Version AH 2.0

Appendix AH

Self-Service Interface Access Control Specification

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 either in the DCC User Interface Specification or the Self-Service Interface Code of Connection.

Business Functional Domain	means a grouping of one or more Functional Components which is used to describe and deliver the functional requirements of Self-Service Interface Users.
Functional Component	means a specific item or set of functionality provided by the Self-Service Interface which is subject to the access controls set out in this Appendix AH.
Job Type Role	means one of the functional roles as set out in the table contained in clause 1.5.2
Order Management System (OMS)	as defined in the CH Handover Support Materials
Security Assertion Markup Language (SAML)	an open, published framework for exchanging security information between online business partners
SSI Baseline Requirements Document	means a document which sets out the design specification of the Self-Service Interface, and which is maintained by the DCC in accordance with Section 1 of this Appendix AH.

1. SELF-SERVICE INTERFACE ACCESS CONTROL SPECIFICATION

The DCC shall ensure that, where the DCC receives a request to access the Self-Service Interface, it shall direct that request to the appropriate URL for dealing with that request, and that such URL shall be implemented and maintained such that communications across it can be authenticated.

Where any fields are found to be invalid, the DCC shall ensure that validation error messages and suggestions for resolution are provided.

1.1. Authorisation

The DCC shall ensure that each user of the Self-Service Interface shall only be permitted to access a Functional Component if it is entitled to do so pursuant to clause 1.5.1 and 1.5.2 given the User ID(s) and Job Type Role(s) that are supplied as attributes of the SAML assertion.

1.2. SAML Authentication

The DCC shall provide to Users a SAML-capable Identity Provider Service for the purpose of authentication of User Personnel to the Self-Service Interface (the "DCC Identity Provider Service").

Each User may use an Identity Provider Service that is not the DCC Identity Provider Service for the purpose of authentication of its User Personnel to the Self- Service Interface.

To authenticate each request from a User Personnel that seeks to access the Self-Service Interface, the DCC shall use either:

(a). a SAML assertion provided by the DCC Identity Provider Service (as defined in clause 1.3); or

(b). a SAML assertion provided by an Identity Provider Service provided by the User (as defined in clause 1.4).

After an Identity Provider Service provides the User Personnel's SAML assertion, the DCC shall store a secure cookie in the User Personnel's browser. Such secure cookie shall be set to expire 8.5 hours after initial authentication by:

(a) the DCC, for the DCC Identity Provider Service; or

(b) the User, where such User is using an Identity Provider Service that is not the DCC Identity Provider Service.

If this cookie exists during subsequent authentication, the DCC shall bypass SAML authentication. Where using either the DCC Identity Provider Service or any other Identity Provider Service, if a User wishes to change the rights of that User Personnel to access the Self-Service Interface, the User shall delete the cookie from the User Personnel's browser cookie store.

The User shall ensure that its browser uses HTTP POST to transfer SAML between its Identity Provider Service and the Self-Service Interface.

Each User shall ensure that SAML assertions are applied when requesting access to the Self-Service Interface.

Each User must, when using any Identity Provider Service, present the Job Type Role(s) for which access to the Functional Component is being requested in the SAML assertion sent to the DCC.

Each User shall ensure that each SAML assertion includes a Digital Signature produced by a DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate in accordance with the FIPS 186-4 Digital Signature Standard using SHA-256 hashing algorithm. The User shall ensure that a SHA-256 hashing algorithm is applied to the SAML assertion.

1.3. SAML Authentication via the DCC Identity Provider Service

Where a User Personnel attempts to access the Self-Service Interface and a non-expired cookie is not stored in the User Personnel's browser cookie store:

1. The DCC shall send a SAML assertion request to the DCC Identity Provider Service via the User Personnel's browser;

2. When requested, the User shall provide the requested credentials (username, password, and certificate) to the DCC Identity Provider Service;

3. As set out in clause 1.1, the DCC shall grant or deny that person's access to the Self-Service Interface by providing a cookie enabling such access to be stored in the User Personnel's browser cookie store. If access is denied, the DCC shall provide a browser message which requests that the User Personnel resubmits their credentials.

