Version: W4.0

Appendix W

DCCKI Registration Authority Policies and Procedures (DCCKI RAPP)

Contents

1. INTRODUCTION

1.1 This DCC Key Infrastructure Registration Authority Policies and Procedures (DCCKI RAPP) sets out the activities undertaken by the DCC as the DCCKI Registration Authority in accordance with Section L of the Code, and DCCKI Certificate Policy.

1.2 This DCCKI RAPP is a SEC Subsidiary Document and is one of the DCCKI SEC Documents as set out in section L13.34 (The DCCKI SEC Documents) of the Code.

2. DCCKI ROLES

2.1 The roles of RDPs, Parties and their User Personnel in the context of access to DCCKI Services and the DCCKI Repository Service as DCCKI Authorised Subscribers, DCCKI Eligible Subscribers, and DCCKI Subscribers are set out in the Code, the DCCKI Certificate Policy (DCCKI CP), this DCCKI RAPP, and the DCCKI Code of Connection.

2.2 This DCCKI RAPP details the procedures to be followed by Parties and RDPs in respect of permitting individuals to act as DCCKI Senior Responsible Officers (DCCKI SROs) or DCCKI Authorised Responsible Officers (DCCKI AROs) on behalf of a Party or RDP.

2.3 This DCCKI RAPP also details the procedures to be followed by the DCCKI Registration Authority including in relation to the individuals acting on its behalf as DCCKI Registration Authority Managers or DCCKI Registration Authority Personnel.

2.4 Where in accordance with Section L13.22 (The DCCKI Repository Service) of the Code, the SMKI PMA makes a request for provision of a copy of any documents or information stored on the DCCKI Repository, such requests shall be made via the Service Desk. Where appropriate, the DCCKI Registration Authority shall provide the requested document(s) or information as soon as is reasonably practicable following receipt of such request.

Party and Registration Data Provider representatives

2.5 Individuals shall be permitted to act as representatives of a Party or RDP in relation to the DCCKI via the DCCKI SRO and DCCKI ARO roles as set out below.

DCCKI Senior Responsible Officer (DCCKI SRO)

2.6 In order to become and continue to be a DCCKI Authorised Subscriber each Party or RDP must have at least one individual undertaking the role of a DCCKI SRO on that organisation’s behalf. A DCCKI SRO shall be an individual that:

(a) is generally authorised by the Party or RDP to fulfil the functions of a DCCKI SRO as set out in this DCCKI RAPP and elsewhere in the DCCKI SEC Documents;

(b) is specifically authorised by the Party or RDP to nominate, and de-nominate, individuals to become DCCKI AROs who may access the DCCKI Services; and

(c) has:

(i) successfully had their identity verified by the SMKI Registration Authority in accordance with the SMKI RAPP; and

(ii) successfully completed the process for becoming a DCCKI SRO on behalf of that Party or RDP in accordance with this DCCKI RAPP.

2.7 The process by which an individual is nominated, their authorisation is checked and their identity verified by the DCCKI Registration Authority, so as to be a DCCKI SRO and act on behalf of a Party or RDP, is set out in sections 3.8 to 3.11 of this DCCKI RAPP.

2.8 A DCCKI SRO may also nominate themselves to become a DCCKI ARO in accordance with section 2.9 of this DCCKI RAPP.

DCCKI Authorised Responsible Officer (DCCKI ARO)

2.9 In order to become and continue to be a DCCKI Authorised Subscriber each Party or RDP must have at least one individual undertaking the role of a DCCKI ARO on that organisation's behalf. The DCCKI SRO for a Party or RDP shall nominate at least one individual to be a DCCKI ARO in respect of that organisation, where each DCCKI ARO shall be an individual that:

(a) is generally authorised by the Party or RDP to fulfil the functions of a DCCKI ARO as set out in this DCCKI RAPP and elsewhere in the DCCKI SEC Documents;

(b) is specifically authorised to act on behalf of the Party or RDP in its capacity as a DCCKI Authorised Subscriber; and

(c) has:

(i) successfully had their identity verified by the SMKI Registration Authority in accordance with the SMKI RAPP; and

(ii) successfully completed the process for becoming a DCCKI ARO on behalf of that Party or RDP in accordance with this DCCKI RAPP.

2.10 All DCCKI AROs are also permitted to access certain DCCKI Services on behalf of the organisation that they represent.

2.11 The process by which an individual is nominated, their authorisation is checked and their identity verified by the DCCKI Registration Authority, so as to be a DCCKI ARO and act on behalf of a Party or RDP, is set out in sections 3.12 to 3.15 of this DCCKI RAPP.

The DCCKI Registration Authority

2.12 The DCC shall ensure that only individuals duly authorised to act in the role of DCCKI Registration Authority Manager or as DCCKI Registration Authority Personnel in accordance with this DCCKI RAPP shall act on behalf of the DCC in respect of matters relating to the DCCKI Registration Authority.

DCCKI Registration Authority Manager

2.13 The DCC shall nominate one or more individuals to become a DCCKI Registration Authority Manager who shall have responsibility for:

(a) management of the DCCKI Registration Authority functions, and DCCKI Registration Authority Personnel;

(b) nomination, verification, authorisation, and provision of the means for authenticating individuals to become DCCKI Registration Authority Personnel;

(c) provision of the means to authenticate access to the DCCKI Services for DCCKI Registration Authority Personnel;

(d) managing the process by which documents and information are lodged in the DCCKI Repository;

(e) approval of DCCKI Certificate Revocation Requests; and

(f) revocation of DCCKI Registration Authority Personnel credentials.

