

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.



# DP319

## ‘SRV 11.3 – Activate Firmware Request Firmware Hash Validation’

### Modification Report

Version 0.1

31 March 2026



## About this document

---

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

## Contents

---

|    |                                         |                                     |
|----|-----------------------------------------|-------------------------------------|
| 1. | Summary .....                           | 3                                   |
| 2. | Issue .....                             | 3                                   |
| 3. | Solution .....                          | 5                                   |
| 4. | Impacts .....                           | 5                                   |
| 5. | Costs .....                             | 7                                   |
| 6. | Implementation approach .....           | <b>Error! Bookmark not defined.</b> |
| 7. | Assessment of the proposal .....        | 7                                   |
| 8. | Case for change .....                   | 8                                   |
|    | Appendix 1: Progression timetable ..... | 10                                  |
|    | Appendix 2: Glossary .....              | 10                                  |
|    | Appendix 3: Prioritisation Matrix ..... | 11                                  |

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

## Contact

---

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

**Georgiana Severin**

020 7770 6921

Georgiana.Severin@talan.com

## 1. Summary

---

This proposal has been raised by Taj Nezami from the Data Communications Company (DCC).

It must be noted that for all Critical Service Requests, the User will first request transformation of the Critical Service Request (“Transform” Command Variant 4) into a SEC Schedule 8 ‘Great Britain Companion Specifications (GBCS)’ Format, and the resulting Pre-Command shall then be returned to the User for correlation and Digital Signing.

The Signed Pre-Command shall then be sent by the User (“Send” Command Variant 5) to the DCC, who shall add any requisite MAC to the signed GBCS Payload extracted from the body of the Signed Pre-Command and send the resultant Command to the relevant Device.

It should also be noted that all Service Requests and Signed Pre-Commands are constructed in XML format, including Header, Body, and Signature elements, in accordance with the DUIS XML Schema.

Service Request Variant (SRV) 11.3 ‘*Activate Firmware*’ (“Transform” Command Variant 4) sent by Users contains one mandatory Data item relating to the Firmware Hash. Currently, the DCC System forwards the Critical Command, CS06, to the target Device without validating the FirmwareHash. This Data item must align with the Manufacturer Image Hash value held in the Central Products List (CPL) for the Device Model. SEC Appendix AD ‘DCC User Interface Specification (DUIS)’ currently does not define any specific validation to be applied for SRV 11.3, beyond general validation applicable to all Requests.

The Proposed Solution would be to make minor updates to DUIS Sections 3.2.5, 3.5.10, and 3.8.125.3 to mandate DCC validation of the FirmwareHash Value provided in the SRV 11.3 Request against the Manufacturer Image Hash value (excluding the colon separator between octet values) of an Entry with ‘Current’ status on the Central Products List (CPL) for the target Device’s Device Model.

To reduce the changes to DUIS and minimise the impact on the DCC User Systems, it is proposed to utilise the existing E57 Response Code to inform the User of the invalid FirmwareHash value supplied in the Service Request, without initiating the GBCS CS06 Use Case towards the target Device.

The costs to implement this modification will be determined as part of the Refinement Process. This modification is expected to impact the Data Service Provider (DSP), and an Impact Assessment will be required from the DCC.

## 2. Issue

---

### What are the current arrangements?

DUIS defines the individual SRVs that a DCC User can request. For all Critical Service Requests, the User will first request transformation of the Critical Service Request (“Transform” Command Variant 4) into GBCS Format, and the resulting Pre-Command shall then be returned to the User for correlation and Digital Signing.

The Signed Pre-Command shall then be sent by the User (“Send” Command Variant 5) to the DCC, who shall add any requisite MAC to the signed GBCS Payload extracted from the body of the Signed Pre-Command and send the resultant Command to the relevant Device.

It should also be noted that all Service Requests and Signed Pre-Commands are constructed in XML format, including Header, Body, and Signature element, in accordance with the DUIS XML Schema.

The Critical SRV 11.3 '*Activate Firmware*' allows DCC Users to request the activation of a firmware image. This requires DSP transformation and User signing before being sent to the target Device.

SRV 11.3 sent by Users contains one mandatory Data Item relating to the Firmware Hash –

*FirmwareHash*: Hash calculated over the Manufacturer Image part of the FirmwareImage as defined by GBCS. This Data Item must align with the Firmware Hash value held in the CPL for the target Device Model.