The DCC shall ensure that, where a User is using the DCC Identity Provider Service, access to the Self-Service Interface is only provided once a User Personnel performs a login and generates a new password the first time that it uses that Identity Provider Service.

1.4. SAML Authentication via an Identity Provider Service that is not the DCC Identity Provider Service

When using an Identity Provider Service that is not the DCC Identity Provider Service, the User shall comply with this clause 1.4.

1.4.1 Authentication Requirements

A User providing a SAML assertion when seeking to access the Self-Service Interface via an Identity Provider Service that is not the DCC Identity Provider Service, shall ensure that its Identity Provider Service:

- prompts the User Personnel to provide their credentials (username, password, and certificate); and
- validates the User Personnel's credentials and (only where successfully validated) sends a SAML response including a SAML assertion to the Self-Service Interface.

The User shall ensure that SAML assertions, provided to the DCC by its Identity Provider Service, comply with the OASIS Standard – Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0.

The User shall ensure that the Identity Provider Service authentication mechanism shall use an appropriate SAML security assertion to demonstrate conformance to UK Government Authentication Framework Level 2.

1.4.2 Enrolment of an Identity Provider Service that is not the DCC Identity Provider Service

Where using an Identify Provider Service that is not the DCC Identify Provider Service, prior to seeking to access the Self-Service Interface for the first time, the User shall obtain at least one DCCKI Infrastructure Certificate in accordance with the DCCKI RAPP, and shall install such DCCKI Certificates on its Identity Provider Service.

The User shall configure their Identity Provider Service as defined in clause 1.4.1 and export and send a copy of the Identity Provider Service metadata to the DCC via secured electronic means, where such metadata shall include the URL of the Identify Provider Service and contact details in respect of the Identity Provider Service. Where the DCC reasonably requires the metadata to include additional information, the DCC shall inform the User of the information required and the User shall provide the information requested.

1.4.3 SAML Profiles, Bindings and Protocols

The User shall ensure that the Identity Provider Service it uses supports the following SAML profile, binding and protocol:

Profile	Web Browser SSO (single sign-on)
Binding	HTTP POST (HTTP/1.1)
Protocol	Authentication Request Protocol

1.4.4 Identity Provider Service SAML Configuration

Where a User notifies the DCC that it wishes to use an Identity Provider Service that is not the DCC Identity Provider Service, the DCC shall upon request provide, to that User via secured electronic means, the following information to be included in each SAML assertion:

- the service provider unique ID to be used by the Identity Provider Service, which is denoted as '[UNIQUE IDENTIFIER SP]' in the SAML attributes list below; and
- the URL formatted identifier of the Self-Service Interface, which is denoted as '[DCC SP URL]' in the SAML attributes list below.

The User shall ensure that their Identity Provider Service:

- shall not sign Authentication Requests (AuthnRequest);
- shall sign SAML Assertions;
- shall not sign Authentication responses;
- shall not encrypt any part of the SAML assertion (other than the Digital Signature);
- shall use persistent and unique nameIDs;
- shall only include NotBefore, NotOnOrAfter or AudienceRestriction in the SAML Condition elements; and
- shall set the SAML assertion nameID to be persistent and unique to the User Personnel.

The User shall ensure that their Identity Provider Service sets the following SAML attributes shown in square brackets, making reference to the information shown after each colon:

- [UNIQUE IDENTIFIER IDP]: a unique ID assigned to the SAML response by the Identity Provider Service.
- [UNIQUE IDENTIFIER SP]: the service provider unique ID for the SAML request, as provided by the DCC.
- [TIMESTAMP]: a timestamp in standard SAML format.
- [DCC SP URL]: the URL formatted identifier for the Self-Service Interface, as provided by the DCC.
- [IDP ISSUER URL]: a URL identifying the Identity Provider Service issuing the SAML assertion.
- [SAML ASSERTION UNIQUE IDENTIFIER]: a unique identifier assigned to the SAML assertion by the Identity Provider Service.

