

# **SMKI Registration Authority Policies and Procedures (SMKI RAPP)**

## Contents

<b>1</b>	<b>Introduction .....</b>	<b>4</b>
1.1	Purpose .....	4
<b>2</b>	<b>SMKI Registration Authority obligations to support DCCKI identity verification .....</b>	<b>5</b>
<b>3</b>	<b>SMKI Roles.....</b>	<b>6</b>
3.1	Party, RDP, SMKI PMA, Panel and DCC representatives.....	6
3.2	SMKI Registration Authority representatives .....	7
<b>4</b>	<b>Party, RDP, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures .....</b>	<b>9</b>
4.1	General registration obligations.....	9
4.1.1	Organisation, individual, and RA obligations .....	9
4.1.2	High level overview of SMKI Registration Authority procedures.....	10
4.1.3	Change of details .....	12
4.1.4	Director or Company Secretary ceasing to be eligible to act on behalf of a Party or RDP ..	13
4.1.5	SROs ceasing to be eligible to act on behalf of a Party or RDP .....	13
<b>5</b>	<b>Detailed Party, RDP, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures and processes.....</b>	<b>14</b>
5.1	Procedure and processes to verify organisational identify .....	14
5.2	Procedure for becoming a Senior Responsible Officer.....	17
5.3	Procedure for becoming an Authorised Responsible Officer .....	20
5.4	Procedure for provision of credentials to AROs for accessing SMKI Services and SMKI Repository Services .....	24
5.5	Procedure for becoming an Authorised Subscriber .....	32
<b>6</b>	<b>SMKI Registration Authority registration procedures .....</b>	<b>36</b>
6.1	General registration obligations.....	36
6.2	Procedure for becoming a SMKI Registration Authority Manager .....	37
6.3	Procedure for becoming a member of SMKI Registration Authority Personnel .....	38
6.4	Procedure for provision of credentials to a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel .....	39
<b>7</b>	<b>Submission of CSRs and Issuance of Certificates .....</b>	<b>41</b>
7.1	Submission of Certificate Signing Requests.....	41
7.2	Issuance of Certificates .....	41
<b>8</b>	<b>Revocation.....</b>	<b>42</b>
8.1	Revocation of Device Certificates.....	42
8.2	Revocation of Organisation Certificates .....	42
8.2.1	General Organisation Certificate revocation obligations.....	42
8.2.2	Procedure for Organisation Certificate Revocation .....	43
8.3	Revocation of SMKI Services and/or SMKI Repository Services access credentials .....	45
8.3.1	General obligations relating to revocation of ARO credentials for accessing SMKI Services and/or SMKI Repository Services.....	45
8.3.2	Procedure for revocation of SMKI Services and/or SMKI Repository Services access credentials for AROs .....	46
8.3.3	General obligations relating to revocation of SMKI Registration Authority Manager or SMKI Registration Authority Personnel credentials for accessing SMKI Services and/or SMKI Repository Services .....	48
8.3.4	Procedure for revocation of SMKI Services access credentials for SMKI Registration Authority Managers and SMKI Registration Authority Personnel .....	49
	<b>Appendix A Organisation Information Form .....</b>	<b>50</b>
	<b>Appendix B Authorised Subscriber / Interface Access Application Form .....</b>	<b>52</b>
	<b>Appendix C SRO Nomination Form .....</b>	<b>54</b>

---

<b>Appendix D</b>	<b>ARO Nomination Form .....</b>	<b>55</b>
<b>Appendix E</b>	<b>Nominee Details Form.....</b>	<b>57</b>
<b>Appendix F</b>	<b>Organisation Certificate Revocation Request Form .....</b>	<b>59</b>
<b>Appendix G</b>	<b>Credential Revocation Request Form .....</b>	<b>60</b>
<b>Appendix H</b>	<b>Definitions.....</b>	<b>61</b>

# **1 Introduction**

## **1.1 Purpose**

The SMKI Registration Authority Policies and Procedures (SMKI RAPP) sets out the activities undertaken by the DCC in its capacity as the SMKI Registration Authority in accordance with Section L of the Code, and Appendices A, B and [reference to IKI Certificate Policy] to the Code. The SMKI RAPP also sets out the activities undertaken by the SMKI Registration Authority in support of the procedures set out in the DCCKI RAPP, as set out in Section 2 of this document.

This SMKI RAPP is a SEC Subsidiary Document and is one of the SMKI SEC Documents, as set out in Section L9.4 of the Code.

## 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, the Panel 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 GPG45 RSDOPS framework, 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 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, the Panel 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.

### 3 SMKI Roles

This SMKI RAPP details the roles of Parties, RDPs, the SMKI PMA, the Panel and DCC in the context of access to SMKI Services and/or SMKI Repository Services 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, the SMKI PMA, the Panel or the DCC (acting in its role as DCC Service Provider) in respect of SMKI Services and SMKI Repository Services.

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 DCC 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, SMKI PMA, Panel and DCC representatives

Individuals permitted to act as representatives of a Party, RDP, the SMKI PMA, the Panel 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, 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 or the DCC (for DCC Service Provider personnel), the SMKI PMA Chair for the SMKI PMA or the Panel Chair for the Panel. 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 SMKI Repository Services. 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 SMKI Repository Services is set out in Section 5.4. The DCC shall permit only AROs to act on behalf of a Party, RDP, SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider) for the purposes of accessing SMKI Services and/or SMKI Repository Services. Depending upon the processes followed, an ARO may also be authorised to act on behalf of a Party 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 SMKI Repository Services on behalf of the organisation that they represent, as set out in the SMKI Repository Interface Design Specification.

Each Party, RDP 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 SMKI Repository Services, 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 SMKI Repository Services 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, the SMKI PMA, the Panel and the DCC (in its role of DCC Service Provider) shall refrain from dealing with DCC personnel (including Registration Authority Managers and Registration Authority Personnel) other than as directed by the DCC Service Desk for the purposes of submitting CSRs and 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; and
- d) provision of the means to authenticate access to SMKI Services and/or SMKI Repository for authorised Party or RDP representatives, SMKI PMA members, Panel Members, 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 to 5.5, incorporating:
  - i. verification of organisational identity;
  - ii. verification and authorisation of individuals nominated to become SROs of 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 SMKI Repository Services for authorised Party or RDP representatives, SMKI PMA members, Panel Members 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 Certificate Revocation Requests; and
- c) processing of requests for revocation of credentials used to access SMKI Services and/or SMKI Repository Services.

