

3. SMKI Roles

This SMKI RAPP details the roles of Parties, RDPs, ~~Manufacturers~~, SECCo and the DCC in the context of access to SMKI Services and/or the SMKI Repository Service as set out in the Code, this SMKI RAPP and the SMKI interface documents. The SMKI RAPP sets out the procedures by which nominated individuals may become Senior Responsible Officers and/or Authorised Responsible Officers in order to act on behalf of a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (acting in its role as DCC Service Provider) in respect of SMKI Services and the SMKI Repository Service.

This SMKI RAPP also details the obligations in respect of the SMKI Registration Authority and the individuals acting on its behalf as SMKI Registration Authority Managers or SMKI Registration Authority Personnel.

From time to time, the SMKI PMA may require documents or information to be lodged in the SMKI Repository. In such instances, it shall submit a request via the Service Desk and provide such documents and/or information to be lodged in the SMKI Repository. The DCC shall lodge documents and/or information provided to the SMKI Repository, as soon as reasonably practicable following receipt.

3.1 Party, RDP, ~~Manufacturer~~, SECCo and DCC representatives

Individuals permitted to act as representatives of a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider) are as set out immediately below:

- Senior Responsible Officer (SRO). The process by which an individual is nominated and their authorisation is checked and their identity verified, so as to be an SRO and act on behalf of an organisation is set out in SMKI RAPP Section 5.2. An individual is nominated to become an SRO by a Director or Company Secretary for a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (for DCC Service Provider personnel). Once an individual has become an SRO, the SRO may at any time nominate individuals to undertake to become Authorised Responsible Officers (AROs) and to access SMKI Services and/or the SMKI Repository Service. An SRO may also nominate themselves to become an ARO as described below.
- Authorised Responsible Officer (ARO). The process by which an individual is nominated, verified and authorised to be an ARO is set out in SMKI RAPP Section 5.3. The means by which AROs are provided with credentials to authenticate access to SMKI Services and/or the SMKI Repository Service is set out in Section 5.4. The DCC shall permit only AROs to act on behalf of a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider) for the purposes of accessing SMKI Services and/or the SMKI Repository Service. Depending upon the processes followed, an ARO may also be authorised to act on behalf of a Party, RDP or the DCC (in its role as DCC Service Provider) to be an Authorised Subscriber for Organisation Certificates, Device Certificates or both, following successful completion of SMKI and Repository Entry Process Tests. All AROs are also permitted to access the SMKI Repository Service on behalf of the organisation that they represent, as set out in the SMKI Repository Interface Design Specification.

Each Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider) that wishes to:

- a) become an Authorised Subscriber for Organisation Certificates and/or Device Certificates;
- b) become an Authorised Subscriber for an IKI Certificate for the purposes of Digitally Signing of files; or
- c) have access only to the SMKI Repository,

shall have at least one ARO successfully appointed (and therefore one SRO).

The DCC shall not be required to repeat processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming an SRO and/or ARO in respect of SMKI Services or the SMKI Repository Service, where the required verification processes have already been carried out for the purposes of identifying them as being a DCCKI SRO and/or DCCKI ARO respectively.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing an ARO or SRO or the Party or RDP becoming an Authorised Subscriber, be treated as if it had taken place after that date.

3.2 SMKI Registration Authority representatives

Individuals acting as representatives of the DCC in its role as SMKI Registration Authority are:

- SMKI Registration Authority Manager. The process by which a SMKI Registration Authority Manager is nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or the SMKI Repository Service is set out in SMKI RAPP Sections 6.2 and 6.4.
- SMKI Registration Authority Personnel. The process by which SMKI Registration Authority Personnel are nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or SMKI Repository is set out in SMKI RAPP Sections 6.3 and 6.4.

The DCC shall ensure that only a SMKI Registration Authority Manager or SMKI Registration Authority Personnel may act on behalf of the DCC in respect of matters relating to the SMKI Registration Authority. Each Party, RDP, ~~Manufacturer~~, SECCo and the DCC (in its role of DCC Service Provider) shall refrain from dealing with DCC Personnel (including SMKI Registration Authority Managers and SMKI Registration Authority Personnel) other than as directed by the Service Desk for the purposes of submitting Certificate Signing Requests (CSRs) and Certificate Revocation Requests (CRRs).

The DCC, in order to perform its role as SMKI Registration Authority, shall nominate at least two individuals to become a SMKI Registration Authority Manager, each of which will have responsibility for:

- a) management of the SMKI Registration Authority function and SMKI Registration Authority Personnel;
- b) nomination of individuals to become SMKI Registration Authority Personnel;
- c) authentication and verification of SMKI Registration Authority Personnel, as set out in Section 6.3 of this document;
- d) provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP, ~~Manufacturer~~ or SECCo representatives and DCC Personnel (including SMKI Registration Authority Personnel);
- e) managing the process by which documents and information are lodged in the SMKI Repository; and
- f) approval of CRRs.

