SEC
Smart Energy Code

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.

MP265

‘Implementing ADT changes in response to a Security Incident’

Modification Report

Version 0.5

3 December 2024

Corporate member of Plain English Campaign
Committed to clearer communication
592

Gemserv

About this document

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

Contents

This document also has three annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the SEC required to deliver the Proposed Solution.
- **Annex C** contains the full DCC Preliminary Assessment response.

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 Gordon Hextall on behalf of the Security Sub-Committee (SSC).

The Data Communications Company (DCC) System is utilised by multiple Service Providers and Service Users, all with different activities. It is the DCC's responsibility to ensure adequate measures are in place to ensure security threats are mitigated.

The SSC considered several scenarios that could have an impact on the Supply of energy to consumers as part of a Major Security Incident exercise to test the ability to respond to a Compromise.

In recovering from a Compromise where Service Requests (SR) have been temporarily suspended, DCC Users would need to amend the User-set Anomaly Detection Thresholds (ADT) to allow increased volumes of SRs to be processed without being quarantined. Where urgent action is required to support recovery and / or multiple DCC Users are involved, the ability to centrally amend User-set ADTs in exceptional circumstances would help to expedite the recovery for DCC Users and minimise any impact for consumers.

The Proposed Solution would be to allow the DCC – in exceptional circumstances, and only with SSC approval – to amend the User-set ADTs for a finite amount of time to facilitate a rapid recovery from a Compromise.

2. Issue

What are the current arrangements?

DCC Security

The DCC has a responsibility under Smart Energy Code (SEC) Section H10 'Business Continuity' to protect the DCC System in the event of compromise to ensure business continuity. This section of the SEC allows the DCC to act by temporarily suspending Service Users in certain circumstances. This suspension can be done in whole or in part and it would cushion or avoid the potential impact of Compromise to the DCC System.

What are Anomaly Detection Thresholds?

Service Users currently provide the DCC with their own ADT files, and these should provide a granular level of control over the volume of SRs that a DCC User may be sending to the DCC.

ADTs will detail the SR forecast and expected pattern of demand for each SR. Service Users will liaise with the DCC when setting their forecast and pattern of demand, and this would normally align with DCC's own thresholds. This is in line with SEC Appendix AA 'Threshold Anomaly Detection Procedures'.

The SSC has an obligation to provide support to the DCC and its DCC Users *'in relation to the causes of security incidents and the management of vulnerabilities on their Systems'* as currently defined in SEC Section G7 'Security Sub-Committee'.

What is the issue?

The SSC has a responsibility under SEC Section G7.19 (b) (i) to conduct risk assessments "*at least once each year in order to identify any new or changed security risks to the End-to-End Smart Metering System.".* As part of this responsibility, the SSC carries out annual security incident exercises to review and assess the risks arising from a Compromise of the End-to-End Smart Metering System and to ensure the ability to respond to and recover from such a Compromise.

There is currently no capability to centrally amend the Service User ADT in the event of recovery from a system Compromise, which could limit the readiness to quickly recover from such an Incident.

The SSC noted that an improvement to the current User-set ADT arrangements could be made whereby the DCC could be directed by the SSC, with appropriate governance, to amend, in exceptional circumstances, the ADT levels of DCC Users. The exceptional circumstances would be where recovery requires a larger number of SRs to be processed than the ADT settings allow. The ADT settings therefore need to be temporarily amended to avoid SRs being quarantined to facilitate a recovery from a Compromise. This would be broadly consistent with existing SEC obligations on the SSC, DCC and DCC Users:

SEC Section G7.21 (b) requires that "*The Security Sub-Committee shall:*

(b) monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the DCC;"

SEC Section G6.10 (b) requires the DCC and DCC Users to have regard to SSC opinion:

"G6.10 The DCC and each User shall, in relation to each Anomaly Detection Threshold that it sets:
(a) keep the Anomaly Detection Threshold under review, having regard to the need to ensure that it continues to function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System and/or User Systems (as the case may be);
(b) for this purpose have regard to any opinion provided to it by the Security Sub- Committee from time to time as to the appropriate level of the Anomaly Detection Threshold;"

SEC Section G6.7 provides for the SSC to advise the DCC on DCC-set ADTs global ADTs:

"G6.7 Where the DCC sets any Anomaly Detection Threshold in accordance with Section G6.6, it shall:
(a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems; and
(b) before doing so consult, and take into account the opinion of, the Security Sub- Committee as to the appropriate level of the Anomaly Detection Threshold."

