Version: T1.0

Appendix T

DCCKI Interface Design Specification

Table of Contents

1. **Introduction** **3**
2. **DCCKI Service Interface** **3**
3. **DCCKI Certificate Signing Request** **9**

Annex A

Definitions **13**

1 INTRODUCTION

Document Purpose

1.1 Pursuant to Section L13.13 of the Code (DCCKI Interface Design Specification), this document is the DCCKI Interface Design Specification.

2 DCCKI SERVICE INTERFACE

Submission of DCCKI Certificate Signing Requests and Issuance of DCCKI Infrastructure Certificates

2.1 In order to request Issuance of a DCCKI Infrastructure Certificate, a Party or RDP that is a DCCKI Eligible Subscriber shall follow the processes defined in the DCCKI RAPP.

2.2 The DCC shall ensure that all DCCKI Certificate Signing Requests are required to be formatted in accordance with the PKCS #10 standard as set out in the DCCKI RAPP. The structure of a DCCKI Certificate Signing Request is defined in section 3 of this DCCKI IDS.

2.3 No further provision is made in this document in relation to requesting and obtaining DCCKI Infrastructure Certificates.

Submission of Personnel Authentication Certificate Applications and Issuance of Personnel Authentication Certificates

2.4 Prior to submitting an initial Personnel Authentication Certificate Application, (but not for any subsequent application), a Party that is a DCCKI Eligible Subscriber in respect of Personnel Authentication Certificates shall submit an Administration User Credentials Request via the approved mechanisms set out in the DCCKI RAPP.

2.5 The DCC shall make a Personnel Credentials Interface accessible via the Self Service Interface for the purpose of accessing DCCKI Services in order to obtain a Personnel Authentication Certificate. The DCC shall ensure that:

(a) the Personnel Credentials Interface uses the HTTPS protocol;

(b) the Personnel Credentials Interface uses Java 7, update 6 (or greater);

(c) the Personnel Credentials Interface supports JavaScript, CSS and images;

(d) initial access to the Personnel Credentials Interface will be authorised through use of username and single use password, the provision of which shall be detailed in the DCCKI RAPP and shall be secured by server side authentication using TLS 1.2;

(e) subsequent access to the Personnel Credentials Interface is secured by mutual authentication using TLS1.2 between the Supported Browser being used by the DCCKI Eligible Subscriber and the Personnel Credentials Interface;

(f) DCCKI Certificates are used for the TLS authentication and shall support the following cipher suites:

i. ECDHE-RSA-AES256-GCM-SHA384

ii. ECDHE-RSA-AES128-GCM-SHA256

iii. ECDHE-RSA-AES256-SHA384

iv. ECDHE-RSA-AES128-SHA256;

(g) access to the Personnel Credentials Interface is denied without a valid credential for Authentication; and

(h) User Personnel are provided with the means to view and update their password and user account information as set out in the Self Service Interface Access Control Specification.

Issuance of Personnel Authentication Certificates to Administration Users

Initial Issuance of a Personnel Authentication Certificate to Administration Users

2.6 In order to obtain an initial Personnel Authentication Certificate, an Administration User shall log onto the Personnel Credentials Interface via the Self Service Interface using the supplied username, and single use password as provided in accordance with the DCCKI RAPP.

2.7 Upon initial login, the SSI Administration User shall be required to:

(a) change the password for the user account from that provided; and

(b) provide answers to security questions that will subsequently be used to confirm the identity of that Administration User if their password is forgotten, their Personnel Authentication Certificate has expired or the Smart Card Token provided to that Administration User is lost or stolen.

2.8 On successful change of the user account password, the Administration User shall be able to request initialisation of the Smart Card Token which will result in a Personnel Authentication Certificate Application.

2.9 In order to initialise the Smart Card Token, the Administration User shall:

(a) connect the Smart Card Token to the system that the Administration User is using to access the Personnel Credentials Interface. The system shall be configured in accordance with sections 2.5 (b) and (c) of this DCCKI IDS; and

(b) request initialisation of the Smart Card Token by following the instructions displayed on the Personnel Credentials Interface.

2.10 Following a successful request for initialisation of the Smart Card Token the DCC shall ensure that, where the Smart Card Token generates a Personnel Authentication Certificate Application, this shall automatically be submitted to the UI DCCKICA.

2.11 The Administration User shall be notified via the Personnel Credentials Interface as soon as reasonably practicable of the Issuance of a Personnel Authentication Certificate for that Administration User.

