

Appendix TBC

VWKI Interface Design Specification

Contents

1	Introduction	3
1.1	Purpose	3
1.2	Target Response Times	3
2	VWKI Service Interfaces	3
2.1	General obligations	3
2.2	Submission of VWD CSR and VWP CSR by Authorised Subscriber	3
2.3	Receipt and validation of VWP CSR or VWD CSR by the DCC	3
2.4	Actions following acceptance of VWP CSR or VWD CSR by the DCC	4
2.5	Conduct Constituting Certificate Acceptance	4
	Annex A – VWKI Service Interface parameters	5
	DCC SharePoint URL	5
	SharePoint Folder Structure	5
	Annex B – Certificate Signing Request Structure	6
	Information to be contained within a VWD CSR.....	6
	Information to be contained within a VWP CSR	7
	Annex C – Definitions for the purpose of this Appendix	8

1 Introduction

1.1 Purpose

Section L18 of the Code sets out the obligation on the DCC to maintain the VWKI Service Interface in accordance with the VWKI Interface Design Specification. Section L18.11 sets out the content of the VWKI Interface Design Specification including the protocols and technical standards which are all based on open standards and defines the technical details of the interfaces to VWKI Services insofar as they relate to Authorised Subscribers

1.2 Target Response Times

For the purposes of service management, the terms "sending" and "receipt" in the context of the VWKI interface are interpreted as follows:

- a) **"receipt"** means the successful upload of Certificate Signing Request (CSR) file to the DCC-managed SharePoint site by a VWKI Authorised Subscriber and notifying the Service Desk following the CSR upload.
- b) **"sending"** means the point at which the DCC makes the files containing the resulting VWKI Certificates available for download by a VWKI Authorised Subscriber and notifying the relevant ARO;
- c) **Standard Processing Time:** The Target Response Time for the DCC to complete "sending" is five (5) business days from the time of "receipt". This is the elapsed time referenced in the VWKI RAPP; and
- d) **Expedited Processing:** In the event of certificate replacement due to the Compromise or suspected Compromise of a relevant Private Key, requests shall be handled in accordance with the Incident Management Policy, outside of standard processing times.

2 VWKI Service Interfaces

2.1 General obligations

- a) The DCC shall ensure that the PKCS#10 standard is used for all CSRs.
- b) VWKI Authorised Subscribers shall ensure that each submitted CSR strictly conforms to the content, structure, and cryptographic requirements defined for the relevant certificate type (VWP Certificates, VWD Certificates or VWKICA Certificates) in Annex B of the VWKI Certificate Policy.
- c) Upon downloading an issued VWKI Certificate, the Subscriber must verify that its contents are consistent with the corresponding CSR. The Certificate is deemed accepted unless the VWKI Authorised Subscriber immediately notifies the Service Desk of its rejection.
- d) This policy does not support Certificate Renewal or Re-Key. Subscribers requiring a new certificate must follow the process for initial issuance to obtain a replacement.

2.2 Submission of VWD CSR and VWP CSR by Authorised Subscriber

- a) A VWKI Authorised Subscriber generates one or more CSRs in line with Appendix B of this document, and Appendix [TBC] of the Code with the relevant VWKI Certificate Profile.
- b) The VWKI Authorised Responsible Officer (ARO) shall upload one or more CSR files to their designated CSR folder in 'SharePoint Folder Structure' on the 'DCC SharePoint URL'.
- c) The VWKI ARO shall notify the Service Desk following the CSR upload.

2.3 Receipt and validation of VWP CSR or VWD CSR by the DCC

Following receipt of a CSR, the DCC shall:

- a) validate the format, and verify the Digital Signature of the CSR in line with Appendix B of this

- document and PKCS#10;
- b) ensure that the Authorised Subscriber is an Eligible Subscriber for the type of certificate;
 - c) perform such additional checks as DCC determines is necessary on the CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the VWKI Certificate Policy;
 - d) either accept; or reject the CSR; and
 - i. where the CSR is accepted, take the actions described in Section 2.4; or
 - ii. where the CSR is rejected,
 - A. log in the error and upload the error details in the designated Rejected CSR folder in 'SharePoint Folder Structure' on the 'DCC SharePoint URL'; and
 - B. notify the ARO of the Subscriber.