A SMKI Registration Authority Manager may nominate individuals to become SMKI Registration Authority Personnel and to act on behalf of the SMKI Registration Authority as set out in this SMKI RAPP and the Code. The primary responsibilities of SMKI Registration Authority Personnel are:

- a) to conduct registration processes as set out in SMKI RAPP Sections 5.1 to 5.5, incorporating:

- i. verification of organisational identity;
 - ii. verification and authorisation of individuals nominated to become SROs or AROs, as set out in Section 5.2 and 5.3 of this document;
 - iii. provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP, ~~Manufacturer~~, SECCo representatives and DCC personnel; and
 - iv. assessment of whether an organisation qualifies to become an Authorised Subscriber for Organisation Certificates and/or Device Certificates.
- b) processing and approval (where required) of Certification Signing Requests and processing of Certificate Revocation Requests; and
 - c) processing of requests for revocation of credentials used to access SMKI Services and/or the SMKI Repository Service.

The DCC shall ensure that SMKI Registration Authority Managers and SMKI Registration Authority Personnel, where required, are available to undertake the obligations in respect of procedures set out in this SMKI RAPP:

- a) in respect of the verification, processing and approval of CRRs, on a 24*7 basis; and
- b) in respect of all other procedures as set out in this SMKI RAPP, on a Working Day basis and during standard working hours in England.

The DCC and any Party, RDP, ~~Manufacturer~~ or SECCo may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, be treated as if it had taken place after that date.

4. Party, RDP, ~~Manufacturer~~, SECCo and DCC (as DCC Service Provider) registration procedures

4.1 General registration obligations

4.1.1 Organisation, individual, and RA obligations

Each Party, RDP, ~~Manufacturer~~, SECCo and the DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

To facilitate this, the SMKI Registration Authority shall:

- a) make the forms as set out in SMKI RAPP Annex A, available from the DCC Website or via the DCC SharePoint site as advised by the DCC;
- b) provide reasonable support and advice to each Party, RDP, ~~Manufacturer~~, SECCo and DCC Service Providers in relation to the procedures as set out in SMKI RAPP sections 5.1 to 5.5;

- c) place no restriction on the number of individuals that can be nominated as SROs or AROs in respect of any Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider);
- d) permit an individual to become an ARO to represent multiple parties, by successfully completing the procedures in SMKI RAPP section 5.3 and 5.4 as are necessary;
- e) store and maintain records relating to the nomination, verification and authorisation of individuals and organisations (but not the personal details of individuals) as set out Sections 5.1 to 5.5, and in accordance with the Code and the DCC's data retention policy and data protection policy;
- f) not permit any nominated individual to access the SMKI Services or relevant the SMKI Repository Service on behalf of a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider) until they have become an ARO;
- g) ensure that credentials issued under the IKI Certificate Policy to AROs have a lifetime of ten years and that such credentials shall cease to be valid after ten years following issuance;
- h) for authentication and file signing credentials issued under the IKI Certificate Policy and where the Key Pair and Certificate Signing Request are both generated by the prospective ARO on a Cryptographic Credential Token during the ARO verification meeting, that the prospective ARO has an opportunity to validate and agree information (e.g. role and other organisation and individual identity) against which the Certificate is Issued is accurate and that it reflects the identity of the ARO or system that is the subject of the Certificate;
- i) for authentication and file signing credentials issued under the IKI Certificate Policy and which are delivered to the SMKI Registration Authority in the form of a Certificate Signing Request generated by the prospective ARO's organisation and provided by the prospective ARO during the ARO verification meeting, that the prospective ARO has an opportunity to validate the information in the resulting Certificate reflects that provided in the Certificate Signing Request and that it is accurate and reflects the identity of the prospective ARO or system that is the subject of the Certificate;
- j) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked; and
- k) produce, each month, and make available to each Party, RDP, ~~Manufacturer~~ and SECCo, a report for that organisation which details the list of SROs, AROs, the credentials that have been issued to each ARO and those AROs for which credentials will expire in the following month.

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, ~~Manufacturer~~, 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.