Subsequent Issuance of a Personnel Authentication Certificate to Administration Users

2.12 Prior to the expiry of a Personnel Authentication Certificate Issued to an Administration User, that Administration User may:

(a) log onto the Personnel Credentials Interface via the Self Service Interface, using their Smart Card Token, username and password; and

(b) reinitialise the Smart Card Token by following the steps set out in section 2.9 of this DCCKI IDS, which will result in the Issuance of a new Personnel Authentication Certificate.

2.13 In the event that a Personnel Authentication Certificate Issued to an Administration User has expired prior to their obtaining a new Personnel Authentication Certificate, that Administration User may:

(a) log onto the Personnel Credentials Interface via the Self Service Interface and obtain a new Personnel Authentication Certificate by:

(i) using their Administration User username and password; and

(ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(b) reinitialise the Smart Card Token by following the steps outlined in section 2.9 above which will result in the Issuance of a new Personnel Authentication Certificate.

2.14 In the event that the Smart Card Token is lost or stolen, an Administration User may:

(a) obtain a new Smart Card Token from their DCCKI ARO in accordance with the DCCKI Code of Connection;

(b) log onto the Personnel Credentials Interface via the Self Service Interface:

(i) using the Administration User's username and password; and

(ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(c) initialise the Smart Card Token by following the steps outlined in section 2.9 of this DCCKI IDS which will result in the Issuance of a new Personnel Authentication Certificate.

Issuance of Personnel Authentication Certificates to other User Personnel

Initial Issuance of a Personnel Authentication Certificate to other User Personnel

2.15 The initial Issuance of a Personnel Authentication Certificate to a User Personnel shall be via the Personnel Credentials Interface following the creation of an account

for that User Personnel by an Administration User.

2.16 In order to provide Authentication credentials to User Personnel, (which shall comprise a single use password and a username) an Administration User may:

(a) log onto the Self Service Interface using their Smart Card Token, username and password in accordance with the Self Service Interface Access Control Specification and Self Service Interface Code of Connection;

(b) create additional user accounts for other User Personnel; and

(c) provide details to those User Personnel including a username and single use password that allows them to log onto the Personnel Credentials Interface via the Self Service Interface.

2.17 In order to obtain an initial Personnel Authentication Certificate, User Personnel of a DCCKI Eligible Subscriber, shall log onto the Personnel Credentials Interface via the Self Service Interface using the agreed username and single use password, as established by the relevant Administration User.

2.18 Upon first login, those User Personnel shall be required to:

(a) change the password for their account; and

(b) provide answers to security questions that will subsequently be used to confirm the identity of that individual if the password is forgotten, their Personnel Authentication Certificate has expired or their Personnel Authentication Certificate is destroyed or, no longer has access to their Personnel Authentication Certificate or Private Key associated with their Personnel Authentication Certificate.

2.19 Upon successful login, the User Personnel shall be able to submit a Personnel Authentication Certificate Application by following the instruction displayed on the Personnel Credentials Interface.

2.20 Following a Personnel Authentication Certificate Application request:

(a) the User Personnel shall be requested to create a password in accordance with the instruction displayed on the Personnel Credentials Interface, to protect the

credentials to be generated by the DCCKICA and transferred to the User Personnel's browser;

(b) the DCCKI Eligible Subscriber shall ensure that the systems of its User Personnel are configured to allow the credentials to be transferred to the User Personnel's browser and in accordance with sections 2.5 (b) and (c) of this DCCKI IDS;

(c) the DCCKICA shall generate the credentials consisting of a Key Pair along with a Personnel Authentication Certificate that is specific to that User Personnel and the systems that User Personnel is using to access the Personnel Credentials Interface and shall make it available to the browser in the form of a PKCS#12 file protected using the password created by the User Personnel;

(d) the User Personnel shall unprotect the PKCS#12 file using the password created by that User Personnel; and

(e) the User Personnel shall download, verify and install the PKCS#12 file in a location accessible to a Supported Web Browser, when requested by the Authentication Credentials Interface.

Subsequent Issuance of a Personnel Authentication Certificate to other User Personnel

2.21 Prior to the expiry of a Personnel Authentication Certificate assigned to a member of User Personnel, in order to obtain a new Personnel Authentication Certificate, that individual:

(a) may log onto the Personnel Credentials Interface via the Self Service Interface, using their existing Personnel Authentication Certificate, username and password; and

(b) follow the steps outlined in sections 2.19 and 2.20 of this DCCKI IDS.

2.22 In the event that their Personnel Authentication Certificate has expired prior to obtaining a new Personnel Authentication Certificate, a member of User Personnel may:

(a) Log onto the Personnel Credentials Interface via the Self Service Interface:

(i) using their username and password; and

(ii) provide answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(b) follow the steps outlined in sections 2.19 and 2.20 of this DCCKI IDS.

