level 4 Processing Times (Asynchronous) | 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 in accordance with the MHHSP\_OPC001\_Operational\_Choreography | All services with the exception of Helix (VAS,MDS,LSS,ISD) and LDSO Services | Yes | No | No |
| E2E1010 | Reliability | Availability | Unplanned Outages | All services (involved in BP affecting the Secured Active process), shall not plan outages within the Secured Active processing window | All Services | No | No | Yes |
| E2E1011 | Performance\_Efficiency | Capacity | Message Throughput (Migration) | During Migration:  DIP, ECS, EES, CSS, DSP, DTN need to accommodate the total daily messages set out in Section 9 of the Migration Threshold document. The message count that should be used is under the upper migration threshold (300,000 MPANs/day) Registration Services and LDSO's need to accommodate the total daily messages set out in Section 9 of the Migration Threshold document. | DIP, ECS, EES, CSS, DSP, DTN, Registration Services and LDSO's | Yes | No | No |