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 Certificate Revocation Requests (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 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 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, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures**

### **4.1 General registration obligations**

#### **4.1.1 Organisation, individual, and RA obligations**

Each Party, RDP, the SMKI PMA, the Panel and the DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or SMKI Repository Services 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 Appendices A to E, available via the internet facing DCC Website;
- b) provide reasonable support and advice to each Party, the SMKI PMA, the Panel 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, the SMKI PMA, the Panel 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 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 SMKI Repository Services on behalf of a Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider) until they have become an ARO;
- g) ensure that authentication credentials issued under the IKI Certificate Policy to AROs have a lifetime of ten years following and that such authentication credentials shall cease to be valid after ten years following issuance;
- h) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked; and
- i) produce, each month, and make available to each Party, RDP, the SMKI PMA and the Panel, a report for that organisation which details the list of SROs, AROs, the access credentials that have been issued to each ARO and those AROs for which authentication 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, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider) to:

- verify their organisational identity;
- become a SRO;
- become an ARO;
- gain credentials for accessing SMKI Services and/or SMKI Repository;
- 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 Digitally Signing 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 the File Signing Certificate to be used for the purposes of Digitally Signing of files.

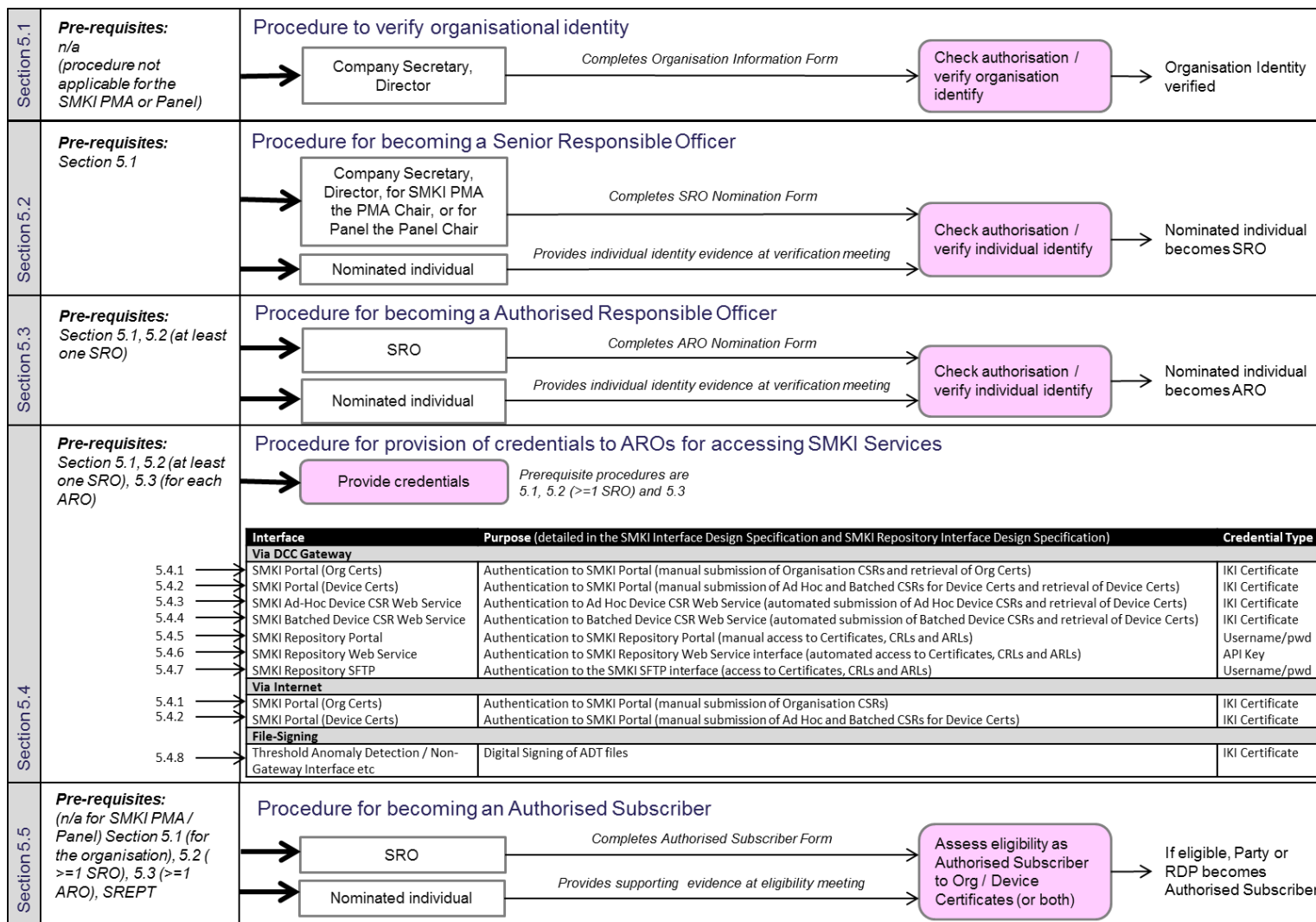


Figure 1: Overview of SMKI access registration processes

- 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 or DCC Service Provider, which shall be conducted where its identity has not previously been established. DCC shall not conduct the procedure in the case that the applicant is the SMKI PMA or the Panel.
- 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, unless (as set out immediately above) the applicant is the SMKI PMA or the Panel.
- 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, unless the applicant is the SMKI PMA or the Panel.
- 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 SMKI Repository Services 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, the SMKI PMA, the Panel or the DCC. Where reasonably practicable, the DCC shall conduct the procedures as set out in SMKI RAPP Sections 5.1 to 5.5 such that where multiple forms are submitted at the same time, multiple procedures can be conducted within a single visit to the DCC's offices 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 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 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 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) 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 the change occurs ; and

- c) 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 8.3.