### What is the issue?

At present, the DCC System only validates general request fields and Execution Timing but does not check the Firmware Hash against the CPL before forwarding the Critical Command (GBCS Use Case CS06<sup>1</sup>) to the Device.

By forwarding CS06 to the target Device, the DCC has identified a serious risk of activating bogus and unapproved Firmware Image. This would have serious consequences and impact both security and operational processes.

### What is the impact this is having?

There are both security risks and operational risks associated with this modification. There is a security risk arising from the DSP not validating the *FirmwareHash* against the authorised 'Current' hash stored in the CPL for the relevant Device Model, which could allow a malicious User to download and install a bogus, unapproved, or otherwise invalid Firmware Image offline and then activate it via a Service Request.

Without this validation, the integrity assurance normally provided by the *FirmwareHash* is lost, meaning tampering could go undetected.

Additionally, malicious firmware could undermine replay-attack protections by ignoring or resetting counters and identifiers, enabling the replay of old commands or the injection of fraudulent messages that appear legitimate.

From an operational standpoint, sending an invalid Service Request downstream without proper validation not only contradicts the zero-trust security framework principle but may also negatively affect DCC Total System and Communication Service Provider (CSP) performance, throughput, and operating costs.

### Impact on consumers

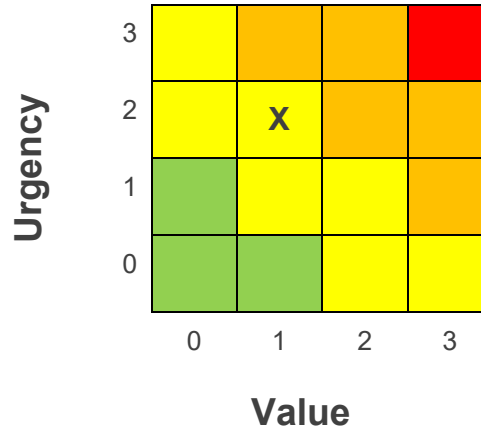
This issue would impact consumers if an unauthorised Firmware Image passes through the Device, as it may lead to the Device being compromised.

---

<sup>1</sup> Activate Firmware Critical Command

## What is the priority of this modification?

This modification has a priority score of medium. This rating is based on the following factors:



This modification was given a priority of medium based on the operational and security improvements the solution to the modification would bring to DCC Users and the DCC System.

Please refer to Appendix 3 for a full breakdown of how the priority score was calculated.

## 3. Solution

### Proposed Solution

The Proposed Solution is to make minor updates to DUIS Sections 3.2.5, 3.5.10, and 3.8.125.3 (see the attached document for proposed updates) to mandate DCC validation of the FirmwareHash Value provided in the SRV 11.3 Request ("Transform" Command Variant 4) against the Manufacturer Image Hash value (excluding the colon separator between octet values) of an Entry with 'Current' status on the Central Products List (CPL) for the target Device's Device Model.

To reduce the changes to DUIS and minimise the impact on the DCC User Systems, it is proposed to utilise the existing E57 Response Code to inform the User of the invalid FirmwareHash value supplied in the Service Request, without initiating the GBCS CS06 Use Case towards the target Device.

## 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 |

| SEC Party Categories impacted |                   |   |     |
|-------------------------------|-------------------|---|-----|
|                               | Other SEC Parties | ✓ | DCC |

By using the existing E57 Response Code, which is currently applicable to the SRV 11.3 Service Request, no SEC Party, other than DCC, shall be impacted by this modification.

The DCC would be directly impacted as the DSP systems would need to implement the new validation logic, and in the event of failed validation, support and integrate the existing E57Response Code into the SRV11.3 Response message back to the User.

## DCC Systems

### DCC System changes

This change would require a DCC System change to implement the new validation logic and, in the event of failed validation, support sending the existing E57 Response Codes, to the user within the DCC System.

### DCC System traffic

This change would provide some improvement on SMWAN traffic by removing the unnecessary exchange of subsequent Signed Pre-Command SRV 11.3 (“Send” Command Variant 5) Service Request from the User, and the GBCS CS06 Command/Response to/from the target Device, with invalid FirmwareHash.

## SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix AD ‘DCC User Interface Specification (DUIS)’

The changes to the SEC required to deliver the proposed solution can be found in the attached updated DUIS document. Annex A.

