APPENDIX AB

Service Request Processing Document

1 Introduction

1.1 This Appendix supplements Section H4 (Processing Service Requests) and sets out the obligations of the DCC and of each User in respect of communications via the DCC User Interface in respect of the following Services:

(a) Enrolment Services;

(b) Local Command Services;

(c) Core Communication Services; and

(d) Elective Communication Services.

2 Obligations of Users: Suspended Devices and Firmware

2.1 A User shall take all reasonable steps to ensure that it does not send Service Requests in relation to Devices that have an SMI Status of 'suspended', other than where:

(a) the Service Requests will (if Successfully Executed) result in the Device's Device Model becoming one that is listed on the Central Products List;

(b) it is necessary to do so in order to update the Device Security Credentials following a change of Responsible Supplier; or

(c) for SMETS1 Devices only, the User is requesting only the production of UTRNs for return to that User.

2.2 A User shall only send an 'Update Firmware' Service Request in respect of a Device or a SMETS1 CH if:

(a) the User has received the following information:

(i) the OTA Header and the associated replacement Manufacturer Image;

(ii) a Digital Signature, created by the person who created the Manufacturer Image, across the concatenation of the OTA Header and the associated replacement Manufacturer Image; and

(iii) the Hash of the replacement Manufacturer Image;

(b)   the User has successfully confirmed that the Digital Signature across the concatenation is that of the person who created the replacement Manufacturer Image (validated as necessary by reference to a trusted party);

(c)   the User has generated its own Hash from the replacement Manufacturer Image, and confirmed that the Hash that the User has generated is the same as the Hash provided; and

(d)   the User has confirmed that a Device Model associated with the replacement Manufacturer Image (as determined by the Hash and the information in the OTA Header) is currently on the Central Products List.

3   Obligations of Users: Pre-Commands and Signed Pre-Commands

3.1   Where a User receives a Pre-Command from the DCC, the User shall:

(a)   Check Cryptographic Protection for the Pre-Command;

(b)   Confirm Validity of the Certificate used to Check Cryptographic Protection for the Pre-Command; and

(c)   subject to the requirements of Clause 3.1(a) and (b) being satisfied, Correlate the Pre-Command.

3.2   Where Correlation of the Pre-Command demonstrates that it is substantively identical to the Service Request that led to the Pre-Command, the User may:

(a)   Digitally Sign the GBCS Payload of the Pre-Command to create the GBCS Payload of an associated Signed Pre-Command; and

(b)   send the associated Signed Pre-Command with its appropriate wrapper and Digital Signature to the DCC.

3.3   Where applicable, Users must comply with their obligations under Section G3.25 (Supply Sensitive Check).

4   Obligations of the User: Communications Received in Error

4.1   Where a User receives a communication via the DCC User Interface which that User was not entitled to receive in accordance with this Code, the User shall notify the DCC

in accordance with the Incident Management Policy.

5   Obligations of the DCC: SMETS2+ Communications Hub firmware

5.1   The DCC shall only send a communication to distribute different firmware to a SMETS2+ Communications Hub if:

(a)   the DCC has received the replacement Manufacturer Image and a Digital Signature, created by the person who created the Manufacturer Image, across that Manufacturer Image;

(b)   the DCC has received information about the Manufacturer Image sufficient to determine whether it is on the Central Products List;

(c)   the DCC has successfully confirmed that the Digital Signature across the replacement Manufacturer Image is that of the person who created the replacement Manufacturer Image (validated as necessary by reference to a trusted party); and

(d)   a Device Model associated with the replacement Manufacturer Image is currently on the Certified Product List, as determined by:

(i)   the Hash the DCC calculates over the Manufacturer Image; and

(ii)   the information about the Manufacturer Image provided pursuant to Clause 5.1(b).

5.2   The DCC shall notify relevant Users of its intention to activate replacement Manufacturer Images in relation to Communications Hubs at least 7 days in advance of doing so; provided that DCC need not notify Users in advance if the activation of the replacement Manufacturer Images is required for urgent security related reasons (and in such circumstances the DCC shall take reasonable steps to notify Users in advance of activating replacement Manufacturer Images or, where it has not notified them in advance, shall notify them of having done so as soon as is reasonably practicable after the event).

