This document is classified as **Clear** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP245 '2023 Review of the SMKI Document set'

Annex A

Legal text – version 1.0

About this document

This document contains the changes required to deliver the Proposed Solution.

SEC Appendix A – 'Device Certificate Policy'

These changes have been redlined against Appendix A version A3.0.

Amend Section 4.1.3 as follows:

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP section 6 in relation to the establishment of an enrolment process in respect of DCA Personnel and DCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the DCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face or video link Authentication of all SMKI Registration Authority Personnel by a SMKI Registration Authority Manager; and

(b) for all SMKI Registration Authority Personnel to have their identify and authorisation verified to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.

Appendix B – 'Organisation Certificate Policy'

These changes have been redlined against Appendix B version 8.0.

Amend Section 4.1.3 as follows:

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP section 6 in relation to the establishment of an enrolment process in respect of OCA Personnel and OCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the OCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face or video link Authentication of all SMKI Registration Authority Personnel by a SMKI Registration Authority Manager; and

(b) for all SMKI Registration Authority Personnel to have their identify and authorisation verified to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.

Appendix C – 'SMKI Compliance Policy'

These changes have been redlined against Appendix C version 2.0.

Amend Section 2.2 as follows:

Quality Requirements

2.2 The quality requirements specified in this Part 2.2 are that the SMKI Independent Assurance Scheme must be a scheme:

(a) which is recognised as an accreditation scheme for the purposes of the eIDAS Regulation (No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market).~~Article 3(2) of Directive 1999/93/EC on a Community framework for electronic signatures~~;

(b) which is based on ISO 27001; and

(c) the provider of which:

(i) is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and

(ii) requires all its scheme assessors to be UKAS certified.

Appendix D – 'SMKI Registration Authority Policies and Procedures'

These changes have been redlined against Appendix D version 5.0.

Amend Section 4.1.2 as follows:

4.1.2 High level overview of SMKI Registration Authority procedures

Figure 1 as set out immediately below provides a high level view of the procedures required in order for a Party, RDP, SECCo or the DCC (in its role as DCC Service Provider) to:

- verify their organisational identity;
- become an SRO;
- become an ARO;
- gain credentials for accessing SMKI Services and/or the SMKI Repository Service;
- become an Authorised Subscriber for:
  - Organisation Certificates or Device Certificates, or both;
  - a File Signing Certificate (issued under the IKI Certificate Policy) for the purposes of verifying Digital Signatures of files in accordance with the Code;
- gain access to Organisation Certificates and/or Device Certificates and other material via the SMKI Repository; and
- gain access to File Signing Certificates, and their corresponding Private Keys to be used for the purposes of Digitally Signing files.

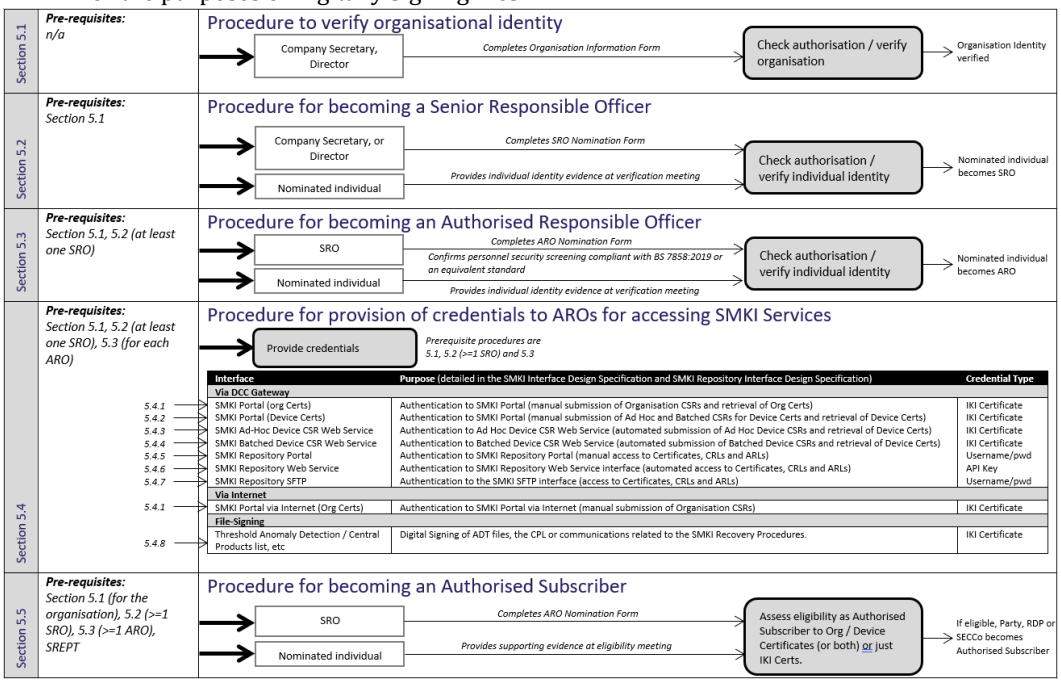

Figure 1: Overview of SMKI access registration processes

- SMKI RAPP Section 5.1 sets out the procedure and detailed processes for confirming the role of the nominating individual and verifying the organisational identity of the Party,

RDP, SECCo or DCC Service Provider, which shall be conducted where its identity has not previously been established.

