

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

MP110 ‘Aligning SEC Appendix D with DCC Processes’

Annex A

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Appendix D ‘SMKI Registration Authority Policies and Procedures’

These changes have been redlined against Appendix D version 2.0.

Amend Section 2 as follows:

2 SMKI Registration Authority obligations to support DCCKI identity verification

The DCCKI RAPP sets out the procedures by which nominated individuals may become DCCKI Senior Responsible Officers and/or DCCKI Authorised Responsible Officers in order to act on behalf of a Party, RDP or a DCC Service Provider in respect of DCCKI Services and DCCKI Repository Services. The DCCKI RAPP also sets out the activities undertaken by the DCC as DCCKI Registration Authority.

Upon request from the DCCKI Registration Authority to verify the identity of an individual nominated to be a DCCKI SRO or DCCKI ARO, the SMKI Registration Authority shall:

- a) arrange a verification meeting with the nominated individual, at a date and time that is mutually agreed;
- b) at the verification meeting, verify the individual identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG 45 (Identity Proofing and Verification of an Individual), or except to the extent that the DCC otherwise notifies the SMKI Registration Authority, to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA for the purposes of verification of individuals to become an SMKI SRO or SMKI ARO;
- c) following the verification meeting, notify the nominated individual whether the process to verify their individual identity has been successful; and
- d) following the verification meeting, ~~confirm in writing to notify~~ the DCCKI Registration Authority whether the identity of the individual has been successfully verified.

All other procedural steps required by which nominated individuals may become DCCKI Senior Responsible Officers and/or DCCKI Authorised Responsible Officers in order to act on behalf of a Party, RDP or DCC Service Provider (acting on behalf of the DCC) in respect of DCCKI Services and DCCKI Repository Services are as set out in the DCCKI RAPP.

Provided that the DCC need not repeat these processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming a DCCKI SRO and/or DCCKI ARO where the required verification processes have already been carried out for the purposes of identifying them as being an SMKI SRO and/or SMKI 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 a DCCKI ARO or DCCKI SRO, be treated as if it had taken place after that date.

Amend Section 4.1.3 as follows:

.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, SECCo or a DCC Service Provider (acting on behalf of the DCC), an SRO shall advise the DCC Service Desk of the change and shall ensure that the procedure and detailed processes as set out in SMKI RAPP Section 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 DCC Service Desk of the change;
- b) where required to do so by the SMKI Registration Authority to 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 Error: Reference source not found or in respect of the revised evidence of identity, as soon as is reasonably practicable after a material ~~the~~ change occurs ; and
- c) where necessary, for an ARO ensure that credentials used to access SMKI Services and/or SMKI Repository Services are revoked as set out in SMKI RAPP Section Error: Reference source not found.

No Party, RDP, 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 to .

Amend Section 4.1.4 as follows:

.1.4 Director or Company Secretary ceasing to be eligible to act on behalf of a Party, RDP or SECCo

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

- a) the Director or Company Secretary themselves, or the another Director or Company Secretary Senior Responsible Officer (SRO) whose identity has previously been verified by the DCC, shall advise the DCC 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 or Company Secretary; and
- c) if b) is successful, the DCC shall update the DCC's records of authorised individuals for the Party, RDP or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP or SECCo.

Amend Section 4.1.5 as follows:

.1.5 SROs ceasing to be eligible to act on behalf of a Party, RDP or SECCo

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

- a) the SRO themselves, or a Director, ~~or~~ Company Secretary or SRO whose identity has previously been verified by the DCC, shall advise the DCC 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 the SRO, an authorised Director or Company Secretary; and
- c) if b) is successful, update the DCC's records of authorised individuals for the Party, RDP or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP or SECCo.