No Party, RDP, the SMKI PMA, Panel 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 or RDP**

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

- a) the Director or Company Secretary themselves, or another Director or Company Secretary 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 or RDP and shall no longer consider the individual to be able to act on behalf of that Party or RDP.

#### **4.1.5 SROs ceasing to be eligible to act on behalf of a Party or RDP**

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

- a) the SRO themselves, or a Director or Company Secretary 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 or RDP and shall no longer consider the individual to be able to act on behalf of that Party or RDP.

## 5 Detailed Party, RDP, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures and processes

Each Party, RDP, the SMKI PMA, the Panel and DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or SMKI Repository Services 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 or DCC Service Provider (acting on behalf of the DCC). As set out in section 4.1.2 of this document, the SMKI Registration Authority shall not complete this procedure in respect of the SMKI PMA or the Panel.

Step	When	Obligation	Responsibility	Next Step
5.1.1	As required	<p>The applicant organisation shall complete the Organisation Information Form, as set out in SMKI RAPP Appendix A. In doing so, the applicant organisation shall ensure that:</p> <ul style="list-style-type: none"> <li>a) the information entered on the form is complete and accurate;</li> <li>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</li> <li>c) the Organisation Information Form is authorised by a Director or Company Secretary on behalf of the applicant organisation.</li> </ul> <p>The applicant organisation shall also complete the Nominee Details Form, as set out in SMKI RAPP Appendix E, 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.</p>	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC Service Provider	5.1.2
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	Director or Company Secretary, on behalf of the	5.1.3

Step	When	Obligation	Responsibility	Next Step
		on the DCC Website	applicant organisation, which shall be a Party, RDP or DCC Service Provider	
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	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 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	SMKI Registration Authority	If complete, accurate and no discrepancies, 5.1.6; if not 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 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	SMKI Registration Authority	5.1.7

Step	When	Obligation	Responsibility	Next Step
		agreement shall not unreasonably be withheld.		
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, Company Secretary, SMKI PMA Chair or Panel Chair, 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 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA; 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) individual identity of the nominating individual to Level 3 (Verified) pursuant to the CESG GPG45 RSDOPS framework, 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
5.1.9	As soon as reasonably practicable, following 5.1.8	Notify the nominating Director or Company Secretary that verification of the organisational identity has been unsuccessful, in writing	SMKI Registration Authority	5.1.5 once issues addressed
5.1.10	As soon as reasonably	Inform the nominating Director or Company Secretary that the organisational identity has been successfully verified, in writing	SMKI Registration Authority	5.1.11



Step	When	Obligation	Responsibility	Next Step
	practicable, following 5.1.8			
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

## 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, the SMKI PMA, the Panel 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 Appendix C and Appendix E. 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: <ol style="list-style-type: none"> <li>a) the nominating individual is:               <ol style="list-style-type: none"> <li>i. for a Party, RDP 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;</li> <li>ii. for the SMKI PMA, the SMKI PMA Chair; or</li> <li>iii. for the Panel, the Panel Chair; and</li> </ol> </li> <li>b) the SRO Nomination Form and Nominee Details Form are both authorised, where applicable, by a Director or Company Secretary, SMKI PMA Chair or Panel Chair on behalf of the applicant organisation</li> </ol>	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC (as DCC Service Provider). If nominated on behalf of the SMKI PMA, the SMKI PMA Chair. If nominated on behalf of the Panel, the Panel Chair.	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 or DCC (as DCC Service Provider). If	5.2.3

Step	When	Obligation	Responsibility	Next Step
			nominated on behalf of the SMKI PMA, the SMKI PMA Chair. If nominated on behalf of the Panel, the Panel Chair.	
5.2.3	As soon as reasonably practicable following receipt of completed SRO Nomination Form	Acknowledge receipt by email to the Director, Company Secretary, SMKI PMA Chair or Panel Chair that has authorised the SRO Nomination Form	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, Company Secretary, SMKI PMA Chair or Panel Chair 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 or DCC (as DCC Service Provider). If nominated on behalf of the SMKI PMA, the SMKI PMA Chair. If nominated on behalf of the Panel, the Panel Chair	5.2.3
5.2.6	As soon as reasonably practicable, following 5.2.4	Contact the Director, Company Secretary, SMKI PMA Chair or Panel Chair 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	SMKI Registration Authority	If confirmed as authorised, 5.2.8; if not confirmed as

Step	When	Obligation	Responsibility	Next Step
		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		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, in writing to the Director, Company Secretary, SMKI PMA Chair or Panel Chair 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, Company Secretary, SMKI PMA Chair or Panel Chair of the applicant organisation who nominated the individual to become a Senior Responsible Officer, a date and time for the nominated individual(s) to attend a verification meeting	SMKI Registration Authority	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 the applicant Director, Company Secretary, SMKI PMA Chair or Panel Chair, 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.	SMKI Registration Authority or applicant organisation, as appropriate	5.2.10
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting, 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 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	SMKI Registration Authority	If not successfully verified, 5.2.11; if successfully verified, 5.2.12
5.2.11	As soon as	Notify the Director, Company Secretary, SMKI PMA Chair or Panel	SMKI Registration Authority	5.2.5 once

Step	When	Obligation	Responsibility	Next Step
	reasonably practicable, following verification meeting	Chair, 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		issues addressed
5.2.12	As soon as reasonably practicable, following verification meeting	Notify the Director, Company Secretary, SMKI PMA Chair or Panel Chair, 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

### 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, the SMKI PMA, the Panel 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 Appendix D and Appendix E, ensuring that; <ul style="list-style-type: none"> <li>a) the information entered on the forms is complete and accurate; and</li> <li>b) the ARO Nomination Form and Nominee Details Form are authorised by an SRO on behalf of the applicant organisation</li> </ul>	SRO on behalf of the applicant organisation, which shall be a Party, RDP, the SMKI PMA, the Panel or DCC (as DCC Service Provider)	5.3.2