### Technical specification versions

This modification would amend the versions of DUIS that contain references to Sections 3.2.5, 3.5.10, and 3.8.125.3, as highlighted in the attached DUIS document.

## Devices

None of the Smart Metering Devices shall be affected by this modification, as they will still be required to perform the same procedure for CS06, as currently applicable.

### Consumers

This modification will have a positive impact on consumers - FirmwareHash validation improves security, privacy, and reliability for consumers by ensuring only trusted firmware runs on their Devices, reducing the risks of malware, tampering, and supply-chain attacks, which could result in breach of the consumer's confidential/consumption information and/or disruptions to their energy supply.

### Other industry Codes

This modification will not impact other industry Codes.

### Greenhouse gas emissions

This modification does not have an impact on greenhouse gas emissions.

## 5. Costs

---

### DCC costs

DCC costs will be assessed during the Refinement Process.

### SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one days 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

SEC Party costs will be assessed during the Refinement Process.

## 6. Assessment of the proposal

---

### Areas for assessment

#### Sub-Committee input

SECAS will engage the Chairs from the Operations Group (OPSG), the Performance Assurance Board (PAB), the Privacy Sub-Committee (PSC), the Smart Metering Device Assurance Sub-Committee (SMDASC), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC), the Smart Metering Key Infrastructure Policy

Management Authority (SMKI PMA) 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                | No input required.                                |
| PAB                 | No input required.                                |
| PSC                 | No input required.                                |
| SMDASC              | No input required.                                |
| SMKI PMA            | No input required.                                |
| SSC                 | Input on solution development and security risks. |
| TABASC              | No input required.                                |
| TAG                 | No input required                                 |

## Observations on the issue

This modification was presented at the SEC Change Issues Group in November 2025.

A SEC Party member questioned whether the issue related to aligning definitions with what is already recorded in the Central Products List (CPL) for each Device Model. The Party added that their support for the modification would be on the basis that the fix is carried out at no cost to industry. They did not believe that the risk justified any additional spending as the existing controls are sufficient. The DCC has added post-meeting that this proposal is not envisaged to have a cost implication for SEC Parties. The DCC would need to include the SRV 11.3 FirmwareHash validation logic in the DSP.

The DCC agreed that SRV 11.3 covered most checks and noted that the associated risks are generally low. However, they went on to explain that a risk can arise when a Supplier downloads a firmware image offline and activates it without the proper verification steps. This would allow an invalid activation image to be sent. Although they agreed the likelihood of this is small, the extra checks would help ensure invalid commands are not authorised.

The DCC confirmed that the modification will impact the DSP and therefore the solution would have an associated cost. The Working Group agreed an appropriate forum to discuss this modification would be the SSC to assess the security implications.

This modification was also presented at the SSC in February 2026. The SSC confirmed that the proposed solution would strengthen security controls and will mitigate future security risks when firmware is distributed via the internet, and on that basis, expressed its support for the modification to be progressed to establish costs.

## 7. Case for change

### Business case

The mandatory validation of the FirmwareHash used in SRV 11.3 against the authorised Firmware Hash stored in the CPL for the relevant Device Model combination ensures that only approved and

current firmware can be activated on a Device by the Supplier, maintaining alignment with the SEC Security Controls Framework.

It also supports smoother DCC System performance by ensuring that only valid, fully-checked messages reach the target Device through the Service User gateway.

Alongside improving security, this change reduces the chance of tampered or incorrect firmware being activated, helps keep Devices running reliably, and creates a more consistent approach across all DCC Users.

It also helps avoid failed activations and unnecessary retries by stopping invalid requests early, and it strengthens audit trails by providing a clear record that firmware was validated before activation.

## Views against the General SEC Objectives

### Proposer's views

The Proposer believes this modification would better facilitate General SEC Objectives (a)<sup>2</sup> and (f)<sup>3</sup>.

The proposed FirmwareHash validation supports SEC Objective (a) by ensuring Devices only operate on authorised and compatible firmware, which improves the overall efficiency and reliability of Smart Metering Systems (SMS).

It also strengthens SEC Objective (f) by preventing tampered or unauthorised firmware from being activated, thereby protecting the security and integrity of data and systems across the smart metering ecosystem.

## Views against the consumer areas

### Improved safety and reliability

This modification will have a positive impact on this consumer area as the implemented solution would improve the safety of FirmwareHash validation.