Amend Section 5.1 as follows:

.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, 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:	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, SECCo	5.1.2

		a) the information entered on the form is complete and accurate; b) the EUI64 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 EUI64 Identifier range for any other User Role, other than where a particular EUI64 Identifier is allowed to be used for more than one 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.	or DCC Service Provider	
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, 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	SMKI Registration Authority <u>DCC Service Desk</u>	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 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	SMKI Registration Authority	If complete, accurate and no discrepancies, 5.1.6; if not

		the submitted EUI64 Identifier ranges are consistent with the restriction set out in step 5.1.1. Where there are omissions/discrepancies or the submitted EUI64 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 or in writing , with the Director or Company Secretary that has authorised the Organisation Information Form		complete and 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, 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 held at DCC's offices unless otherwise agreed by the DCC Chief Information Security Officer, where such DCC agreement shall not unreasonably be withheld via a video link or face to face if preferred.	SMKI Registration Authority	5.1.7
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 telephone , 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, an SRO shall inform the SMKI Registration Authority, by email and telephone , 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 Level 3 (Verified) pursuant to the CESG GPG46 (Organisation Identity) , or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA;	SMKI Registration Authority	If not successful, 5.1.9; if successful, 5.1.10

		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 listed on the Organisation Information Form and the Nominee Details Form; and d) <u>the</u> individual identity of the nominating individual to Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.		
5.1.9	As soon as reasonably practicable, following 5.1.8	<u>If verification in 5.1.8 is unsuccessful, n</u> otify the nominating Director, or Company Secretary <u>or SRO</u> that verification of the organisational identity has been unsuccessful, in writing <u>by e-mail</u>	SMKI Registration Authority	5.1.5 once issues addressed
5.1.10	As soon as reasonably practicable, following 5.1.8	<u>If verification in 5.1.8 is unsuccessful, i</u> nform the nominating Director, or Company Secretary <u>or SRO</u> that the organisational identity has been successfully verified, by e-mail <u>in writing</u>	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 of Appendix A to the Code and Section 4.1.2 of Appendix B to the Code	SMKI Registration Authority	End of procedure

Amend Section 5.2 as follows:

.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, SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.2.1	As required	Complete the SRO Nomination Form and Nominee Details Form, as set out in SMKI RAPP Annex A (A3) and Annex A (A5). In doing so, the individual completing the 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, 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 SRO Nomination Form and Nominee Details Form are both authorised, where applicable, by a Director or Company Secretary on behalf of the applicant organisation	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, SECCo or DCC (as DCC Service Provider).	5.2.2
5.2.2	As required, following 5.2.1	Submit the completed 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, SECCo or DCC (as DCC Service Provider).	5.2.3
5.2.3	As soon as reasonably practicable following receipt of completed SRO Nomination Form	Acknowledge receipt by email to the Director or Company Secretary that has authorised the SRO Nomination Form	DCC Service Desk SMKI Registration Authority	5.2.4

5.2.4	As soon as reasonably practicable following 5.2.3	Analyse the information entered on the SRO Nomination Form and Nominee Details Form, to: a) determine completeness and any discrepancies; and b) confirm, using the DCC's records or using publicly available information, that the Director or Company Secretary that has authorised the SRO Nomination Form has the role indicated on the SRO Nomination Form. Where there are omissions/discrepancies, agree actions with the nominating individual, via email or in writing	SMKI Registration Authority	If complete, 5.2.6; if not complete, 5.2.5
5.2.5	Once omissions / discrepancies addressed	Submit a revised 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, SECCo or DCC (as DCC Service Provider).	5.2.3
5.2.6	As soon as reasonably practicable, following 5.2.4	<u>If the SMKI Registration Authority has any questions about the information submitted,</u> contact the Director or Company Secretary that nominated the individual, via telephone, using the telephone number provided previously in the Organisation Nomination Form, to confirm whether each nominated individual on the SRO Nomination Form is authorised to act on behalf of the organisation as SRO and seek confirmation of information provided on the SRO Nomination Form in order to provide confidence that the correct person has been contacted	SMKI Registration Authority	If confirmed as authorised, 5.2.8; if not confirmed as authorised, 5.2.7
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, <u>by e-mail in writing</u> to the Director, or Company Secretary <u>or SRO</u> that has authorised the SRO Nomination Form	SMKI Registration Authority	5.2.6 once issues resolved
5.2.8	As soon as reasonably practicable, following 5.2.6	Agree, via email with the Director or Company Secretary of the applicant organisation who nominated the individual <u>nominated</u> to become a Senior Responsible Officer, a date and time for the nominated individual(s) to attend a <u>face to face</u> verification meeting <u>in person or by video link</u>	SMKI Registration Authority	5.2.9
5.2.9	As soon as	If it is identified that SMKI Registration Authority Personnel will be	SMKI Registration Authority or	5.2.10