2.14 The process by which an individual is nominated, their authorisation is checked and their identity verified, so as to be a DCCKI Registration Authority Manager is set out in section 4 of this DCCKI RAPP.

DCCKI Registration Authority Personnel

2.15 A DCCKI Registration Authority Manager may nominate individuals to become DCCKI Registration Authority Personnel and to act on behalf of the DCCKI Registration Authority as set out in this DCCKI RAPP. These DCCKI Registration Authority Personnel shall, in accordance with the processes and procedures set out in this DCCKI RAPP:

(a) conduct enrolment processes in relation to Parties and RDPs, and individuals nominated to act on behalf of those Parties or RDPs, as set out in this DCCKI RAPP, incorporating assessment of whether:

(i) a nominated individual qualifies to become a DCCKI SRO or DCCKI ARO on behalf of that Party or RDP; and

(ii) a Party or RDP qualifies to become an DCCKI Authorised Subscriber.

(b) undertake the processing of:

(i) DCCKI Certificate Signing Requests;

(ii) DCCKI Certificate Revocation Requests; and

(iii) Administration User Credentials Requests; and

(c) manage the processes relating to:

(i) Parties or RDPs ceasing to be DCCKI Authorised Subscribers; and

(ii) revocation of access to the DCCKI Services by DCCKI SROs or DCCKI AROs.

2.16 The process by which an individual is nominated, their authorisation is checked and their identity verified, so as to become DCCKI Registration Authority Personnel is set out in section 4 of this DCCKI RAPP.

3. PARTY AND REGISTRATION DATA PROVIDER ENROLMENT

General enrolment obligations

Party and Registration Data Provider obligations

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

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

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

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

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

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

3.3 Each Party or RDP may:

(a) nominate multiple DCCKI SROs and multiple DCCKI AROs when requesting enrolment as a DCCKI Authorised Subscriber; and

(b) nominate additional individuals to be DCCKI SROs or DCCKI AROs at any time.

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

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

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

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

changes, that Party or RDP shall:

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

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

3.5 Where a Party or RDP becomes aware that any individual ceases to be entitled to act on its behalf as either a DCCKI SRO or a DCCKI ARO in accordance with the provisions of the Code, that Party or RDP shall, as soon as reasonably practicable, follow the procedures set out in sections 3.27 to 3.30 of this DCCKI RAPP such that the DCCKI Registration Authority is able to remove the individual from its list of current DCCKI SROs and DCCKI AROs.

3.6 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 DCCKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this DCCKI RAPP for the purposes of appointing a DCCKI ARO or DCCKI SRO or the Party or RDP becoming a DCCKI Authorised Subscriber, be treated as if it had taken place after that date.

DCCKI Registration Authority obligations

3.7 The DCCKI Registration Authority shall:

(a) ensure that forms that are substantively the same as those set out in Annex A to this DCCKI RAPP are made available to Parties and RDPs via the DCC Website for the purposes set out herein;

(b) provide reasonable support and advice to each Party and RDP in relation to the procedures as set out in this DCCKI RAPP, including via the DCC Website;

(c) obtain confirmation from the Registration Authority for the SMKI Services that each Party or RDP applying to be a DCCKI Authorised Subscriber is a SMKI Authorised Subscriber for Organisation Certificates;

(d) in all cases satisfy itself, via confirmation from the SMKI Registration Authority, that:

(i) any individual nominated to become a DCCKI SRO has had their identity verified in accordance with the SMKI RAPP; and

(ii) any individual nominated to become a DCCKI ARO has had their identity verified in accordance with the SMKI RAPP;

(e) where it receives a nomination for an individual to become a DCCKI SRO or a DCCKI ARO, and that individual has not had their identity verified by the SMKI Registration Authority:

(i) refer the nominated individual to the SMKI Registration Authority to allow such identity verification to be undertaken; and

(ii) provide the SMKI Registration Authority with all relevant information supplied by the nominating Party or RDP to support the identity verification;

(f) place no restriction on the number of individuals that can be nominated as DCCKI SROs or DCCKI AROs in respect of any Party or RDP;

(g) permit an individual to become a DCCKI SRO or ARO to represent multiple Parties or RDPs, by successfully completing the procedures in section 3 of this DCCKI RAPP as necessary in relation to each;

(h) not permit any individual to become a DCCKI SRO or DCCKI ARO in respect of any Party or RDP where it reasonably believes that the individual presents a material risk to DCCKICA Systems which may result in Compromise;

(i) store and maintain records relating to the nomination, verification and authorisation of individuals and organisations as set out in this DCCKI RAPP, and in accordance with the Code and the DCC's data retention policy and data protection policy;

(j) not permit any nominated individual to access the DCCKI Services on behalf of a DCCKI Authorised Subscriber until they have become a DCCKI ARO; and

(k) on successful completion of the enrolment process, provide DCCKI Authorised Subscribers and DCCKI AROs with access to the DCCKI Services in accordance with the provisions of the Code, the DCCKI CP and the DCCKI Code of Connection.

Procedure for becoming a DCCKI Senior Responsible Officer

3.8 Individuals that are an SRO in relation to SMKI Services may be nominated by the organisation that they act in that role for to become a DCCKI SRO for that same organisation.

