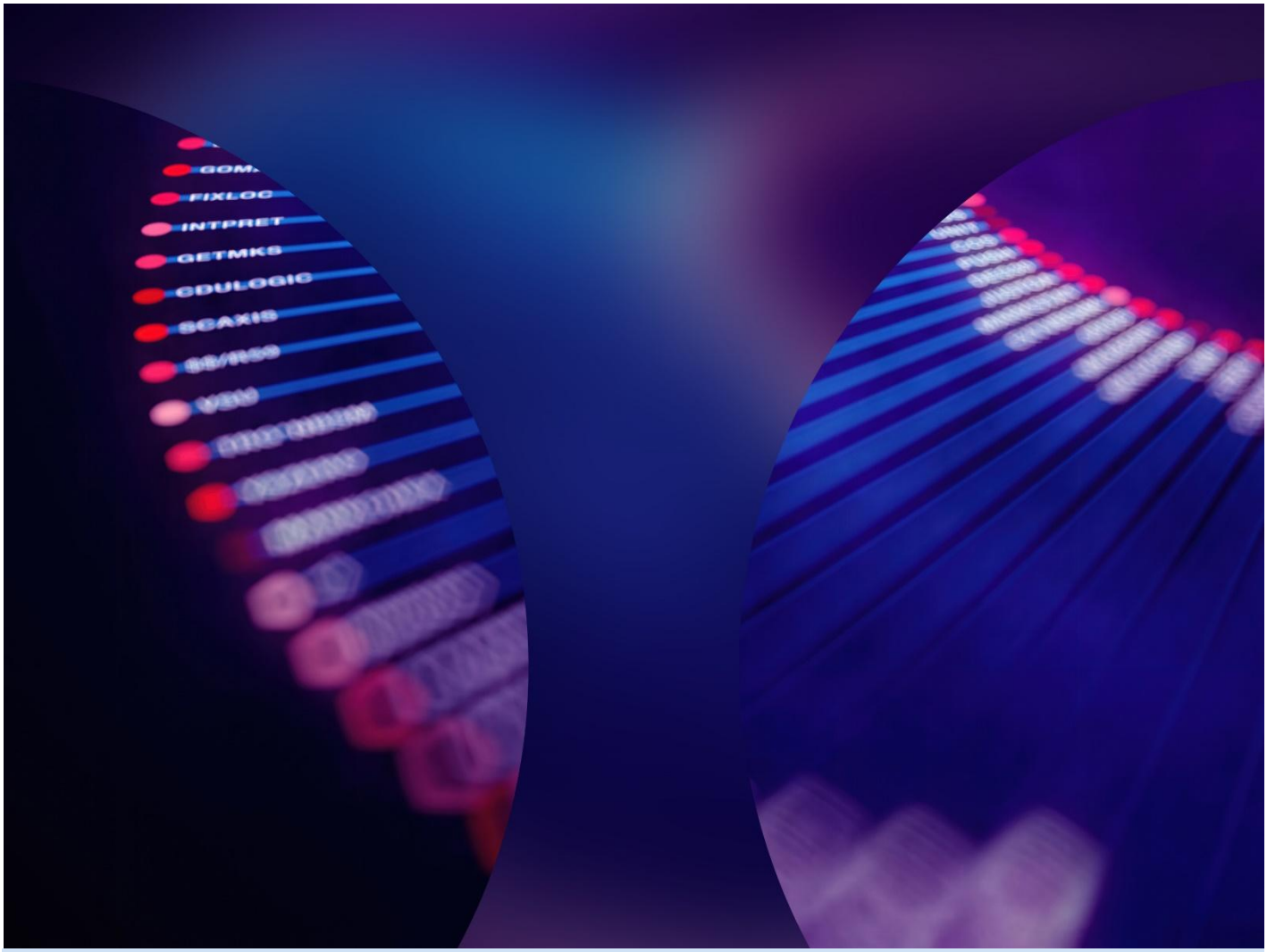
DIP Change Report June 2026

Public

Document owner	Document number	Date	Meeting
DIP Manager	**18/02**	9 June 2026	**DCAB18**



ELEXON | DIP

Summary

About this document

The DIP Change Report is a monthly summary of all active DIP Change Requests (CR), containing text updates on changes since the last report. This report covers updates from **5 May 2026** until **2 June 2026**.

Executive summary

The DIP CR summary table details the stage and progression routes of a DIP CR.