	reasonably practicable on becoming aware of unavailability	unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the nominated individual and the applicant Director or Company Secretary by email and telephone , 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 inform the SMKI Registration Authority, by email and telephone, and shall agree and confirm an alternative date and time.	applicant organisation, as appropriate	
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting <u>in person or by video link</u> , 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 Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by SMKI PMA	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 practicable, 5.2.12	Add the relevant SRO to the DCC's list of SROs, in accordance with Section 4.1.2 of Appendix A to the Code and Section 4.1.2 of Appendix B to the Code	SMKI Registration Authority	End of Procedure

Amend Section 5.3 as follows:

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, SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.3.1	As required	Complete the 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; and b) the ARO Nomination Form and Nominee Details Form are authorised by an SRO on behalf of the applicant organisation	SRO on behalf of the applicant organisation, which shall be a Party, RDP, SECCo or DCC (as DCC Service Provider)	5.3.2
5.3.2	As required, following 5.3.1	Submit the completed 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, the SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.3	As soon as reasonably practicable following receipt of completed ARO Nomination Form and Nominee Details Form	Acknowledge receipt by email to the SRO as identified on the ARO Nomination Form	SMKI Registration Authority DCC Service Desk	5.3.4
5.3.4	As soon as reasonably practicable following 5.3.3	Analyse the information entered on the ARO Nomination Form and Nominee Details Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email or in writing	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 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, SECCo or DCC (as	5.3.3

			DCC Service Provider)	
5.3.6	As soon as reasonably practicable, following 5.3.4	<u>If the SMKI Registration Authority has any questions about the information submitted,</u> C 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 following rejection	Notify <u>the individual and</u> an SRO that the procedure for becoming an ARO has not been successful for relevant nominated individual, <u>by e-mail in writing</u>	SMKI Registration Authority	5.3.5 once issues addressed
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 an SRO for the applicant organisation and the nominated individual <u>and the SRO</u>	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 RA 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 telephone , 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 telephone , 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 b) verify the identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	SMKI Registration Authority	If verified, 5.3.12; if not verified, 5.3.11
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	SMKI Registration Authority	If successful, 5.3.12; otherwise 5.3.5 once issues are addressed

		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		
5.3.12	As soon as reasonably practicable, following ARO verification meeting	Notify <u>Ensure that the applicant organisation is notified of the individuals whose identity has been verified and have become AROs by e-mail or via the DCC Service Desk, ensuring that there is a record for audit purposes, to the SRO on behalf of the applicant organisation, in writing of the individuals whose identity has been verified and have become AROs</u>	SMKI Registration Authority <u>or</u> <u>DCC Service Desk</u>	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	SMKI Registration Authority	Procedure as set out in SMKI RAPP section

Amend Section 5.4 as follows:

.4 Procedure for provision of credentials to AROs for accessing SMKI Services and SMKI Repository Services 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 SMKI Repository Services or for file signing to Authorised Responsible Officers in respect of a Party, RDP 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, 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 Organisation CSRs 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, SECCo or DCC Service Provider has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to	SMKI Registration Authority	5.4.2

		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 Organisation CSRs and retrieval of 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 Organisation CSRs 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, 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, 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	IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection	SMKI Registration Authority	5.4.3

	and after becoming an ARO	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 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 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: 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 Device CSRs 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; and a) a CA/Browser Forum recognised certificate which enables verification of the Ad Hoc Device CSR Web Service interface server identity, and that will be used as part of mutual authentication to the Ad Hoc Device CSR Web Service interface If the Supplier Party or DCC (in its role as DCC Service 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.	SMKI Registration Authority	5.4.4
-------	---	--	-----------------------------	-------