- [MESSAGE SIGNATURE]: a Digital Signature generated by the signing of the SAML assertion message using the DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate.
- [USERNAME]: a unique username assigned to the User Personnel by the Identity Provider Service.
- [SESSION EXPIRY]: a valid SAML date/time object describing the expiry time of the session associated with the user.
- [ASSERTION START]: a valid SAML date/time object describing the start time of the validity of the SAML assertion.
- [ASSERTION EXPIRY]: a valid SAML date/time object describing the expiry time of the validity of the SAML assertion.
- [SAML AUTHENTICATION CONTEXT]: a valid SAML Authentication Context Class describing the authentication that the user has completed with the Identity Provider Service.
- [Role name]: Job Type Role(s) as described in section 1.5. Multiple roles should be specified by separating role names using commas (,).
- [OrgID]: a list of User ID(s) in relation to which the User has been granted permission to access information held on the Self-Service Interface by the other User(s) to whom that information pertains. Such permission having been granted in accordance with clause 1.1.1 and not having been rescinded in accordance with clause 1.5.4. Multiple User IDs should be specified by separating values with commas (,).

1.5. Roles

1.5.1 DCC defined access

The DCC shall provide to User Personnel of each User access to each Functional Component that the User is eligible to access as set out in Section H8.16 or, where not specified in Section H8.16, as set out in this clause 1.5. Such access shall either be full or conditional, where:

- 'Full' means that the User can access data and use all functions associated with the specific Functional Component; and
- 'Conditional' means that a User's entitlement to access data and use all functions associated with the specific Functional Component is based on the access rules for conditional access set out below.

BFD ID	Business Functional Domain Name	Service capability	Functional Component	DCC Defined Access
			Raise service management Incidents UC_RaiseSMI_001 UC_RaiseSMI_002	Full

BFD01	Service Management	Provide service management capabilities in accordance with H9.4 and the Incident Management Policy, enabling Users to: • Raise, update, view and track Incidents. • Track and view detailed Problem information related to Incidents.	UC_RaiseSMI_003 UC_RaiseSMI_004	
			Update service management Incidents UC_UpdateSMI_001	Conditional. Access shall be granted as set out in Section H9.
			View service management Incidents UC_ViewSMI_001 UC_ViewSMI_002	Conditional. Access shall be granted as set out in Section H9.
			Problem management UC_ProblemManagement_001, UC_ProblemManagement_002	Conditional. Access shall be granted in accordance with Section H9.
BFD02	Smart Metering Inventory	Enable Users to search and query current information on Smart Meter Inventory down to individual Devices in accordance with H8.16(a). Provide detailed information on a Device and any associated Devices.	Smart metering inventory UC_Inventory_001, UC_Inventory_002	Full
BFD03	DCC Service Status	Provide Users with a dashboard of component availability for DCC Services in accordance with H8.16(g).	DCC service status UC_ServiceDashboard_001	Full
BFD04	Service Audit Trails	Enable Users to query information on Service Audit Trails, showing a record of service activity in accordance with H8.16(b). Only the records pertaining to that User will be shown in search and individual message view, where the records pertaining to a User are those for: • the User IDs for that User; and • any User IDs for which that User has been granted permission to access the information in accordance with clause 2.5.3 and such permission has not been rescinded in accordance with clause 2.5.4.	Service Audit Trails UC_ServiceAudit_001, UC_ServiceAudit_002	Conditional. Access shall be granted as set out in Section H8.16(b).
BFD05	Forward Schedule of Change	Enable Users to query and view detailed information on Planned Maintenance, changes scheduled or change freezes affecting any of the following elements of	Forward schedule of change UC_Schedule_001,	Full