6   Obligations of the DCC: Processing Service Requests

6.1   Subject to Clause 18 (Obligations of the DCC: Non-Device Service Requests), where

the DCC receives a Service Request from a User, the DCC shall send an Acknowledgement to the User, and (whether before or after such Acknowledgement is sent) apply the following checks:

(a)   Verify the Service Request;

(b)   confirm that the Service Request has been sent by a User whose right to send that Service Request has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for that Service Request;

(c)   in the case of Non-Critical Service Requests (other than an 'Update Firmware' Service Request, a 'CoS Update Security Credentials' Service Request or a 'Top Up Device' SMETS1 Service Request with a Command Variant value of 2)) and SMETS1 Critical Service Requests, confirm that the SMI Status of the Device identified in the Service Request is: (i) 'commissioned'; (ii) 'installed not commissioned'; (iii) 'whitelisted'; or (iv) 'pending';

(d)   Check Cryptographic Protection for the Service Request;

(e)   Confirm Validity of the Certificate used to Check Cryptographic Protection for the Service Request;

(f)   subject to Clause 6.2, in the case of Non-Critical Service Requests and SMETS1 Critical Service Requests, confirm (using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory) that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request:

(i)   for all times within any date range requested;

(ii)   where there is no such date range, at the specified time for execution; or

(iii)   where there is no date range and no date for execution is specified, at the time at which the check is being carried out;

(g)   in the case of a 'CoS Update Security Credentials' Service Request, confirm that

the User ID contained within each of the Organisation Certificates included within the Service Request is associated with the User submitting the Service Request and that the MPRN or MPAN included within the Service Request is Associated with the Device identified within the Service Request;

(h)   in the case of a 'Restore HAN Device Log' or a 'Restore Gas Proxy Function Device Log' Service Request, confirm that the Device Log Data to be restored originates from a Communications Hub Function or Gas Proxy Function that forms (or formed immediately prior to its replacement) part of a Smart Metering System for which the User making such Service Request is (or, immediately prior to its replacement, was) the Responsible Supplier;

(i)   in the case of an 'Update Firmware' Service Request, confirm that the Hash calculated across the Manufacturer Image contained within the Service Request is the same as the entry within the Central Products List (as identified by the Device ID, information in the Smart Metering Inventory and the firmware version specified in the Service Request);

(j)   in the case of any Service Request that contains any Certificates, Confirm Validity of those Certificates;

(k)   in the case of an 'Update HAN Device Log' Service Request requesting the addition of a Smart Meter to the Device Log of a Communications Hub Function confirm (using the Registration Data and the MPRN or MPAN in the Service Request) that the User sending the Service Request is a Responsible Supplier in respect of that MPRN or MPAN;

(l)   in the case of a 'Set CHF Sub GHz Configuration' Service Request, that the settings requested would only allow a CHF to use Sub GHz Available Channels (as defined in the GBCS); and

(m)   in respect of a SMETS1 Critical Service Request, a 'Request Handover of DCC Controlled Device' SMETS1 Service Request, a 'CoS Update Security Credentials' SMETS1 Service Request or a 'Top Up Device' SMETS1 Service Request, confirm that the Service Request is not a Replay.

6.2   The step set out at Clause 6.1(f) shall not apply in the following circumstances (and,

where it is necessary to identify a Responsible Supplier, the DCC shall do so using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory):

(a)   an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Smart Meter sends a 'Join Service' Service Request to join that Gas Smart Meter to a Gas Proxy Function;

(b)   an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Proxy Function sends a 'Restore GPF Device Log' Service Request to restore the Device Log of that Gas Proxy Function; or

(c)   the Service Request has been sent by a User acting in the User Role of 'Other User'.

6.3   Where any of the checks in Clause 6.1 are not satisfied in respect of a Service Request, the DCC shall not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Service Request (and, save where Clause 6.1(d) is not satisfied, notify the User of such rejection and of the reasons for such rejection via the DCC User Interface).

6.4   Clause 6.5 shall apply subject to:

(a)   (in relation to SMETS2+ Service Requests only) Clauses 8 (Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and Corresponding Pre-Commands), 9 (Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests), and 11 (User and DCC Obligations: 'Join Service' and 'Unjoin' Service Requests for Pre-Payment Meter Interface Devices and Gas Smart Meters); and

(b)   (for all Service Requests) Clause 18 (Obligations of the DCC: Non-Device Service Requests).