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 is not a Supplier Party or the DCC, in accordance with the steps set out in Section 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 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; and a CA/Browser Forum recognised certificate which enables verification of the Batched Device CSR Web Service interface server identity, and that will be used as part of mutual authentication to the Batched Device CSR Web Service interface. 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	SMKI Registration Authority	5.4.5

		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. 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 the SMKI Repository Interface Design Specification.	SMKI Registration Authority	5.4.6
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, 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	5.4.7

		SMKI Registration Authority shall provide, on electronic media as set out in the SMKI Repository User Guide, the ARO with: a) the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification, and b) a CA/Browser Forum recognised certificate which enables verification of the SMKI Repository Web Service interface server identity, and that will be used as part of mutual authentication to the SMKI Repository Web Service interface.		
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. 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.	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	SMKI Registration Authority	5.4.9

		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 in accordance with the SMKI Interface Design Specification.		
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 <u>to confirm credential issuance either manually or digitally and give the form to the ARO, retaining a copy of the original.</u> 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) <u>either manually or digitally. The SMKI Registration Authority shall retain a copy of the receipt.</u> 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.	SMKI Registration Authority ARO	End of procedure

Amend Section 5.5 as follows:

.5 Procedure for becoming an Authorised Subscriber

An organisation is an Authorised Subscriber for IKI File Signing Certificates where it has successfully appointed and maintains in place at least one SRO and at least one ARO.

The procedure detailed immediately below shall be conducted by the DCC, in order to determine whether a Party or RDP has become an Authorised Subscriber for Organisation Certificates, an Authorised Subscriber for Device Certificates, or both.

Step	When	Obligation	Responsibility	Next Step
5.5.1	As required	Complete the Authorised Subscriber Application Form as set out in SMKI RAPP Annex A (A2), ensuring that the information entered on the form is complete and accurate, and the Authorised Subscriber Application Form is authorised by an SRO on behalf of the applicant organisation	Nominating officer or SRO on behalf of the applicant organisation, which shall be a Party or RDP	5.5.2
5.5.2	As required, following 5.5.1	Submit the completed Authorised Subscriber Application Form to the SMKI Registration Authority in writing, as directed on the DCC Website	Applicant organisation, which shall be a Party or RDP	5.5.3
5.5.3	As soon as reasonably practicable following 5.5.2	Acknowledge receipt by email to the SRO or nominating officer as identified on the Authorised Subscriber Application Form	SMKI Registration Authority	5.5.4
5.5.4	As soon as reasonably practicable following 5.5.3	Analyse the information entered on the Authorised Subscriber Application Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email or in writing	SMKI Registration Authority	If complete, 5.5.6; if not complete, 5.5.5
5.5.5	Once omissions / discrepancies are addressed	Submit a revised Authorised Subscriber Application 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 or RDP	5.5.3
5.5.6	As soon as reasonably practicable, following 5.5.4	Contact the SRO as identified on the Authorised Subscriber Application Form via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority. The SMKI Registration Authority shall verbally confirm details for the SRO as held by the DCC to verify that the correct individual has been contacted. The SMKI Registration Authority shall confirm the applications indicated on the Authorised Subscriber Application Form are authorised	SMKI Registration Authority	If confirmed as authorised, 5.5.8; if not authorised, 5.5.7
5.5.7	As soon as reasonably practicable following rejection	Notify the SRO as identified on the Authorised Subscriber Application Form that the procedure in respect of the application has not been successful, in writing	SMKI Registration Authority	5.5.5 once issues addressed
5.5.8	As requested	Where the application organisation is not a DCC Service Provider, conduct the SMKI and Repository Entry Process Tests if SMKI and Repository Entry Process Tests have not been completed previously, in accordance with Sections H14.22 to H14.31 of the Code	Applicant organisation, in respect of the corresponding Authorised Subscriber Application Form	If successful or the applicant organisation is a DCC Service Provider (acting on