Step	When	Obligation	Responsibility	Next Step
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 SMKI PMA, the Panel 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	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, the SMKI PMA, the Panel or DCC (as DCC Service Provider)	5.3.3
5.3.6	As soon as reasonably practicable, following 5.3.4	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 an SRO that the procedure for becoming an ARO has not been successful for relevant nominated individual, in writing	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	SMKI Registration Authority	5.3.9

Step	When	Obligation	Responsibility	Next Step
5.3.9	As soon as reasonably practicable on becoming aware of unavailability	<p>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.</p> <p>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.</p>	SMKI Registration Authority or applicant organisation, as appropriate	5.3.10
5.3.10	In ARO verification meeting	<p>At the ARO face-to-face verification meeting, the SMKI Registration Authority shall, in person, for the nominated individual:</p> <p>a) check proof of individual identity provided against the information listed on the ARO Nomination Form and Nominee Details Form; and</p> <p>b) verify the identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA</p>	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	<p>Notify:</p> <p>a) the nominated individual that they have become an ARO, verbally; or</p> <p>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</p>	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	Notify the applicant organisation, to the SRO on behalf of the applicant organisation, in writing of the individuals whose identity has been verified and have become AROs	SMKI Registration Authority	5.3.13

Step	When	Obligation	Responsibility	Next Step
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 5.4

## 5.4 Procedure for provision of credentials to AROs for accessing SMKI Services and SMKI Repository Services

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 to Authorised Responsible Officers in respect of a Party, RDP, the SMKI PMA, the Panel 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, the SMKI PMA, the Panel 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	<p><b>IKI credentials for submission of Organisation CSRs using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet</b></p> <p>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 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:</p> <p>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.</p> <p>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</p>	SMKI Registration Authority	5.4.2



Step	When	Obligation	Responsibility	Next Step
		<p>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.</p> <p>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.</p>		
5.4.2	During ARO verification meeting and after becoming an ARO	<p><b>IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet</b></p> <p>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 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:</p> <p>a) If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing</p>	SMKI Registration Authority	5.4.3

Step	When	Obligation	Responsibility	Next Step
		<p>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.</p> <p>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 Device CSRs and retrieval of corresponding Device 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.</p> <p>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.</p>		

Step	When	Obligation	Responsibility	Next Step
5.4.3	During ARO verification meeting and after becoming an ARO	<p><b>IKI credentials for Ad Hoc Device CSR Web Service</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>a) 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</li> <li>b) 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</li> </ul> <p>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.</p>	SMKI Registration Authority	5.4.4
5.4.4	During ARO verification meeting and after becoming	<p><b>IKI credentials for Batched Device CSR Web Service</b></p> <p>If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for</p>	SMKI Registration Authority	5.4.5

Step	When	Obligation	Responsibility	Next Step
	<p>an ARO</p>	<p>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 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 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:</p> <ul style="list-style-type: none"> <li>a) 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</li> <li>b) 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.</li> </ul> <p>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.</p>		

Step	When	Obligation	Responsibility	Next Step
5.4.5	During ARO verification meeting and after becoming an ARO	<p><b>Credentials for SMKI Repository Portal</b></p> <p>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.</p> <p>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:</p> <p>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.</p>	SMKI Registration Authority	5.4.6

Step	When	Obligation	Responsibility	Next Step
5.4.6	During ARO verification meeting and after becoming an ARO	<p><b>Credentials for SMKI Repository Web Service</b></p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>a) the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification; and</li> <li>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.</li> </ul>	SMKI Registration Authority	5.4.7

Step	When	Obligation	Responsibility	Next Step
5.4.7	During ARO verification meeting and after becoming an ARO	<p><b>Credentials for SMKI Repository Portal SFTP</b></p> <p>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.</p> <p>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.</p>	SMKI Registration Authority	5.4.8
5.4.8	During ARO verification meeting and after becoming an ARO	<p><b>IKI credentials for file signing</b></p> <p>If the applicant organisation wishes the ARO to be Issued with a File Signing Certificate for the purposes as set out in the Code:</p> <ul style="list-style-type: none"> <li>a) the SMKI Registration Authority shall provide the ARO with a Cryptographic Credential Token enabling the ARO to submit a CSR for a File Signing Certificate;</li> <li>b) 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</li> <li>c) 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.</li> </ul>	SMKI Registration Authority	End of procedure

## 5.5 Procedure for becoming an Authorised Subscriber

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 Appendix B, 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



Step	When	Obligation	Responsibility	Next Step
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 it 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 5.4 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

Step	When	Obligation	Responsibility	Next Step
5.5.12	As soon as possible, following 5.5.11	Other than in the case of a Party who is a Supplier Party or a DCC Service Provider, 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 reasonable evidence to suggest that it is necessary for the applicant organisation to become such an Authorised Subscriber in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises.	SMKI Registration Authority	If determined to be an Authorised Subscriber for Device Certificates, 5.5.16; otherwise 5.5.14
5.5.13	As soon as possible, following 5.5.12	Confirm in writing, 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	If the applicant organisation wishes to refer the matter to the SMKI PMA or Panel, 5.5.14, otherwise End of procedure
5.5.14	As soon as possible, following 5.5.13	Determine whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become such an Authorised Subscriber in order for them to carry out business process that will, or are likely to, lead to the installation of Devices in premises. The SMKI PMA or Panel shall confirm the outcome to the DCC, in writing.	SMKI PMA or Panel	If determined to be an Authorised Subscriber for Device Certificates, 5.5.15; otherwise End of procedure

Step	When	Obligation	Responsibility	Next Step
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 in writing, 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.	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

## 6 SMKI Registration Authority registration procedures

The procedures as set out in SMKI RAPP Sections 6.2 to 6.4 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.

### 6.1 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 6.2 or 6.3 have been successfully completed;
- b) in performing the procedures as set out in SMKI RAPP Sections 6.2 and 6.3, 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 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 6.2 or 6.3 in respect of the revised evidence of identity.

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.

## 6.2 Procedure for becoming a SMKI Registration Authority Manager

The procedure for becoming a SMKI Registration Authority Manager as detailed immediately below shall be conducted by DCC's Chief Information Security Officer (CISO) on behalf of the DCC, in order to nominate, authorise and verify a SMKI Registration Authority Manager.