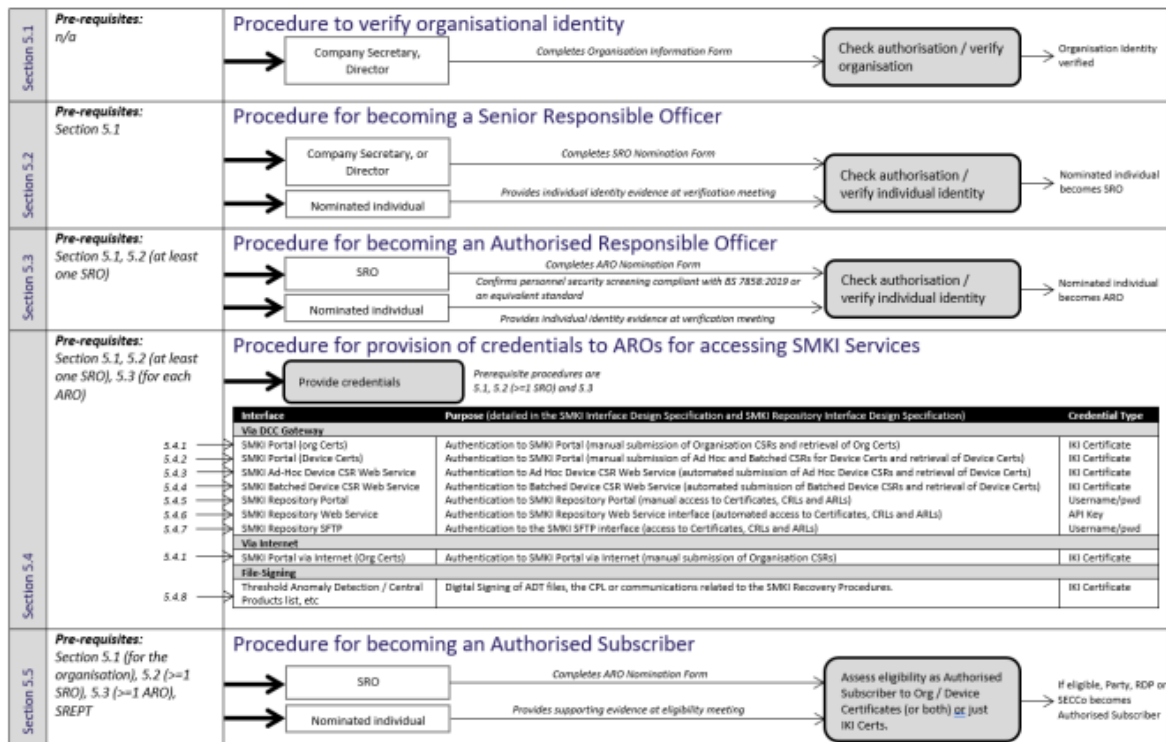


Figure 1: Overview of SMKI access registration processes

- 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, Manufacturer, 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, ~~Manufacturer~~, 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 via a video link by the applicant's nominated individuals.

4.1.3 Change of details

If there is a change to any of the information used to verify the organisational identity of any Party, RDP, ~~Manufacturer~~, SECCo or a DCC Service Provider (acting on behalf of the DCC), an SRO shall advise the Service Desk of the change and shall ensure that the procedure and detailed processes as set out in SMKI RAPP Section 5.1 is undertaken in respect of the revised evidence of identity, as soon as is reasonably practicable after the change occurs.

If there is a material change to any of the information used to verify the identity of any SRO or ARO, an SRO shall:

- a) advise the Service Desk of the change;
- b) where required to do so by the SMKI Registration Authority, check the name and address of an ARO before issuing a replacement token, ensure that its SRO or ARO undertakes the procedures as set out in SMKI RAPP Sections 5.2 or 5.3 in respect of the revised evidence of identity, as soon as is reasonably practicable after a material change occurs; and
- c) where necessary, for an ARO ensure that credentials used to access SMKI Services and/or the SMKI Repository Service are revoked as set out in SMKI RAPP Section 8.3.

No Party, RDP, ~~Manufacturer~~, SECCo or the DCC (acting as DCC Service Provider) shall unreasonably withhold information that is required by the SMKI Registration Authority in order to perform the procedures as set out in SMKI RAPP Sections 5.1 to 5.5.

4.1.4 Director or Company Secretary ceasing to be eligible to act on behalf of a Party, RDP, ~~Manufacturer~~ or SECCo

Where Director or Company Secretary ceases to be eligible to act on behalf of a Party, RDP, ~~Manufacturer~~ or SECCo in respect of the procedures set out in the SMKI RAPP:

- a) the Director or Company Secretary themselves, or a Senior Responsible Officer (SRO) whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;
- b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from a Director, Company Secretary or SRO; and
- c) if b) is successful, the DCC shall update the DCC's records of authorised individuals for the Party, RDP, ~~Manufacturer~~ or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP, ~~Manufacturer~~ or SECCo.

4.1.5 SROs ceasing to be eligible to act on behalf of a Party, RDP, ~~Manufacturer~~ or SECCo

Where an SRO ceases to be eligible to act on behalf of a Party, RDP, ~~Manufacturer~~ or SECCo in respect of the procedures set out in the SMKI RAPP:

- a) the SRO themselves, or a Director, Company Secretary or SRO whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;

- b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from an SRO, Director or Company Secretary; and
- c) if b) is successful, update the DCC's records of authorised individuals for the Party, RDP, ~~Manufacturer~~ or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP, ~~Manufacturer~~ or SECCo.