				behalf of the DCC), 5.5.10; if not successful, 5.5.9
5.5.9	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing, to SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the SMKI and Repository Entry Process Tests were not completed successfully	DCC	5.5.8 once issues addressed
5.5.10	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing to the relevant Party that the SMKI and Repository Entry Process Tests have been completed successfully	DCC	5.5.11
5.5.11	As soon as reasonably practicable, following 5.5.10	If the applicant organisation has indicated on its Authorised Subscriber Application Form that it wishes to become an Authorised Subscriber in respect of the Organisation Certificate Policy, the SMKI Registration Authority shall confirm in writing to the SRO as identified on the Authorised Subscriber Application Form that the applicant organisation has become an Authorised Subscriber for Organisation Certificates Where appropriate, the DCC shall issue credentials enabling the applicant to act as an Authorised Subscriber for Organisation Certificates, in accordance with the procedural steps as set out in section of this document.	SMKI Registration Authority	If the applicant organisation has indicated that it wishes to become an Authorised Subscriber for Organisation Certificates, 5.5.12; otherwise, 5.5.13
5.5.12	As soon as possible, following 5.5.11	If the applicant organisation has indicated on the Authorised Subscriber Application Form that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy, the SMKI Registration Authority shall assess whether there is evidence to confirm that the Party has completed the User Entry Process (defined in Section H1.10) and will use a DCC Gateway Connection to obtain Device Certificates.	SMKI Registration Authority	If determined to be an Authorised Subscriber for Device Certificates, 5.5.15; otherwise 5.5.13
5.5.13	As soon as possible, following 5.5.12	Confirm in writing by e-mail, to the SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the DCC has determined that applicant organisation is not eligible to become an Authorised Subscriber for Device Certificates.	SMKI Registration Authority	5.5.14
5.5.14	As soon as possible, following 5.5.13	<u>In the case of a dispute by the SRO or nominating officer</u> Where where the DCC has determined that there is no evidence as defined in 5.5.12 to support the applicant organisation to become such an Authorised Subscriber, the DCC shall notify the SMKI PMA of the refusal.	SMKI PMA or Panel	End of procedure

5.5.15	As soon as reasonably practicable, following 5.5.14, or, where a Supplier Party or the DCC (in its role as DCC Service Provider) has indicated that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy	The SMKI Registration Authority shall confirm <u>by e-mail in writing</u> , to the SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the applicant organisation has become an Authorised Subscriber for Device Certificates <u>and will also notify the DCC Service Desk</u> .	SMKI Registration Authority	5.5.16
5.5.16	As soon as reasonably practicable, following 5.5.15	The SMKI Registration Authority shall arrange and conduct a meeting, as soon as reasonably practicable, at which the credentials as set out in steps 5.4.2, 5.4.3 and 5.4.5 (as set out in Section 5.4 of this document) shall be provided, as appropriate.	SMKI Registration Authority	5.5.17
5.5.17	As soon as reasonably practicable, following 5.5.15 or 5.5.16	Update the DCC's list of Authorised Subscribers for Organisation Certificates and/or Device Certificates, for audit purposes.	SMKI Registration Authority	End of procedure

Amend Section 6.1 as follows:

6 SMKI Registration Authority registration procedures

The procedures as set out in SMKI RAPP Sections Error: Reference source not found to shall be undertaken in order for nominated individuals to act on behalf of the SMKI Registration Authority as a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel.

.1 General registration obligations

The SMKI Registration Authority shall:

- a) not permit any nominated individual to access Systems used to provide SMKI Services and/or SMKI Repository Services as a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel until the procedures in SMKI RAPP Sections Error: Reference source not found or Error: Reference source not found have been successfully completed;
- b) in performing the procedures as set out in SMKI RAPP Sections Error: Reference source not found and Error: Reference source not found, store and maintain records relating to individuals becoming SMKI Registration Authority Managers and SMKI Registration Authority Personnel, in accordance with the Code and the DCC's data retention policy;
- c) ensure that, at all times, there are at least two SMKI Registration Authority Managers; ~~and~~
- d) if there is a material change to any of the information used to verify the identity of any SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, ensure that its SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel undertakes the procedures as set out in SMKI RAPP Sections Error: Reference source not found or Error: Reference source not found in respect of the revised evidence of identity; ~~and~~;
- e) check the name and address of the SMKI Registration Authority manager or member of the SMKI Registration Authority Personnel before issuing a replacement token.