6.5   Subject to Clause 6.4, where all of the requirements of Clause 6.1 are satisfied in respect of a Service Request, the DCC shall:

(a)   where the Service Request is not a SMETS1 Service Request, Transform the Service Request and:

    (i)   in the case of a Non-Critical Service Request, send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands); or

    (ii)   in the case of a Critical Service Request, send the Transformed Service Request to the User who submitted the Service Request;

(b)   where the Service Request is a SMETS1 Service Request and the DCC is holding a stored SMETS1 Future Dated Critical Service Request which:

    (i)   is addressed to the same Device; and

    (ii)   has the same Service Reference Variant,

delete the stored SMETS1 Future Dated Critical Service Request;

(c)   where the Service Request is a SMETS1 Service Request but is not a SMETS1 Future Dated Critical Service Request:

    (i)   identify the relevant SMETS1 Service Provider using the target Device ID within the Service Request;

    (ii)   create the contents of a Countersigned Service Request and Countersign it; and

    (iii)   send the Countersigned Service Request to the relevant SMETS1 Service Provider; and

(d)   where the Service Request is a SMETS1 Future Dated Critical Service Request:

    (i)   create a stored SMETS1 Future Dated Critical Service Request (unless the execution date/time has been set by the User to Never); and

    (ii)   unless removed in the interim in accordance with Clause 6.5(b), at the execution date/time specified in the stored SMETS1 Future Dated Critical Service Request, re-apply all requirements of Clause 6.1 except for Clause 6.1(m) and, where all of the requirements of Clause 6.1 (other than 6.1(m))

are met:

    (A)   create the contents of a Countersigned Service Request and Countersign it;

    (B)   send the Countersigned Service Request to the relevant SMETS1 Service Provider; and

    (C)   once the DCC (including, where relevant, the SMETS1 Service Provider) has completed its processing in relation to the Countersigned Service Request, delete the stored SMETS1 Future Dated Critical Service Request.

7   Obligations of the DCC: Processing Signed Pre-Commands

7.1   Where the DCC receives a Signed Pre-Command from a User, the DCC shall provide an Acknowledgement to the User and (whether before or after such Acknowledgement is sent) apply the following checks:

    (a)   Verify the Signed Pre-Command;

    (b)   confirm that the Signed Pre-Command has been sent by a User whose right to send that message has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for a Service Request of the type corresponding with the Signed Pre-Command;

    (c)   Check Cryptographic Protection for the Signed Pre-Command; and

    (d)   Confirm Validity of the Certificate used to Check Cryptographic Protection for the Signed Pre-Command.

7.2   Subject to Clauses 14 (Obligations of the DCC: Orchestration of Service Requests), where all of the requirements of Clause 7.1 are satisfied, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands).

7.3   Where any of the checks in Clause 7.1 are not satisfied in respect of a Signed Pre-Command, the DCC shall not be obliged to undertake any of the other checks that

remain to be undertaken, and the DCC shall:

(a)   reject the Signed Pre-Command; and

(b)   save where Clause 7.1(d) is not satisfied, notify the User of such rejection and of the reasons for such rejection via the DCC User Interface.

8   Obligations of the DCC: 'CoS Update Security Credentials' Service Requests (other than SMETS1 Service Requests) and Corresponding Pre-Commands

8.1   The following shall apply in respect of each 'CoS Update Security Credentials' Service Request which is not a SMETS1 Service Request:

(a)   where all of the requirements of Clause 6.1 are satisfied in respect of such a Service Request, the DCC shall send a Digitally Signed communication containing the CoS Update Security Credentials Service Request to the CoS Party; and

(b)   following receipt of the resulting communication, and immediately prior to creating any corresponding Update Security Credentials Signed Pre-Command referred to in Clause 8.2, the CoS Party shall:

(i)   Check Cryptographic Protection for both the communication and for the Service Request included within it;

(ii)   Confirm Validity of the Certificates used to Check Cryptographic Protection for both the communication and for the Service Request included within it;

(iii)   confirm that User ID of the User who submitted the Service Request and the User ID contained within in each of the Organisation Certificates included within the Service Request are all associated with the same User; and

(iv)   confirm that the User ID in each of the Organisation Certificates included within the Service Request is that of the Party who is identified via:

(A)   the relevant MPRN or MPAN (as applicable) included within the Service Request; and

10

(B)   the Registration Data for that relevant MPRN or MPAN,

as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

8.2   Where, in respect of the communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are satisfied, the CoS Party shall:

(a)   generate the GBCS Payload of an 'Update Security Credentials' Signed Pre-Command that is substantively identical to the 'CoS Update Security Credentials' Service Request;

(b)   Digitally Sign the GBCS Payload; and

(c)   send the resultant communication as a Signed Pre-Command to the DCC.