What is the impact this is having?

In the event that a Party is Compromised, and the Smart Metering Service is put at risk, the DCC may wish to take action to protect Services to other Users and may suspend a Service User.

Noting the allowance of SEC Section H10, there is currently no SEC compliant method by which DCC may override a DCC User provided ADT in efforts to recover Services after a Compromise.

Impact on consumers

The impact on consumers relates to mitigating against a risk of loss of key smart metering services as a result of an attack.

3. Solution

Proposed Solution

The Proposed Solution would look to allow the DCC to amend the User-set ADTs as part of the recovery process from a Compromise. The SSC would meet as the Smart Metering Incident Response Team (SMIRT) and determine the best approach to recovering after a Compromise, including temporary amendments to User-set ADTs.

Amendments to User-set ADTs would be made by the DCC for a period determined by the SSC to allow quarantined messages to pass through the DCC System to aid in the recovery process. Following resolution of the Compromise, the DCC would revert the User-set ADTs back to the original values, removing the need for DCC Users to re-submit Comma Separated Values (CSV) files.

Affected Users would be notified as part of the recovery process.

The Business Requirements to deliver the Proposed Solution can be found in Annex A.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
✓	Electricity Network Operators	✓	Gas Network Operators
✓	Other SEC Parties	✓	DCC

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
	Device Manufacturers		Flexibility Providers
✓	DCC Other Users		MAPs/ MAMs

All DCC Users will be impacted, however this would be seen as a positive impact – the Proposed Solution would help deliver quicker recovery after a Compromise and minimise the disruption to DCC User activity.

The DCC would be impacted as it would be required to amend User-set ADTs in cases where the SSC deems it necessary to mitigate recovery after a Compromise.

DCC Systems

DCC System changes

The DCC Service Desk and Service Management team will have to update existing, and potentially create new, processes to handle directions from the SSC to change the existing ADT-related processes and handle requests.

The full impacts on DCC Systems and DCC's proposed testing approach can be found in the DCC Preliminary Assessment response in Annex C.

DCC System traffic

This modification will not impact System traffic.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section G 'Security'

The changes to the SEC required to deliver the proposed solution can be found in Annex B.

Devices

This modification will not impact Devices.

Consumers

This modification will not impact Consumers. However, Consumers may be impacted if recovery after a Compromise is not carried out swiftly as it may lead to temporary loss of smart metering functionality.

Other industry Codes

This modification will not impact other industry Codes.

Greenhouse gas emissions

This modification will not impact greenhouse gas emissions.

5. Costs

DCC costs

The estimated DCC implementation costs to implement this modification is between £200,000 – £300,000. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design, Build and Pre-Integration Testing (PIT)	£200,000 - £300,000
Systems Integration Testing (SIT)	TBC
User Integration Testing (UIT)	TBC
Implement to Live	TBC
Application Support	TBC

More information can be found in the DCC Preliminary Assessment response in Annex C.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day of effort, amounting to approximately £600. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

Any SEC Party costs associated with this modification will be determined during the Refinement Consultation.

6. Assessment of the proposal

Areas for assessment

Amending User-set ADTs in Major Security Incidents

As part of the next steps of this Modification, the governance arrangements that will apply to the SSC decision-making will be clarified. This will include, but is not limited to, clarification of the quorum for decision-making and examples of the exceptional circumstances where User-set ADTs could need to be amended when the SSC meets as the SMIRT.

How will the ADTs be returned to their previous levels once a security incident is over?

Change Sub-Committee (CSC) members noted concerns around the reversal process following a Compromise. They wondered whether DCC Users would be required to provide new ADTs or whether the DCC would automatically revert to the original values before the Compromise occurred.

ADTs will be reverted to the original values following recovery from the incident, without the need for DCC Users to provide new CSV files.

How will affected DCC Users be notified?