The DCC shall ensure that:

- a) for authentication credentials issued under the IKI Certificate Policy to Authorised Responsible Officers, ensure that such authentication credentials have a lifetime of ten years following issuance of such authentication credentials and shall cease to function upon after ten years following issuance; and
- b) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked.

Amend Section 6.4 as follows:

.4 Procedure for provision of credentials to a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel

The procedure for provision of credentials to a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, as detailed immediately below, shall be conducted by the DCC's CISO in respect of a SMKI Registration Authority Manager or a SMKI Registration Authority Manager in respect of a member of SMKI Registration Authority Personnel.

Step	When	Obligation	Responsibility	Next Step
6.4.1	In verification meeting, following confirmation of becoming a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel	Provide credentials in accordance with step 6.4.2 or 6.4.3 below, depending on whether the individual has become a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel	<u>DCC CISO or SMKI Registration Authority Manager</u>	If providing to a SMKI Registration Authority Manager, 6.4.2; if providing to a member of SMKI Registration Authority Personnel, 6.4.3
6.4.2	In verification meeting, following confirmation of becoming a SMKI Registration Authority Manager	Provide the SMKI Registration Authority Manager with credentials as listed immediately below, to be used to perform activities on behalf of the SMKI Registration Authority: a) one Cryptographic Credential Token containing authentication credentials issued under the IKI Certificate Policy which can be used to authenticate the individual to the SMKI RA Portal; and b) usernames and passwords enabling for the purposes of authentication to the SMKI Repository Portal.	<u>DCC's CISO</u> <u>DCC CISO or SMKI Registration Authority Manager</u>	6.4.4
6.4.3	In verification meeting, following	Provide the member of SMKI Registration Authority Personnel with credentials as listed immediately below, to be used to perform activities on behalf of the SMKI	SMKI Registration Authority Manager	6.4.4

	confirmation of becoming a member of SMKI Registration Authority Personnel	Registration Authority: a) one Cryptographic Credential Token containing authentication credentials issued under the IKI Certificate Policy which can be used to authenticate the individual to the SMKI RA Portal; and b) usernames and passwords enabling for the purposes of authentication to the SMKI Repository Portal.		
6.4.4	In verification meeting, following issuance of credentials	The SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel shall sign that they accept the credentials issued to them on the Cryptographic Credential Token. Where the SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel does not accept the credentials they shall notify the DCC's CISO (in the case of the SMKI Registration Authority Manager) or otherwise the SMKI Registration Authority Manager) and shall not sign for the Cryptographic Credential Token.	SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel	End of Procedure

Amend Section 8.2.1 as follows:

.2 Revocation of Organisation Certificates

18.2.1 General Organisation Certificate revocation obligations

The DCC shall permit each of the following individuals to request the revocation of an Organisation Certificate, where the reasons for such revocation request must be one of the permitted reasons for Organisation Certificate revocation as set out in Section 4.9 in Appendix B of the Code:

- a) Any SMKI PMA member, on behalf of the SMKI PMA;
- b) Any Senior Responsible Officer for a Subscriber for an Organisation Certificate; or
- c) Any SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, on behalf of the DCC.

The DCC, in its role as SMKI Registration Authority, shall only accept CRRs through the following mechanisms (or a combination of such mechanisms):

- a) in writing, via registered post;
- b) via a secured electronic means; or
- c) in Person, at the offices of the SMKI Registration Authority, where the address of such offices shall be as set out on the DCC Website.

The revocation of an Organisation Certificate shall be permanent and the SMKI Registration Authority shall ensure that no revoked Organisation Certificate may be reinstated.

The DCC shall, each month, prepare and submit a report to the SMKI PMA regarding the number and nature of Organisation Certificate revocations. A null report is not required.

