

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.



DP291 'DNO Alerts to Suppliers'

Modification Report

Version 0.1

13 May 2025



About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1.	Summary	3
2.	Issue	3
3.	Assessment of the proposal	5
	Appendix 1: Progression timetable	7
	Appendix 2: Glossary	7

Contact

If you have any questions on this modification, please contact:

Georgiana Severin

020 7770 6921

Georgiana.Severin@gemserv.com

1. Summary

This proposal has been raised by Alison Godden from E.ON Next. This proposal is co-sponsored by Julie Brown from British Gas.

Suppliers have obligations under the Standard Licensing Conditions (SLC), Utilities Act 2000 and Retail Energy Code (REC) to proactively identify and investigate potential meter tampering/Energy theft on consumers' premises. This is done by building modelling mechanisms with Data currently available to Suppliers, including Consumption Patterns and Meter Readings. While Suppliers will endeavour to utilise the most appropriate Data to ensure the modelling mechanism is as robust as possible, the Proposer has identified the need for further Events and Alerts that could make the mechanism even more accurate.

This issue can lead to non-compliance with Supplier obligations and comes at a high cost to industry (estimated between £830 – £1.388bn per year in 2023¹). There are also impacts on consumers, as meter tampering/Energy theft can lead to injuries or damages to consumers' premises.

The Potential Solution for the modification is for specific Events and Alerts that are currently only available to Distribution Network Operators (DNOs) to be made available to Suppliers. These Events and Alerts would allow Suppliers to overlay these Events and Alerts to the Data already used to create more robust modelling mechanisms to determine whether a Smart Metering System (SMS) has been tampered with.

2. Issue

What are the current arrangements?

What is the current method for Suppliers to identify meter tampering/Energy theft?

Suppliers will utilise modelling mechanisms with Data available to them pertaining to SMS in their portfolios. The Data used to create these modelling mechanisms includes Consumption Data/Patterns, Meter Readings as well as two Events/Alerts: AD1 'Power Outage Event' and 81C0 Supply Disconnect Failure (Valve or Load Switch).

Using these modelling mechanisms, the Supplier's Revenue Protection team will look to investigate potential meter tampering/Energy theft.

What are the obligations for Suppliers to detect and prevent Energy theft/meter tampering?

Suppliers have obligations to detect and prevent Energy theft/tampering, which are stipulated in the following:

- Electricity SLC 12.1 to detect & prevent theft or abstraction of electricity or interference with metering equipment.
- REC Schedule 7 Energy Theft Reduction to achieve Theft Detection Incentive Scheme targets.

¹ [New report estimates energy theft costs consumers up to £1.4bn yearly - Retail Energy Code Company](#)

- REC Annex A: Theft Charter to investigate the theft of energy legally actively.

Suppliers should also monitor Anomalous Alerts and Events and take reasonable action to resolve these in line with Smart Energy Code (SEC) Sections G3.15-G3.16:

G3.15 Each Supplier Party shall take reasonable steps to ensure that its User Systems are capable of detecting Anomalous Events, in particular by reference to the:

(a) sending or receipt (as the case may be) of Service Requests, Pre-Commands, Signed Pre-Commands, Service Responses and Alerts;

(b) audit logs of each Device for which it is the Responsible Supplier; and

(c) error messages generated by each Device for which it is the Responsible Supplier.

G3.16 Each Supplier Party shall:

(a) take reasonable steps to ensure that its User Systems detect all Anomalous Events; and

(b) ensure that, on the detection by its User Systems of any Anomalous Event, it takes all of the steps required by its User Information Security Management System.

What is the issue?

Data available to Suppliers via Smart Metering Technical Specifications (SMETS)1 SMS before Enrolment and Adoption (E&A) included two additional Alerts – 8F35 ‘Supply Outage Restored’ and 8F36 ‘Supply Outage Restored - Outage >= 3 minutes’. However, the introduction of SMETS2 SMS, SEC Schedule 8 ‘Great British Companion Specifications’ (GBCS) and subsequent Data Communications Company (DCC) User Roles led to Suppliers no longer having visibility of these Alerts and Events.

This is creating difficulty for Suppliers to create robust and near-failproof modelling mechanisms that would determine whether an SMS has been tampered with or if Energy theft activity has taken place.

What is the impact this is having?

The robustness of the modelling mechanisms to determine whether an SMS has been tampered with is directly impacted by the Data available to Suppliers when building these mechanisms. Without these robust modelling mechanisms, there is a risk that Suppliers may not be able to ascertain beyond reasonable doubt that the SMS has been tampered with or establish a clear case for Energy theft.

This has a negative impact on the industry, costing between £830m to £1.388bn annually across Great Britain. Additionally, it can be a contributing factor to non-compliance against Utilities Act 2000 Sections 11.4A and 15.3C regarding health and safety duties covering Supplier employees and customers (consumers). It also contributes to non-compliance to the Electricity SLC 12.1, REC non-compliance with Schedule 7 ‘Energy Theft Reduction to achieve Theft Detection Incentive Scheme targets’ and non-compliance to REC Annex A ‘Theft Charter’ to investigate the theft of Energy actively.