Step	When	Obligation	Responsibility	Next Step
6.2.1	As required	Nominate an individual to become a SMKI Registration Authority Manager, who shall be an employee of the DCC or be contracted to the DCC, and advise the nominated individual of the evidence to be provided in order to verify their identity	DCC Chief Information Security Officer, on behalf of the DCC	6.2.2
6.2.2	As soon as reasonably practicable following 6.2.1	Confirm verification meeting date/time with nominated individual	DCC Chief Information Security Officer, on behalf of the DCC	6.2.3
6.2.3	In verification meeting	The DCC shall, in accordance with the provisions of Sections G4.4 to G4.8: a) check proof of identity provided against the information provided by the nominated individual; and b) verify the identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	DCC Chief Information Security Officer, on behalf of the DCC	If verified, 6.2.5. If not verified, 6.2.4
6.2.4	In verification meeting	If the identity of the nominated individual is not successfully verified, provide reasons for the failure to the individual and notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification	DCC Chief Information Security Officer, on behalf of the DCC	6.2.5
6.2.5	In verification meeting	If the identity of the nominated individual is successfully verified, notify the individual verbally and subsequently in writing that they have become a SMKI Registration Authority Manager and notify the SMKI PMA that the nominated individual has become a SMKI Registration Authority Manager	DCC Chief Information Security Officer, on behalf of the DCC	6.2.6

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

### 6.3 Procedure for becoming a member of SMKI Registration Authority Personnel

The procedure for becoming a member of SMKI Registration Authority Personnel as detailed immediately below shall be conducted by a SMKI Registration Authority Manager on behalf of the SMKI Registration Authority, in order to nominate, verify, authorise and provide means for authenticating access to Systems used to provide SMKI Services and/or SMKI Repository Services in respect of a member of SMKI Registration Authority Personnel.

Step	When	Obligation	Responsibility	Next Step
6.3.1	As required	Nominate an individual to become a member of SMKI Registration Authority Personnel, who shall be an employee of the DCC or be contracted to the DCC	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.2
6.3.2	As soon as reasonably practicable following 6.3.1	Confirm verification meeting date/time with nominated individual	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.3
6.3.3	In verification meeting	In the verification meeting, the DCC shall, in accordance with the provisions of Sections G4.4 to G4.8: a) check proof of identity provided against the information provided by the nominated individual; and b) verify the identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	If successful, 6.3.5. If not successful, 6.3.4
6.3.4	In verification meeting	If the identity of the nominated individual is not successfully verified, provide reasons for the rejection to the individual and notify the individual that a further meeting is required to remedy the affected elements of the verification	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.2

Step	When	Obligation	Responsibility	Next Step
6.3.5	As soon as reasonably practicable, following 6.3.3	If the identity of the nominated individual is successfully verified, notify the individual verbally and subsequently in writing that they have become a member of SMKI Registration Authority Personnel.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.6
6.3.6	As soon as reasonably practicable following 6.3.5	Record the details of the individual that has become a member of SMKI Registration Authority Personnel in respect of the SMKI Registration Authority, in a manner which is auditable	SMKI Registration Authority	Procedure as set out in SMKI RAPP Section 6.4

#### 6.4 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	DCC	If providing to a SMKI Registration Authority Manager, 6.4.2; if providing to a member of SMKI Registration Authority Personnel, 6.4.3

Step	When	Obligation	Responsibility	Next Step
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.	DCC's CISO	End of procedure
6.4.3	In verification meeting, following confirmation of becoming a member of SMKI Registration Authority Personnel	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 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.	SMKI Registration Authority Manager	End of procedure



## **7 Submission of CSRs and Issuance of Certificates**

### **7.1 Submission of Certificate Signing Requests**

The SMKI Interface Design Specification and the Code sets out the provisions in respect of:

- a) the mechanism established for this purpose is in accordance with the procedure in PKCS#10;
- b) naming restrictions in respect of the Subject of each Certificate in accordance with the relevant Certificate Profile;
- c) the circumstances in which an Authorised Subscriber may submit a Certificate Signing Request (CSR) in respect of a Device Certificate and the means by which it may do so;
- d) the circumstances in which an Authorised Subscriber may submit a CSR in respect of an Organisation Certificate and the means by which it may do so; and
- e) requirements in respect of validation of the format of a CSR, checking that the submitting organisation is an Eligible Subscriber for the Certificate and rejection if such requirements are not met.

The SMKI Registration Authority shall validate the Subject of each Certificate to ensure that each CSR corresponds with an EUI64 Identifier range that is applicable to the relevant User Role, as provided in the Organisation Information Form.

Subject to the provisions of the Code and this SMKI RAPP, the DCC shall accept requests for copies of Organisation Certificates and/or Device Certificates from non DCC Users by phone via the DCC Service Desk or via the SMKI Portal via the Internet. The DCC shall, following such a request, provide the relevant information as soon as is reasonably practicable, via a secured electronic means.

### **7.2 Issuance of Certificates**

The SMKI Interface Design Specification sets out the provisions in respect of:

- a) the circumstances in which the DCA shall issue Device Certificates;
- b) the circumstances in which the OCA shall issue Organisation Certificates; and
- c) the obligations in respect of lodging Certificates in the SMKI Repository.

## 8 Revocation

### 8.1 Revocation of Device Certificates

In line with the SMKI Device Certificate Policy, Device Certificates cannot be revoked. As a result:

- a) no organisation shall submit a Certificate Revocation Request (CRR) in respect of a Device Certificate; and
- b) the DCC shall not be obliged to maintain a Device Certificate Revocation List (CRL) Device Authority Revocation List (ARL).