5. Detailed Party, RDP, ~~Manufacturer~~, SECCo and DCC (as DCC Service Provider) registration procedures and processes

Each Party, RDP, ~~Manufacturer~~, SECCo and DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

5.1 Procedure and processes to verify organisational identity

The processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to verify the organisational identity of a Party, RDP, ~~Manufacturer~~, SECCo or DCC Service Provider (acting on behalf of the DCC).

Step	When	Obligation	Responsibility	Next Step
5.1.1	As required	The applicant organisation shall complete the Organisation Information Form, as set out in SMKI RAPP Annex A (A1). In doing so, the applicant organisation shall ensure that: a. the information entered on the form is complete and accurate; b. the EUI-64 Compliant identifier range for any particular User Role is defined by the applicant organisation such that the range is continuous and does not overlap with the EUI-64 Compliant identifier range for any other User Role, other than where a particular EUI64 Compliant identifier is allowed to be used for more than one	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC Service Provider	5.1.2

		User Role in accordance with H1.5; and c. the Organisation Information Form is authorised by a Director or Company Secretary on behalf of the applicant organisation. The applicant organisation shall also complete the Nominee Details Form, as set out in SMKI RAPP Annex A (A5), for the Director or Company Secretary that has authorised the Organisation Information Form. In doing so, the applicant organisation shall ensure that the information entered on the form is complete and accurate.		
5.1.2	As required following 5.1.1	Submit the completed Organisation Information Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider.	5.1.3
5.1.3	As soon as reasonably practicable following receipt of completed Organisation Information Form	Acknowledge receipt by email to the Director or Company Secretary that has authorised the Organisation Information Form.	Service Desk	5.1.4
5.1.4	As soon as reasonably practicable following 5.1.3	Confirm that the nominating Director or Company Secretary holds such a position within the application	SMKI Registration Authority Personnel	If complete, accurate and no discrepancies, 5.1.6; if not complete and

		organisation, via a public information source. Analyse the information entered on the Organisation Information Form and Nominee Details Form, to determine completeness, discrepancies and whether the submitted EUI64 Compliant identifier ranges are consistent with the restriction set out in step 5.1.1. Where there are omissions/discrepancies or the submitted identifier ranges are not consistent with the restriction set out in step 5.1.1, the SMKI Registration Authority shall agree actions and/or amendments, via email, with the Director or Company Secretary that has authorised the Organisation Information Form.		accurate or any discrepancies, 5.1.5
5.1.5	Once omissions / discrepancies addressed	Submit a revised Organisation Information Form and/or Nominee Details Form to the SMKI Registration Authority, or in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider	5.1.3
5.1.6	As soon as reasonably practicable, following 5.1.4	Agree with the applicant organisation and confirm, by email, the date and time of a meeting to verify the organisation identity to the Director, or Company Secretary that has signed the Organisation Information Form. The meeting shall be	SMKI Registration Authority	5.1.7

		held via a video link or face to face if preferred.		
5.1.7	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the applicant Director or Company Secretary by email, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the individual(s) shall inform the SMKI Registration Authority, by email, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.1.8
5.1.8	In meeting to verify organisational identity	Verify: a. the organisational identity of the applicant organisation to the level pursuant to the SMKI PMA Guidance on "Verifying Organisation Identity" published on the Website; b. via information held by SECCo, that the applicant organisation has the User Role or User Roles as specified in Organisation Information Form; c. proof of individual identity provided for the nominating individual against the information	SMKI Registration Authority Personnel	If not successful, 5.1.9; if successful, 5.1.10

		listed on the Organisation Information Form and the Nominee Details Form; and d. the individual identity of the nominating individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.		
5.1.9	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is unsuccessful, notify the nominating Director, Company Secretary or SRO that verification of the organisational identity has been unsuccessful, by email.	SMKI Registration Authority Personnel	5.1.5 once issues addressed
5.1.10	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is successful, inform the nominating Director or Company Secretary that the organisational identity has been successfully verified, by email.	SMKI Registration Authority	5.1.11
5.1.11	As soon as reasonably practicable, following 5.1.10	Add the verified organisation to the DCC's list of such organisations, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	End of procedure

5.2 Procedure for becoming a Senior Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become a Senior Responsible Officer in respect of that Party, RDP, [Manufacturer](#), SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.2.1	As required	Complete the SMKI SRO Nomination Form and	Director or Company Secretary, on behalf	5.2.2