The DIP CR stages are:

- **Open**, which means the CR has been raised and is not considered new. The DIP Manager (and proposer if applicable) is continuing to progress the request.
- **New**, which means a CR raised between the DIP Change report covers.
- **Consultation,** which means a CR is being consulted on.
- **Workgroup,** which means a CR is being developed as part of a working group.
- **Decision,** which means the DIP CR will be or has been presented for decision.
- **Awaiting implementation**, which means a DIP CR is ready to be implemented, and the release it is a part of hasn't occurred yet.
- **Implemented**, which means the DIP CR was implemented.

To note, DIP CR can be in more than one stage.

Progression route is aligned with DSD004 – DIP Change and Document Management, 2.2 Process Overview.

DIP CR Summary table

CR	Stage	Progression	Explanation
DCR0005 'Extending SIT-A Testing Environment	Open, workgroup.	Further assessment, industry workgroup	The DIP Manager is seeking to engage the proposer to discuss next steps on how to progress this DIP CR.
DCR0006 'Management of Significant DIP incidents.'	Open, upcoming consultation	Further assessment post consultation	The DIP Manager has developed a new legal text, which is being reviewed.
DCR0009 'DIP Status Error Messages affecting Licensed Distribution System Operators'	Open	Raised	The DIP Manager has started to develop a solution for this DIP CR.
DCR0011 Change to DIP Portal controls to allow Lead Admin to manage organisation MFA reset	Open	Raised	The DIP Manager has added this CR to the system backlog and is seeking to develop this change for the DIP Manager's November release.
DCR0014 'Restrict DCP Access to MPIDs and Certificates from the Organisational Level to the DCP Level.'	Open,	Raised	A DIP user submitted CR 0014 to address the problem that Connection Providers can access MPIDs of organizations they do not manage. The DIP

			Manager has added this issue to the system backlog and plans to implement functionality to restrict Connection Providers' access by November 2026.
DCR0017 ‘Amendment of L4 Rejection Non Functional Timing Requirements and exemption.’	Open	Raised	The DIP Manager has discussed with the proposer the solution and is developing legal text.
DCR0018: ‘DIP Swagger alignment with Energy Market Data Specification (EMDS)	Open,	Raised, Initial Assessment	The DIP Manager has raised a DIP CR to note the changes made to DIP Swagger to align with EMDS
DIP CR 0019 ‘Defining the Sender Unique References (SUR) in the DIP Rules’	Open	Raised, Initial Assessment, Consultation	The consultation for this DIP CR is ending in early June. The DIP Manager will review responses.
DCR0020: ‘Decreasing the Retention Period for the DIP Archive’	Open	Raised, Initial Assessment, Consultation	The consultation for this DIP CR is ending in late May. The DIP Manager is reviewing responses
DCR0021: ‘Enabling early DIP On-Boarding for Applicants and Potential DIP Users’	Open	Raised, Initial Assessment, Consultation	The consultation for this DIP CR is ending in early June. The DIP Manager will review responses

Detailed DIP CR updates

DIP CR: 0005 'Extending SIT-A Testing Environment

- **Raised** on 8 August 2025.
- **Proposer**: E.ON.
- **Target Implementation**: To be determined post-workgroup.
- **Current status**: Further assessment, industry workgroup
- **DIP CR Tier**: One.

Topic	Explanation
Update	The DIP Manager is seeking to engage the proposer to discuss next steps for this DIP CR.
Next event/stage	Discussing with the proposers how to progess this CR in late June.
Issue	As part of the Market-wide Half-Hourly Settlement (MHHS), the MHHS Programme (MHHSP) has engaged market participants to ensure the functionality of the MHHS design. Participants must demonstrate the functional, non-functional, and migration-related characteristics of the MHHS Market Interfaces and Services. The MHHSP utilized Systems Integration Testing (SIT) to validate the end-to-end (E2E) MHHS Design. SIT A, used for testing since January 2025, is scheduled for decommissioning in October 2025. This poses a risk, as the lack of a testing environment could hinder the ability to address major incidents or changes, potentially jeopardizing the implementation of the MHHS design.
Current solution	The DIP Manager introduces its own testing environments to support DIP Users in testing changes to DIP functionality. Additionally, the DIP Manager should seek to develop testing requirements within the DIP Rules.
History	DCAB17 Rules Change Report

DIP CR: 0006 'Management of Significant DIP incidents.'