3.9 Individuals that are not an SRO in relation to SMKI Services may be nominated to become a DCCKI SRO subject to having their identity verified by the SMKI Registration Authority in accordance with section 3.7 (e) of this DCCKI RAPP.

Submission of application

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

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

(b) the information provided is complete and accurate;

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

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

DCCKI Registration Authority processing of DCCKI SRO nominations

3.11 On receipt of a duly completed DCCKI SRO Nomination Form, the DCCKI Registration Authority shall, as soon as is reasonably practicable:

(a) acknowledge receipt via the Service Desk to the individual who submitted the DCCKI SRO Nomination Form via telephone or in writing, using the contact details provided on that form;

(b) satisfy itself that:

(i) the Party or RDP has provided all required information to allow the application to be progressed; and

(ii) the individual nominated to become a DCCKI SRO is an SRO in relation to SMKI Services in respect of the nominating Party or RDP or has had their identity verified by the SMKI Registration Authority, as evidenced by confirmation of this fact by the SMKI Registration Authority;

(c) contact the individual via the Service Desk who submitted the DCCKI SRO Nomination Form, via telephone or in writing, using contact details as provided, to confirm whether the application has been successful or unsuccessful;

(d) either:

(i) notify the Director or Company Secretary via the Service Desk that authorised the DCCKI SRO Nomination Form that the application has been unsuccessful, in writing; or

(ii) notify the Director or Company Secretary via the Service Desk that authorised the DCCKI SRO Nomination Form that the application has been successful, in writing; and

(e) where the application has been successful, add the relevant individual to the DCCKI Registration Authority list of DCCKI SROs maintained in accordance with the DCCKI CPS.

Procedure for becoming a DCCKI Authorised Responsible Officer

3.12 Individuals that are AROs in relation to SMKI Services may be nominated by the organisation that they act in that role for to become a DCCKI ARO for that same organisation.

3.13 Individuals that are not an ARO in relation to SMKI Services may be nominated to become a DCCKI ARO subject to having their identity verified by the SMKI Registration Authority in accordance with section 3.7 (e) of this DCCKI RAPP.

Submission of DCCKI ARO nomination

3.14 Where a Party or RDP wishes to nominate an individual to become a DCCKI ARO, a DCCKI SRO, Director or Company Secretary of that Party or RDP shall ensure that:

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

(b) the information provided is complete and accurate;

(c) the DCCKI ARO Nomination Form is authorised by a DCCKI SRO, Director or Company Secretary; and

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

DCCKI Registration Authority processing of DCCKI ARO nominations

3.15 On receipt of a duly completed DCCKI ARO Nomination Form, the DCCKI Registration Authority shall, as soon as is reasonably practicable:

(a) acknowledge receipt via the Service Desk to the DCCKI SRO, Director or Company Secretary who submitted the DCCKI ARO Nomination Form via telephone or in writing, using the contact details provided on that form;

(b) satisfy itself that:

(i) the Party or RDP has provided all required information to allow the application to be progressed; and

(ii) the individual nominated to become an DCCKI ARO is an ARO in relation to SMKI Services in respect of the nominating Party or RDP or has had their identity verified by the SMKI Registration Authority, as evidenced by confirmation of this fact by the SMKI Registration Authority;

(c) contact the DCCKI SRO, Director or Company Secretary via the Service Desk who submitted the DCCKI ARO Nomination Form, via telephone or in writing, using contact details as provided, to confirm whether the application has been successful;

(d) either:

(i) notify the DCCKI SRO, Director or Company Secretary via the Service Desk that authorised the DCCKI ARO Nomination Form that the application has been unsuccessful, in writing; or

(ii) notify the DCCKI SRO, Director or Company Secretary via the Service Desk that authorised the DCCKI ARO Nomination Form that the application has been successful, in writing; and

(e) where the application has been successful, add the relevant individual to the DCCKI Registration Authority list of DCCKI AROs maintained in accordance with the DCCKI CPS.

Procedure for becoming a DCCKI Authorised Subscriber

Submission of request

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

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

(b) the information provided is complete and accurate;

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

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

DCCKI Registration Authority processing of DCCKI Authorised Subscriber Applications

3.17 On receipt of a DCCKI Authorised Subscriber Application, the DCCKI Registration Authority shall, as soon as is reasonably practicable thereafter:

(a) acknowledge receipt via the Service Desk to the individual who submitted that DCCKI Authorised Subscriber Application via telephone or in writing, using the contact details provided as part of the submission;

(b) satisfy itself that the Party or RDP:

(i) has provided all required information to allow the DCCKI Authorised Subscriber Application to be progressed; and

(ii) is an Authorised Subscriber in relation to Organisation Certificates, as evidenced by confirmation of this fact by the SMKI Registration Authority;

(c) satisfy itself that no material risk of Compromise to any part of the DCC Systems would result from permitting the Party or RDP to become a DCCKI Authorised Subscriber;

(d) contact the individual who submitted the DCCKI Authorised Subscriber Application, via telephone or in writing, using contact details as provided, to confirm whether the application has been successful;

(e) either:

(i) notify the Director, Company Secretary or DCCKI SRO via the Service Desk that authorised the DCCKI Authorised Subscriber Application that the application has been unsuccessful, in writing; or

(ii) notify the Director, Company Secretary or DCCKI SRO via the Service Desk that authorised the DCCKI Authorised Subscriber Application that the application has been successful, in writing;

(f) where the application has been successful, enable access to the DCCKI Services for the relevant Party or RDP in accordance the provisions of the Code, the DCCKI CP and the DCCKI Code of Connection; and

(g) add the relevant Party or RDP to the DCCKI Registration Authority list of DCCKI Authorised Subscribers maintained in accordance with the DCCKI CPS.