### 8.2 Revocation of Organisation Certificates

#### 8.2.1 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.

## 8.2.2 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 SRO on behalf of a Subscriber, the DCC or the SMKI PMA shall submit, using the mechanisms set out in SMKI RAPP Section 8.2.1, 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 Appendix F : 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.	Subscriber requiring Organisation Certificate revocation	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.	SMKI Registration Authority Personnel	8.2.2.3
8.2.2.3	As soon as reasonably practicable following receipt	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: a) Where submitted in writing, the SMKI Registration Authority shall telephone 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	SMKI Registration Authority Manager	If validated, 8.2.2.5; if invalid (considered malicious and/or inauthentic) or incomplete, 8.2.2.4

Step	When	Obligation	Responsibility	Next Step
		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		
8.2.2.4	As soon as reasonably practicable following unsuccessful validation	Reject the revocation request and notify the Senior Responsible Officer in respect of the Party that was contacted in step 7.2.2.3 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 successful validation	Notify the Senior Responsible Officer that was contacted in step 7.2.2.3 to validate the revocation request and the DCC's CISO by phone that the revocation request has been accepted	SMKI Registration Authority Manager	8.2.2.6
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, in writing	SMKI Registration Authority Manager	End of procedure

## 8.3 Revocation of SMKI Services and/or SMKI Repository Services access credentials

### 8.3.1 General obligations relating to revocation of ARO credentials for accessing SMKI Services and/or SMKI Repository Services

A Senior Responsible Officer on behalf of a Party, RDP, the SMKI PMA 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, the SMKI PMA or the DCC (as DCC Service Provider), using the form as set out in Appendix G 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 the credentials of an ARO to be revoked.
- b) A Party, RDP, SMKI PMA or the DCC (as DCC Service Provider), of which the ARO is a representative, becomes ineligible to access SMKI Services and/or SMKI Repository Services 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, DCC (as DCC Service Provider) or the SMKI PMA 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 SMKI Repository Services.
- 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, SMKI PMA or DCC (as DCC Service Provider) wishes to receive new access credentials, that Party, RDP, SMKI PMA or DCC (as DCC Service Provider) shall submit a new ARO Nomination Form.

### 8.3.2 Procedure for revocation of SMKI Services and/or SMKI Repository Services access credentials for AROs

The procedure for verification and, where verified, revocation of authentication credentials 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 Appendix G, 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, DCC (as DCC Service Provider) or member of the SMKI PMA	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, DCC (as DCC Service Provider) or member of the SMKI PMA	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	SMKI Registration Authority	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, DCC (as DCC Service Provider) or member of the SMKI PMA	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 via telephone, 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

Step	When	Obligation	Responsibility	Next Step
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, in writing	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 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 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 8.3.2.9	Notify the SRO that was contacted in step 7.3.2.3 of the successful revocation of credentials for the ARO. 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	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 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

Step	When	Obligation	Responsibility	Next Step
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, plus update the DCC's list of AROs, in a manner which is auditable	SMKI Registration Authority	End of procedure

### 8.3.3 General obligations relating to revocation of SMKI Registration Authority Manager or SMKI Registration Authority Personnel credentials for accessing SMKI Services and/or SMKI Repository Services

The following parties may request the revocation of authentication credentials in respect of SMKI Registration Authority Personnel, using the form as set out in Appendix G :

- a) Any SMKI PMA member, on behalf of the SMKI PMA; and
- b) Any member of SMKI Registration Authority Personnel or a SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority.

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

- a) A SMKI Registration Authority Manager wishes the credentials of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel to be revoked
- b) A member of SMKI Registration Authority Personnel becomes ineligible to access SMKI Services and/or SMKI Repository Services.
- c) A member of SMKI Registration Authority Personnel fails to comply with Appendix A and Appendix B of the Code, or this SMKI RAPP.
- d) Any information used to verify the identity of a member of SMKI Registration Authority Personnel changes, the individual leaves the employment of the DCC, or moves within DCC to a role in which they are not entitled to access SMKI Services and/or SMKI Repository Services.
- e) A SMKI Registration Authority Manager becomes aware that the member of SMKI Registration Authority Personnel or a SMKI Registration Authority Manager is a potential threat to the security, integrity, or stability of the SMKI Services and/or SMKI Repository Services.
- f) The information on which the identity of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel was established is known, or is suspected, to be inaccurate.
- g) The authentication credentials issued to the member of SMKI Registration Authority Personnel are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to a member of SMKI Registration Authority Personnel 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.



### 8.3.4 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 Appendix G, ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised: 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.	SMKI Registration Authority Personnel or SMKI Registration Authority Manager	8.3.4.2
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 or SMKI Registration Authority Manager	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	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	End of procedure

## Appendix A Organisation Information Form

### Organisation Information

Each Party, RDP or DCC Service Provider wishing to access SMKI Services shall complete this in respect of the Party or DCC Service Provider.

This section is to be filled in by the organisation applying for access to any part of SMKI Services. All fields must be completed.

A.1 Full name of Organisation

A.2 Registered Office address

A.3 Company Registration No.

A.4 Party Signifier or RDP Signifier

A.5 EUI64 Identifier range, as allocated by the Code Administrator on behalf of the Panel

A.6 Role(s) in respect of the application

Role(s)	EUI-64 Identifier range (where applicable)
<input type="checkbox"/> Electricity Import Supplier	
<input type="checkbox"/> Electricity Export Supplier	
<input type="checkbox"/> Electricity Distributor	
<input type="checkbox"/> Gas Supplier	
<input type="checkbox"/> Gas Transporter	
<input type="checkbox"/> Registered Supplier Agent (Meter Operator or Meter Asset manager)	
<input type="checkbox"/> DCC Service Provider	
<input type="checkbox"/> Other User	
<input type="checkbox"/> RDP	

### Nominating Officer Information

Nomination of a Party, RDP or DCC Service Provider for verification of organisational identity shall be made by a Director or Company Secretary on behalf of the organisation.

#### Details of the nominating officer

A.6 Full name

A.7 Role

A.8 Phone Number (Daytime)  Phone Number (Out of Hours)

A.9 Email Address

A.10 Signature of nominating officer



## Appendix B Authorised Subscriber / Interface Access Application Form

### Nature of Authorised Subscriber Application

This section is to be filled in by the organisation applying for access to SMKI Services, to confirm the nature of the application. All fields are required.