- Raised on **10 August 2026**.
- **Proposer**: DIP Manager.
- **Target Implementation**: 5 November 2026
- **Current status**: Further Assessment
- **DIP CR Tier**: One

Topic	Explanation
Update	The redrafted legal text is currently being reviewed internally. Once this exercise is complete, the DIP Manager will consult on the changes to the text.
Next event/stage	Consult on the changes made to the legal text.
Issue	The DIP is a middleware service supporting industry-wide real-time messaging between Market Participants, with its requirements defined in the DIP Rules, Supplement, and Subsidiary Documents (DSDs). However, there are currently no provisions within these rules outlining how major incidents impacting the DIP should be managed. As the Market-wide Half-Hourly Settlement Programme progresses to Milestone 8, where all participants will rely on the DIP, this gap introduces risks of poor coordination, delays in incident resolution, and increased operational inefficiencies. Consequently, DIP Users may face service access issues, reduced performance, and additional costs, while the DIP Manager is exposed to reputational risk if reliability standards defined in the DSDs are not met. This lack of defined major incident management processes represents a significant gap in the current DIP governance framework.
Current solution	The proposed outcome is to introduce a structured major incident management framework within the DIP Rules, enabling the DIP Manager to effectively coordinate responses. This would include clearly defined roles and responsibilities for the DIP Manager, DIP Users, and their contracted service providers during major incidents, alongside enforceable Service Level Agreements (SLAs). Additionally, a central record of agreed actions should be maintained to ensure transparency and accountability, and a formal incident review process should be established to assess root causes and determine whether enduring solutions are required to prevent recurrence.
History	DCAB17 Rules Change Report

DIP CR: 0009 ‘DIP Status Error Messages affecting Licensed Distribution System Operators’

- **Raised on:** 4 November 2025
- **Proposer**: National Grid Electricity Distribution.
- **Target Implementation**: November 2026
- **Current status**: Initial Assessment
- **DIP CR Tier**: 2

Topic	Explanation
Update	The DIP Manager has started to develop a solution for DCR009 and will publish its written assessment in the near future.
Next event/stage	Draft amendments to DSD002, Annex, 8.10
Issue	The DIP currently generates status error messages in scenarios where IF messages from MPRS are received before the corresponding IF-050 has created the MPAN (resulting in “Invalid MPAN” errors such as IF-043 or IF-009), and where no Supplier is available for routing (resulting in “no primary recipient” errors such as IF-003 and IF-020). In these cases, LDSOs receive error notifications that do not require any action but still require manual investigation, creating unnecessary operational overhead and cost. Additionally, these non-actionable errors introduce noise into monitoring systems, increasing the risk that genuine issues may be overlooked or delayed in being identified.
Current solution	The proposed change is to introduce distinct error codes within the DIP (or implement revised routing logic) to clearly identify these scenarios as non-actionable. This would reduce the volume of low-value or false error messages reaching LDSO helpdesks, eliminate the need for manual investigation of known non-actionable cases, and improve the visibility of genuine issues requiring attention. It would also ensure greater consistency between LDSO processes, DIP behaviour, and the intended market design.
History	DCAB17 Rules Change Report

DIP CR: 0011 Change to DIP Portal controls to allow Lead Admin to manage organisation MFA reset

- Raised on **1 December 2025**.
- **Proposer**: ESG Limited.
- **Target Implementation**: 5 November 2026
- **Current status**: Initial Assessment
- **DIP CR Tier**: Two

Topic	Explanation
Update	The DIP Manager has added the CR to the Forward Schedule of System Change for the current DIP Year.
Next event/stage	Draft Initial Assessment after June 2026.
Issue	This Change Request proposes enabling DIP Portal Lead Administrators to directly reset MFA for users, reducing reliance on the current ServiceNow-based process involving Elexon ServiceDesk and Avanade. At present, MFA issues—such as device loss, application failure, or authentication errors—result in user lockout and require multiple handoffs, causing delays, increased workload, and dependency on SLA response times. These challenges are compounded by the mandated use of Microsoft Authenticator, which lacks simple device migration and may require personal accounts or devices, creating usability, compliance, and cost concerns. Allowing Lead Admins to manage MFA resets via a UI enhancement would streamline resolution, minimise disruption, and improve operational efficiency, particularly as case volumes increase under MHHS.
Current solution	The proposed solution is to provide User Administrators within an organisation access to functionality in the DIP Portal that enables them to reset MFA for users belonging to their own organisation. It is recognised that organisations may have a mix of internal and external resources (e.g. DCP users) registered within the portal; therefore, appropriate controls are required. The functionality should validate that the email domain of the administrator matches that of the user before allowing an MFA reset, ensuring it is only applied to users within the same organisation. Additionally, this capability should be restricted exclusively to users with the User Admin role.
History	DCAB17 Rules Change Report

DIP CR: **0014 'Restrict DCP Access to MPIDs and Certificates from the Organisational Level to the DCP Level.'**