Procedure for providing credentials to DCCKI AROs in order to allow Administration Users to use the Self Service Interface

3.18 In order to obtain access to the Self Service Interface (SSI) in accordance with the Self Service Interface Access Control Specification, each DCCKI Authorised Subscriber that is a DCCKI Eligible Subscriber in relation to Personnel Authentication Certificates may submit an Administration User Credentials Request in order to obtain credentials for a member of the User Personnel of that organisation nominated to become an Administration User via the procedures set out immediately below.

Submission of Administration User Credentials Requests

3.19 A DCCKI ARO of a DCCKI Authorised Subscriber that meets the conditions set out in section 3.18 of this DCCKI RAPP may submit an Administration User Credentials Request to the DCCKI Registration Authority using the form provided for the purpose on the DCC Website, which shall be substantively in the form set out in Annex A (A5) to this DCCKI RAPP.

3.20 In submitting an Administration User Credentials Request, a DCCKI ARO of a DCCKI Subscriber shall provide the required details of the User Personnel who are to be provided with Smart Card Tokens, single use passwords and usernames for the purposes of establishing access to the Personnel Credentials Interface, and submitting a Personnel Authentication Certificate Application as Administration Users.

DCCKI Registration Authority processing of Administration User Credentials Requests

3.21 On receipt of an Administration User Credentials Request, DCCKI Registration Authority Personnel shall;

(a) confirm via the Service Desk to the DCCKI ARO that submitted the request that such request has been received, where this notification may be made via telephone or in writing using the contact details established as part of enrolment to the DCCKI Services;

(b) ensure that the submitting organisation meets the conditions set out in section 3.18 of this DCCKI RAPP; and

(c) ensure that all required information has been provided.

3.22 Where the Administration User Credentials Request is valid, the DCCKI Registration Authority shall in relation to that request:

(a) ensure that single use passwords and usernames are generated for each member of User Personnel whose details are provided;

(b) provide, via a secured electronic means as set out on the DCC Website, the usernames to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface;

(c) provide, via secure post, the single use passwords to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface; and

(d) provide one Smart Card Token for each member of User Personnel identified:

(i) to the DCCKI ARO that submitted the request or their named alternative, whose details have been provided by that DCCKI ARO at the time the request was made. This delivery may be in person, via a nominated employee, or via a commercial courier service. (Any person delivering the materials shall have information that enables verification of the materials and the sending organisation, and allows authentication of that person's identity); and

(ii) ensure that the DCCKI ARO that submitted the request (or their named alternative) is advised in advance of any such delivery, including the means of delivery, and the name of the person that shall be making that delivery. This notification may be made via telephone or in writing using the contact details established as part of enrolment to the DCCKI Services.

3.23 If the Administration User Credentials Request is not valid, the DCCKI Registration Authority Manager shall ensure that a DCCKI SRO of the submitting organisation and the DCCKI ARO who submitted that request is notified of the reasons for its rejection.

Establishment of Administration User credentials

3.24 On receipt of the Smart Card Tokens, usernames and single use passwords from the DCCKI Registration Authority, the DCCKI ARO shall ensure the distribution of the required materials to the relevant User Personnel within their organisation. Those User Personnel may then use the materials to access the Personnel Credentials Interface for the purposes of submitting a Personnel Authentication Certificate Application and obtaining a Personnel Authentication Certificate in accordance with the procedures set out in the DCCKI Interface Design Specification.

3.25 Following successfully obtaining a Personnel Authentication Certificate, the User Personnel nominated by that DCCKI ARO shall be an enabled Administration User who may then create usernames and single use passwords for other User Personnel within their organisation in accordance with the DCCKI Interface Design Specification.

3.26 In the event that, following provision of Smart Card Tokens, usernames and single use passwords by a DCCKI ARO, relevant User Personnel are unable to successfully obtain a Personnel Authentication Certificate, that DCCKI ARO shall raise an Incident in accordance with the Incident Management Policy, in order to resolve the matter.

Maintenance of information relating to DCCKI SROs and DCCKI AROs

Procedures for providing changes in information relating to DCCKI SROs and DCCKI AROs

3.27 Where either:

(a) the contact details provided to the DCCKI Registration Authority for a DCCKI SRO or DCCKI ARO change; or

(b) a Party or RDP determines that a DCCKI SRO or DCCKI ARO is no longer entitled to act as such in relation to that organisation;

a DCCKI SRO, a Director or Company Secretary of that Party or RDP shall notify the DCCKI Registration Authority in accordance with section 3.28 below.

3.28 The Party or RDP making the notification shall contact the DCCKI Registration Authority via the means set out on the Website, and provide the following information:

(a) the name of the person making the notification, their contact details and the name of the organisation that they represent;

(b) the name of the DCCKI SRO or DCCKI ARO whose details require amendment; and

(c) whether that DCCKI SRO or DCCKI ARO is still entitled to act as such on behalf of the notifying Party or RDP.