		DCC Smart Metering ecosystem in accordance with H8.16(g): • Communications Hub firmware. • Parse & Correlate software. • SMIKI software. • DCC-impacting SEC Releases. • Other major DCC releases. • Meter firmware (Meter firmware events will only be visible to Users for Devices for which they are the Responsible Supplier)	UC_Schedule_002, UC_Schedule_003	
BFD06	Meter Read Transactions	Enable Users to query information on Meter Read Transactions for all users in accordance with H8.16(c).	Meter Read Transactions UC_Inventory_001	Full
BFD07	CSP SMWAN Network Coverage	Enable Users to query information on SM WAN network coverage down to premises level across each of the three GB regions in accordance with H8.16(f).	SM WAN network coverage UC_CSPCoverage_001 UC_CSPCoverage_002	Full
BFD08	DCC Service Alerts	Enable Users to view details of any Service affecting news / Alerts and other useful text relating to the quality of service delivery and service management in accordance with H8.16(g).	DCC Service Alerts UC_ServiceAlerts_001, UC_ServiceAlerts_002	Full
BFD09	Service Requests	Enable Users to: • Browse a catalogue of available DCC Service Requests. • Raise and update service management Service Requests with DCC from their service catalogue. Enables Users to track and update the status of raised requests within DCC service management system. • View full details of the raised Service Request User Personnel will only be able to access requests raised by the User with which they are associated.	Service catalogue publication and call off UC_ServiceCatalogue_001, UC_ServiceCatalogue_002, UC_ServiceCatalogue_003	Full
BFD10	Communications Hub Availability & Diagnostics	Enable Users to query information on Communication Hub availability and diagnostics down to individual Communications Hubs. Allows Users to attempt to diagnose and resolve Incidents	Communications Hub availability and diagnostics UC_HubStatus_001 UC_HubStatus_002	Conditional. Access shall be granted to the Responsible Supplier, the

		relating to any Communications Hubs for which they are the Responsible Supplier, the Network Party or Registered Supplier Agent, using DCC's remote diagnostic tools.		Network Party or Registered Supplier Agent for any Smart Metering System of which the Communication s Hub Function in question forms a part.

BFD11	Reporting	Enable users to access on demand a standard set of pre-defined reports. Allow Users to view and download individual reports from a defined set of published reports.	Reporting UC_Reports_001	Conditional. Users will only be permitted to view reports which pertain to them.

BFD12	Knowledge Management, Search and FAQ's	Enable Users to access the following functionality in accordance with H8.16(g) where applicable: • Knowledge management. This allows Users to view help and support information enabling early triage of User issues and queries, including access to the anonymous resolution details of service management problems and Incidents. • FAQ information. • DCC User Manuals detailing the operation of DCC Services. • Search capability, allowing Users to search for content provided by the SSI using tagged keywords, or textual content of page titles and descriptions.	Knowledge management UC_KnowledgeManagemen t_001	Full
			FAQs UC_FAQ_001	Full
			DCC user manuals UC_Manuals_001	Full
			UC_Search_001	Full

BFD13	Forecasting and Ordering	Enable Users to access OMS in accordance with H8.16(e). In OMS Users can submit orders and forecasts of future orders for Communications Hubs and Communication Hub Auxiliary Equipment.	Forecasting and ordering of Communications Hubs and auxiliary equipment UC_CSPOMS_001	Full

		Manage the verification of User identities requesting login access to SSI and DCC	Log In UC_Login_001	Full

BFD14	User Identity & Login Access Management	Platforms. Manage the functionality available to individual Users based on their User Role. This includes the following capabilities: • Enable Users to use DCC Identity Provider Service to assign access to functionality to their User Personnel based on Job Type Role and manage the SSI accounts and associated settings (e.g. password resets) for User Personnel accounts subsequently created by an Administration User. • Enable Administration Users to unlock, delete and manage the details of another account created within their organisation. • Enable an Administration User to create a new account for User Personnel within their organiszation. • Enable User Personnel to view detailed information about the account they are accessing via SSI including the functionality they have access to. Ensure secure communications between DCC systems and Users.	User account management UC_OrgManager_001, UC_OrgManager_002, UC_OrgManager_003	Conditional. Access shall be granted to Administration Users.
			User profile information UC_Profile_001	Full

