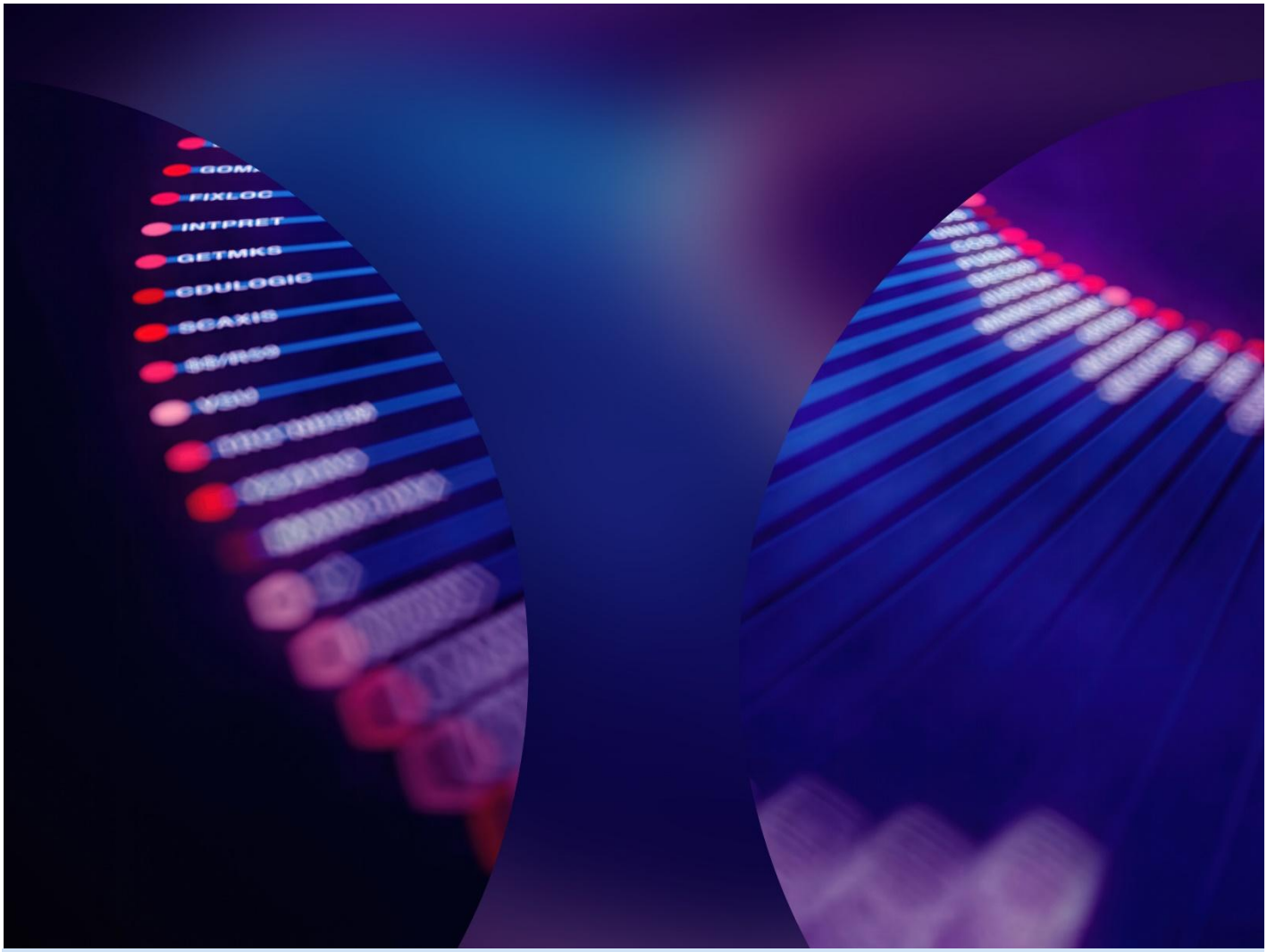
DIP Change Report April 2026

Public

Document owner	Document number	Date	Meeting
DIP Manager	**16/02**	14 April 2026	**DCAB016**



ELEXON

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 **3 March 2026** until **7 April 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 holding workgroups to support this CR. The most recent workgroup was held on 5 March 2026. The workgroup focused on the DIP Manager system release process, the forward schedule of system changes, and the testing environment used by the DIP Manager.
DCR0006 'Management of Significant DIP incidents.'	Open, upcoming consultation	Further assessment post consultation	The DIP Manager has been developing the legal text for this DIP CR to address the comments raised by consultation respondents. The DIP Manager is seeking to reconsult on this DIP CR later this month or early next month.
DCR0009 'DIP Status Error Messages affecting	Open	Raised	The DIP Manager is addressing introducing the response codes into the DIP