As part of the security incident management exercise, DCC Users should be notified of any Compromise. However, whether this communication comes from the DCC, or the SSC would depend on the nature of the security incident and how many DCC Users are affected.

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 SSC, the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) and 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	None
SMKI PMA	None
SSC	Input on business requirements and solution development
TABASC	Input on business requirements and solution development
TAG	None

Observations on the issue

Views of the Change Sub-Committee

CSC members suggested that part of the solution should include communicating with DCC Users to improve the understanding of ADTs. While DCC Users may be setting reasonable ADT levels, it would be useful to be made aware when changes are needed.

CSC members queried whether part of the next steps would be taking the modification to be reviewed by TABASC, which may be needed if the developed solution requires a system change. SECAS noted that TABASC would be interested if the process involved system changes.

Solution development

Views of the Working Group

A member of the Working Group questioned how the process would work if the amendment of ADTs would only come under authorisation of the SSC. It was explained that once a Compromise happens,

the SSC and the DCC meet as part of the SMIRT and at that point they would decide next steps, including SSCs recommendation for ADTs to be temporarily amended.

Another member of the Working Group questioned what would happen once the ADTs have been reverted to their original numbers as presumably it would cause backlog of SRs. ADTs are set both Northbound and Southbound and setting these to zero for a period of time and reverting back may cause issues. The DCC confirmed that the aim for the DCC to amend these ADTs in recovering from a Compromise and only revert back to the original ADT levels once quarantined messages and alert backlogs have cleared. The DCC highlighted it would be a judgement call depending on the scale of the issue.

Another member of the Working Group questioned whether during the recovery period, the DCC would look at a backup processes, such as emails notifying the Service User that ADT limits had been exceeded. It was confirmed this would be the aim.

7. Case for change

Business case

The aim of the modification is to provide a solution that would reduce the time taken to amend User-set ADTs in circumstances where there has been a Compromise. The reduction in time to amend User-set ADTs would be beneficial in the recovery from a Compromise as it would allow the DCC to process large amounts of quarantined SRs and minimise disruption.

Views against the General SEC Objectives

Proposer's views

The Proposer believes the modification would better facilitate SEC Objective (f)[1], as it would add another option to utilise in the event of a Compromise which would aid in providing a swift resolution.

Industry views

Industry views will be collated during the Refinement Consultation.

Views against the consumer areas

Improved safety and reliability

The modification will have a positive impact on this consumer area. Amending ADTs in exceptional circumstances will help reduce the recovery time and therefore improve reliability.

Lower bills than would otherwise be the case

This modification will have a neutral impact on this area.

[1] ensure the protection of Data and the security of Data and Systems in the operation of this Code

Reduced environmental damage

This modification will have a neutral impact on this area.

Improved quality of service

This modification will have a neutral impact on this area.

Benefits for society as a whole

This modification will have a neutral impact on this area.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	13 Feb 2024
Presented to CSC for initial comment	20 Feb 2024
Modification discussed with Proposer	Feb-Mar 2024
Business Requirements discussed with DCC and the Proposer	Mar – Aug 2024
CSC converts Draft Proposal to Modification Proposal	17 Sep 2024
Modification discussed with Working Group	2 Oct 2024
DCC Preliminary Assessment Requested	9 Oct 2024
DCC Preliminary Assessment Received	28 Nov 2024
Modification discussed with SSC	*11 Dec 2024*
Modification discussed with Working Group	*15 Jan 2025*
Refinement Consultation	*22 Jan – 12 Feb 2025*
Modification discussed with Working Group	*5 Mar 2025*
Impact Assessment costs approved by Change Board	*26 Mar 2025*
Impact Assessment Requested	*27 Mar 2025*
Impact Assessment Received	*23 May 2025*
Modification Report approved by CSC	*24 Jun 2025*
Modification Report Consultation	*25 Jun – 16 Jul 2025*
Change Board Vote	*27 Aug 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**
ADT	Anomaly Detection Threshold
CSC	Change Sub-Committee
CSV	Comma Separated Values
DCC	Data Communications Company
OPSG	Operations Group
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMIRT	Smart Metering Incident Response Team
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SR	Service Request
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group