Where a User is entitled to conditional access to more than one Functional Component, the DCC shall apply permissions such that any User Personnel can access any of those Functional Components that the User is eligible to access, subject to such User Personnel being entitled to such access on the basis of the Job Type Role(s) as further set out in 1.5.2.

1.5.2 Administration User defined access

In addition to the full and conditional access restrictions applied by the DCC in 1.5.1, Administration Users, appointed in accordance with the process set out in the DCCKI RAPP, may further define access restrictions for User Personnel to individual Functional Components by assigning one or more Job Type Roles to User Personnel in relation to one or more User IDs. Where a User is using the DCC Identity Provider Service, the DCC shall enable an Administration User to do this through the use of the Functional Component User Account Management.

The DCC shall ensure that access to Functional Components is only provided to the Job Type Role(s) presented to the DCC by the User in the SAML assertion accompanying the request for access to the Functional

Component, on the basis of the Functional Components that the Job Type Role is entitled to access as set out in the table below.

The table below shows which Functional Components that User Personnel with a given Job Type Role are only permitted to access (User Personnel with a given Job Type Role may only access those Functional Components where there is a 'Y' in the corresponding box).

Where the SAML assertion presented to the DCC when seeking to access the Functional Component(s) contains multiple Job Type Roles, the DCC shall grant access to that User Personnel to all of the Functional Components that it is entitled to access in all of those Job Type Roles.

	Job Type Role										
Functional Component	**All Access**	**Organisational Administrator**	**Security User**	**Lead Agent**	**Call Centre User**	**MI User**	**Service Management User**	**Smart Meter Operations User**	**Asset Management Ordering**	**SEC Contract Manager**	**Logistics**
BFD01 Service Management											
Raise service management incidentsUC_RaiseSMI_001 UC_RaiseSMI_002 UC_RaiseSMI_003 UC_RaiseSMI_004	Y	Y	Y	N	N	N	Y	N	N	N	Y
Update service management incidents UC_UpdateSMI_001	Y	Y	Y	N	N	N	Y	N	N	N	Y
View service management incidents UC_ViewSMI_001 UC_ViewSMI_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y
Problem management UC_ProblemManagement_001, UC_ProblemManagement_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y
BFD02 Smart Metering Inventory											

Smart metering inventory UC_Inventory_001, UC_Inventory_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BRD03 DCC Service Status											
DCC service status UC_ServiceDashboard_001	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
BDF04 Service Audit Trails											
Service audit trails UC_ServiceAudit_001, UC_ServiceAudit_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
BFD05 Forward Schedule Of Change											
Forward schedule of change UC_Schedule_001, UC_Schedule_002, UC_Schedule_003	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD06 Meter Read Transactions											
Meter Read Transactions UC_Inventory_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
BFD07 CSP SMWAN Network Coverage											
SM WAN network coverage UC_CSPCoverage_001 UC_CSPCoverage_002	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
BFD08 DCC Service Alerts											
DCC service alerts UC_ServiceAlerts_001, UC_ServiceAlerts_002	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD09 Service Requests											
Service catalogue publication and call offUC_ServiceCatalogue_001, UC_ServiceCatalogue_002, UC_ServiceCatalogue_003	Y	Y	N	Y	N	N	N	N	Y	N	Y
BFD10 Communications Hub Availability & Diagnostics											
Communications Hub availability and	Y	Y	N	Y	Y	N	Y	Y	N	N	Y