8.3   Where, in respect of a communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are not satisfied:

(a)   the CoS Party shall not undertake any further processing of the communication, and shall notify the DCC; and

(b)   the DCC shall notify the User that sent the original Service Request that the Service Request cannot be processed (such notification to be sent via the DCC User Interface).

8.4   Where the DCC receives a Signed Pre-Command from the CoS Party, the DCC shall apply the following checks:

(a)   confirm that the User ID within each Organisation Certificate within the Signed Pre-Command is the same as the User ID within the corresponding Organisation Certificate in the original 'CoS Update Security Credentials' Service Request;

(b)   confirm that the Device ID within the Signed Pre-Command is the same as the Device ID included in the corresponding 'CoS Update Security Credentials' Service Request;

(c)   confirm that the message originated from the CoS Party by Checking the Cryptographic Protection for the message;

(d)   Confirm Validity of the Certificate used to Check Cryptographic Protection for the message;

(e)   Confirm Validity of all Certificates contained within the Signed Pre-Command; and

(f)   Confirm that the User ID in each of the Organisation Certificates included within the Signed Pre-Command is that of the Party who is identified via:

(i)   the relevant MPRN or MPAN (as applicable) with which the Device specified in the Signed Pre-Command is associated in the Smart Metering Inventory; and

(ii)   the Registration Data for that relevant MPRN or MPAN,

as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

8.5   Subject to Clause 14 (Orchestration of Service Requests), where all of the requirements of Clause 8.4 are satisfied in respect of a Signed Pre-Command received from the CoS Party, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands).

8.6   Where any of the checks in Clause 8.4 are not satisfied in respect of a Signed Pre-Command received from the CoS Party, the DCC shall:

(a)   not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Signed Pre-Command;

(b)   save where Clause 8.4(c) is not satisfied, notify the CoS Party of such rejection and of the reasons for such rejection; and

(c)   notify the User that sent the original 'CoS Update Security Credentials' Service Request.

9 **Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests**

9.1 This Clause 9 only applies to 'Request Handover of DCC Controlled Device' Service Requests that are not SMETS1 Service Requests. Where all of the requirements of Clause 6.1 are satisfied in relation to such a Service Request, the DCC shall:

(a) generate the corresponding GBCS Payload (corresponding in this case meaning that the Service Request and the GBCS Payload request the replacement of the same Device Security Credentials on the same Device at the same time);

(b) Digitally Sign the GBCS Payload; and

(c) Confirm Validity of any Certificates contained within the communication.

9.2 Where all of the requirements of Clause 9.1 are satisfied in respect of such a communication, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands).

9.3 Where any of the checks in Clause 9.1 are not satisfied in respect of such a communication, the DCC shall not undertake any of the other checks that remain to be undertaken, and the DCC shall reject the communication and notify the User that sent the original 'Request Handover of DCC Controlled Device' Service Request (such notification to be sent via the DCC User Interface).

10 **User and DCC Obligations: 'Restore HAN Device Log' Service Requests**

10.1 Where a Supplier Party replaces a Communications Hub (other than a SMETS1 CH) in a premises then that Supplier Party must, as soon as reasonable practicable after the replacement, send the necessary Service Requests to the DCC to ensure that:

(a) the Device Log of the new Communications Hub Function replicates that of the old Communications Hub Function;

(b) the Device Log of the new Gas Proxy Function is replaced with that of the old Gas Proxy Function (or replicates that of the old Gas Proxy Function);

(c) following steps (a) and (b) above, the new Gas Proxy Function is added to the Device Log of the Gas Smart Meter; and

(d)   following the step set out in (c) above, the Communications Hub Function and the Gas Proxy Function comprising the Communications Hub that has been replaced are decommissioned (through the sending of a 'Decommission Device' Service Request).

10.2   An Import Supplier shall not send a Service Request to add or remove a Gas Proxy Function to or from the Device Log of a Gas Smart Meter other than as part of managing the replacement of a Communications Hub (by it or another Responsible Supplier) pursuant to Clause 10.1.

10.3   The DCC shall, following the decommissioning of a Communications Hub Function and the associated Gas Proxy Function (arising as a consequence of the processing of a 'Decommission Device' Service Request), send a DCC Alert to all Responsible Suppliers and Network Parties for Smart Metering Systems which incorporated either or both of those Devices, notifying them of the decommissioning (other than to the Responsible Supplier which sent the 'Decommission Device' Service Request).

