MP203 'Security Assurance of Device Triage Facilities'

Annex A

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Section G ‘Security’

These changes have been redlined against Section G version 16.0.

Add Section G12 as follows:

G12 Security Assurance of Device Triage Facilities

G12.1 Some of the expressions used in this Section G12 are defined in Section G12.9.

G12.2 Where the SSC Guidance for Device Security Assurance and Triage specifies that independent assurance of Triage Facility Providers is required to achieve appropriate levels of security assurance in accordance with the requirements of this Code, this Section G12 shall apply.

Triage Facility Provider Obligations

G12.3 In order to become a Triage Facility Provider, an entity must either be an existing Party or accede to this Code and become a Party. A Triage Service Provider is not required to be a User.

G12.4 Each Triage Facility Provider shall:

(a) not attempt to undertake Triage Activities on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process);

(b) only use the Triage Tool and Triage System Interface provided by a Device's Manufacturer to access the Manufacturer's Triage System and not use any other electronic devices, interfaces or IT systems for carrying out Triage Activities;

(c) ensure multi-factor authentication and role-based access controls are used within its Triage Facility to control access to the graphical user interface (GUI) of the Triage Tool, and to control access to the Triage System Interface;

(d) at all times prevent unauthorised use of the Triage Tool and Triage System Interface, and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities;

(e) ensure that all the required tamper-protection seals are fitted to Devices on completing the Triage Activities;

(f) maintain an asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility, including details of:

(i) the Requestor of any change to the configuration of a Device;
(ii) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities;
(iii) details of Triage Activities successfully undertaken;
(iv) details of any failed attempts to complete Triage Activities; and
(v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor;

(g) when requested by the Security Sub-Committee, provide the Security Sub-Committee with an up-to-date copy of the records maintained pursuant to Section G12.3(f);

(h) provide all reasonable assistance that may be requested by the Security Sub-Committee or the User Independent Security Assurance Service Provider for the purposes of conducting a User Security Assessment;

(i) subject to Section G12.5, comply with the requirements of Sections G1, G3 to G5, G7 and G8;

(j) comply with the requirements of Sections G12.6 to G12.8; and

(k) act in accordance with Good Industry Practice.

G12.5 For the purposes of Sections G1, G3 to G5, G7 and G8, unless the SSC Guidance for Device Security Assurance and Triage states otherwise, a Triage Facility Provider shall be treated as if it is a User and:

(a) any reference to a 'User' shall be deemed to include a reference to a 'Triage Facility Provider';

(b) except for where the SSC Guidance for Device Security Assurance and Triage states otherwise, obligations in those Sections which are expressed to apply to a User shall apply to a Triage Facility Provider;

(c) references in those obligations to 'User Systems' shall be deemed, for the purpose of their application to the Triage Facility Provider, to be references to the Triage Activities undertaken at the Triage Facility, and

(d) the Security Sub-Committee shall provide Triage Facility Providers and other Parties with guidance on interpretation of Sections G1, G3 to G5, G7 and G8 in respect of their application to Triage Facility Providers and Triage Activities.

User Security Assessments of Triage Facilities

G12.6 Prior to undertaking any Triage Activities, each Triage Facility Provider shall be subject to an initial Full User Security Assessment by a User Independent Security Assurance Service Provider following the process in Sections G8.22 to G8.30.

Approval

G12.7 On receipt of the initial Full User Security Assessment Report and the User Security Assessment Response, the assurance status shall be set in accordance with Sections G8.35 to G8.36 and:

(a) where the assurance status is set to ‘approved’ under Section G8.36(a) then the Triage Facility Provider may undertake Triage Activities as set out in the SSC Guidance for Device Security Assurance and Triage;

(b) where the assurance status is set to ‘approved' subject to conditions (as set under Section G8.36(b)) then the Triage Facility Provider will require explicit approval from the Security Sub-Committee before undertaking Triage Activities; and

(c) where the assurance status is ‘deferred’ or ‘rejected’ under Section G8.36(c) or (d), respectively, then the Triage Facility Provider is not approved to undertake Triage Activities.

Second and subsequent User Security Assessments

G12.8 Within 12 months following completion of the initial and each subsequent User Security Assessment, the Triage Facility Provider shall schedule a subsequent User Security Assessment with the User Independent Security Assurance Provider. The Security Sub-Committee shall determine the category of each such User Security Assessment to be carried out and, in doing so shall:

(a) consider any security risks identified during or since the previous User Security Assessment;

(b) take account of the volume of Devices for which Triage Activities are carried out;

(c) reach a determination based on a proportionate assessment of the security risks as to whether the next User Security Assessment should be:

(i) a Full User Security Assessment;
(ii) a Verification User Security Assessment; or
(iii) a User Security Self-Assessment.

Definitions

G12.9 For the purpose of this Section G12:

Requestor	means an entity (such as a Party or a meter asset provider) that requests that Triage Activities are undertaken by a Triage Facility Provider.
SSC Guidance for Device Security Assurance and Triage	means the document published by the Security Sub-Committee under Section G7.19(g), which sets out guidance on the requirements and processes (including security controls and security assurance) to be followed by Triage Facility Providers undertaking Triage Activities.
Triage	means the diagnosis, upgrading or resetting of a Device.
Triage Activities	means any Triage-related activity carried out in circumstances where the SSC Guidance for Device Security Assurance and Triage requires independent assurance, including in such circumstances: a) the breach of the tamper-protection boundary; b) any unlocking of internal non-operational ports; c) any changes to the configuration of the Device Data; d) confirmation of the firmware version on the Device when Triage has been completed; and e) completion of Triage by replacing all internal non-operational port seals required pursuant to the CPA Security Characteristics and all tamper-protection boundary seals.
Triage Facility	means a premises where Triage Activities are undertaken.
Triage Facility Provider	means a Party which operates a Triage Facility for the purpose of carrying out Triage Activities.

Triage System Interface	means a secure IPsec virtual private network, site to site encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a Triage Facility, which provides confidentiality and integrity of communications.
Triage System	means a secure IT system established for the purposes of Triage and operated by a Manufacturer, as part of its Device manufacturing capability, which the Triage Facility Provider connects to using the Triage Tool and Triage System Interface, and which is compliant with the requirements of the NCSC Commercial Product Assurance (CPA) Scheme and the associated CPA Security Characteristics.
Triage Tool	means an electronic device provided by a Manufacturer, which is used to Triage Devices in accordance with SSC Guidance for Device Security Assurance and Triage, and which is cryptographically authorised such that it can only be used for Triage Activities and cannot be given additional capabilities by an operator in a Triage Facility.