- Raised on **3 March 2026**.
- **Proposer**: **Good Energy**.
- **Target Implementation**: 5 November
- **Current status**: Raised
- **DIP CR Tier**: Two

Topic	Explanation
Update	New CR
Next event/stage	Initial Assessment
Issue	Currently, the DIP does not provide functionality to restrict a DIP Connection Provider (DCP) from accessing MPIDs within an organisation that they do not manage. Where multiple MPIDs exist under a single organisation, a DCP with the certificate admin role can view certificates associated with all MPIDs linked to that organisation. This lack of segregation means that DCPs can access certificate information for MPIDs outside of their operational responsibility. The issue is not specific to Good Energy and affects multiple suppliers who operate with more than one DCP.
Current solution	Introduce functionality within the DIP to allow MPID-level access controls for DCPs, ensuring that: · DCPs can only view, manage, and administer certificates for the MPIDs they are explicitly assigned to. · Certificate admin permissions can be scoped at the MPID level rather than applied at the organisational level. · Visibility and management of certificates for other MPIDs within the same organisation are explicitly restricted unless authorised.
History	DCAB17 Rules Change Report

DIP CR: **0015 'Introducing Level 3 and Level 4 response Codes into the DIP Rules**

- Raised on **17 March 2026**
- **Proposer**: DIP Manager.
- **Target Implementation**: 25 June 2026
- **Current status**: Industry Consultation
- **DIP CR Tier**: One

Topic	Explanation
Update	DCAB approved DCR0015 for implementation in November 2026
Next event/stage	The DIP Manager will implement this change in November 2026
Issue	The DIP Rules outline the obligations that DIP Users must fulfill, including the process for validating messages exchanged between each other. Message validations within a message channel are categorised into four levels, ranging from 1 to 4. Levels 1 and 2 involve synchronous and asynchronous validations performed by the DIP, while the DIP Users themselves handle Levels 3 and 4, also with both synchronous and asynchronous validations. However, the DIP Rules do not specify response codes for DIP Users to utilise at Levels 3 and 4. This lack of clarity is affecting how applicants, potential users, and existing DIP Users develop their systems to manage both synchronous and asynchronous validations.
Current solution	To address this issue, this DIP CR proposes introducing response codes into the DIP Rules by adding a new Annex to DSD0002 – DIP Connection and Operation requirements as part of the DIP Managers' June Release.
History	DCAB17 Rules Change Report

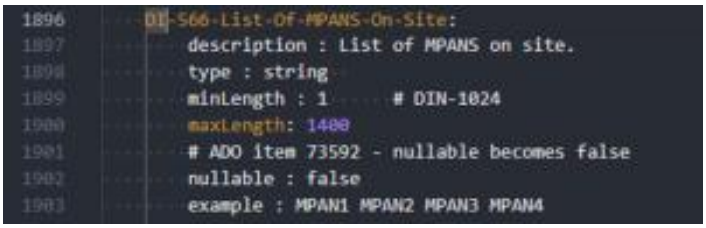
DIP CR: **0017 'Amendment of L4 Rejection Non Functional Timing Requirements and exemption.'**

- Raised on 24 March 2026.
- **Proposer**: OVO.
- **Target Implementation**: TBC
- **Current status**: Raised
- **DIP CR Tier**: One

Topic	Explanation
Update	The DIP Manager has started drafting the legal text and initial assessment.
Next event/stage	Publishing the initial Assessment.
Issue	Level 4 (L4) validations are essential to reject incorrectly sent flows based on participant and MPAN data. Current compliance rules require asynchronous rejections to be sent within 6 seconds, as per Non Functional Requirement (NFR) E2E1009. However, the current turnaround time does not reflect this validation need. These compliance rules apply to several PUB flows under MHHS and also affect REP flows, which require additional processing for validation. To establish realistic SLAs across DIP users, we propose adjusting NFRs so that 90% of messages are processed within 60 minutes, allowing for proper handling of rejections while maintaining operational flow. Furthermore, we argue that REP flows should be exempt from this validation as they lack MPAN data. This change is necessary for Suppliers and Data & Metering Services DIP roles.
Current solution	Relax the timing Non-Functional Requirements to allow an asynchronous response within 60 minutes for 90% of cases, instead of the current 6 seconds, which is unrealistic for MPAN-level validation. Exempt REP Flows from this NFR as they don't involve MPAN-level flows.
History	DCAB17 Rules Change Report

DIP CR: **DCR0018: 'DIP Swagger alignment with Energy Market Data Specification (EMDS)**