3.29 On receipt of updated information from a Party or RDP, the DCCKI Registration Authority shall, as soon as is reasonably practicable:

(a) acknowledge receipt in writing via the Service Desk to the person making the notification;

(b) verify the completeness of the information contained in the notification;

(c) contact the DCCKI SRO, a Director or Company Secretary via the Service Desk of that Party making the notification by telephone or in writing using the registered contact details for the DCCKI SRO, a Director or Company Secretary of that Party as held by the DCCKI Registration Authority to confirm the notification is authorised;

(d) amend its records in accordance with the information received; and

(e) provide confirmation in writing via the Service Desk to both the individual who made the notification, and the relevant DCCKI SRO or DCCKI ARO that the DCCKI Registration Authority has made the requested updates, and what those updates are.

DCCKI Registration Authority Amendments to DCCKI SRO or DCCKI ARO Information

3.30 In circumstances where:

(a) the DCCKI Registration Authority reasonably believes that a DCCKI SRO or DCCKI ARO has materially failed to comply with the DCCKI policies as set out in the DCCKI Certificate Policy, this DCCKI RAPP, or the Code; and

(b) that individual has been notified of the fact by the DCCKI Registration Authority including the nature of the non-compliance;

the DCCKI Registration Authority may amend its records such that the individual is no longer authorised to act in the role of a DCCKI SRO or DCCKI ARO for a Party or RDP as the case may apply.

3.31 Where the DCCKI Registration Authority has amended its records in accordance with section 3.30 of this DCCKI RAPP, it shall inform the relevant individual of the fact, and:

(a) in the case of a DCCKI SRO, inform a Director or Company Secretary of the relevant DCCKI Authorised Subscriber using the registered contact details of the Director or Company Secretary of that Party as held by the DCCKI Registration Authority; or

(b) in the case of a DCCKI ARO, inform a DCCKI SRO of the relevant DCCKI Authorised Subscriber.

Reapplying to be a DCCKI SRO or DCCKI ARO

3.32 In circumstances where an individual has ceased to be a DCCKI SRO or a DCCKI ARO for a Party or RDP, nothing shall preclude them from re-applying to become a DCCKI SRO or DCCKI ARO on behalf of that or another Party or RDP by following the procedures set out in this DCCKI RAPP.

4. DCCKI REGISTRATION AUTHORITY ENROLMENT PROCEDURES

4.1 The procedures set out in this section 4 shall be undertaken in order for nominated individuals to act on behalf of the DCCKI Registration Authority as either a DCCKI Registration Authority Manager or a member of DCCKI Registration Authority Personnel.

General registration obligations

4.2 The DCC shall be responsible for ensuring that only those individuals authorised in accordance with the DCCKI CP, the DCCKI CPS, and this DCCKI RAPP are appointed to the roles of DCCKI Registration Authority Manager and DCCKI Registration Authority Personnel. The DCC shall ensure that its CISO ensures that such authorisations are made in accordance with the procedures set out in this DCCKI RAPP.

4.3 In respect of DCCKI Registration Authority Managers and DCCKI Registration Authority Personnel, the DCCKI Registration Authority shall:

(a) not permit any individual to access DCCKICA Systems used to provide DCCKI Services or DCCKI Repository Services as a DCCKI Registration Authority Manager or member of DCCKI Registration Authority Personnel until the procedures in this section 4 of this DCCKI RAPP are successfully completed;

(b) store and maintain records relating to individuals becoming DCCKI Registration Authority Managers and DCCKI Registration Authority Personnel, in accordance with the Code and DCC data retention policy;

(c) ensure that there is at least one DCCKI Registration Authority Manager at all times;

(d) if there is a change to any of the information used to verify the identity of any DCCKI Registration Authority Manager or member of DCCKI Registration Authority Personnel, ensure that the relevant DCCKI Registration Authority Manager or member of DCCKI Registration Authority Personnel undertakes the procedures as set out in this DCCKI RAPP in respect of the revised evidence of identity; and

(e) ensure that authentication credentials provided to DCCKI Registration Authority Managers and DCCKI Registration Authority Personnel in accordance with section 4.12 of this DCCKI RAPP shall expire three years following issuance of such authentication credentials.

Procedure for becoming a Registration Authority Manager

4.4 The DCC CISO, or an individual they have authorised on their behalf to act in this capacity, shall be responsible for:

(a) nomination of individuals to fulfil the role of DCCKI Registration Authority Manager;

(b) confirmation to each nominated individual of a location, date and time for a verification meeting, to be held at DCC premises; and

(c) advising each nominated individual of the evidence to be provided in order to verify their identity.

4.5 At the verification meeting, DCC shall:

(a) check proof of identity provided against the information provided by the nominated individual; and

(b) verify the identity of the nominated individual in accordance with the provisions of Section G4.6 (Obligations on the DCC) of the Code.

4.6 Where the identity of the nominated individual is not successfully verified, DCC shall:

(a) provide reasons for the failure to the individual and the DCC CISO; and

(b) notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification.

4.7 Where the identity of the nominated individual is successfully verified, DCC shall:

(a) notify the individual verbally and subsequently make notification in writing to both the individual and the DCC CISO that the individual has become a DCCKI Registration Authority Manager;

(b) record the details of the individual that has become a DCCKI Registration Authority Manager; and

(c) provide the DCCKI Registration Authority Manager with credentials as defined in the DCCKI CPS to be used to perform activities on behalf of the DCCKI Registration Authority.