10.4   The DCC shall, where it has processed a Service Request which successfully replaces the Device Log of a Communications Hub Function, send a DCC Alert to all Responsible Suppliers for that Communications Hub Function (other than the Responsible Supplier which sent the original Service Request) notifying them of the replacement.

10.5   The DCC shall, where it has processed a Service Request to successfully replace the Device Log of a Gas Proxy Function, send a DCC Alert to the Gas Supplier who is the Responsible Supplier for that Gas Proxy Function (save where it is the Gas Supplier that has sent the Service Request).

11   Obligations of the DCC: 'Join Service' and 'Unjoin' Service Requests for Pre-Payment Meter Interface Devices and Gas Smart Meters

11.1   Where all of the requirements of Clause 6.1 are satisfied in respect of a 'Join Service' or 'Unjoin Service' Service Request for a Pre-Payment Meter Interface Device, or a Gas Smart Meter and where the Service Request is not a SMETS1 Service Request, the DCC shall:

(a)   Transform the Service Request;

(b)   where a Pre-Payment Meter Interface Device is to be joined to a Gas Smart Meter, include within the resultant communication the Device Certificate of the relevant Gas Smart Meter that has a key usage of 'keyAgreement';

(c)   where a Gas Smart Meter is to be joined to a Pre-Payment Meter Interface Device, include within the resultant communication the Device Certificate of the relevant Pre-Payment Meter Interface Device that has a key usage of 'keyAgreement';

(d)   where the resultant communication is destined for a Pre-Payment Meter Interface Device, Digitally Sign the Communication and send the associated Command in accordance with Clause 13 (Obligations of the DCC: Sending Commands); and

(e)   where the resultant communication is ultimately destined for a Gas Smart Meter, send the resultant communication as a Pre-Command to the User that sent the original Service Request.

11.2   Where the DCC receives a Response in respect of a Command sent to join or unjoin a Pre-Payment Meter Interface Device, the DCC shall send the Response (as a Service Response) to the User that sent the corresponding Service Request.

12   Threshold Anomaly Detection

12.1   The DCC shall apply Threshold Anomaly Detection where an Anomaly Detection Threshold has been established under Section G6 (Anomaly Detection Thresholds) in respect of the SMETS1 Service Request, Transformed Service Request or Signed Pre-Command.

12.2   Where the DCC applies Threshold Anomaly Detection to either a SMETS1 Service Request, a Transformed Service Request or a Signed Pre-Command and the check is failed, the DCC shall, subject to Clause 21 of the SMETS1 Supporting Requirements, notify the User and quarantine the SMETS1 Service Request, Transformed Service Request or Signed Pre-Command.

12.3   Where the DCC has quarantined a SMETS1 Service Request, Transformed Service Request or Signed Pre-Command it shall maintain such quarantine until:

(a) such time as the relevant User instructs the DCC to process the Service Request or Signed Pre-Command, in which case the DCC shall continue to process the Service Request or Signed Pre-Command in accordance with the provisions of this Service Request Processing document;

(b) the Service Request or Signed Pre-Command is confirmed by the User to be anomalous or to otherwise require deletion, in which case the DCC shall delete it from the DCC Systems; or

(c) the Service Request or Signed Pre-Command is required to be deleted in accordance with the Threshold Anomaly Detection Procedures, in which case the DCC shall delete it from the DCC Systems.

12.4 Where the DCC applies Threshold Anomaly Detection (other than in relation to a value of the type referred to in (b)(ii) of the definition of Anomaly Detection Threshold) to a Signed Pre-Command, Transformed Service Request or SMETS1 Service Request (for the purposes of this Clause, each being a "**Relevant Communication**"), the DCC shall:

(a) determine the Service Reference Variant of the Service Request that pertains to the Relevant Communication;

(b) determine the cumulative number of all other Relevant Communications to which that Service Reference Variant pertains that it has processed over the period of time to which the Anomaly Detection Threshold relates;

(c) increment the cumulative number by 1; and

(d) compare that incremented cumulative number to the relevant Anomaly Detection Threshold.

13 DCC Obligations: Sending Commands

13.1 Where the DCC is required to send a Command (other than an Instruction), it shall only apply any necessary Message Authentication Code to the relevant communication and send the resulting Command if:

(a)   Threshold Anomaly Detection has been applied to the associated Transformed Service Request or Signed Pre-Command (or, where in response to a Service Request from an Eligible User a Command is to be Digitally Signed by the DCC, that Command prior to the addition of a Message Authentication Code); and

(b)   either (i) the Threshold Anomaly Detection check is passed; or (ii) the User that sent the original Service Request or Signed Pre-Command has instructed DCC to process a quarantined Service Request or Signed Pre-Command in accordance with Clause 12.3(a).

