Version AI 3.0

Appendix AI

Self-Service Interface Code of Connection

Contents

Definitions . . . 2

1. SELF-SERVICE INTERFACE CODE OF CONNECTION . . . 3

General Obligations . . . 3

Restrictions on Physical Connections . . . 4

Connection Mechanisms . . . 4

Communications Authentication . . . 4

Technical Infrastructure . . . 5

Use of DCC Identity Provider Service . . . 5

Use of an Identity Provider Service that is not the DCC Identity Provider Service . . . 5

Interface Usage . . . 6

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 Access Control Specification, the SSI Baseline Requirements Document or the DCC User Interface Specification.

Administration User	means, in relation to a particular User, a member of User Personnel who has been appointed to act in such a role in accordance with the DCCKI RAPP (and who has not subsequently ceased to carry out such a role).
Administration User Credentials Request	has the meaning given to that expression in the DCCKI RAPP.
Identity Provider Service	means a service that authenticates that an individual member of User Personnel is who they purport to be for the purposes of access control.
Network Address Translation	means a mechanism by which Users map one Self-Service Interface IP address space to another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

Personnel Authentication Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.

Policy Enforcement Point (PEP)	a logical entity that enforces policies for admission control and policy decisions in response to a request for access. It is the logical boundary between the DCC Systems and connecting systems, namely User Systems, RDP Systems or any other systems used to access the Self-Service Interface. The PEP ensures that: the policies in the applicable Code of Connection relevant to the applicable Party or RDP are being enforced; there is appropriate separation of the DCC Systems from the connecting systems of the applicable Party or RDP; and all the connections to the User Systems, RDP Systems, systems used to access the Self-Service Interface, or DCC Systems are compliant with the same applicable Code of Connection.

Supported Web Browser	Internet Explorer versions 9, 10 and 11, and a minimum of 2 other browsers as listed on the DCC Website (such list as updated from time to time).

TLS	means transport layer security in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website.

UI DCCKICA Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.

Uniform Resource Locator (URL)	a reference to a resource that specifies the location of the resource on a computer network and a mechanism for retrieving it.

W3C WCAG AA	means the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG) for making content accessible. AA is one of three conformance levels.

1. SELF-SERVICE INTERFACE CODE OF CONNECTION

1.1 These provisions apply to the DCC and any User seeking to access information via the Self-Service Interface as described in Section H8.16 of the Code.

General Obligations

1.2 The DCC and each User shall inform each other of the contact details of one or more persons working for their respective organisations for the purposes of communications associated with the use of the Self-Service Interface (in the case of the User, where the contact details for such persons are not already held by the DCC). The following information shall be provided in relation to each such person (and subsequently kept up to date by the Party and/or the DCC):

(a) contact name;

(b) contact email;

(c) contact telephone number;

(d) contact address; and

(e) any other contact details as may be reasonably required by the DCC or the User from time to time.

Restrictions on Physical Connections

1.3 Each User shall only access the Self-Service Interface over a DCC Gateway Connection.

1.4 Each User acknowledges that use of a DCC Gateway Connection for the purposes of accessing the Self-Service Interface will utilise some of the available bandwidth of that connection and may consequently reduce the rate at which information may be exchanged when accessing other Services over that connection.

Connection Mechanisms

1.5 Each User shall route all communications to the Self-Service Interface through its Policy Enforcement Point.

1.6 The DCC shall make the Self-Service Interface available on a set of Internet Protocol version 4 addresses.

1.7 The DCC shall provide details of the set of IP addresses and network configuration to each User, via secured electronic means, as part of the process for obtaining a connection to the Self-Service Interface.

1.8 Each User shall use Network Address Translation to map internal Internet Protocol addresses to the published DCC provided IP addresses within the User’s firewall prior to accessing the Self-Service Interface.

1.9 Each User shall use Network Address Translation to remap incoming DCC traffic Internet Protocol addresses from the published IP addresses within the User’s firewall to IP addresses within their subnet, as notified by the DCC via secured electronic means.

1.10 Each User shall establish a TLS connection between their User Personnel browsers and either the Self-Service Interface or an Identity Provider Service, in accordance with clause 1.14.

1.11 The DCC shall provide access to the Self-Service Interface to each User using a Supported Web Browser with a minimum screen resolution of 1280x1024 pixels.

1.12 The DCC shall provide reasonable notice to Users of changes to the list of Supported Web Browsers.

Communications Authentication

1.13 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 TLS connection to the Self-Service Interface in accordance with the Self-Service Interface Access Control Specification, where such DCCKI Certificates shall be obtained as set out in the DCCKI RAPP.

1.14 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 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

1.15 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 1.7.

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

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

Use of DCC Identity Provider Service

1.18 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.

1.19 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.

1.20 The DCC shall provide an Identity Provider Service that shall, pursuant to clause 1.26, 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

1.21 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 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.

1.22 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.

1.23 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 Access Control Specification, are applied to access requests prior to establishing a TLS session.

1.24 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.

Interface Usage

1.25 Each User shall not use any systems to apply automated tools in order to interact or operate with the Self-Service Interface.

1.26 Each User shall configure each User Personnel’s browser to enable the storage of cookies by the DCC in the browser’s cookie store.

1.27 Each User consents to the recording and storage by the DCC of details that they make available to the DCC through SAML authentication and request parameters for the purposes of auditing, diagnostics and capacity planning.

1.28 Each User agrees to the recording and storage by the DCC of requests processed by the Self-Service Interface for the purposes of auditing, diagnostics and capacity planning.

1.29 The DCC shall ensure that the Self-Service Interface complies with the W3C Web Content Accessibility Guidelines at an ‘AA’ conformance level (“W3C WCAG AA”).

1.30 The DCC shall log information associated with all requests processed by the Self- Service Interface. Logged information includes data such as the User Personnel’s organisation, the User Personnel’s username, the URL requested and any inputs provided.

1.31 The DCC shall, upon request, make available to a User, reports summarising the information in clause 1.30 in relation to that User’s User Personnel.

1.32 Prior to first use of the Self-Service Interface or where there are any material changes to the following information, each User shall estimate and notify to the DCC:

(a) maximum total active User Personnel accounts;

(b) maximum number of User Personnel concurrently accessing the Self- Service Interface;

(c) average activity (requests/hour/account) for a typical Working Day; and

(d) maximum peak activity in relation to each User Personnel account (the maximum number of requests and the corresponding hour) for a typical Working Day.