Licensed Distribution System Operators'			Rules before addressing how status error messages can be resolved
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.
DCR0012 'House Keeping Changes'	Open	Initial Assessment	The DIP Manager has drafted an Initial Assessment and is seeking to implement this change in the coming weeks.
DCR0014 'Restrict DCP Access to MPIDs and Certificates from the Organisational Level to the DCP Level.'	Open, new	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.
0015 'Introducing Level 3 and Level 4 response Codes into the DIP Rules	Open, new, consultation	Initial Assessment, Consultation	The DIP Manager is consulting on introducing Level 3 and Level 4 response codes into the DIP Rules
DCR0016 'Implementation of the data refresh message to ensure alignment of the MHHS design.'	New, Implemented	Implementation	The DIP Manager has drafted a Change Request with an initial and final assessment for the Balancing and Settlement Code Change Proposal 1607
DCR0017 'Amendment of L4 Rejection Non Functional Timing Requirements and exemption.'	New	Raised	A DIP User submitted CR 0017 to change the Level 4 validation timing requirements in the DIP Rules.

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 holding workgroups to support this CR. The most recent workgroup was held on 5 March 2026. The workgroup focused on the DIP Manager system release process, the forward schedule of system changes, and the testing environment used by the DIP Manager.
Next event/stage	The DIP Manager will hold a third working group before discussing with the proposer the next steps for this DIP CR.
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	See DCAB15 DIP 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 DIP Manager drafted amendments to the legal text. This is current under internal approval.
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	See DCAB15 DIP Change Report

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

- Raised on **DAY MONTH YEAR**.
- **Proposer**: ADD.
- **Target Implementation**:
- **Current status**:
- **DIP CR Tier**:

Topic	Explanation
Update	The DIP Manager will develop this change once DCR0015 has been implemented (if agreed to by DCAB).
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	See DCAB15 DIP 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	See DCAB15 DIP Change Report

DIP CR: **0012 'House Keeping Changes'**

- Raised on **3 March 2026**.
- **Proposer**: DIP Manager.
- **Target Implementation**: 12 May 2026
- **Current status**: Initial Assessment
- **DIP CR Tier**: Housekeeping

Topic	Explanation
Update	Initial Assessment
Next event/stage	Initial Assessment
Issue	The DIP Rules, which include the DIP Supplement and DIP Subsidiary Documents (DSDs), are amended from time to time by a BSC modification or a DIP Change Request (DCR). When either a modification or DCR is approved, the DIP Rules text can change. Any changes to the text in the DIP Rules must reflect what has been approved by the Authority, for BSC Modifications, or the DIP Change and Advisory (DCAB), for DCRs.
Current solution	Reformat the DIP Rules to ensure they are consistent with documents that have been approved by the Authority.
History	See DCAB15 DIP 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	New CR

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	New CR
Next event/stage	Consultation
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	New CR

DIP CR: **0016 'Implementation of the data refresh message to ensure alignment of the MHHS design.'**

- Raised on 23 March 2026.
- **Proposer**: DIP Manager.
- **Target Implementation**: 23 March 2026.
- **Current status**: Implemented
- **DIP CR Tier**: DIP Message Defintion Change

Topic	Explanation
Update	New CR
Next event/stage	Implemented
Issue	There is no established mechanism for realigning data among services like the Supplier Registration Service (SMRS), Data Integration Platform (DIP), Energy Enquiry Service (EES), and Market-wide Data Service (MDS) during major incidents that affect data quality. This absence poses a risk since the information is crucial for determining Meter Point Administration Number (MPAN) ownership and Consumption Component Class (CCC), both of which are essential for settlement accuracy. Additionally, EES serves as a reference for market participants, and a significant data misalignment could disrupt core industry processes.
Current solution	Implement a new DIP message - IF-0XX 'Data Refresh' (message number to be allocated later upon approval). This will be generated by the SMRS as needed and sent to the DIP, EES, or MDS for data resetting or realignment. The message can be exchanged via the DIP or through secured JSON files in password-protected ZIPs. It can be sent to one or all parties, depending on the incident, with exchange mechanisms and processing times agreed bilaterally between the SMRS and recipients. The refresh message aims for bulk data correction after significant incidents, while individual MPAN discrepancies will still be handled case-by-case using existing MHHS Design guidance. Suppliers, Data Services, and Metering Services will access refreshed data from EES using existing functionality.
History	New CR

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	New CR
Next event/stage	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	New CR

DIP Change Request timeline

RED = Solution Development

ORANGE = Service Provider Dependencies

YELLOW = DIP Manager Dependencies

GREEN = Decision Stage

	April	May	June	July	August	September	October	November
DCR005	Workgroup							
DCR006	Internal Approval of redrafted Legal text	Consultation		Review responses			Draft Final Assessment	Present to DCAB for Decision
DCR009	Draft Legal text		Consultation	Review responses			Draft Final Assessment	Decision & Implementation
DCR0011	System development							Decision & Implementation
DCR0012	Draft Final Assessment, decision, and implementation							
DCR0014	System development							Decision & Implementation
DCR0015	Consultation	Draft Final Assessment & DCAB Decision	Implementation					
DCR0016	Implemented							
DCR0017	Determine next steps							