- SMKI RAPP Section 5.2 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an SRO. The DCC shall ensure that an individual cannot become an SRO until the organisational identity of the applicant has been verified.
- SMKI RAPP Section 5.3 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an ARO. The DCC shall ensure that an individual cannot become an ARO until the organisation has at least one SRO and the organisational identity of the applicant has been verified.
- Once an individual has become an ARO, SMKI RAPP Section 5.4 sets out the procedure and detailed processes by which the appropriate credentials used to access SMKI Services and/or the SMKI Repository Service are provided to AROs.
- Where an applicant wishes to be an Authorised Subscriber for Organisation Certificates or Device Certificates or both, Section 5.5 of the SMKI RAPP sets out the procedure and detailed processes by which the DCC determines if the applicant is eligible to become an Authorised Subscriber for such Organisation Certificates or Device Certificates or both.

In respect of the procedures and detailed processes set out in SMKI RAPP Sections 5.1 to 5.5, the DCC shall place no restriction on the number of forms that can be submitted by an individual Party, RDP, SECCo or the DCC. Where reasonably practicable, the DCC shall conduct the procedures as set out in SMKI RAPP Sections 5.1 to 5.5 such that where multiple forms are submitted at the same time, multiple procedures can be conducted ~~within a single visit to the DCC's offices~~ via a video link by the applicant's nominated individuals.

Amend Section 6.2 as follows:

6.2 Procedure for becoming a SMKI Registration Authority Manager

The procedure for becoming a SMKI Registration Authority Manager as detailed immediately below shall be conducted by DCC's Chief Information Security Officer (CISO), or an individual that they have authorised to act on their behalf in this capacity, on behalf of the DCC, in order to nominate, authorise and verify a SMKI Registration Authority Manager.

Step	When	Obligation	Responsibility	Next Step
6.2.1	As required	Nominate an individual to become a SMKI Registration Authority Manager, who shall be an employee of the DCC or be contracted to the DCC, and advise the nominated individual of the evidence to be provided in order to verify their identity.	DCC Chief Information Security Officer, on behalf of the DCC	6.2.2
6.2.2	As soon as reasonably practicable following 6.2.1	Confirm verification meeting date/time with nominated individual.	DCC Chief Information Security Officer, on behalf of the DCC	6.2.3
6.2.3	In verification meeting	The CISO shall, in accordance with the provisions of Sections G4.4 to G4.8:	DCC Chief Information Security Officer, on behalf of the DCC	If verified, 6.2.5. If not

		a. check proof of identity provided against the information provided by the nominated individual; and b. verify the identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.		verified, 6.2.4

6.2.4	In verification meeting	If the identity of the nominated individual is not successfully verified, provide reasons for the failure to the individual and notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification.	DCC Chief Information Security Officer, on behalf of the DCC	6.2.5

6.2.5	In verification meeting	If the identity of the nominated individual is successfully verified, notify the individual verbally and subsequently in writing that they have become a SMKI Registration Authority Manager and notify the SMKI PMA that the nominated individual has become a SMKI Registration Authority Manager.	DCC Chief Information Security Officer, on behalf of the DCC	6.2.6

6.2.6	As soon as reasonably practicable following 6.2.5	Record the details of the individual that has become a SMKI Registration Authority Manager, in a manner which is auditable.	SMKI Registration Authority	Procedure as set out in SMKI RAPP Section 6.4

Appendix Q 'IKI Certificate Policy'

These changes have been redlined against Appendix Q version 5.0.

Amend Section 4.1.3 as follows:

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP section 6 in relation to the establishment of an enrolment process in respect of ICA Personnel and ICA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the ICA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face or video link Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to the level pursuant to the SMKI PMA Guidance on 'Verifying Individual Identity' published on the Website.

Appendix W 'DCCKI Registration Authority Policies and Procedures'

These changes have been redlined against Appendix W version 3.0.