13.2   Where the requirements of Clause 13.1 are met, the DCC shall apply the required Message Authentication Code (as required by the GB Companion Specification) to the relevant communication to create a Command and send that Command to (as specified in the originating Service Request):

(a)   the relevant Device (provided that this option is only available in respect of Devices associated with Commissioned Communications Hub Functions); and/or

(b)   the User who sent the originating Service Request via the DCC User Interface.

13.3   Where a Transformed Service Request (other than a SMETS1 Service Request) is received by the DCC Systems that apply Message Authentication Codes, the DCC shall:

(a)   undertake no further processing of that Service Request; and

(b)   raise an Incident.

14   DCC Obligations: Sending Countersigned Service Requests

14.1   Where the DCC is required to send a Countersigned Service Request, it shall only Countersign the relevant communication and send the resulting Countersigned Service Request to the relevant SMETS1 Service Provider if:

(a)   Threshold Anomaly Detection has been applied to the Service Request (provided that the DCC shall not be required to apply Threshold Anomaly Detection in relation to Anomaly Detection Thresholds of the type referred to in

Sub-Paragraph (b)(ii) of the definition of Anomaly Detection Threshold; and

(b)   either (i) the Threshold Anomaly Detection check is passed; or (ii) the User that sent the original Service Request has instructed DCC to process the quarantined Service Request in accordance with Clause 12.3(a).

15   Orchestration of Service Requests

15.1   In the case of a Service Request for a Sequenced Service, the DCC shall:

(a)   where the Service Request is not a SMETS1 Service Request, only send the Command following the Successful Execution of the Command resulting from the Service Request upon which such Sequenced Service is dependent; and

(b)   where the Service Request is a SMETS1 Service Request, only send the Countersigned Service Request to the relevant SMETS1 Service Provider following the Successful Execution of the Equivalent Step(s) resulting from the Service Request upon which such Sequenced Service is dependent.

15.2   The DCC shall ensure that it sends each 'Update Security Credentials' Command resulting from a 'CoS Update Security Credentials' Service Request as close to the specified execution time as is reasonably practicable whilst still allowing time for the Command to be received and executed by the relevant Device.

15.3   The DCC shall not continue to process any Service Requests (or associated Pre-Commands or Signed Pre-Commands) where the services have been cancelled in accordance with Sections H3.18 to H3.20 (Cancellation of Future-Dated or Scheduled Services).

16   Obligations of a SMETS1 Service Provider: Countersigned Service Request Processing

16.1   Where a SMETS1 Service Provider receives a Countersigned Service Request from the DCC, the SMETS1 Service Provider shall apply the following checks:

(a)   Check Cryptographic Protection for the both the Countersigned Service Request and for the Service Request included within it;

(b)   Confirm Validity of all Certificates used to Check Cryptographic Protection for

both the Countersigned Service Request and for the Service Request included within it;

(c)   confirm it is the relevant SMETS1 Service Provider for the Device(s) identified in the Countersigned Service Request;

(d)   if the Countersigned Service Request contains a Critical Service Request, a 'CoS Update Security Credentials' SMETS1 Service Request or a 'Request Handover of DCC Controlled Device' SMETS1 Service Request, apply the checks at Clause 6.1, except for those at Clauses 6.1 (d) and (e), to the Service Request contained within the Countersigned Service Request; and

(e)   if the Countersigned Service Request contains an 'Update Firmware' Service Request, then:

(i)   if it is destined for a Communications Hub, Check Cryptographic Protection for the Upgrade Image contained within the Service Request using the relevant Device Security Credentials that relate to the Import Supplier for the relevant SMETS1 CHF and Confirm Validity for all of the Certificates used to Check Cryptographic Protection; or

(ii)   if it is destined for a Smart Meter, Check Cryptographic Protection for the Upgrade Image contained within the Service Request using the relevant Device Security Credentials held that relate to the Responsible Supplier for the Device and Confirm Validity for all of the Certificates used to Check Cryptographic Protection.