		Nominee Details Form, as set out in SMKI RAPP Annex A (A3) and Annex A (A5). In doing so, the individual completing the SMKI SRO Nomination Form and Nominee Details Form shall ensure that the information entered on the forms is complete and accurate, and that: a. the nominating individual is for a Party, RDP, Manufacturer, SECCo or the DCC (as DCC Service Provider), a Director of, or Company Secretary of and an employee of, the applicant organisation or its parent organisation; and b. the SMKI SRO Nomination Form and Nominee Details Form are both authorised, where applicable, by a Director or Company Secretary on behalf of the applicant organisation. entered on the form is complete and accurate.	of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider).	
5.2.2	As required, following 5.2.1	Submit the completed SMKI SRO Nomination Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider).	5.2.3
5.2.3	As soon as reasonably practicable following receipt of completed	Acknowledge receipt to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	Service Desk	5.2.4

	SRO Nomination Form			
5.2.4	As soon as reasonably practicable following 5.2.3	Analyse the information entered on the SMKI SRO Nomination Form and Nominee Details Form, to: - determine completeness and any discrepancies; and - confirm, using the DCC's records or using publicly available information, that the Director or Company Secretary that has authorised the SMKI SRO Nomination Form has the role indicated on the SMKI SRO Nomination Form. Where there are omissions/discrepancies, agree actions with the nominating individual, via email.	SMKI Registration Authority Personnel	If complete, 5.2.6; if not complete, 5.2.5
5.2.5	Once omissions / discrepancies addressed	Submit a revised SMKI SRO Nomination Form and/or Nominee Details Form to the SMKI Registration Authority, in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider).	5.2.3
5.2.6	As soon as reasonably practicable, following 5.2.4	If the SMKI Registration Authority has any questions about the information submitted, contact the Director or Company Secretary that nominated the individual, via telephone, using the telephone number provided previously in the SMKI SRO Nomination Form,	SMKI Registration Authority Personnel	If confirmed as authorised, 5.2.8; if not confirmed as authorised, 5.2.7

		to confirm whether each nominated individual on the SMKI SRO Nomination Form is authorised to act on behalf of the organisation as SRO and seek confirmation of information provided on the SMKI SRO Nomination Form in order to provide confidence that the correct person has been contacted.		
5.2.7	As soon as reasonably practicable following rejection	Inform the applicant organisation that the application to become a Senior Responsible Officer has not been successful, by email to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	SMKI Registration Authority Personnel	5.2.6 once issues resolved
5.2.8	As soon as reasonably practicable, following 5.2.6	Agree, via email with the individual nominated to become a Senior Responsible Officer, a date and time for the nominated individual(s) to attend a face to face verification meeting in person or by video link.	SMKI Registration Authority Personnel	5.2.9
5.2.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the nominated individual, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) nominated to act on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the nominated individual shall	SMKI Registration Authority or applicant organisation, as appropriate	5.2.10

		inform the SMKI Registration Authority, by email and telephone, and shall agree and confirm an alternative date and time.		
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting in person or by video link, the SMKI Registration Authority shall, in person: a. check proof of individual identity provided for each nominated individual against the information listed on the SRO Nomination Form and the Nominee Details Form; and b. verify the individual identity for each nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority	If not successfully verified, 5.2.11; if successfully verified, 5.2.12
5.2.11	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has not been verified successfully and has not become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.5 once issues addressed
5.2.12	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.13
5.2.13	As soon as reasonably	Add the relevant SRO to the DCC's list of SROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the	SMKI Registration Authority	End of Procedure

	practicable, 5.2.12	Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.		
--	---------------------	--	--	--

5.3 Procedure for becoming an Authorised Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become an Authorised Responsible Officer in respect of that Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.3.1	As required	Complete the SMKI ARO Nomination Form and Nominee Details Form as set out in SMKI RAPP Annex A (A4) and Annex A (A5), ensuring that: a. the information entered on the forms is complete and accurate; b. the SMKI ARO Nomination Form and Nominee Details Form are authorised by an SRO on behalf of the applicant organisation; and c. the SRO has confirmed that the SMKI ARO Nominee has been subject to a standard that is compliant with BS 7858:2019 or an equivalent standard.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider).	5.3.2
5.3.2	As required, following 5.3.1	Submit the completed SMKI ARO Nomination Form and Nominee Details Form to the SMKI Registration Authority in writing, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.3	As soon as reasonably	Acknowledge receipt by email to the SRO as identified on	Service Desk	5.3.4