Procedure for becoming a member of Registration Authority Personnel

4.8 The DCCKI Registration Authority Manager, acting on behalf of the DCCKI Registration Authority, shall:

(a) nominate individuals to become members of DCCKI Registration Authority Personnel;

(b) confirm a location date and time for a verification meeting, to be held at DCC premises to each nominated individual; and

(c) advise each nominated individual of the evidence to be provided in order to verify their identity.

4.9 At the agreed verification meeting, the DCCKI Registration Authority Manager shall:

(a) check proof of identity provided against the information provided by the nominated individual; and

(b) verify the identity of the nominated individual in accordance with the provisions of Section G4.6 (Obligations on the DCC) of the Code.

4.10 Where the identity of the nominated individual is not successfully verified, the DCCKI Registration Authority Manager shall:

(a) provide reasons for the failure to the individual; and

(b) notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification.

4.11 Where the identity of the nominated individual is successfully verified, the DCCKI Registration Authority Manager shall:

(a) notify the individual verbally and subsequently in writing that they have become a member of DCCKI Registration Authority Personnel;

(b) record the details of the individual that has become a member of DCCKI Registration Authority Personnel; and

(c) provide the member of DCCKI Registration Authority Personnel with credentials as defined in the DCCKI CPS to be used to perform activities on behalf of the DCCKI Registration Authority.

Procedure for provision of credentials to a Registration Authority Manager or a Registration Authority Personnel

4.12 The DCC shall ensure that the DCCKI CPS details the procedure for provision of credentials to a DCCKI Registration Authority Manager or DCCKI Registration Authority Personnel.

5. SUBMISSION OF REQUESTS FOR AND ISSUANCE OF DCCKI CERTIFICATES

General DCCKI Registration Authority Obligations

5.1 The DCCKI Registration Authority shall ensure that:

(a) no DCCKICA Certificates are signed using a Root DCCKICA Private Key after the expiry of the Validity Period of the corresponding Root DCCKICA Certificate;

(b) no DCCKI Infrastructure Certificates are Issued using a EII DCCKICA Private Key after the expiry of the Validity Period of the corresponding EII DCCKICA Certificate;

(c) no Personnel Authentication Certificates are Issued using a UI DCCKICA Private Key after the expiry of the Validity Period of the corresponding UI DCCKICA Certificate;

(d) DCCKI Certificates are Issued only in accordance with the provisions set out in this DCCKI RAPP, the DCCKI Certificate Policy, and the DCCKI Interface Design Specification;

(e) each EII DCCKICA Certificate and UI DCCKICA Certificate that is Issued by the Root DCCKI CA has been verified to be correct and complete;

(f) each DCCKI Infrastructure Certificate that is Issued by the EII DCCKICA has been verified to be correct and complete and complies with the DCCKI Certificate Signing Request received;

(g) each Personnel Authentication Certificate that is Issued by the UI DCCKICA has been verified to be correct and complies with the Personnel Certificate Application received via the Personnel Credentials Interface;

(h) all DCCKI Infrastructure Certificates shall be Issued within one (1) Working Day of receipt of a valid DCCKI Certificate Signing Request from a DCCKI Eligible Subscriber;

(i) all Personnel Authentication Certificates shall be Issued as soon as is reasonably possible following the receipt of a valid Personnel Authentication Certificate Application;

(j) a record of all DCCKI Certificates which have been Issued by the DCCKICA and accepted by a DCCKI Eligible Subscriber is maintained;

(k) the Root DCCKICA Certificate and EII DCCKICA Certificate are made available to DCCKI Relying Parties via the DCCKI Repository; and

(l) the name of the subject of each DCCKI Certificate that is Issued is consistent with the information provided via the DCCKI Certificate Signing Request or Personnel Authentication Application received via the Personnel Credentials Interface as the case may be.

General DCCKI Eligible Subscriber Obligations

5.2 DCCKI Authorised Subscribers that are DCCKI Eligible Subscribers in respect of DCCKI Infrastructure Certificates as set out in the DCCKI CP may submit DCCKI Certificate Signing Requests in accordance with the procedures set out in this DCCKI RAPP, the DCCKI Interface Design Specification and the DCCKI Code of Connection.

5.3 In the case of DCCKI Infrastructure Certificates, a DCCKI Eligible Subscriber may only request Issuance via submission of a DCCKI Certificate Signing Request and where that DCCKI Eligible Subscriber is a SMKI Subscriber in relation to an Organisation Certificate in accordance with section 5.6 of this DCCKI RAPP.

5.4 In the case of Personnel Authentication Certificates, a DCCKI Eligible Subscriber may only submit a Personnel Authentication Certificate Application via the Personnel Credentials Interface in accordance with the provisions of the DCCKI Interface Design Specification.

DCCKI Certificate Signing Requests

5.5 DCCKI Certificate Signing Requests may only be submitted by a DCCKI ARO of the DCCKI Eligible Subscriber, and in relation to DCCKI Infrastructure Certificates.

5.6 In submitting a DCCKI Certificate Signing Request, a DCCKI ARO of a DCCKI Eligible Subscriber shall:

(a) generate a Key Pair within a Cryptographic Module;

(b) generate a DCCKI Certificate Signing Request, containing the attributes and format defined within the DCCKI Interface Design Specification, and in accordance with the DCCKI CP;

(c) ensure that the DCCKI Certificate Signing Request is Digitally Signed using the Private Key associated with the Public Key contained in the DCCKI Certificate Signing Request in accordance with PKCS#10;

(d) verify the accuracy of details contained within the DCCKI Certificate Signing Request and on success, shall use the Private Key associated with the corresponding Public Key in an Organisation Certificate for which it is a Subscriber to Digitally Sign the DCCKI Certificate Signing Request as set out in the DCCKI Interface Design Specification; and

(e) send the DCCKI Certificate Signing Request to the DCCKI Registration Authority via secured electronic means as set out on the DCC Website.