B.1	Full name of Organisation	<input style="width: 100%; height: 20px;" type="text"/>
B.2	Company Registration No.	<input style="width: 100%; height: 20px;" type="text"/>
B.3	Nature of Authorised Subscriber Application (if any)	<input type="checkbox"/> Authorised Subscriber in respect of the Organisation Certificate Policy only <input type="checkbox"/> Authorised Subscriber in respect of the Device Certificate Policy only <input type="checkbox"/> No change in Authorised Subscriber status required
B.4	Interface access credentials requested	<p><b>SMKI interfaces and SMKI Repository interfaces via DCC Gateway Connection:</b></p> <input type="checkbox"/> SMKI Portal interface for Authorised Subscribers for Organisation Certificates <input type="checkbox"/> SMKI Portal interface for Authorised Subscribers for Device Certificates (enabling Ad Hoc and Batch Device CSR submission) <input type="checkbox"/> Ad Hoc Device CSR Web Service interface <input type="checkbox"/> Batched Device CSR Web Service interface <input type="checkbox"/> SMKI Repository Portal interface <input type="checkbox"/> SMKI Repository Web Service interface <input type="checkbox"/> SMKI Repository SFTP interface
		<p><b>SMKI interfaces via the Internet:</b></p> <input type="checkbox"/> SMKI Portal interface for Authorised Subscribers for Organisation Certificates <input type="checkbox"/> SMKI Portal interface for Authorised Subscribers for Device Certificates (enabling Ad Hoc and Batch Device CSR submission) <input type="checkbox"/> SMKI Repository content access
		<p><b>File Signing:</b></p> <input type="checkbox"/> File Signing Certificate
B.5	Party Signifier or RDP Signifier	<input style="width: 100%; height: 20px;" type="text"/>

### Nominating Officer Information

Nomination of a Party, RDP or DCC Service Provider to become an Authorised Subscriber for Organisation and/or Device Certificates, or access to the SMKI Repository shall be made by a SMKI SRO on behalf of the organisation.

#### Details of the nominating officer

B.6	Full name	<input type="text"/>	
B.7	Role	<input type="text"/>	
B.8	Phone Number (Daytime)	<input type="text"/>	Phone Number (Out of Hours)
		<input type="text"/>	<input type="text"/>
B.9	Email Address	<input type="text"/>	
B.10	Signature of nominating officer	<input type="text"/>	

### Additional Information to be provided by Applicants wishing to become Authorised Subscribers in respect of the Device Certificate Policy

No information is required from Supplier Parties or DCC Service Providers.

For applicants other than Supplier Parties, please provide information to demonstrate that it is necessary for you to become an Authorised Subscriber for Device Certificates in order to carry out business process that will, or are likely to, lead to the installation of Devices in premises. Examples of such information may include evidence for, or confirmation from a Supplier Party that you have been engaged to procure or install Devices on its behalf, or that you are a manufacturer or prospective manufacturer of such Devices.

## Appendix C SMKI SRO Nomination Form

### Nominated SRO Information

Each Party, RDP, the SMKI PMA, the Panel or DCC Service Provider wishing to access SMKI Services and/or SMKI Repository Services shall have in place at least one SMKI Senior Responsible Officer, in accordance with SMKI RAPP Section 5.2. The following evidence shall be presented and verified at the verification meeting to establish the identity of the nominated individual:

- a) personal identification evidence which must be a photographic driving licence, passport, or national identity card

#### Details of the individual nominated to act on behalf of the Party, RDP, SMKI PMA, Panel or DCC Service Provider as SMKI SRO

C.1	Full name	<input style="width: 100%;" type="text"/>	
C.2	Role	<input style="width: 100%;" type="text"/>	
C.3	Phone Number (Daytime)	<input style="width: 50%;" type="text"/>	Phone Number (Out of Hours) <input style="width: 50%;" type="text"/>
C.4	Email Address	<input style="width: 100%;" type="text"/>	
C.5	Full name of organisation	<input style="width: 100%;" type="text"/>	
C.6	Party Signifier or RDP Signifier	<input style="width: 100%;" type="text"/>	

### Nominating Officer Information

Nomination of an individual to become a SMKI Senior Responsible Officer shall be made by a Director or Company Secretary on behalf of the Party, RDP or DCC Service Provider. For the SMKI PMA, the nomination shall be made by the SMKI PMA Chair. For the Panel, the nomination shall be made by the Panel Chair.

#### Details of the nominating officer

C.7	Full name	<input style="width: 100%;" type="text"/>	
C.8	Role	<input style="width: 100%;" type="text"/>	
C.9	Phone Number (Daytime)	<input style="width: 50%;" type="text"/>	Phone Number (Out of Hours) <input style="width: 50%;" type="text"/>
C.10	Email Address	<input style="width: 100%;" type="text"/>	
C.11	Signature of nominating officer	<input style="width: 100%; height: 40px;" type="text"/>	

## Appendix D SMKI ARO Nomination Form

### Nominations to become Authorised Responsible Officer(s)

The following evidence shall be presented at the verification meeting to establish the identity of the individual nominated to become a SMKI ARO:

- a) personal identification evidence which must be a photographic driving licence, passport, or national identity card

**D.1 List of Nominees to become SMKI ARO on behalf of the Party, RDP, the SMKI PMA, the Panel or DCC (in its role as DCC Service Provider) and credentials requested (tick all that apply)**

Full Name of Nominee	A	B	C	D	E	F	G	H

Where:

Credential reference (as above)	Credential description
A	IKI Certificate for SMKI Portal in respect of Organisation CSRs/Certificates
B	IKI Certificate for SMKI Portal in respect of Device CSRs/Certificates
C	SMKI Ad Hoc Device CSR Web Service
D	SMKI Batched Device CSR Web Service
E	SMKI Repository Portal
F	SMKI Repository Web Service
G	SMKI Repository SFTP
H	File Signing Certificate

### Nominating Officer Information

Nomination of an individual to become a SMKI Authorised Responsible Officer shall be a SMKI Senior Responsible Officer on behalf of the Party, RDP, the SMKI PMA or DCC (in its role as DCC Service Provider). For the SMKI PMA, the nomination shall be made by the SMKI PMA Chair. For the Panel, the nomination shall be made by the Panel Chair.