- Raised on 23 April 2026.
- **Proposer**: DIP Manager.
- **Target Implementation**: 13 August 2026
- **Current status**: Raised
- **DIP CR Tier**: One

Topic	Explanation
Update	The DIP Manager discussed this change with DCUSA. There were no concerns that this change impact their data items.
Next event/stage	Initial Assessment
Issue	Currently, there is a misalignment between EMDS and DIP Swagger concerning the list of Meter Point Administration Numbers (MPANs) on site in the REP900 file. This has created misalignment between EMDS and DIP Swagger.
Current solution	Amend the REP900 file to: • DI-566-List-Of-MPANS-On-Site – nullable becomes false 
History	DCAB17 Rules Change Report

```
1896        DI-566-List-Of-MPANS-On-Site:
1897            description : List of MPANS on site.
1898            type : string
1899            minLength : 1       # DIN-1024
1900            maxLength: 1400
1901            # ADO item 73592 - nullable becomes false
1902            nullable : false
1903            example : MPAN1 MPAN2 MPAN3 MPAN4
```

DIP CR: **DIP CR 0019 'Defining the Sender Unique References (SUR) in the DIP Rules**

- Raised on 4 May 2026.
- **Proposer**: DIP Manager.
- **Target Implementation**: 13 August 2026
- **Current status**: Initial Assessment
- **DIP CR Tier**: Two

Topic	Explanation
Update	Consultation ongoing.
Next event/stage	Initial Assessment, Consultation
Issue	When sending and receiving messages through the DIP, Users are required to use a 'Sender Unique Reference' (SUR) to identify the origin of the Message. This reference must consist solely of alphanumeric characters (such as A, B, C, 1, 2, 3). However, some users have been using non-alphanumeric characters (such as £, $, %, or -), which have caused validation issues and disrupted message flow among DIP users.
Current solution	To address this problem, it is proposed that the SUR requirements be defined in the DIP Rules (DSD002, Annex 2), mandating that only alphanumeric characters be used. This change aims to reduce the risk of validation failures. The implementation of DCR0019 is scheduled to occur as part of the DIP Manager monthly release in **August 2026**
History	DCAB17 Rules Change Report

DIP CR: **DCR0020: 'Decreasing the Retention Period for the DIP Archive'**

- Raised on 7 May 2026.
- **Proposer**: DIP Manager.
- **Target Implementation**: Post M15
- **Current status**: Initial Assessment
- **DIP CR Tier**: Two

Topic	Explanation
Update	New CR
Next event/stage	Initial Assessment, Consultation
Issue	The Data Integration Platform (DIP) currently provides message archiving, replay, and re-queue services to support users in scenarios such as data loss or system failure. Under existing DIP Rules, messages are retained for two years, and users must demonstrate equivalent data retention capability during onboarding. However, a recent cost assessment conducted by the DIP Manager with the DIP Service Provider, Avanade, has identified that data storage costs—particularly those associated with message indexing (blob index tags in Microsoft Azure)—are increasing significantly. As more participants qualify under Market-wide Half-Hourly Settlement (MHHS), these costs are expected to continue rising and will ultimately be borne by DIP Payees from July 2027.
Current solution	To ensure the DIP remains efficient and cost-effective, it is proposed to reduce the archive retention period from two years to 90 days. This change would materially reduce storage and indexing costs while maintaining sufficient capability to support core recovery functions such as message replay and re-queue.
History	New CR

DIP CR: **DCR0021: 'Enabling early DIP On-Boarding for Applicants and Potential DIP Users'**

- Raised on 14 May 2026.
- **Proposer**: DIP Manager.
- **Target Implementation**: 24 June 2026
- **Current status**: Initial Assessment
- **DIP CR Tier**: Two

Topic	Explanation
Update	New CR
Next event/stage	Initial Assessment, Consultation
Issue	The DIP Rules, outlined in the DIP Subsidiary Document (DSD) 002, titled "DIP Connection and Operation," specify the procedures that DIP Applicants and Users must follow when using the DIP. A key part of this process involves transitioning an Applicant or Potential User to the Production Environment, which occurs after they have qualified under an Industry Code or the MHHS Qualification. In the coming months, a large number of market participants will pursue the MHHS Qualification and subsequently seek to be on-boarded to the DIP. This situation poses a risk for the DIP Manager and could impact the service and support provided.
Current solution	To mitigate this risk, the DIP Change Request (CR) aims to empower the DIP Manager to onboard select market participants early. This proactive measure is intended to prevent any service or support disruptions that may arise from the increase in MHHS qualification volumes. The DIP Manager plans to implement this change as part of a non-standard release scheduled for **June**.
History	New CR