

SECAS Guidance Notes: Managing Critical Alerts where there is DCC User to Non-User Churn

Purpose

The purpose of this document is to show Suppliers the process and requirements for dealing with Critical Alerts where there is DCC User to Non-User Churn. Network Operators and Device Manufacturers may also find this information useful. This document includes:

- A description of the [SEC Party Operations Contact List](#) that is hosted securely on the SEC website;
- The process detailing how a DCC User Supplier will forward Critical Alerts to the relevant Non-DCC User Supplier;
- The process detailing how SECAS and SEC Parties maintain the Operations Contact List; and
- The list of relevant Critical Alerts from the [Great Britain Companion Specification \(GBCS\) SEC Schedule 8](#) that this process will apply to.

Introduction

The DCC will not be developing a Non-Gateway Interface solution for use by non-DCC Users as part of its wider solution.

In the absence of a Non-Gateway solution, the old Supplier (DCC User) whose security credentials remain on the meter will continue to receive any [Critical Alerts](#) sent by that meter.

An interim process has been developed to ensure that the new Supplier (non-DCC User) is provided with any Critical Alerts received by the old Supplier.

This guide documents the process and highlights Suppliers' responsibilities to ensure that they continue to act with a duty of care for their customers.

Critical Alert Definition

In the context of this document, a Critical Alert can be defined as: an Alert, a message generated by a Device in response to a problem or risk of a potential problem in relation to supply being affected, financial fraud or the compromise of Device security.

Overview of the Supplier-to-Supplier Process

The diagram below highlights the high-level process that must be followed to provide the requisite duty of care to customers.



Responsibility of the old Supplier

If a DCC User receives a Critical Alert for an MPxN for which it is no longer the current Supplier, the DCC User (old) Supplier should, as a minimum, forward the details of the Alert to the new Supplier that the customer moved to.

The old Supplier should identify the new Supplier for that MPxN using registration information available via [ECOES](#), [Data Enquiry Service \(DES\)](#), and / or registration dataflows received by the Supplier during the Change of Supplier (CoS) process.

The old Supplier should use their best endeavours to identify the acquiring Supplier for the customer.

The old Supplier should then forward the details of the Alert by email to the new Supplier, using the contact details available on the [Operations Contact List](#). There are no requirements on ensuring secure exchanges of emails over and above what Suppliers have already established for various existing industry processes.

Information Requirements

The old Supplier should forward the relevant information from the original XML Critical Alert in human-readable format, which will allow the new Supplier to take relevant action. At a minimum, the email must include the following information:

- MPxN that the Alert relates to;
- Alert Code; and
- Alert Code date / time stamp as per original XML Alert received from the DCC.

If you cannot reach the new Supplier via the contacts on the Operations Contact List, please contact the [SECAS Helpdesk](#).

Responsibility of the new Supplier

The Non-DCC User (new) Supplier must acknowledge receipt of the email from the sender and take the relevant action(s). If the new Supplier is not, or is no longer, the current Supplier for the MPxN that the Alert relates to, then the new Supplier will need to identify the correct acquiring Supplier via the Operations Contact List and forward on the Critical Alert.

What to do when using Shared Resource Providers

Suppliers that use Shared Resource Providers must establish how they deliver the principles above for a Supplier-to-Supplier solution. This may involve the Shared Resource Provider undertaking the work on behalf of a Supplier.

What are Relevant Critical Alerts?

The list of relevant Critical Alerts for this process is found in Table 1 below. These Alerts have been identified as **safety related** and mandated by GBCS SEC Schedule 8 as being important to maintain secure supply. Therefore, these are the Alerts expected to be forwarded.

Alert Code	Alert Name
0x8F1F	Low Battery Capacity
0x8F3F	Unauthorised Physical Access - Tamper Detect
0x8F73	Unauthorised Physical Access - Battery Cover Removed
0x8F74	Unauthorised Physical Access - Meter Cover Removed
0x8F75	Unauthorised Physical Access - Strong Magnetic field
0x8F76	Unauthorised Physical Access - Terminal Cover Removed
0x8F77	Unauthorised Physical Access - Second Terminal Cover Removed
0x8F78	Unauthorised Physical Access - Other
0x8F1D	Gas Smart Metering Equipment (GSME) Power Supply Loss

Table 1: Relevant Critical Alerts to be forwarded.

Suppliers must also forward any other Critical Alerts that they believe are also covered by their general duty of care and responsibilities. Further information on Alerts and their requirements can be found in [GBCS SEC Schedule 8](#).

What is the Operations Contact List?

In order for the old Supplier to provide the new Supplier with the Critical Alert information, an [Operations Contact List](#) is hosted securely and maintained on the SEC Website.

This list can only be accessed by SECAS, the DCC and SEC Parties once they have logged in to the SEC website.

All Supplier SEC Parties are required to provide SECAS with the relevant contact information to be included on this list, and inform SECAS of any changes by either [email](#) or using our [Online Change in Details Form](#). Contact information is required in the following format:

	Name	Phone	Email Address
Primary Contact: To initially receive the forwarded Critical Alerts. This is preferably a general inbox that is constantly monitored.			

Secondary Contact:

For escalation purposes if issues arise, e.g. the recipient did not acknowledge receipt of email. This is preferably an appropriate responsible person.

How can SECAS help you?

As well as processing ad-hoc changes upon request, SECAS contacts all SEC Parties each quarter to check whether your details on the Operations Contact List need to be updated.

Following each update, SECAS publishes the current version of the spreadsheet on the SEC website [here](#).

Supplier to Supplier Process

Steps	Process	Timescales*	Responsibilities	
			From	To
1	Device generates GBCS Critical Alert which is sent to the DCC User (old) Supplier	-	-	-
2	Old Supplier to identify acquiring Supplier from ECOES, DES, or registration dataflow	-	DCC User	-
3	Old Supplier to forward Critical Alert to new Supplier using contacts from Operations Contact List	Within 1 WD / As soon as reasonably practicable after that	DCC User	Non-DCC User
4	New Supplier to acknowledge receipt of email	Upon receipt / 1 WD	Non-DCC User	DCC User
5	1. Acquiring Supplier to take any required action on the Critical Alert	-	-	Non-DCC User
	OR			
	2. Non-DCC (new) Supplier to go through Step 2 if it is not the acquiring Supplier	Upon receipt / 1 WD	Non-DCC User	Non-DCC User

SEC Party Operations Contact List - SECAS Quarterly Update

Steps	Process	Timescales*	Responsible Party	
			From	To
1	SECAS to email all SEC Parties to obtain contact details	Quarterly	SECAS	SEC Parties
2	SEC Parties to update SECAS on contact detail changes	5 WDs	SEC Parties	SECAS
3	SECAS to acknowledge receipt of email	Upon receipt	SECAS	SEC Parties
4	SECAS to update Operations Contact List and publish list on SEC website	1 WD	SECAS	-

SEC Party Operations Contact List - Ad-Hoc Requests

Steps	Process	Timescales*	Responsibilities	
			From	To
1	SEC Party to notify SECAS of change in contact details via email or Online Form	Upon change occurring	SEC Party	SECAS
2	SECAS to acknowledge receipt of email	Upon receipt	SECAS	SEC Party
3	SECAS to update Operations Contact List and publish on SEC website	1 WD	SECAS	-

If you have any questions, please contact SECAS by emailing our [SECAS Helpdesk](#) or call 020 7090 7755.