	practicable following receipt of completed ARO Nomination Form and Nominee Details Form	the SMKI ARO Nomination Form.		
5.3.4	As soon as reasonably practicable following 5.3.3	Analyse the information entered on the SMKI ARO Nomination Form and Nominee Details Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email.	SMKI Registration Authority	If complete, 5.3.6; if not complete, 5.3.5
5.3.5	Once omissions / discrepancies are addressed	Submit a revised SMKI ARO Nomination Form and/or Nominee Details Form to the Registration Authority in writing as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.6	As soon as reasonably practicable, following 5.3.4	If the SMKI Registration Authority has any questions about the information submitted, contact an SRO of the applicant organisation via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm whether the nominated individual is authorised to become an ARO.	SMKI Registration Authority	If confirmed as authorised, 5.3.8; if not authorised, 5.3.7
5.3.7	As soon as reasonably practicable	Notify the individual and an SRO that the procedure for becoming an ARO has not been successful for relevant	SMKI Registration Authority	5.3.5 once issues addressed

	following rejection	nominated individual, by email.		
5.3.8	As soon as reasonably practicable, following 5.3.6	Agree with the applicant organisation and confirm the date and time for the ARO verification meeting, via email to the nominated individual and an SRO of the applicant organisation.	SMKI Registration Authority	5.3.9
5.3.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform an SRO and the nominated individual, by email, and shall agree and confirm an alternative date and time. If it is identified that the nominated individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, an SRO shall inform the SMKI Registration Authority, by email, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.3.10
5.3.10	In ARO verification meeting	At the ARO face-to-face verification meeting, the SMKI Registration Authority shall, in person, for the nominated individual: a. check proof of individual identity provided against the information listed on the ARO Nomination Form and Nominee Details Form; and	SMKI Registration Authority	If verified, 5.3.12; if not verified, 5.3.11

		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.		
5.3.11	As soon as reasonably practicable, following ARO verification meeting	Notify: a. the nominated individual that they have become an ARO, verbally; or b. in writing to the SRO, that the verification has not been successful for the nominated individual, that the nominated individual has not become an ARO, and provide reasons for the rejection and request that the nominated individual is required to attend a further ARO verification meeting once the issues have been remedied.	SMKI Registration Authority	If successful, 5.3.12; otherwise 5.3.5 once issues are addressed
5.3.12	As soon as reasonably practicable, following ARO verification meeting	Ensure that the applicant organisation is notified of the individuals whose identity has been verified and have become AROs by email or via the Service Desk updating the relevant ticket, ensuring that there is a record for audit purposes.	SMKI Registration Authority or Service Desk	5.3.13
5.3.13	As soon as reasonably practicable, following 5.3.12	Add the relevant individual to the DCC's list of AROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	Procedure as set out in SMKI RAPP section 5.5

5.4 Procedure for provision of credentials to AROs for accessing SMKI Services and the SMKI Repository Service and file signing

The procedure and processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to provide credentials for accessing SMKI Services and/or the SMKI Repository Service or for file signing to Authorised Responsible Officers in respect of a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider). The SMKI Registration Authority shall not provide such credentials to an individual on behalf of a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider), other than where the organisation has completed SMKI and Repository Entry Process Tests and such individuals have become Authorised Responsible Officers.

Step	When	Obligation	Responsibility	Next Step
5.4.1	During ARO verification meeting and after becoming an ARO	IKI credentials for submission of CSRs in respect of Organisation Certificates using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Organisation Certificates and/or Device Certificates, and where the Party, RDP, Manufacturer, SECCo or DCC Service Provider has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal interface, provide the ARO with: a. If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Organisation Certificates and retrieval of	SMKI Registration Authority	5.4.2

		corresponding Organisation Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. b. If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of CSRs in respect of Organisation Certificates and retrieval of corresponding Organisation Certificates. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal		
--	--	--	--	--

		Interface via a DCC Gateway Connection. Where the Party, RDP, Manufacturer, SECCo or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
5.4.2	During ARO verification meeting and after becoming an ARO	IKI credentials for submission of CSRs in respect of Device Certificates using SMKI Portal via DCC Gateway Connection If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where	SMKI Registration Authority	5.4.3

		there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with: a. If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Device Certificates and retrieval of corresponding Device Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. Where the Party, RDP or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process		
--	--	--	--	--

		Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
5.4.3	During ARO verification meeting and after becoming an ARO	IKI credentials for Ad Hoc Device CSR Web Service If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Ad Hoc Device CSR Web Service, the SMKI Registration Authority shall, if the applicant organisation has access to a DCC Gateway Connection and is a Supplier Party or the DCC, and where the Supplier Party or DCC (in its role as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via USB token or optical media, with Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided, via USB token or optical media, by the applicant organisation in accordance with the SMKI Interface Design Specification, sections 2.4 xv, xvi & xvii. If the Supplier Party or DCC (in its role as DCC Service	SMKI Registration Authority	5.4.4

		Provider) has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the Supplier Party or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.		
5.4.4	During ARO verification meeting and after becoming an ARO	IKI credentials for Batched Device CSR Web Service If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Batched Device CSR Web Service, the SMKI Registration Authority shall determine, if the applicant organisation has access to a DCC Gateway Connection and the applicant is not a Supplier Party or the DCC, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device	SMKI Registration Authority	5.4.5

		Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the appointed ARO, via USB token or optical media, with Batched Device CSR Web Service access credentials for Device Certificates, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification, sections 2.5 xxvi & xxvii. If the applicant organisation has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Batched Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.		
--	--	--	--	--

5.4.5	During ARO verification meeting and after becoming an ARO	Credentials for SMKI Repository portal If the applicant organisation has access to a DCC Gateway Connection, and it wishes to access the SMKI Repository via the SMKI Repository Portal and has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password, to be accessed via the SMKI Repository Portal, that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification, section 2.1.2. If the applicant organisation has access to a DCC Gateway Connection, it wishes to access the SMKI Repository via the SMKI Repository Portal but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting: a. DCC shall, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password via secured electronic means that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in	SMKI Registration Authority	5.4.6
-------	---	--	-----------------------------	-------

		the SMKI Repository Interface Design Specification, section 2.1.2.		
5.4.6	During ARO verification meeting and after becoming an ARO	Credentials for SMKI Repository web service If the applicant organisation has access to a DCC Gateway Connection, and wishes to access the SMKI Repository Web Service interface and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification section 2.2.1, along with a certificate which enables verification of the SMKI Repository Web Service server identity. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository Web Service interface but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on electronic media as set out in the "SMKI Repository User Guide", the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface	SMKI Registration Authority	5.4.7

		Design Specification section 2.2.1.		
5.4.7	During ARO verification meeting and after becoming an ARO	Credentials for SMKI Repository Portal SFTP If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface, as set out in the SMKI Repository Interface Design Specification section 2.3.1. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via the SMKI Repository Portal profile page, with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface, as set out in the SMKI Repository Interface Design Specification section 2.3.1.	SMKI Registration Authority	5.4.8

5.4.8	During ARO verification meeting and after becoming an ARO	IKI credentials for file signing If the applicant organisation wishes the ARO to be Issued with a File Signing Certificate for the purposes as set out in the Code, the SMKI Registration Authority shall either: a. provide the ARO with a Cryptographic Credential Token enabling the ARO to submit a CSR for a File Signing Certificate; in which case, the ARO shall use the software on the Cryptographic Credential Token to generate a Private Key for a File Signing Certificate to submit a CSR for a File Signing Certificate; and if the CSR is valid, the ICA shall Issue a File Signing Certificate under the IKI Certificate Policy, to be used for the purposes as set out in the Code; or b. provide the appointed ARO, via USB token or optical media, with an IKI File Signing Certificate, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation.	SMKI Registration Authority	5.4.9
5.4.9	During ARO verification meeting and after issuance of credentials	Acceptance of credentials issued in steps 5.4.1 to 5.4.8 The SMKI Registration Authority shall complete the relevant sections of the Nominee Details Form in Annex A (A5) accordingly to	SMKI Registration Authority ARO	End of procedure

		confirm credential issuance either manually or digitally and give the form to the ARO, retaining a copy of the original. The ARO shall confirm receipt of and acceptance of the credentials issued by completing the relevant sections of the Nominee Details Form in Annex A (A5) either manually or digitally. The SMKI Registration Authority shall retain a copy of the receipt. Should the ARO not wish to accept these credentials, the ARO shall notify the SMKI Registration Authority immediately and not sign for the Certificate and / or Cryptographic Credential.		
--	--	--	--	--

8.3 Revocation of SMKI Services and / or the SMKI Repository Service access credentials and / or IKI File Signing Certificates

8.3.1 General obligations relating to revocation of ARO credentials for accessing SMKI Services and / or the SMKI Repository Service and / or File Signing Certificates

A Senior Responsible Officer on behalf of a Party, RDP, ~~Manufacturer~~, SECCo or the DCC (in its role as DCC Service Provider) may request the revocation of access credentials in respect of an Authorised Responsible Officer acting on behalf of that Party, RDP, ~~Manufacturer~~, SECCo or the DCC (as DCC Service Provider) or revocation of an IKI File Signing Certificate for which that Party, RDP, ~~Manufacturer~~, SECCo is an Authorised Subscriber, using the form as set out in Annex A (A7) and clearly identifying the credentials to be revoked.

The permitted reasons for revocation of authentication credentials shall be as listed immediately below:

- a) An applicant wishes an IKI File Signing Certificate or the credentials of an ARO to be revoked.
- b) A Party, RDP, ~~Manufacturer~~, SECCo or the DCC (as DCC Service Provider), of which the ARO is a representative, becomes ineligible to access SMKI Services and/or the SMKI Repository Service or ceases to become an Authorised Subscriber for Device Certificates or Organisation Certificates, or both, as appropriate.
- c) If there is a change to any of the information that was used to verify the identity of an ARO (but where the renewal or replacement of documents used to verify such identity, where the identity information remains the same, shall not constitute a change).
- d) A Party, RDP, ~~Manufacturer~~, DCC (as DCC Service Provider), or SECCo notifies the SMKI Registration Authority that it reasonably believes that the ARO is a threat to the security, integrity, or stability of the SMKI Services and/or the SMKI Repository Service.

