

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0062 ‘Northbound Application Traffic Management - Alert Storm Protection’

Business Requirements – version 2.0

About this document

This document outlines the detailed business requirements for SECMP0062.

Summary

The DCC and Service Users communicate through the use of DCC Systems for sending service requests and alerts for different registered devices. Due to the DCC system having a finite capacity for how many requests and alerts it can handle, if this system becomes overloaded, it will affect the stability and performance of the system. This system is also vulnerable to Alert Storms, a state where individual devices will encounter a scenario where they frequently generate the same Alert and send it through the DCC Systems. This adds needless traffic to the DCC Systems and, as a result, slows down the response time for other Alerts and Service Requests that have to use the same system as a means of communication. Alert Storms therefore need to be avoided as much as possible, or alternatively, traffic management needs to be in place to prevent repeated Alerts from a faulty device entering the system.

This solution will protect against the scenario in which a specific Alert is generated repeatedly and rapidly by individual devices. However, it is noted that it will not, and is not intended to, protect the DCC Systems against a large quantity of devices that generate a small number of alerts which enter the DCC Systems (e.g. due to a power outage over a large area).

Business Requirements

Requirement 1: The DCC will implement a mechanism that will block Alerts from entering the DSP Central System and being routed on to the User where the number received exceeds a given threshold.

The DSP (Data Service Provider) System will monitor the number Alerts received from a Device. When the total number of Alerts received from an individual Device within a rolling time period T exceeds a threshold A, an incident is created for that Device.

While an incident is open, the DSP System will monitor the number of each specific Alert received from the Device. When the total number of copies of a specific Alert received from the Device within a rolling time period R exceeds a threshold B, the Device/Alert combination will be marked as overloaded and an additional incident is created for that specific Device/Alert.

As part of the Impact Assessment, DCC will specify the expected Service Level Agreements for DCC and DCC Users to respond to incidents.

When a Device/Alert combination is marked as overloaded, only 1 in N copies of the Alert will be passed to the User, with all other copies being blocked by the DSP System. The copies of the Alert that are allowed through will still be subject to the normal Target Response Times.

A Device/Alert combination will no longer be overloaded when the number of copies of that Alert received in a rolling time period R falls below threshold B. At this point, those Alerts will no longer be blocked. The number of blocked Alerts will still be counted in determining this threshold.

The values to be set upon implementation of SECMP0062 are:

- T = 30 minutes
- A = 50
- R = 5 minutes
- B = 10
- N = 10

The values of T, A, R, B and N will be configurable values in the DSP System that can be changed at any time. They will not be hard-wired into the System.

The parameters will be 'global' values that are applicable to all DCC Users. It will not be possible for different Users to set different values specific to them.

This process will be applied to all SMETS (Smart Metering Equipment Technical Specification) 2 Alerts. It will also be applied to any SMETS1 Alerts that have been mapped to an equivalent SMETS2 Alert.

As part of the Impact Assessment, DCC is asked to provide details of what will happen to blocked Alerts in terms of storage and discarding.

Requirement 2: The relevant User will be notified when Alerts have been subject to throttling.

Users will be notified that Alerts have been blocked through the non-mandatory metadata fields of those Alerts that are allowed through. Users will be required to update their systems if they wish to be able to receive this additional information.

It is expected that this requirement will be implemented through a new DCC User Interface Specification (DUIS) version.

The Working Group is considering the potential for a staggered implementation approach where Requirements 1, 3, 4, 5 and 6 are implemented as soon as possible while the DUIS changes for Requirement 2 are implemented in a later SEC Release. To inform the appropriate way forward, DCC is asked to provide an approach to be taken for alerting DCC Users in the interim period, to include the expected time period in which DCC Users will be notified of when the throttling of Alerts begin if the mechanism is in operation, as part of its Impact Assessment response.

Additionally, as part of the Impact Assessment response, DCC is asked to provide a full analysis of a solution with email notification during the first stage during this staggered approach, and one without.

Requirement 3: There will be a configurable list of exempted Alerts that will not be subject to throttling or subject to a different level of throttling.

The DSP System will contain a configurable list of Alerts that will not be subject to this mechanism or will be subject to this mechanism but with different values for the parameters R, B and/or N. The number of copies of these Alerts received will still be used to determine a breach of the threshold A. This list should be capable of being updated at any time and will not be hard-wired into the System.

Any variations set using this Requirement 3 will be 'global' variations that are applicable to all DCC Users. It will not be possible for different Users to set different values specific to them.

Requirement 4: DCC will not amend the list of exempted Alerts without approval from the Panel or a delegated Panel Committee.

DCC will not amend the list of exempted Alerts without obtaining approval from the Panel (the Panel may delegate this responsibility to a Panel Committee determined by the Panel).

Requirement 5: DCC will not change the values of the parameters without approval from the Panel or a delegated Panel Committee, except in well-defined exceptional circumstances.

DCC may change parameter values without consent in clearly defined circumstances which will be agreed as part of the solution definition in response to an urgent need to amend one or more parameters. It will then retrospectively report any changes of these to the Panel.

Otherwise, DCC will not change the values of parameters without obtaining approval from the Panel (the Panel may delegate this responsibility to a Panel Committee determined by the Panel).

As part of the Impact Assessment, the DCC is asked to provide examples of where it would need to urgently respond to events that warrant a rapid change of the parameter values. The Working Group will use this to determine if any such circumstances should be defined.

Requirement 6: DCC will provide reporting on the use of throttling of Alerts.

DCC will report on how often the mechanism introduced under SECMP0062 is used. This will cover the number of incidents raised and the number of Device/Alert combinations that are classed as overloaded within a given reporting period. As part of this report, DCC will provide a full updated list of

Alert parameter values and any exempted Alerts or Alerts with different parameters, so DCC Users know which restrictions are placed against each types of Alert.