16.2   Only where all of the requirements of Clause 16.1 are satisfied, the SMETS1 Service Provider shall:

(a)   in the case of a Countersigned Service Request that contains a Service Request with Service Reference Variant 2.2 (Top Up Device):

(i)   apply Threshold Anomaly Detection in the circumstances where a relevant Anomaly Detection Threshold of the type referred to in Sub-Paragraph (b)(ii) of the definition of Anomaly Detection Threshold has been set ; and

(ii) if the checks in Sub-Clause (a)(i) are passed, undertake further processing as required by the SMETS1 Supporting Requirements;

(b) in relation to any other Service Request contained within a Countersigned Service Request, for the target Device identified within the Service Request:

(i) apply Threshold Anomaly Detection in the circumstances where a relevant Anomaly Detection Threshold has been set pursuant to Section G6.6(b); and

(ii) if the checks in Sub-Clause (b)(i) are passed, ensure that the Equivalent Steps are taken and that either the resultant SMETS1 Response or a SMETS1 Service Provider Alert is generated; and

(c) ensure that any resulting SMETS1 Response or SMETS1 Alert is Digitally Signed, and send any such SMETS1 Response or SMETS1 Alert to the DCC.

17 Obligations of the DCC: Service Responses and Alerts

17.1 Where the DCC receives an Alert from a Communications Hub Function, the DCC shall Digitally Sign the Alert, and send it as a DCC Alert to (as specified in the DCC User Interface Specification) the Responsible Supplier(s), the Electricity Distributor and/or the Gas Transporter for the Smart Metering Systems of which the Communications Hub Function forms part (as identified in the Registration Data).

17.2 Where the DCC receives from a Device either a Response that is destined for a Remote Party or an Alert which is destined for one or more Remote Parties and/or Supplementary Remote Parties, then the DCC shall send the Response (as a Service Response) or the Alert (as a DCC Alert or Device Alert) to those Remote Parties and/or Supplementary Remote Parties as prescribed by the DCC User Interface Specification.

17.3 Where the DCC receives from an SMETS1 Service Provider:

(a) a SMETS1Response;

(b) a SMETS1 Alert; or

(c) a S1SP Alert,

which is destined for one or more Remote Parties and/or Supplementary Remote Parties, then the DCC shall Countersign the relevant communication and send it to those Remote Parties and/or Supplementary Remote Parties as prescribed by the DCC User Interface Specification as a Countersigned SMETS1 Response, a Countersigned SMETS1 Alert or Countersigned SISP Alert.

17.4   Where the DCC successfully processes a Service Request to replace the Security Credentials of a User that are held on a Device, or to place a User's Security Credentials on to a Device, then (other than to the extent that the User is notified via a Service Response) the DCC shall send a DCC Alert to the relevant User informing it of the change.

17.5   Where the DCC successfully processes a Service Request that changes the Security Credentials of a User that are held by a SMETS1 Service Provider in relation to a Device then (other than to the extent that the User is notified via a Countersigned SMETS1 Response) the DCC shall send a DCC Alert to the relevant User informing it of the change.

17.6   Where the DCC receives a Response or an Alert from a Device which is destined for an Unknown Remote Party, the DCC shall:

(a)   Check Cryptographic Protection for the Response or Alert;

(b)   Confirm Validity of the Certificate used to Check Cryptographic Protection for the Response or Alert; and

(c)   subject to (a) and (b) being successful, send the Response (as a Service Response) or the Alert (as a Device Alert or DCC Alert) to the recipient(s) identified in the Response or Alert.

17.7   Where the DCC receives a Sub GHz Alert (as defined in the GBCS) from a Communications Hub Function, the DCC shall:

(a)   Check Cryptographic Protection for the Sub GHz Alert;

(b)   Confirm Validity of the Certificate used to Check Cryptographic Protection for the Sub GHz Alert; and

(c)   subject to (a) and (b) being successful, create a DCC Alert containing the Sub GHz Alert, Digitally Sign the DCC Alert, and send the signed DCC Alert to the Responsible Supplier(s) for the Smart Metering System(s) of which the Communications Hub Function forms part (as identified using the Registration Data).

