Draft Legal Text

SECMP0058:

Changes to the governance of the Self-Service Interface

SECAS Contact:

Name:

Joe Hehir

Number:

020 7770 6874

Email:

SEC.change@gemserv.com

Summary

This modification seeks to remove the Self-Service Interface Design Specifications from the SEC and include them in a new lower level document which is created and maintained by the DCC with any future changes being consulted on and agreed by the SEC Panel. This will ensure that improvements can be implemented to the Self-Service Interface in a timelier manner whilst also ensuring that the industry remain in control of what new functionality is deployed, along with the associated costs.

About this document

This document contains the draft SEC legal text that will deliver the intent of SECMP0058.

Administered by Gemserv, 8 Fenchurch Place, London EC3M 4AJ

1. Draft Legal Text

This section sets out the draft Legal Text Changes for SECMP0058. These changes have been drafted against the Smart Energy Code (SEC) version 5.23[1].

Section A 'Definitions and Interpretations'

Add the following definition in alphabetical order

SSI Baseline Requirements Document	means a document produced and maintained by the DCC in accordance with the Self-Service Interface Access Control Specification.

Amend the following definitions

Self-Service Interface ~~Design~~ Access Control Specification	means the SEC Subsidiary Document of that name set out in Appendix AH.
Technical Code Specifications	means the Technical Specifications, the GB Companion Specification, the DCC Gateway Connection Code of Connection, the DCC User Interface Code of Connection, the DCC User Interface Specification, the Self-Service Interface ~~Design~~ Access Control Specification, the SSI Baseline Requirements Document, the Self-Service Interface Code of Connection, the Registration Data Interface Documents, the Message Mapping Catalogue, the Incident Management Policy, the DCC Release Management Policy, the Panel Release Management Policy, the SMKI Interface Design Specification, the

[1]Note that if a new version of the SEC is designated before the submission of the Final Modification Report to the Change Board or Authority, the drafting will be checked to make sure there are no consequential impacts.

SMKI Code of Connection, the SMKI Repository Interface Design Specification, the SMKI Repository Code of Connection, and the SMETS1 Supporting Requirements.

Section H 'DCC Services'

Amends Section H8.15(a)

Self-Service Interface

H8.15 The DCC shall maintain and keep up-to-date an interface (the **Self-Service Interface**) which:

(a) complies with the specification required by the Self-Service Interface ~~Design~~ Access Control Specification and the SSI Baseline Requirements Document;

(b) is made available to Users in accordance with the Self-Service Interface Code of Connection via DCC Gateway Connections; and

(c) allows each User to access the information described in Section H8.16 as being accessible to that User (and also allows other Users to access that information to the extent permitted by the first User in accordance with the Self-Service Interface ~~Design~~ Access Control Specification).

H8.16 The Self-Service Interface must (as a minimum) allow the following categories of User to access the following:

(a) the Smart Metering Inventory, which shall be available to all Users and capable of being searched by reference to the following (provided that there is no requirement for the DCC to provide information held on the inventory in respect of Type 2 Devices other than IHDs):

(i) the Device ID, in which case the User should be able to extract all

information held in the inventory in relation to (I) that Device, (II) any other Device Associated with the first Device, (III) any Device Associated with any other such Device; and (IV) any Device with which any of the Devices in (I), (II) or (III) is Associated;

(ii) the MPAN or MPRN, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meter to which that MPAN or MPRN relates, or in relation to any Device Associated with that Smart Meter or with which it is Associated;

(iii) post code and premises number or name, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked to that postcode and premises number or name, or in relation to any Device Associated with those Smart Meters or with which they are Associated;

(iv) the UPRN (where this has been provided as part of the Registration Data), in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked by that UPRN, or in relation to any Device Associated with those Smart Meters or with which they are Associated;

(b) a record of the Service Requests and Signed Pre-Commands sent by each User, and of the Acknowledgments, Pre-Commands, Service Responses and Alerts received by that User (during a period of no less than three months prior to any date on which that record is accessed), which shall be available only to that User;

(c) a record, which (subject to the restriction in Section I1.4 (User Obligations)) shall be available to all Users:

(i) of all 'Read Profile Data' and 'Retrieve Daily Consumption Log' Service Requests in relation to each Smart Meter (or Device Associated with it) that were sent by any User during a period of no less than three months prior to any date on which that record is accessed; and

(ii) including, in relation to each such Service Request, a record of the type of the Service Request, whether it was successfully processed, the time and date that it was sent to the DCC, and the identity of the User which sent it;

(d) the Incident Management Log, for which the ability of Users to view and/or amend data shall be as described in Section H9.4 (Incident Management Log);

(e) the CH Order Management System, which shall be available to all Users;

(f) any and all information in respect of the SMETS1 SM WAN as the DCC is required to make available under the Self-Service Interface ~~Design~~ Access control Specification and the SSI Baseline Requirements Document, which shall be made available to all Users; and the following information in respect of the SMETS2+ SM WAN, which shall be available to all Users (and which shall be capable of interrogation by post code and postal outcode):

(i) whether a Communications Hub Function installed in a premises at any given location:

(A) is expected to be able to connect to the SM WAN;

(B) is expected to be able to connect to the SM WAN from a particular date before 1 January 2021, in which case the date shall be specified; or

(C) cannot be confirmed as being able to connect to the SM WAN before 1 January 2021;

(ii) any known issues giving rise to poor connectivity at any given location (and any information regarding their likely resolution); and

(iii) any requirement to use a particular WAN Variant (and, where applicable, in combination with any particular Communications Hub Auxiliary Equipment) for any given location in order that the Communications Hub will be able to establish a connection to the SM

WAN;

(g) additional information made available by the DCC to assist with the use of the Services and diagnosis of problems, such as service status (including information in respect of Planned Maintenance and Unplanned Maintenance) and frequently asked questions (and the responses to such questions), which shall be available to all Users; and

(h) anything else expressly required by a provision of this Code.