Amend Section 3.2 as follows:

3. PARTY AND REGISTRATION DATA PROVIDER ENROLMENT

General enrolment obligations

Party and Registration Data Provider obligations

3.1 Each Party or RDP that wishes to use the DCCKI Services is required to become a DCCKI Authorised Subscriber.

3.2 In order to become a DCCKI Authorised Subscriber, a Party or RDP must:

(a) be an Authorised Subscriber under the Organisation Certificate Policy;

(b) submit a DCCKI Authorised Subscriber application in accordance with this DCCKI RAPP via the means set out on the DCC Website and the guidance on DCC SharePoint;

(c) have at least one individual who is a DCCKI SRO for that Party or RDP; and

(d) have at least one individual who is a DCCKI ARO for that Party or RDP.

Amend Section 3.4 as follows:

3.4 Where the information provided to the DCCKI Registration Authority in relation to:

(a) the Party or RDP being a DCCKI Authorised Subscriber;

(b) individuals who are acting in the role of DCCKI SRO for that Party or RDP; or

(c) individuals who are acting in the role of DCCKI ARO for that Party or RDP;

changes, that Party or RDP shall:

(d) advise the Service Centre, via email,~~Desk~~ of such change; and

(e) ensure that the procedures as set out in section 3.27 of this DCCKI RAPP are undertaken in respect of providing revised information to the DCCKI Registration Authority, as soon as reasonably practicable thereafter.

Amend Section 3.10 as follows:

Submission of application

3.10 ~~Where a Party or RDP wishes to nominate an individual to become a DCCKI SRO, a Director, Company Secretary or existing DCCKI SRO of that Party or RDP shall ensure that:~~Nomination of an individual to become a DCCKI Senior Responsible Officer shall be made by a Director, Company Secretary or existing DCCKI SRO on behalf of the Party or RDP or to the level pursuant to the SMKI PMA Guidance on 'Verifying Organisation Identity'. Nomination of an individual to become a DCCKI Authorised Responsible Officer shall be made by a DCCKI Senior Responsible Officer on behalf of the Party or RDP.

(a) a DCCKI SRO Nomination Form is completed in accordance with this DCCKI RAPP and any instructions, help or advice provided by the DCCKI Registration Authority from time to time, including via the DCC Website;

(b) the information provided is complete and accurate;

(c) the DCCKI SRO Nomination Form is authorised by a Director, or Company Secretary of that Party or RDP; and

(d) the completed DCCKI SRO Nomination Form is submitted to the DCCKI Registration Authority via the means set out on the DCC Website.

Amend Section 3.16 as follows:

Procedure for becoming a DCCKI Authorised Subscriber

Submission of request

3.16 Where a Party or RDP wishes to become a DCCKI Authorised Subscriber, a Director, Company Secretary or DCCKI SRO of that Party or RDP shall ensure that:

(a) a DCCKI Authorised Subscriber Application is submitted in accordance with this DCCKI RAPP and any instructions, help or advice provided by the DCCKI Registration Authority from time to time, including via the DCC Website, and including the provision of such information as is set out in the form contained in Annex A (A3~~4~~) to this DCCKI RAPP;

(b) the information provided is complete and accurate;

(c) the DCCKI Authorised Subscriber Application is authorised by a Director or Company Secretary of that Party or RDP, or DCCKI SRO; and

(d) the DCCKI Authorised Subscriber Application is submitted to the DCCKI Registration Authority via the means set out on the DCC Website.

Amend Section 5.12 as follows:

5.12 In the event of a DCCKI Certificate Signing Request being rejected, the DCCKI Registration Authority shall:

(a) create a record of the rejection on the DCCKI Certificate Signing Request Rejection Form, which shall contain the information and be substantively as set out in Annex A (A4~~6~~) to this DCCKI RAPP;

(b) notify a DCCKI ARO of the organisation via the Service Desk that submitted the DCCKI Certificate Signing Request of its rejection, this may be via telephone or in writing, using the contact details established as part of enrolment for the DCCKI Services; and

(c) provide a copy of the DCCKI Certificate Signing Request Rejection Form via secured electronic means as set out on the DCC Website.

Amend Annex A as follows:

ANNEX A – FORM TEMPLATES

The Form Templates listed in Appendix A are available from the DCC Website or via SharePoint as provided by the DCC.

The DCC may, subject to the approval of the SMKI PMA, modify the form templates from time to time.

A1. DCCKI SRO NOMINATION FORM

A2. DCCKI ARO NOMINATION FORM

A3. DCCKI AUTHORISED SUBSCRIBER APPLICATION FORM

A4. DCCKI CERTIFICATE SIGNING REQUEST REJECTION FORM

A5. ADMINISTRATION USER CREDENTIALS REQUEST FORM

A6. DCCKI CERTIFICATE REVOCATION REQUEST FORM

~~**A7. NOMINEE DETAILS FORM**~~