

## SECTION H: DCC SERVICES

### H5 SMART METERING INVENTORY AND ENROLMENT SERVICES

#### Post-Commissioning Obligations

H5.33 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, the DCC shall ~~ensure that~~:

- (a) ~~ensure that~~ the Communications Hub Function re-generates its Private Keys, and ~~ensure that the Communications Hub Function's~~ its Device Security Credentials ~~Certificates~~ are stored on ~~the Device; and it~~;
- (b) ~~at least unless~~ one of the Organisation Certificates comprising its Device Security Credentials ~~has already been replaced on the execution of a Command sent to the Communications Hub Function's Device Security Credentials~~ by the DCC during Commissioning, ensure that one such Certificate is replaced (~~provided that and~~ for ~~such~~ these purposes an Organisation Certificate may be replaced with the same ~~Organisation Certificate~~); and
- (c) unless the DCC has previously done so following receipt of the associated Communications Hub from its manufacturer, interrogate the Communications Hub Function in order to confirm that, within its Device Security Credentials, the Organisation Certificate in the Trust Anchor Cell that has a Remote Party Role corresponding to 'Recovery' is the Recovery Certificate.

H5.34 ~~The DCC shall notify the Lead Supplier if~~ if any one or ~~both~~ more of the steps in Section H5.33 fails. ~~Where a Lead Supplier receives such a notification, it shall, as soon as reasonably practicable (and in any event with 7 days) following the Commissioning of the Communications Hub Function, replace the,~~ the DCC shall, except where the relevant Communications Hub Function ~~is replaced~~;

- (a) set the SMI Status of the Communications Hub Function to 'suspended';

- (b) so far as reasonably practicable, continue to attempt the successful completion of the failed steps;
- (c) if it is able successfully to complete the failed steps, set the SMI Status of the Communications Hub Function to that which it was immediately prior to being 'suspended'; and
- (d) not otherwise change the SMI Status of the Communications Hub Function unless it is Decommissioned.

H5.35 Where it takes either of the steps described in Section H5.34(a) or (c), the DCC shall notify the Responsible Supplier for any Smart Metering System of which the relevant Communications Hub Function forms part that it has done so and of its reasons for doing so.

H5.36 Where, pursuant to Section H5.34(a), a Communications Hub Function has its SMI Status set to 'suspended', the Responsible Supplier for any Smart Metering System of which that Communications Hub Function forms part may replace the associated Communications Hub and may return it to the DCC in accordance with Section F8 (Removal and Return of Communications Hubs) relying on the reason specified at Section F9.5(f) (Reasons).

H5.37 ~~H5.35~~ As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Smart Meter or a Gas Proxy Function, the Lead Supplier shall send a Service Request in respect of that Device to:

- (a) ensure that the Device Security Credentials which pertain to the Network Party are those of the Electricity Distributor or Gas Transporter (as applicable);
- (b) ensure that the Device Security Credentials which pertain to the Supplier Party are those of the Responsible Supplier;
- (c) ~~re-generate~~ensure that the Device re-generates its Private Keys and ~~ensure that the Device's~~sits Device Certificates are stored on ~~the Device; and it;~~
- (d) ~~in the case of a Smart Meter only, ensure that at least~~unless one of the Organisation Certificates comprising the ~~Smart Meter's~~ Device Security

Credentials ~~is replaced (provided that for such~~ of the Device has already been replaced on the execution of a Command sent to that Device by the DCC during Commissioning, ensure that one such Certificate is replaced (and for these purposes an Organisation Certificate may be replaced with the same ~~Organisation~~ Certificate); and

(e) unless the Lead Supplier has previously done so following receipt of the Device from its manufacturer, interrogate the Device in order to confirm that, within its Device Security Credentials, the Organisation Certificate in the Trust Anchor Cell that has a Remote Party Role corresponding to 'Recovery' is the Recovery Certificate.

H5.38 ~~H5.36~~ If any one or ~~both~~ more of the steps in Section ~~H5.35~~ H5.37 (c) ~~or to (d) fails, as soon as reasonably practicable (and in any event with 7 days) following the Commissioning of the relevant Device~~ e) fails, the Lead Supplier ~~for that Device shall replace the Device.~~ shall, unless the relevant Device is replaced:

(a) ensure that the SMI Status of the Device is set to 'suspended';

(b) so far as reasonably practicable, continue to attempt the successful completion of the failed steps; and

(c) not subsequently seek to change the SMI Status of the Device unless either the failed steps are successfully completed or the Device is Decommissioned.

H5.39 Where, pursuant to Section H5.38(a), a Gas Proxy Function has its SMI Status set to 'suspended', the Responsible Supplier for any Smart Metering System of which that Gas Proxy Function forms part may replace the associated Communications Hub and may return it to the DCC in accordance with Section F8 (Removal and Return of Communications Hubs) relying on the reason specified at Section F9.5(f) (Reasons).

H5.40 ~~H5.37~~ As soon as reasonably practicable (and in any event within ~~7~~ 14 days) following the ~~Commissioning~~ commissioning of any Type 1 Device (other than as referred to in Section H5.33 or ~~H5.35~~ H5.37), the Lead Supplier shall send a Service Request in respect of that Device to: ensure that the Device Security Credentials which pertain to the Supplier Party are those of the Responsible Supplier.

- ~~(a) ensure that the Device Security Credentials which pertain to the Supplier Party are those of the Responsible Supplier; and~~
- ~~(b) re-generate its Private Keys and ensure that the Device's Device Certificates are stored on the Device.~~