### Lower bills than would otherwise be the case

This modification would have a neutral impact on this consumer area.

### Reduced environmental damage

This modification would have a neutral impact on this consumer area.

### Improved quality of service

This modification would have a positive impact on this consumer area. It would eliminate the unnecessary traffic flow arising from invalid SRV 11.3 Service Requests from the User and the

---

<sup>2</sup> facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain

<sup>3</sup> ensure the protection of Data and the security of Data and Systems in the operation of this Code

subsequent CS06 Command/Response exchanges. As such, it is expected to improve the quality of service to consumers.

### Benefits for society as a whole

This modification would have a neutral impact on this consumer area.

## Appendix 1: Progression timetable

| Timetable                                             |                |
|-------------------------------------------------------|----------------|
| Event/Action                                          | Date           |
| Draft Proposal raised                                 | 18 Mar 2026    |
| Presented to CSC for initial comment                  | 14 Apr 2026    |
| CSC converts Draft Proposal to Modification Proposal  | 14 Apr 2026    |
| Business requirements developed with Proposer and DCC | Apr – May 2026 |
| Preliminary Assessment requested                      | May 2026       |
| Preliminary Assessment returned                       | May 2026       |
| Modification discussed with Working Group             | Jun 2026       |
| Modification discussed with Security Sub-Committee    | Jun 2026       |
| Refinement Consultation                               | Jun – Jul 2026 |
| Impact Assessment costs approved by Change Board      | 22 Jul 2026    |
| Impact Assessment requested                           | 23 Jul 2026    |
| Impact Assessment returned                            | Sep 2026       |
| Modification discussed with Working Group             | 4 Nov 2026     |
| Modification Report approved by CSC                   | Nov 2026       |
| Modification Report Consultation                      | Nov - Dec 2026 |
| Change Board Vote                                     | Dec 2026       |

*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             |
| CPL      | Central Products List |

| Glossary |                                                                |
|----------|----------------------------------------------------------------|
| Acronym  | Full term                                                      |
| CSC      | Change Sub-Committee                                           |
| CSP      | Communication Service Provider                                 |
| DCC      | Data Communications Company                                    |
| DSP      | Data Service Provider                                          |
| DUIS     | DCC User Interface Specification                               |
| ESME     | Electricity Smart Metering Equipment                           |
| GBCS     | Great Britain Companion Specification                          |
| GSME     | Gas Smart Metering Equipment                                   |
| OPSG     | Operations Group                                               |
| PAB      | Performance Assurance Board                                    |
| PSC      | Privacy Sub-Committee                                          |
| SEC      | Smart Energy Code                                              |
| SECAS    | Smart Energy Code Administrator and Secretariat                |
| SMKI PMA | Smart Metering Key Infrastructure Policy Management Authority  |
| SMS      | Smart Metering System                                          |
| SRV      | Service Request Variant                                        |
| SSC      | Security Sub-Committee                                         |
| TABASC   | Technical Architecture and Business Architecture Sub-Committee |
| TAG      | Testing Advisory Group                                         |

## Appendix 3: Prioritisation Matrix

| Prioritisation Matrix <sup>4</sup>         |                                       |                             |                               |                               |       |         |          |
|--------------------------------------------|---------------------------------------|-----------------------------|-------------------------------|-------------------------------|-------|---------|----------|
| Legal & regulatory compliance <sup>i</sup> | Operational performance <sup>ii</sup> | Cost benefit <sup>iii</sup> | Consumer impact <sup>iv</sup> | Security impacts <sup>v</sup> | Value | Urgency | Priority |
| 0                                          | 2                                     | 0                           | 0                             | 2                             | 1     | 2       | Medium   |

<sup>i</sup> Ensure that Parties (including the DCC) meet the obligations of all relevant laws, regulations and licence obligations

<sup>ii</sup> Deliver performance improvements enhancing speed, quality, costs, flexibility and dependability

<sup>iii</sup> Realise financial benefits compared to the cost of the change and the impact of doing nothing

<sup>iv</sup> Meet or enhance consumer and end user needs and expectations through offering better services

<sup>v</sup> Deliver or enhance the smart metering security arrangements or reduce the risk of a security incident arising

<sup>4</sup> The impact or improvement in each area is measured on a 0-1-2-3 rating system, where 0 is equal to no expected impact or improvement and 3 is equal to a major expected impact or improvement.