18   Obligations of the DCC: Non-Device Service Requests

18.1   Where the DCC receives a Non-Device Service Request from a User, the obligations of the DCC under this Appendix shall be modified as follows (and where a Non-Device Service Request is not specifically identified below, they shall be applied un-modified):

(a)   the DCC shall not send an Acknowledgement in respect of the Service Request;

(b)   the checks set out in Clause 6.1 shall be modified as follows:

    (i)   the check set out in Clause 6.1(c) does not apply to the following Service Requests:

        (A)   'Update Inventory';

        (B)   'Read Inventory';

        (C)   'Request WAN Matrix';

        (D)   'Device Pre-notification';

        (E)   'Communications Hub Status Update- Install Success';

        (F)   'Communications Hub Status Update - Install No SM WAN';

        (G)   'Communications Hub Status Update – Fault Return'; and

        (H)   'Communications Hub Status Update – No Fault Return'; and

    (ii)   the check set out in the Clause 6.1(f) does not apply to the following Service Requests:

        (A)   'Read Inventory';

        (B)   'Request WAN Matrix';

(C) 'Device Pre-notification';

(D) 'Communications Hub Status Update- Install Success';

(E) 'Communications Hub Status Update - Install No SM WAN';

(F) 'Communications Hub Status Update – Fault Return'; and

(G) 'Communications Hub Status Update – No Fault Return';

(c) the DCC shall not, in any event, be required to apply Threshold Anomaly Detection in relation to Non-Device Service Requests;

(d) where the checks set out in Clause 6.1 (as modified by this Clause 18) are satisfied, the DCC shall not Transform the Service Request or Countersign a Countersigned Service Request (as would otherwise be required by Clause 6) and shall instead send the User a Service Response notifying the User whether or not the Non-Device Service Request has been successful, and where successful:

(i) in the case of any Non-Device Service Request that changes or creates information held (or intended to be reflected) on the DCC Systems (including the Smart Metering Inventory), update the information held on DCC Systems accordingly; and/or

(ii) in the case of a 'Read Inventory' or 'Request WAN Matrix' Service Request, include within the Service Response the relevant information requested by the Service Request;

(iii) in the case of a 'Device Pre-Notification' Service Request, add the relevant Device to the Smart Metering Inventory with an SMI Status of 'pending';

(iv) in the case of a 'Create Schedule' Service Request,

(A) create a schedule of the Service Request type identified in the 'Create Schedule' Service Request;

(B) include within the Service Response the identifier of any

23

schedule that has been successfully created;

(C)   at each point in time set out in the schedule (and subject to the further arrangements set out in the DCC User Interface Specification), create a Service Request (without a Digital Signature from the User) of the appropriate type and in relation to the relevant Device (in each case as specified in the original 'Create Schedule' Service Request);

(D)   process the Service Requests referred to in (C) above in accordance with Clause 6 as if they had been received from the User that sent the original 'Create Schedule' Service Request, provided that the checks identified under Clause 6.1(c) and 6.1(d) do not apply;

(v)   in the case of a 'Read Schedule' Service Request, where it is received from the same User that sent the originating 'Create Schedule' Service Request for all schedules identified within it, include within the Service Response details of the relevant schedule(s) so identified (and otherwise reject the 'Read Schedule' Service Request, and notify (via the Service Response) the User that sent the Service Request of such rejection);

(vi)   in the case of a 'Delete Schedule' Service Request, where it is received from the same User that sent the originating 'Create Schedule' Service Request for all schedules identified within it, delete the relevant schedule(s) so identified (and otherwise reject the 'Delete Schedule' Service Request, and notify (via the Service Response) the User that sent the Service Request of such rejection);

(vii)   in the case of a 'Decommission Device' Service Request:

(A)   set the SMI Status of the relevant Device to 'decommissioned';

(B)   where the relevant Device is a Smart Meter, disassociate the Device in the Smart Metering Inventory from any MPRN or MPAN with which it is Associated; and

(C)   where the relevant Device is a Communications Hub Function, set the SMI status of the associated Gas Proxy Function to 'decommissioned'; or

(viii)   in the case of an 'Update Firmware' Service Request:

(A)   include within the Service Response the details of any Devices that were listed within the Service Request to which, by virtue of the checks DCC has carried out, DCC does not propose to send a communication to update the firmware; and

(B)   to all other Devices so listed, send a communication to update the firmware of those Devices ensuring that the communication reaches the SMETS1 CHF (in the case of updates to a SMETS1 CHF) or (in the case of updates to all other Devices) the Communications Hub Functions associated with all such Devices (in each case, within the timescales specified in the DCC User Interface Services Schedule).

19   Incident Management

19.1   Where the Device Security Credentials of a Device erroneously include Data from one or more of a Party's Organisation Certificates, that Party shall cooperate with other Parties in order to rectify the position (including, were necessary, by sending Service Requests to update the Device Security Credentials).