Version AH 4.0

Appendix AH

Self-Service Interface Access Control Specification

Contents

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 the SSI Functions and Roles Policy.

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 with the process described in Section 1.5.1 of this Appendix AH.

SSI Functions and Roles Policy	means a document which sets out the definitions and rules governing the assignment and functional entitlement provided by Job Type Roles, and which is maintained by the DCC in accordance with Section 1.5.1 of this Appendix AH.

1. SELF-SERVICE INTERFACE ACCESS CONTROL SPECIFICATION

1.1. Authorisation

The DCC shall ensure that access to Functional Components and information is only permitted to individual members of User Personnel using the Self-Service Interface according to the Job Type Role(s) and User IDs assigned to their respective SSI Account within the SSI, in compliance with the Functional Components that the Job Type Role is entitled to access as set out in the SSI Functions and Roles Policy.

Where a member of User Personnel's SSI Account has been configured with multiple Job Type Roles and/or User IDs, the DCC shall grant access to that member of User Personnel to all of the Functional Components and information that it is entitled to access in all of those Job Type Role and User ID combinations.

1.2. Authentication

The DCC shall provide to Users an identity provider service for the purpose of authentication of User Personnel to the Self-Service Interface (the "DCC Identity Provider Service").

To authenticate each request from a person that seeks to access the Self-Service Interface, the DCC shall use the DCC Identity Provider Service. Upon successful authentication of a relevant request, 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.

If a non-expired cookie exists during subsequent authentication, the DCC shall bypass authentication.

1.3. Authentication via the DCC Identity Provider Service

Where a person 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 redirect the person to the DCC Identity Provider Service via the person's browser;

2. When requested, the person shall provide the requested credentials (username, password, and multi-factor authentication confirmation) to the DCC Identity Provider Service, in accordance with clause 1.2; and

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 Identity Provider Service shall be configured in such a way that on the first authentication against an SSI Account, the person authenticating must successfully complete the following steps:

1. Authenticate using their assigned SSI Account username and initial password; and

2. Provide a new password, which will replace the initial password; and

3. Register a multi-factor authentication option for the SSI Account, in compliance with the DCC Internet Access Policy.

A person shall not be authenticated to the SSI until they have completed this process.

1.4. User administration and SSI Accounts

All members of User Personnel requiring access to the SSI shall require a unique SSI Account, which shall be used to:

(a) identify the particular individual,

(b) enable login authentication; and

(c) allow management of access to specific functions and information

within the SSI.

Each SSI Account may only be assigned to, and used by, one individual and must not be shared with any other individuals at any time.

1.4.1 SSI Account Management (creation, updates and retirement)

SSI Accounts shall be managed by Administration Users via the Self-Service Interface in conformance with the SSI Functions and Roles Policy.

In exceptional cases, including but not limited to (a) the creation of the first SSI Account for a User, and (b) the assignment of Job Type Roles with specific security implications, an SSI Account may be managed by the DCC on behalf of a User, in accordance with the SSI Functions and Roles Policy.

Each Party shall ensure that an Administration User shall, when managing SSI Accounts:

- Only create and assign SSI Accounts to named individuals within (or acting on behalf of) their organisation on a one-to-one basis, i.e. one SSI Account may only be used by one individual, and an individual may only have one account assigned to them;

- Ensure that all individuals are explicitly and correctly identified within the respective SSI Account configuration, including the individual's name and email address;

- Ensure that SSI Account details are maintained and up to date, e.g. for changes in name or contact details; and

- Ensure that all applicable SSI Accounts are retired in a timely fashion, where the respective individual ceases to act in a role for which they require an SSI Account.

1.4.2 Assignment of User IDs to SSI Accounts

An Administration User may assign one or more User IDs to each SSI Account associated with that User, provided that they are an Administration User for those User IDs.

1.4.3 Assignment of Job Type Roles to SSI Accounts

An Administration User may assign one or more allowable Job Type Roles, in relation to one or more User IDs for which they are an Administration User, to each individual SSI Account via the SSI user administration function. Allowable Job Type Roles shall be limited by the SSI to those roles which are appropriate/permissible to the User according to their User Roles, as detailed in SSI Functions and Roles Policy. An Administration User may assign any of these allowable Job Type Roles to one or many SSI Accounts, at their discretion.