3 DCCKI CERTIFICATE SIGNING REQUEST

Information to be contained within DCCKI Certificate Signing Requests

3.1 A DCCKI Certificate Signing Request in respect of a DCCKI Infrastructure Certificate for the purpose of signing SAML assertions to the DCC shall contain the information set out in the table immediately below:

Subject	**Attributes**	**Values**
Version		V3 (as per RFC 2986)
Subject	Common Name	<Party Signifier>
Subject Public Key Info	Public Key Algorithm	RSA
	Subject Public Key (2048 bits)	Public Key value
Key Usage	Criticality	True
	Key Usage	digitalSignature
Signature Algorithm		rsa-with-SHA256

3.2 A DCCKI Certificate Signing Request in respect of a DCCKI Infrastructure Certificate for the purpose of establishing TLS communications to the DCC shall contain the information set out in the table immediately below:

Subject	**Attributes**	**Values**
Version		V3 (as per RFC 2986)
Subject	Common Name	Fully Qualified Domain Name configured on the Policy Enforcement Point
	Organisation Identifier	Party Signifier or RDP Signifier
Subject Public Key Info	Public Key Algorithm	RSA
	Subject Public Key (2048 bits)	Public Key value
Key Usage	Criticality	True
	Key Usage	digitalSignature

		keyEncipherment
Signature Algorithm		rsa-with-SHA256

3.3 A DCCKI Certificate Signing Request in respect of a DCCKI Infrastructure Certificate for the purpose of establishing FTPS communications to the DCC shall contain the information set out in the table immediately below:

Subject	**Attributes**	**Values**
Version		V3 (as per RFC 2986)
Subject	Common Name	Party Signifier or RDP Signifier
Subject Alt Name		<Fully Qualified Domain Name>
Subject Public Key Info	Public Key Algorithm	RSA
	Subject Public Key (2048 bits)	Public Key value
Key Usage	Criticality	True
	Key Usage	digitalSignature keyEncipherment
Signature Algorithm		rsa-with-SHA256

DCCKI Certificate Signing Request format

3.4 DCCKI Certificate Signing Request requests shall be formatted according to PKCS #10, Base64 encoded.

3.5 The standard format shall be ASN.1 DER, including one of the immediately following two styles of PEM header:

(a) -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----; or

(b) -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----

Acceptable DCCKI Certificate Signing Request variants

3.6 The DCC shall accept the following PKCS#10 variants:

(a) Base64 all in one line;

(b) Base64 with line breaks at 64 or 76 characters; and

(c) if line breaks are used the \n and \r\n are both acceptable.

Signing the DCCKI Certificate Signing Request using a Private Key associated with a SMKI Organisation Certificate

3.7 Following the creation of the DCCKI Certificate Signing Request in accordance with section 3.4 of this DCCKI IDS, the DCCKI Eligible Subscriber shall Digitally Sign the DCCKI Certificate Signing Request with a Private Key associated with a SMKI Organisation Certificate for which it is a Subscriber.

3.8 The DCCKI Eligible Subscriber shall ensure that the Digital Signature shall:

a) use, as the digital signature technique, Elliptic Curve Digital Signature Algorithm (ECDSA) (as specified in Federal Information Processing Standards Publications (FIPS PUB) 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at section D.1.2.3) and SHA-256 as the Hash function;

b) be applied to the entirety of the PKCS#10 file, including header and footer; and

c) be converted to Base64 and appended to the footer within the PKCS#10 file itself with a preceding "," separator.

3.9 Prior to Digitally Signing the DCCKI Certificate Signing Request, the DCCKI Eligible Subscriber shall append to the footer of the PKCS#10 file, the Issuer which shall be URL encoded (as specified in the IETF RFC 2253) and serial number of the SMKI Organisation Certificate with preceding "," separators.

Availability and Service Continuity

3.10 The DCC shall ensure that the DCCKI Service Interface is available, in accordance with Section L13.12 (the DCCKI Service Interface) of the Code.

3.11 The DCC shall notify Parties and RDPs in advance of any planned outages of the

DCCKI Service Interface.

ANNEX A

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- any expressions not defined here or in section A of the Code have the meaning given to them in the DCCKI Certificate Policy, the DCCKI Registration Authority Policies and Procedure or the Self Service Interface Specification.

Issuer	The name of the signer of the DCCKI Infrastructure Certificate as described in the DCCKI Certificate Policy.