- e) The information on which the identity of an ARO was established is known, or is reasonably suspected, to be inaccurate.
- f) The authentication credentials issued to the ARO are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to an ARO is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

Where access credentials have been revoked and the Party, RDP, ~~Manufacturer~~, SECCo or DCC (as DCC Service Provider) wishes to receive new access credentials, that Party, RDP, ~~Manufacturer~~, SECCo or DCC (as DCC Service Provider) shall submit a new ARO Nomination Form.

8.3.2 Procedure for revocation of SMKI Services and / or the SMKI Repository Service access credentials for AROs and / or IKI File Signing Certificates

The procedure for verification and, where verified, revocation of authentication credentials or IKI File Signing Certificates is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.2.1	As required	Complete the Credential Revocation Request Form as set out in SMKI RAPP Annex A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised by an SRO on behalf of the applicant organisation.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider)	8.3.2.2
8.3.2.2	As required, following 8.3.2.1	Submit the completed Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer , SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.3	As soon as reasonably practicable following 8.3.2.2	Acknowledge receipt by email to the SRO as identified on the Credential Revocation Request Form or via the Service Desk updating the relevant ticket, ensuring a record is kept.	SMKI Registration Authority or Service Desk	8.3.2.4
8.3.2.4	As soon as reasonably practicable	Analyse the information entered on the Credential Revocation Request Form;	SMKI Registration Authority	If complete, 8.3.2.6; if not

	following 8.3.2.3	determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with an SRO via email.		complete, 8.3.2.5
8.3.2.5	Once omissions / discrepancies are addressed	Submit a revised Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.6	As soon as reasonably practicable, following 8.3.2.4	Contact the SRO as identified on the Credential Revocation Request Form, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm the application identified by the Credential Revocation Request Form is authorised.	SMKI Registration Authority	If confirmed as authorised, 8.3.2.8; if not authorised, 8.3.2.7
8.3.2.7	As soon as reasonably practicable following rejection	Notify the SRO that was contacted in step 8.3.2.3, that the procedure in respect of the application has not been successful, by email.	SMKI Registration Authority	End of procedure
8.3.2.8	As soon as reasonably practicable following 8.3.2.6	Notify the SRO that was contacted in step 8.3.2.3, and the DCC's CISO by email that the revocation request has been accepted.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.9
8.3.2.9	As soon as reasonably practicable following 8.3.2.8	Revoke the credentials for the relevant service, for the identified ARO or relevant IKI File Signing Certificate as indicated by the SRO on the Credential Revocation Request Form. In doing so, the DCC shall, where required to revoke the credentials, revoke all associated IKI	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.10

		Certificates. DCC shall ensure that access to the relevant service is prevented from the point of revocation.		
8.3.2.10	As soon as reasonably practicable following 8.3.2.9	Notify the SRO that was contacted in step 8.3.2.3 of the successful revocation of credentials for the ARO or relevant IKI File Signing Certificate. Where such revocation results in the individual that is the subject of the Credential Revocation Request Form no longer having any valid credentials issued to them in accordance with the SMKI RAPP, the SMKI Registration Authority shall notify the SRO that was contacted in step 8.3.2.3 that the individual is no longer an ARO, by email.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.11
8.3.2.11	As soon as reasonably practicable following 8.3.2.10	Where the revoked credentials were issued on a Cryptographic Credential Token or Cryptographic Credential Tokens, the Party, RDP, Manufacturer , SECCo or DCC Service Provider shall, where such Cryptographic Credential Tokens are in the possession of the applicant organisation, send the Cryptographic Credential Token or Cryptographic Credential Tokens to the DCC, via secure courier.	SRO on behalf of the applicant organisation	8.3.2.12
8.3.2.12	As soon as reasonably practicable following 8.3.2.11	The DCC shall verifiably destroy all Secret Key Material or Certificates contained on the returned Cryptographic Credential Token.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.2.13

8.3.2.13	As soon as reasonably practicable following 8.3.2.12	Record the details of the credentials that have been revoked in respect of the ARO as identified on the Credential Revocation Request Form or relevant IKI File Signing Certificate, plus, if relevant, update the DCC's list of AROs, in a manner which is auditable.	SMKI Registration Authority	End of procedure
----------	--	--	-----------------------------	------------------

Annex B. Definitions

Authorised Responsible Officer (ARO)	Means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, Manufacturer , SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).
Senior Responsible Officer (SRO)	Means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, Manufacturer , SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).