Managing Critical Alerts where there is DCC User to Non-User Churn Guidance Note

Version 1

Version History

Version	Date of Issue	Status	Change Summary
0.1	02/09/2016	Draft	Initial Draft of the document for consultation
1	19/10/2016	Final	First issue

Gemserv

Contents

Gemserv

Managing Critical Alerts where there is DCC User to Non-User Churn

1.   Introduction

The DCC, as concluded on by the former Department of Energy and Climate Change (now Department of Business, Energy and Industrial Strategy (BEIS)[1], will not be developing a Non-Gateway Interface solution for use by a non-DCC User as part of its wider solution. In the absence of a non-gateway solution, on customer churn from a DCC User to a non-DCC User, the Supplier (DCC User) whose security credentials remain on the meter will continue to receive any Critical Alerts sent by the meter.

An interim process has been developed through Energy UK engagement with Suppliers to ensure that the new Supplier (non-DCC User) is provided with any Critical Alerts received by the old Supplier[2].

BEIS also participated in the engagement process on this matter, maintaining a watching brief over the development of the delivery principles to ensure that the resulting process is in keeping with government policy objectives, and has produced a cost effective solution.

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

1.1   Terminology

In the context of this guidance note 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[3].

2.   Purpose

The purpose of this guidance note is to illustrate the process and requirements for dealing with Critical Alerts where there is DCC User to Non-User churn. This guidance includes:

- the DCC User Suppliers, Non-DCC User Suppliers, and SECAS process steps;

- a description of the Supplier Contact List that will be hosted securely on the SEC website;

- a process map outlining how a DCC User Supplier will forward critical alerts to the relevant Non-DCC User Supplier (provided in Appendix A);

---

[1] Page 75 - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/484710/15_11_26_December_2015_SEC_Government_Response_final.pdf
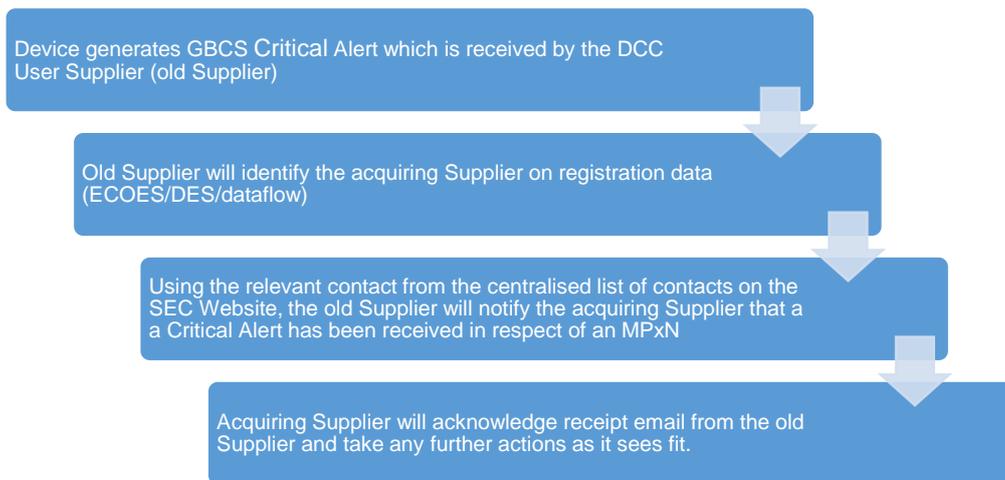
[2] This process to apply in the enduring phase to cater for potential delay in processing new Supplier's security credentials onto smart meter.

[3] Definition is based on the combined GBCS definitions of Alert and Critical Messages.

Administered by

Gemserv

- a process map outlining the process SECAS and Suppliers undertake to maintain the Supplier Contact List (Appendix B); and

- the list of relevant Critical Alerts (Appendix C) that this process will apply to.

3. Supplier-to-Supplier Process

The below highlights the high-level process that should be followed in order to provide the required duty of care to customers. The process is expanded in further detail in the subsequent sections.

Device generates GBCS Critical Alert which is received by the DCC User Supplier (old Supplier)

Old Supplier will identify the acquiring Supplier on registration data (ECOES/DES/dataflow)

Using the relevant contact from the centralised list of contacts on the SEC Website, the old Supplier will notify the acquiring Supplier that a a Critical Alert has been received in respect of an MPxN

Acquiring Supplier will acknowledge receipt email from the old Supplier and take any further actions as it sees fit.

Figure 1: High Level Process for Managing Critical Alerts

3.1 DCC User Supplier Process

In the case where a DCC User receives a Critical Alert for an MPxN for which it is not the current Supplier, the DCC User Supplier should as a minimum forward the details of the alert to the Supplier the customer churned to. The DCC User Supplier can choose to identify the current Supplier for that MPxN using registration information available via ECOES, DES, and/or registration dataflows as received by the Supplier during the Change of Supplier (CoS) process. The DCC User Supplier should use their best endeavours to identify the acquiring Supplier for the customer.