2.4 Actions following acceptance of VWP CSR or VWD CSR by the DCC

Where a VWKI CSR is accepted by the DCC, the DCC shall:

- a) Issue a corresponding VWD Certificate or VWP Certificate that is compliant with the profiles in Annex B of the VWKI Certificate Policy;
- b) lodge the resulting VWD Certificate or VWP Certificate in the VWKI Repository;
- c) upload the Certificate files to their designated Certificate folder in 'SharePoint Folder Structure' on the 'DCC SharePoint URL'; and
- d) notify the ARO of the Subscriber of the above.

2.5 Conduct Constituting Certificate Acceptance

- a) An issued certificate is considered to be accepted by the organisation on whose behalf the corresponding CSR was submitted upon download unless immediately rejected by notification to the Service Desk. The organisation accepting the certificate will be treated as a VWKI Subscriber for that Certificate.

Annex A – VWKI Service Interface parameters

DCC SharePoint URL

<https://capitaitservices.sharepoint.com/sites/LIVEDCC/testservices/SitePages/Home.aspx>

SharePoint Folder Structure

DCC shall provide the following folder structure for each VWKI Authorised Subscriber on the SharePoint.



A sub-folder shall be created for the day for each file upload in the YYYYMMDD format.

Annex B – Certificate Signing Request Structure**Information to be contained within a VWD CSR**

Section	Attributes	Value
Version		Version 0
Subject	Common Name (CN) Organisation (O) Country (C)	VWD EUI64 The Party Signifier of the VWKI Subscriber GB
Subject Public Key Information	Public Key Algorithm Named Curve	id-ecPublicKey secp256r1
	Prime256r1 (256 bit)	Public Key Value
Key Usage	Criticality	True
	Key Usage	digitalSignature
	Criticality	False, or absent
	Extended Key Usage	id-kp-clientAuth
Signature Algorithm		ecdsa-with-SHA256

Notes on CSR Submission Format:

1. CSRs submitted to the VWKI Service Interface shall be in PKCS#10 format.
2. The DCC shall accept the following variants for the format of the CSR files: a) **With PEM Headers:** The file may include standard Privacy-Enhanced Mail (PEM) headers, such as -----BEGIN CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST-----. b) **Without PEM Headers:** The file may consist only of the raw Base64 encoded data. c) **Line Breaks:** The Base64 data may be presented as a single, continuous line or with line breaks (typically at 64 or 76 characters). Both \n (LF) and \r\n (CRLF) line endings are acceptable.

Information to be contained within a VWP CSR

Section	Attributes	Value
Version		Version 0
Subject	Common Name (CN) Organisation (O) Country (C)	The Fully Qualified Domain Name of the VWP instance (FQDN) The Party Signifier of the VWKI Subscriber GB
Subject Public Key Information	Public Key Algorithm Named Curve	id-ecPublicKey secp256r1
	Prime256r1 (256 bit)	Public Key Value
Key Usage	Criticality	True
	Key Usage	digitalSignature
	Criticality	False, or absent
	Extended Key Usage	id-kp-serverAuth (Server Authentication)
Signature Algorithm		ecdsa-with-SHA256

Notes on CSR Submission Format:

1. CSRs submitted to the VWKI Service Interface shall be in PKCS#10 format.
2. The DCC shall accept the following variants for the format of the CSR files: a) **With PEM Headers:** The file may include standard Privacy-Enhanced Mail (PEM) headers, such as -----BEGIN CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST-----. b) **Without PEM Headers:** The file may consist only of the raw Base64 encoded data. c) **Line Breaks:** The Base64 data may be presented as a single, continuous line or with line breaks (typically at 64 or 76 characters). Both \n (LF) and \r\n (CRLF) line endings are acceptable.

Annex C – Definitions for the purpose of this Appendix

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 VWKI Certificate Policy and the VWKI Registration Authority Policies and Procedures.