diagnostics UC_HubStatus_001 UC_HubStatus_002											
BFD11 Reporting											
Reporting UC_Reports_001	Y	Y	N	Y	N	Y	N	N	N	Y	Y
BFD12 Knowledge Management, Search and FAQ											
Knowledge management UC_KnowledgeManagement_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
FAQsUC_FAQ_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DCC user manuals UC_Manuals_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
UC_Search_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BFD13 Forecasting and Ordering											
Forecasting and ordering of Communications Hubs and auxiliary equipment UC_CSPOMS_001	Y	Y	N	N	N	Y	N	N	Y	N	Y
BFD14 User Identity & Access Management											
Log InUC_Login_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
User account management UC_OrgManager_001 , UC_OrgManager_002 , UC_OrgManager_003	N	Y	N	N	N	N	N	N	N	N	N
User profile information UC_Profile_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

1.5.3 Users granting access to other Users

Information available through the Self-Service Interface that relates to one or more User IDs of a User may be shared with another User where that other User is also willing to share information relating to one or more of its User IDs with the first User.

Where two Users wish to grant access to each other's information accessible through the Self-Service Interface, each of those Users shall submit, via secured electronic means, a notification to the DCC which includes:

- that the notification relates to granting to another User access to its data which is available via the Self-Service Interface;

- the list of User IDs of both of the relevant Users, for which mutual access for the two Users is being granted; and

- details of the DCCKI SRO responsible for the relevant User IDs that is authorising such access on behalf of the User submitting the notification, which shall comprise:

    - the name of the authorising DCCKI SRO;

    - telephone and email contact details for the DCCKI SRO; and

    - signature of the DCCKI SRO.

Upon receipt of such notifications, the DCC shall confirm if each request is authentic, by:

- verification of the DCCKI SRO; and

- by confirming that the User IDs provided by each User granting access are User IDs that have been assigned to each such User by the Panel in accordance with H1.6.

Where both of the notifications are confirmed to be authentic, the DCC shall:

- configure the Self-Service Interface to enable any Administration User acting on behalf of either of the two Users to grant access to its User Personnel to information available via the Self-Service Interface relating to any of such User IDs; and

- confirm in writing, to each DCCKI SRO submitting a notification that such access has been granted.

Where either or both of the notifications are not confirmed to be authentic, the DCC shall confirm in writing, to each of the DCCKI SRO submitting a notification, that such access has been rejected and giving the reasons for rejection.

1.5.4 Users rescinding access permission to other Users

Where a User wishes to rescind permission to allow another User to access its information available through the Self-Service Interface for a defined set of User IDs, having previously granted such access, the User wishing to remove access shall submit, in writing via secured electronic means, a notification to the DCC which includes:

- that the User wishes to rescind access to its information on the Self-Service Interface by another User;

- the list of User IDs pertaining to the User submitting the notification, for which it wishes to rescind access to another User (each a "Rescinding User ID");

- the list of User IDs pertaining to the other User for which access is to be rescinded (each a "Rescinded User ID"); and

- details of a DCCKI SRO that is authorising such rescinding of access on behalf of the User submitting the notification, which shall comprise:

    - the name of the authorising DCCKI SRO;

    - telephone and email contact details for the DCCKI SRO; and

- signature of the DCCKI SRO.

Upon receipt of such a notification, the DCC shall confirm if the request is authentic, by:

- verification of the DCCKI SRO; and
- by confirming that the User IDs provided by the User notifying that access should be rescinded, are User IDs that have been assigned to that User by the Panel in accordance with H1.6.

Where the notification is confirmed to be authentic, the DCC shall:

- configure the Self-Service Interface to remove access to information relating to Rescinding User IDs by any User Personnel of the second User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinded User ID;
- configure the Self-Service Interface to remove access to information relating to Rescinded User IDs by any User Personnel of the first User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinding User ID; and
- confirm in writing, to the DCCKI SROs of both affected Users that such access has been rescinded.

Where the notification is not confirmed to be authentic, the DCC shall confirm in writing, to the DCCKI SRO, that the notification of permission to be rescinded has been rejected.