The old Supplier shall then forward the details of the alert via email, using the contact details available on the centralised list of contacts available on the SEC Website. 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 sending Supplier should forward the relevant information from the original XML critical alert that would allow the new Supplier to take the relevant action. The critical alert will be received by the DCC User Supplier in an XML format and should be forwarded on in a human readable format.

At a minimum, the email should 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 DCC.

If the sending Supplier cannot reach the acquiring Supplier via the contacts on the list, please contact the SECAS helpdesk.

3.2 Non-DCC User Supplier

The Non-DCC User Supplier will need to acknowledge receipt of the email from the sender, and take any action as it sees fit. If the Non-DCC User Supplier is not the current supplier for the MPxN that the alert relates to, then that Supplier will need to identify the correct acquiring Supplier and forward on the critical alert as per the process set out in Section 3.1.

3.3 Use of Shared Service Providers

Suppliers that use shared service providers will need to establish how they deliver the principles captured for a Supplier-to-Supplier solution. This may or may not involve the shared service provider undertaking the work on behalf of a Supplier.

3.4 Relevant Critical Alerts

The list of relevant Critical Alerts for which this process will apply is provided in Appendix C. The relevant alerts have been identified through Energy UK engagement with suppliers as 'safety related' and therefore are the alerts expected to be forwarded. There is nothing to prevent suppliers forwarding other Critical Alerts that it believes are also covered by its general Duty of Care responsibilities.

4. Supplier Contact List

In order for the old Supplier to provide the relevant Supplier with the Critical Alert information, a centralised contact list of suppliers will be hosted and maintained on the SEC Website.

All Suppliers are requested to provide SECAS with the relevant contact information to include on the centralised list, and proactively inform SECAS should these details change.

Information required from Suppliers will be requested in the following format:

	Name	Telephone Number	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 email. This is preferably an appropriate responsible person.			
Individual contacts who will require access to the Centralised List			

4.1   SECAS Support

SECAS will update and securely publish the Supplier Contact List on the SEC Website. The list will be available via a login to the SEC Website. SECAS will request each supplier to provide the contact details of those who will require access to the list to allow accounts to be established.

List Updates

Following the initial request for contacts to be provided to SECAS, it will be the Supplier's responsibility to ensure that these contact details remain up to date.

As well as any ad-hoc updates that are required, on a quarterly basis, SECAS will require confirmation from each supplier that the contact details listed are correct.

Following each quarterly and ad-hoc update, SECAS will publish the updated version of the supplier contact list on the SEC website and email the relevant contacts with a notification that an update has been made.

5.   Process and Procedures

5.1   Supplier to Supplier Process

Steps	Process	Timescales*	Responsibilities	
			From	To
1	Device generates GBCS Critical alert which is sent to the DCC User Supplier	-	-	-
2	Supplier to identify acquiring Supplier from GUID, ECOES, DES, or registration dataflow	-	DCC User	-
3	DCC User Supplier to forward Critical Alert to acquiring Supplier using contact from centralised contacts list	Within 1 WD / As soon as reasonably practicable after that.	DCC User	Non-DCC User

Administered by

Gemserv

4	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 Supplier to go through step 2 if it is not the acquiring Supplier	Upon receipt / 1 WD	Non-DCC User	Non-DCC User

Administered by

Gemserv

5.2 Supplier Contact List – SECAS to initiate

Steps	Process	Timescales*	Responsible Party	
			From	**To**
1	SECAS to email to all Suppliers to obtain contact details	Quarterly	SECAS	Suppliers
2	Suppliers to update SECAS on contact details or confirm no changes are necessary	5 WDs	Suppliers	SECAS
3	SECAS to acknowledge receipt of email	upon receipt / 1 WD	SECAS	Suppliers
4	SECAS to update supplier contact list & to publish list on SEC website	1 WD	SECAS	-
5	SECAS to inform SEC parties of updated contact list via email & news item on website	1 WD	SECAS	Suppliers

5.3 Supplier Contact List – Supplier to initiate

Steps	Process	Timescales*	Responsibilities	
			From	**To**
1	Supplier to notify SECAS of change in contact details	Upon change occurring	Suppliers	SECAS
2	SECAS to acknowledge receipt of email	1 WD	SECAS	Suppliers
3	SECAS to update supplier contact list & publish list on SEC website	1 WD	SECAS	-
4	SECAS to inform relevant contacts of updated contact list via email & news item on website	1 WD	SECAS	Suppliers

*Timescales are provided as a guide for best practice responses.

Administered by

Gemserv