Amend Section 8.2.2 as follows:

.2.2 Procedure for Organisation Certificate Revocation

The procedure for authorisation, verification and, where verified, revocation of Certificates is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.2.2.1	As soon as reasonably practicable when Certificate revocation is required	An SMKI PMA Member on behalf of the SMKI PMA, an SRO on behalf of a Subscriber or the SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel on behalf of the DCC shall submit, using the mechanisms set out in SMKI RAPP Section 1, a CRR to the SMKI Registration Authority. The reason for such CRR shall be one of the permitted reasons for Organisation Certificate revocation as set out in Section 4.9 in Appendix B of the Code. Each CRR shall contain the following information, as set out in SMKI RAPP Annex A (A7) : a) Identify the Subscriber; b) Identify the Subscriber's SRO who is submitting the CRR; c) Unambiguously (i.e. by specifying the serial number of the Certificate) identify the Certificate to be revoked; and d) State the reason for the Certificate revocation.	SMKI PMA Member, Subscriber requiring Organisation Certificate revocation or SMKI Registration Authority Manager or SMKI Registration Authority Personnel	8.2.2.2
8.2.2.2	As soon as reasonably practicable, following 8.2.2.1	On receipt of a CRR, notify the SMKI Registration Authority Manager for verification, processing and/or approval. The SMKI Registration Authority shall treat each CRR and any associated circumstances as confidential. Where the CRR is submitted by an SMKI Registration Authority Manager, the approval in this step must be sought from a different SMKI Registration Authority Manager or the DCC's CISO.	SMKI Registration Authority Personnel	8.2.2.3
8.2.2.3	As soon as reasonably practicable	Where it has been submitted by an SRO, validate the Certificate Revocation Request by contacting a Senior Responsible Officer and confirming details for the SRO as provided in the original application to become an SRO:	SMKI Registration Authority Manager	If validated, 8.2.2.5; if invalid (considered

	following receipt	a) Where submitted in writing, the SMKI Registration Authority shall <u>send an e-mail to telephone</u> a Senior Responsible Officer. The SMKI Registration Authority shall 1) confirm such information from the relevant SRO Nomination Form, in order to provide confidence that the request is from an authorised SRO; and 2) confirm the details of the Organisation Certificate to which the revocation request received relates (as provided in the submitted letter) b) Where submitted in person, the SMKI Registration Authority shall 1) verify the handwritten signature of the Senior Responsible Officer against that held by the SMKI Registration Authority; 2) confirm details provided in the relevant SRO Nomination Form, in order determine that the request is authentic; and 3) confirm the details of the Organisation Certificate to which the CRR received relates. Where the Certificate Revocation Request was submitted by a SMKI Registration Authority Manager, a member of the SMKI Registration Authority Personnel or a member of the SMKI PMA, validate the Certificate Revocation Request by contacting a SMKI Registration Authority Manager or the SMKI PMA to confirm details of the Certificate Revocation Request.		malicious and/or inauthentic) or incomplete, 8.2.2.4
8.2.2.4	As soon as reasonably practicable following unsuccessful validation	<u>Where the Certificate Revocation Request is not validated as in 8.2.2.3, R</u> reject the revocation request and notify the Senior Responsible Officer (or where relevant member of the SMKI PMA) in respect of the Party that was contacted in step 8.2.2.3 to validate the revocation request, in writing, including the reasons for rejection and identify resulting steps to be taken	SMKI Registration Authority Manager	End of procedure
8.2.2.5	As soon as reasonably practicable following	<u>Notify the Senior Responsible Officer or member of the SMKI PMA that was contacted in step 8.2.2.3 to validate the revocation request and the DCC's CISO by phone that the revocation request has been accepted</u> <u>Where the Certificate Revocation Request is validated as in 8.2.2.3, the DCC shall carry out a check that the correct Certificate is to</u>	SMKI Registration Authority Manager	8.2.2.6

	successful validation	<u>be revoked and to obtain and record two-party approval of the authorisation and record the time from which the revocation is to take effect.</u>		
8.2.2.6	As soon as reasonably practicable following 8.2.2.5	Revoke the identified Organisation Certificate that is the subject of the CRR	SMKI Registration Authority Manager	8.2.2.7
8.2.2.7	As soon as reasonably practicable following notification, or every hour (whichever is sooner)	Update the relevant Certificate Revocation List (CRL) and publish such CRL to the SMKI Repository, as set out in the SMKI Interface Design Specification and the Appendix B of the Code.	SMKI Registration Authority	8.2.2.8
8.2.2.8	Following revocation	Notify the SRO submitting the CRR of the successful revocation of the Organisation Certificate in the CRR, <u>in writing by e-mail</u>	SMKI Registration Authority Manager	End of procedure