The DCC shall not be required to oversee the assignment of such Job Type Roles – it shall be the sole responsibility of the User.

Selected Job Type Roles, which are identified as such in the SSI Functions and Roles Policy, may only be assigned to SSI Accounts by the DCC. For these Job Type Roles only, Administration Users may raise an SMSR to request that the DCC assigns these Job Type Roles to nominated members of User Personnel (SSI Accounts), provided that the requestor also has a Job Type Role which is defined as entitled to nominate the requested Job Type Role, as also defined in the SSI Functions and Roles Policy.

Upon receiving such a request, the DCC shall confirm that: (a) the requester is entitled to make such a nomination and thereafter (b) perform any additional validation that is required, both in accordance with the SSI Functions and Roles Policy.

If any required additional validation is successful, the DCC shall:

(a) make the assignment of the nominated Job Type Role to the nominated SSI Account which shall take effect either immediately or upon the next occasion that the individual authenticates with the DCC Identity Provider Service (typically the following day);

(b) confirm the assignment to the requester via the SMSR response; and

(c) notify the nominated individual member of User Personnel of their assignment,

If the validation is unsuccessful, the DCC shall notify the requester of the reason for failure via the SMSR response.

1.5. Job Type Roles

1.5.1 SSI Functions and Roles Policy

The DCC shall maintain and keep up to date a document which sets out in detail the structure and definition of Job Type Roles within the Self-Service Interface policy (the **SSI Functions and Roles Policy**). Any changes to the SSI Functions and Roles Policy shall be prepared and consulted upon with SEC Parties by the DCC and approved by the Panel. This content will also be reflected in the **SSI Baseline Requirements Document,** which will follow the same governance process.

1.5.2 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 and that is assigned to their respective SSI Account in compliance with the SSI Functions and Roles Policy.

1.5.3 Users granting access permission to other Users

A User may elect to share access to information and functionality available through the Self-Service Interface that relates to one or more of its User IDs with another User, enabling that User to act on its behalf.

Where a User wishes to grant such access to a second User, the granting User shall submit an SMSR via the Self-Service Interface, which includes the list of User IDs of the granting User, for which mutual access for the two Users is being granted.

The DCC shall ensure that such an SMSR shall only be submissible in circumstances where:

- the requesting SSI Account is authorised to make such a request, in compliance with the Job Type Roles assigned to the account, as defined in SSI Functions and Roles Policy;
- the User IDs submitted by the granting User are User IDs that have been assigned to the grantee User by the Panel in accordance with H1.6; and
- the grantee User is configured within the SSI to be able to receive such access permission.

Once the SMSR has been submitted, and after passing the validation checks above, 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 within SSI to both Users that such access has been granted.

1.5.4 Users rescinding access permission which has been granted to other Users

Where a User, having previously granted access permission to another User, wishes to rescind that permission, the User shall submit an SMSR via the SSI. This SMSR shall include the list of User IDs for which access for the grantee User is to be rescinded.

The DCC shall ensure that such an SMSR shall only be submissible if:

- the requesting SSI Account is authorised to make such a request, in compliance with the Job Type Roles assigned to the account, as defined in SSI Functions and Roles; and
- the User IDs submitted by the granting User are User IDs that have been assigned to the grantee User.

Where the SMSR has been submitted, after passing such validation, the DCC shall:

- remove the ability for any Administration User acting on behalf of the grantee User to grant access to its User Personnel to information available via the Self-Service Interface relating to any of such User IDs;

- configure the Self-Service Interface to remove any existing access for any User Personnel of the grantee User to information available via the Self-Service Interface relating to any of such User IDs; and

- confirm within SSI to both Users that such access has been rescinded.

1.6. SSI Baseline Requirements Document

The DCC shall maintain and keep up to date a document which sets out the technical details of each Functional Component and how these are used to provide services to Users via the Self-Service Interface (the **SSI Baseline Requirements Document**). Any changes to the SSI Baseline Requirements Document shall be prepared and consulted upon with SEC Parties by the DCC and approved by the Panel.