Appendix I 'CH Installation and Maintenance Support Materials'

Updates to references in Appendix I

5 **COMMUICATIONS HUB DIAGNOSTICS**

5.1 Where, following successful installation of a Communications Hub and Commissioning of the related Communications Hub Function, a Supplier Party identifies a potential Communications Hub fault, pursuant to Section H9.6 of the Code, that Supplier Party shall take all reasonable steps to complete the Communications Hub Availability and Diagnostics Check procedure prior to raising an Incident with the DCC.

Communications Hub Availability and Diagnostics Check

5.2 A Supplier Party may undertake a Communications Hub Availability and Diagnostics Check, by either:

(a) utilising the Self-Service Interface to complete the Communications Hub availability and diagnostic check as defined in the Self-Service Interface ~~Design~~ Access Control Specification and the SSI Baseline Requirements Document; or

(b) sending Service Requests 6.13: (Read Event or Security Log) for the CHF event log and Service Request 8.9: (Read Device Log) for the CHF Device Log, in accordance with DUIS and interpreting the Service Responses received.

Appendix AH 'Self Service Interface Design Specification'

Please see the full Appendix AH redlining provided in a separate attachment

Appendix AI 'Self-Service Interface Code of Connection'

Amends definitions in Appendix AI

Definitions

In this document, except where the context otherwise requires:

- expressions defined in section A1 of the Code (Definitions) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- any expressions not defined here or in section A1 of the Code have the meaning given to them in the Self-Service Interface ~~Design~~ Access Control Specification, the SSI Baseline Requirements Document or the DCC User Interface Specification.

Updates to references in Appendix AI

Communications Authentication

1.14 Each User shall install a valid Root DCCKICA Certificate, UI DCCKICA Certificate and Personnel Authentication Certificate in its User Personnel's browser prior to establishing a TLS1.2 connection to the Self-Service Interface in accordance with the Self-Service Interface ~~Design~~ Access Control Specification, where such DCCKI Certificates shall be obtained as set out in the DCCKI RAPP.

1.15 The User shall secure the connection between its User Personnel browser and the Self Service Interface or the Identity Provider Service used by the User, using TLS 1.2 in accordance with RFC5246 and will make use of:

(a) for the Identity Provider Service, mutual authentication using PKCS #3 Ephemeral Diffie Hellman key exchange to generate a shared secret for communications encryption, utilising one of the following cipher suites:

(i) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDHE-RSA-AES128-SHA256;

(ii) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDHE-RSA-AES256-SHA384;

(iii) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256; or

(iv) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDHE-RSA-AES256-GCM-SHA384; or

(b) for the Self Service Interface, server-side authentication.

Technical Infrastructure

1.16 The DCC shall provide the User, via secured electronic means, with details of a Uniform Resource Locator (URL) to access the Self Service Interface, corresponding with each applicable IP address provided in accordance with clause **Error! Reference source not found.**.

1.17 The DCC shall give reasonable advance notification to each User of any changes to the Self-Service Interface URL.

1.18 The DCC shall ensure that the IP addresses of the Self-Service Interface shall remain static.

Use of DCC Identity Provider Service

1.19 Each User using the DCC Identity Provider Service shall follow the processes set out in the DCCKI RAPP in order to obtain Personnel Authentication Certificates for its User Personnel prior to accessing the Self-Service Interface.

1.20 Each User that elects to use the DCC Identity Provider Service may create, modify or remove accounts for its User Personnel using the Self-Service Interface as further set out in the Self-Service Interface Specification, save that in the case of accounts for an Administration User, the DCCKI Registration Authority shall, upon receiving an Administration User Credentials Request as set out in the DCCKI RAPP, create, modify or remove the accounts.

1.21 The DCC shall provide an Identity Provider Service that shall, pursuant to clause **Error! Reference source not found.**, store secure cookies on each User Personnel's browser(s) to validate login sessions and shall ensure that such cookies do not include storage of information that permits personal identification.

Use of an Identity Provider Service that is not the DCC Identity Provider Service

1.22 The DCC shall only permit the use of an Identity Provider Service which conforms to the Identity Provider Service requirements set out in the Self-Service Interface ~~Design~~ Access Control Specification. The DCC shall not provide access to the Self-Service Interface where a User uses an Identity Provider Service that does not conform to such requirements.

1.23 When using an Identity Provider Service that is not the DCC Identity Provider Service, a User shall provide to the DCC the following details of its authentication arrangements:

(a) identity provider – <name of external Identity Provider Service>; and

(b) identity provider - <External Identity Provider Service URL>

and shall inform the DCC if the details change.

1.24 Each User that elects to use an Identity Provider Service that is not the DCC Identity Provider Service shall ensure that the SAML assertions, as set out in the Self-Service Interface ~~Design~~ Access Control Specification, are applied to access requests prior to establishing a TLS session.

1.25 Where a User elects to operate an Identity Provider Service that is not the DCC Identity Provider Service, the DCC shall regard an authentic signature on the SAML token for a member of User Personnel as confirmation that the User has appropriately performed verification, validation, role assignment and authentication of that member of User Personnel.