Amend Section 8.3.2 as follows:

.3.2 Procedure for revocation of SMKI Services and/or SMKI Repository Services 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, 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 in writing or via a secured electronic means, as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party, RDP, 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 <u>or via the DCC Service Desk</u> to the SRO as identified on the Credential Revocation Request Form <u>ensuring a record is kept</u>	SMKI Registration Authority <u>or DCC Service Desk</u>	8.3.2.4
8.3.2.4	As soon as reasonably practicable following 8.3.2.3	Analyse the information entered on the Credential Revocation Request Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email or in writing	SMKI Registration Authority	If complete, 8.3.2.6; if not 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 in writing or via a secured electronic means, as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party, RDP, SECCo or DCC (as DCC Service Provider)	8.3.2.6
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 <u>via telephone</u> , 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 7.3.2.3, that the procedure in respect of the application has not been successful, <u>in writing by e-mail</u>	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 7.3.2.3, and the DCC's CISO in writing <u>by e-mail</u> 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 Certificates. DCC shall ensure that access to the relevant service is prevented from the point of revocation.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.10
8.3.2.10	As soon as reasonably practicable following	Notify the SRO that was contacted in step 7.3.2.3 of the successful revocation of credentials for the ARO or relevant IKI File Signing	SMKI Registration Authority Personnel, on behalf of the	8.3.2.11

	8.3.2.9	Certificate. Where such revocation results in the individual that is the subject of the Credential Revocation Request 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 7.3.2.3 that the individual is no longer an ARO, in writing by e-mail	SMKI Registration Authority	
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 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

Amend Section 8.3.4 as follows:

3.4 Procedure for revocation of SMKI Services access credentials for SMKI Registration Authority Managers and SMKI Registration Authority Personnel

The procedure for verification and, where verified, revocation of credentials in respect of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.4.1	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:	SMKI Registration Authority Personnel DCC CISO, SMKI Registration Authority Manager,	8.3.4.2

		a) for a member of SMKI Registration Authority Personnel, by a SMKI Registration Authority Manager; or b) for a SMKI Registration Authority Manager, by the DCC's CISO.	or SMKI PMA Member.	
8.3.4.2	As required, following 8.3.4.1	Submit the completed Credential Revocation Request Form to a SMKI Registration Authority Manager, by hand in person	SMKI Registration Authority Personnel DCC CISO, SMKI Registration Authority Manager, or SMKI PMA Member.	8.3.4.3
8.3.4.3	As soon as reasonably practicable following 8.3.4.2	Analyse the information entered on the Credential Revocation Request Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree amendments and adjust form contents	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.4
8.3.4.4	As soon as reasonably practicable following 8.3.4.3	Revoke the credentials of the identified SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel as indicated on the Credential Revocation Request Form. <u>Where the Credential Revocation Request is validated as in 8.3.4.3, the DCC shall carry out a check that the correct Credential is to be revoked and record approval of the authorisation.</u>	SMKI Registration Authority Manager, as directed by the DCC's CISO	8.3.4.5
8.3.4.5	As soon as reasonably practicable following 8.3.4.4	Where such revoked credentials were issued on a Cryptographic Credential Token, the DCC shall retrieve such Cryptographic Credential Token from the identified SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel and shall verifiably destroy all Secret Key Material or Certificates contained on the Cryptographic Credential Token	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.6
8.3.4.6	As soon as reasonably practicable following 8.3.4.5	Record the details of the credentials that have been revoked in respect of the member of SMKI Registration Authority Personnel or SMKI Registration Authority Manager as identified on the Credential Revocation Request Form	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.7
8.3.4.7	As soon as reasonably practicable following 8.3.4.5	Notify the SMKI Registration Authority Personnel, SMKI Registration Authority Manager, or SMKI PMA Member who submitted the original CRR Form that the revocation has been completed.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	End of procedure