#### Details of the nominating officer

D.2 Full name

D.3 Role

D.4 Phone Number (Daytime)  Phone Number (Out of Hours)

D.5 Email Address

D.6	Signature of nominating officer	<input type="text"/>
D.7	Full name of organisation	<input type="text"/>
D.8	Party Signifier or RDP Signifier	<input type="text"/>



## Appendix E Nominee Details Form

### Nominee Details

This section is to be filled in by the nominated individual and will be used, along with evidence presented at the verification meeting, to establish the identity of an individual. All fields shall be completed. The DCC shall maintain and publish a list of acceptable documentation on the DCC Website, which should be presented at the verification meeting to establish the identity of the nominated individual.

E.1	Full name	<input type="text"/>			
E.2	Gender	<input type="checkbox"/> Male	<input type="checkbox"/> Female		
E.3	Date of Birth	/	/		
E.4	Nationality	<input type="text"/>			
E.5	Personal Identification	Document 1 <i>(select one)</i>	<input type="text"/>	Document No.	<input type="text"/>
		Document 2 <i>(select one)</i>	<input type="text"/>	Document No.	<input type="text"/>
		Document 3 <i>(if applicable, select one)</i>	<input type="text"/>	Document No.	<input type="text"/>
E.6	Residential address	<input type="text"/>			
E.7	Occupation	<input type="text"/>			
E.8	Affiliation with Organisation	Employee No. <i>(if applicable)</i>	<input type="text"/>	Evidence Type	<input type="text"/>
E.9	Work Phone Number	<input type="text"/>			
E.10	Email Address	<input type="text"/>			
E.11	Signature of nominee	<input type="text"/>			
E.12	Date	<input type="text"/>			

### Nominating Officer Information

Nomination of an individual to become a SMKI Senior Responsible Officer shall be made by a Director or Company Secretary on behalf of the Party, RDP or DCC (in its role as DCC Service Provider). For the SMKI PMA, the nomination shall be made by the SMKI PMA Chair. For the Panel, the nomination shall be made by the Panel Chair. Nomination of an individual to become a SMKI Authorised Responsible Officer shall be a SMKI Senior Responsible Officer on behalf of the Party, RDP, the SMKI PMA, the Panel or DCC (as DCC Service Provider).

**Details of the nominating officer**

E.13	Full name	<input type="text"/>	
E.14	Role	<input type="text"/>	
E.15	Phone Number (Daytime)	<input type="text"/>	Phone Number (Out of Hours) <input type="text"/>
E.16	Email Address	<input type="text"/>	
E.17	Signature of nominating officer	<input type="text"/>	
E.18	Date	<input type="text"/>	

# Appendix F Organisation Certificate Revocation Request Form

## Organisation Certificate Revocation Request Form

This section is to be filled in by the organisation or the SMKI PMA that is applying for revocation of a particular Organisation Certificate. Completion of all fields in the form is mandatory.

F.1	Full name of Subscriber	<input type="text"/>
F.2	64 bit Entity Identifier of the subject of the Certificate	<input type="text"/>
F.3	Name of person submitting the Certificate Revocation Request	<input type="text"/>
F.4	Role of person submitting the Certificate Revocation Request <small>(e.g. SMKI SRO, RA Personnel)</small>	<input type="text"/>
F.5	Contact telephone number for person submitting the Certificate Revocation Request	<input type="text"/>
F.6	Certificate Serial Number	<input type="text"/>
F.7	Distinguished Name of Subject in Certificate (X.509)	<input type="text"/>
F.8	Certificate Description	<input type="text"/>
F.9	Reason for Certificate Revocation	<input type="text"/>

## Appendix G Credential Revocation Request Form

### Credential Revocation Request Form

This form shall be completed by any organisation applying for revocation of credentials in respect of a SMKI Authorised Responsible Officer, SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel. All fields in the form shall be completed.

G.1	Full name of organisation <small>(Party, SMKI Registration Authority or DCC Service Provider)</small>	
G.2	Organisation EUI-64 Identification Number	
G.3	Name of person submitting the credential revocation request	
G.4	Role of person submitting the credential revocation request <small>(e.g. SMKI SRO, SMKI RA Personnel)</small>	
G.5	Contact telephone number for person submitting the credential revocation request	
G.6	Person whose credentials are the subject of the credential revocation request	
G.7	Credentials to be revoked <small>(select all relevant options)</small>	<input type="checkbox"/> IKI Certificate for SMKI Portal in respect of Organisation CSRs/Certificates <small>Token serial number(s) _____</small> <input type="checkbox"/> IKI Certificate for SMKI Portal in respect of Device CSRs/Certificates <small>Token serial number(s) _____</small> <input type="checkbox"/> SMKI Ad Hoc Device CSR Web Service <input type="checkbox"/> SMKI Batched Device CSR Web Service <input type="checkbox"/> SMKI Repository Portal <input type="checkbox"/> SMKI Repository Web Service <input type="checkbox"/> SMKI Repository SFTP <input type="checkbox"/> File Signing Certificate
G.8	Reason for credential revocation	

## Appendix H Definitions

Term	Meaning as defined in SEC
Ad Hoc Device CSR Web Service Interface	The system-to-system interface provided to the SMKI for the purposes of SMKI Subscribers refreshing Device Certificates following a Device CSR for the respective Device being approved through a Batch or Ad Hoc CSR to the SMKI Portal
Authorised Responsible Officer (ARO)	Means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP a DCC Service Provider, the SMKI PMA or the Panel in accordance with the SMKI RAPP
Batched Device CSR Web Service Interface	The system-to-system interface provided to the SMKI for the purposes of SMKI Subscribers refreshing Device Certificates following a Device CSR for the respective Device being approved following the submission of a Batched Certificate Signing Request
Cryptographic Credential Token	Means a FIPS 140-2 Level 3 token containing Secret Key Material, as issued in accordance with the SMKI RAPP
SMKI Registration Authority Manager	Means an individual who acts on behalf of the SMKI Registration Authority to perform tasks relating to the management of the SMKI Registration Authority, as set out in the SMKI RAPP
SMKI Registration Authority Personnel	Means those persons who are engaged by DCC, in so far as such persons carry out functions of the SMKI Registration Authority as set out in the SMKI RAPP
Senior Responsible Officer (SRO)	Means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, a DCC Service Provider, the SMKI PMA or the Panel in accordance with the SMKI RAPP