5.7 As soon as reasonably practicable following receipt of the DCCKI Certificate Signing Request, the DCCKI Registration Authority Personnel shall acknowledge receipt in writing via the Service Desk to the DCCKI ARO who submitted the DCCKI Certificate Signing Request, using the contact details established as part of enrolment to the DCCKI Services.

Authentication of DCCKI Certificate Signing Requests

5.8 DCCKI Registration Authority Personnel shall validate that for each DCCKI Certificate Signing Request submitted:

(a) the organisation submitting the DCCKI Certificate Signing Request is a DCCKI Eligible Subscriber in relation to DCCKI Infrastructure Certificates in accordance with the DCCKI CP;

(b) the format of the DCCKI Certificate Signing Request is valid in relation to requests for DCCKI Certificates as specified in the DCCKI Interface Design Specification; and

(c) the DCCKI Certificate Signing Request is correctly signed in accordance with section 5.6 of this DCCKI RAPP.

5.9 If a DCCKI Certificate Signing Request so submitted is not valid, the DCCKI Registration Authority shall reject the DCCKI Certificate Signing Request, and shall follow the process for the rejection of DCCKI Certificate Signing Request set out in this DCCKI RAPP.

5.10 Where the DCCKI Certificate Signing Request is valid, the DCCKI Registration Authority shall submit it to the EII DCCKICA.

Rejection of DCCKI Certificate Signing Requests

5.11 Rejection of a DCCKI Certificate Signing Request may occur where:

(a) the DCCKI Certificate Signing Request cannot be validated in accordance with section 5.8 of this DCCKI RAPP; or

(b) the DCCKI Certificate Signing Request is not compliant with the DCCKI CP, the DCCKI Interface Design Specification or other provisions of the Code.

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

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

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

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

Certificate Issuance in response to a DCCKI Certificate Signing Request

5.13 Upon successful validation of the information provided in the DCCKI Certificate Signing Request by the DCCKI Registration Authority, the EII DCCKICA, shall generate the DCCKI Infrastructure Certificate based on the information contained within the DCCKI Certificate Signing Request.

5.14 Following Issuance of the DCCKI Infrastructure Certificate, the DCCKI Registration Authority shall:

(a) publish the DCCKI Infrastructure Certificate to the DCCKI Repository in accordance with the DCCKI CP; and

(b) notify the DCCKI ARO via the Service Desk that submitted the DCCKI Certificate Signing Request of its Issuance, in writing, using the contact details established as part of enrolment for the DCCKI Services.

Acceptance or Rejection of DCCKI Certificates Issued following a DCCKI Certificate Signing Request submission

5.15 As soon as is reasonably practicable following notification of Issuance of a DCCKI Infrastructure Certificate as set out in section 5.14 above, the DCCKI Eligible Subscriber that submitted the DCCKI Certificate Signing Request shall:

(a) validate the DCCKI Infrastructure Certificate published on the DCCKI Repository; and

(b) notify the DCCKI Registration Authority if the DCCKI Infrastructure Certificate is rejected, in writing, using the contact details established as part of the enrolment of the DCCKI Services.

5.16 Where the DCCKI Registration Authority receives a valid notification of the rejection of a DCCKI Infrastructure Certificate, it shall revoke that DCCKI Infrastructure Certificate in accordance with the procedures set out in section 6 of this DCCKI RAPP.

5.17 Not In Use.

Personnel Authentication Certificate Application

5.18 Provision is made in the DCCKI Interface Design Specification in relation to the mechanism by which a DCCKI Eligible Subscriber may request a Personnel Authentication Certificate Application. Prior to requesting a Personnel Authentication Certificate Application, DCCKI Eligible Subscribers shall follow the procedures set out in sections 3.18 to 3.26 of this DCCKI RAPP.

Issuance of User Personnel Authentication Certificates

5.19 Personnel Authentication Certificates shall be Issued to User Personnel following a Personnel Authentication Certificate Application via the Personnel Credentials Interface.

5.20 User Personnel of DCCKI Eligible Subscribers who are not Administration Users shall have the Private Key associated with the Personnel Authentication Certificate delivered to them along with the Personnel Authentication Certificate in accordance with the DCCKI Interface Design Specification.

5.21 The DCCKI Interface Design Specification sets out further provisions in respect of the circumstances in which the UI DCCKICA shall Issue Personnel Authentication Certificates.

Rejection and Acceptance of a Personnel Authentication Certificate

5.22 Use of the Private Key associated with a Personnel Authentication Certificate to Authenticate to the SSI shall be deemed to constitute acceptance of the Personnel Authentication Certificate by the DCCKI Eligible Subscriber.

5.23 To reject a Personnel Authentication Certificate, a DCCKI Eligible Subscriber shall raise an Incident in accordance with the Incident Management Process.

5.24 Where the DCCKI Registration Authority receives a valid notification of the rejection of a Personnel Authentication Certificate, it shall revoke that Personnel Authentication Certificate in accordance with the procedures set out in section 6 of this DCCKI RAPP.