Lastly, an Ofgem open letter to all Suppliers due to ‘poor’ performance² and REC scrutiny due to non-compliance to Theft Charter creates risks of penalties to Suppliers.

² [Open letter on supplier energy theft obligations](#)

Impact on consumers

Without a solution in place, meter tampering can have a detrimental impact on consumers. Stolen energy may be billed in proven cases of theft, which may create debt and affordability vulnerabilities to customers. Theft or tampering may indicate other consumer vulnerabilities, such as third-party stealing or tampering. Meter tampering can also be a potential risk to injury or to life, as well as damages to consumer premises.

In 2023, it was estimated that Energy theft/meter tampering cost consumers and Suppliers between £830m to £1.388bn per year across Great Britain. This means that Energy theft/meter tampering costs consumers between £28 – £48 annually³ on domestic consumers' bills across Great Britain.

3. Assessment of the proposal

Areas for assessment

Alerts and Events for the potential solution

The Proposer and the co-sponsor would like the Proposed Solution to make two Alerts and Events that are visible to Distribution Network Operators (DNOs) also available to Suppliers. These two Alerts are: 8F35 'Supply Outage Restored' and 8F36 'Supply Outage Restored - Outage >= 3 minutes'.

During the April 2025 Issues Group, this potential solution was presented to attendees. A member of the Issues Group questioned whether any consideration had been given to extending the Alert list to cover three-phase Electricity Smart Metering Equipment (ESME). The co-sponsor agreed this should be looked into as part of solution development. Following the Issues Group meeting, the Proposer and co-sponsor agreed that three-phase ESME Alerts should be included in the scope of the potential solution - 0x8F3B 'Supply Outage Restored on Phase 3 Restored' and 0x8F3C 'Supply Outage Restored on Phase 3 Restored - Outage >= 3 minutes'.

Increased traffic as part of the potential solution

During the Issues Group, the Data Communications Company (DCC) raised questions regarding the potential for increased traffic as part of the solution, recommending this be included in the solution development for the modification to ascertain whether it would increase traffic and likely by how much.

GBCS impact of the potential solution

A final point raised during the Issues group discussion related to the impact of the Potential Solution on GBCS. The Issues Group highlighted that GBCS related solutions take a significant amount of time to be implemented. Given that the potential solution would look to add Suppliers as recipients of a number of Events and Alerts, the Issues Group questioned the method by which this would be achieved. If the Proposer would simply require the Data Service Provider (DSP) to duplicate the Data and send to the Supplier, this would likely be more time effective. Following the Working Group, the Proposer has expressed a wish for the solution to be implemented without avoidable delays. Their

³ [Open letter on supplier energy theft obligations](#)

view is for the Potential Solution to be delivered as close to real time as possible and be able to cope with the request volume.

Benefits of implementing the potential solution

Outside of Suppliers' strengthened ability to identify and proactively manage Energy theft/meter tampering, the potential solution is likely to have further benefits, namely:

- **Increased safety for consumers.** Tampering with meters and cutting into wires or pipes to interfere with Energy supplies can cause fires, gas leaks and electrocutions. If Suppliers can proactively identify these, there is an implied understanding that the number of accidents will be lowered.
- **Reduced Energy theft.** Between 2017 and 2021, there was an almost 400% increase in reported incidents of Energy theft. With more robust means of identifying theft, it may lead to reduction in cases, as proactive action will deter repeat offenders.
- **Reduced costs for consumers.** Energy theft currently costs consumers between £29 - £48 annually. Identifying and resolving cases of meter tampering will lead to lowering annual costs for consumers.

These benefits will be investigated during the refinement process. Any benefits not yet identified will also be added to the modification as it progresses.

Sub-Committee input

The Smart Energy Code Administrator and Secretariat (SECAS) will engage with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC), the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA), the Privacy Sub-Committee (PSC), the Smart Metering Device Assurance Sub-Committee (SMDASC) and the Testing Advisory Group (TAG) to confirm what input is required from these forums. SECAS believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	Input on operational impact of the potential solution.
PSC	No input required
SMDASC	No input required
SMKI PMA	No input required
SSC	No input required
TABASC	Input on the technical architecture of the potential solution.
TAG	No input required.

Appendix 1: Progression timetable

Timetable	
Event/Action	Date
Draft Proposal raised	13 May 2025
Presented to CSC for initial comment	20 May 2025
CSC converts to Modification proposal	20 May 2025
Request for Information	21 May 2025 – 20 June 2025

Italics denote planned events that could be subject to change

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	Full term
CSC	Change Sub-Committee
DCC	Data Communications Company
DNO	Distribution Network Operator
DSP	Data Service Provider
E&A	Enrolment and Adoption
ESME	Electricity Smart Metering Equipment
GBCS	Great British Companion Specifications
OPSG	Operations Group
PSC	Privacy Sub-Committee
REC	Retail Energy Code
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SLC	Standard Licensing Conditions
SMETS	Smart Metering Equipment Technical Specifications
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SMDASC	Smart Metering Device Assurance Sub-Committee
SMS	Smart Metering System
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group