6. REVOCATION

DCCKI Certificate Revocation

6.1 The circumstances under which DCCKI Subscribers and the DCC may request revocation of a DCCKI Certificate are set out in the DCCKI CP. In all cases, the procedures set out in this DCCKI RAPP shall be followed in respect of DCCKI Certificate revocation.

6.2 Where DCC reasonably believes that there has been a material breach of obligations under the Code that could lead to a material Compromise of DCC Systems, it may request revocation of the DCCKI Certificates issued to the relevant Party or RDP. This revocation shall not preclude the affected Party or RDP from applying for further DCCKI Certificates once any material breach has been remedied, or following any determination to the contrary by the Panel.

Revocation of DCCKI Infrastructure Certificate

6.3 Each DCCKI Relying Party shall raise an Incident as soon as possible following awareness of Compromise or suspected Compromise of any DCCKI Infrastructure Certificate.

6.4 On notification of an Incident, the DCC may raise a DCCKI Certificate Revocation Request via the procedure set out in section 6.8 and 6.9 below in response to the Incident. Any grace period during which the relevant DCCKI Infrastructure Certificates are not revoked shall be agreed at the time that the DCCKI Certificate Revocation Request is made.

6.5 Where a DCCKI Subscriber is aware of Compromise or suspected Compromise of a DCCKI Infrastructure Certificate Issued to it, the DCCKI Subscriber shall request revocation of that DCCKI Infrastructure Certificate in accordance with sections 8 and 9 of this DCCKI RAPP, and raise an Incident as soon as reasonably practicable.

6.6 Where the DCCKI Registration Authority Personnel has issued a DCCKI Infrastructure Certificate incorrectly the DCCKI Infrastructure Certificate may be revoked provided;

(a) the certificate has not been issued to an DCCKI ARO; and

(b) the revocation request is approved by a the DCCKI Registration Authority Manager.

6.7 Where the DCCKI Registration Authority Personnel has issued a DCCKI Infrastructure Certificate incorrectly and it has been issued to the DCCKI ARO the DCCKI Infrastructure Certificate may be revoked provided:

(a) an incident is raised; and

(b) the requesting DCCKI ARO is notified and a new Certificate Signing Request is submitted;

Procedure for DCCKI Certificate Revocation Requests

6.8 DCCKI Certificate Revocation Requests shall be made in writing, via the means set out on the DCC Website, to the DCCKI Registration Authority.

6.9 A DCCKI Certificate Revocation Request shall:

(a) identify the DCCKI Subscriber;

(b) identify the individual making the request, and their role, which shall be:

(i) in the case of a DCCKI Subscriber, a DCCKI SRO of that organisation; or

(ii) in the case of the DCC, the DCC CISO, or an individual that they have authorised to act on their behalf in this capacity;

(c) identify the DCCKI Certificate to be revoked; and

(d) state the criteria for the revocation.

6.10 On receipt of a valid DCCKI Certificate Revocation Request, the DCCKI Registration Authority shall:

(a) validate the revocation request by contacting:

(i) in the case of a DCCKI Subscriber, the DCCKI SRO, using the contact details of the DCCKI SRO as provided in the original application to become a DCCKI SRO; or

(ii) in the case of the DCC, the DCC CISO, using the registered contact details for the DCC CISO as held by the DCCKI Registration Authority

to confirm that the DCCKI Certificate Revocation Request is authentic;

(b) where the validation is unsuccessful, reject the DCCKI Certificate Revocation Request and notify the DCCKI SRO or the DCC CISO via the Service Desk of the rejection;

(c) where the validation is successful, notify the DCCKI SRO or the DCC CISO via the Service Desk of the acceptance of the DCCKI Certificate Revocation Request, and then:

(i) revoke the DCCKI Infrastructure Certificate;

(ii) update the EII DCCKICA CRL and lodge the updated EII DCCKICA CRL in the DCCKI Repository; and

notify the DCCKI SRO or the DCC CISO of the revocation via the Service Desk.

Revocation of Personnel Authentication Certificates

6.11 If a Personnel Authentication Certificate is suspected of Compromise, the DCCKI Subscriber shall request a new Personnel Authentication Certificate in accordance with this DCCKI RAPP and the DCCKI Interface Design Specification.

6.12 On receipt of a new Personnel Authentication Certificate Application for a User Personnel already Issued with a Personnel Authentication Certificate, the UI DCCKICA shall revoke the existing Personnel Authentication Certificate.

6.13 Retirement of an SSI account for a member of a Party's User Personnel shall result in the revocation of the Personnel Authentication Certificate associated with that SSI account.

Ceasing to be a DCCKI Authorised Subscriber

6.14 A Party or RDP shall cease to be a DCCKI Authorised Subscriber where:

(a) that Party or RDP makes a request to the DCCKI Registration Authority to cease to be a DCCKI Authorised Subscriber;

(b) the DCC reasonably believes that Party or RDP, or any of its DCCKI SROs or DCCKI AROs as individuals, have failed or are failing materially to comply with the DCCKI policies as set out in the DCCKI Certificate Policy, this DCCKI RAPP, or any other provision of the Code such that there is a material risk of Compromise to the DCC Systems; or

(c) they fail to have in place at any time at least one DCCKI SRO and at least one DCCKI ARO.

6.15 Where a Party or RDP ceases to be a DCCKI Authorised Subscriber, the DCCKI Registration Authority shall:

(a) notify the Party or RDP via the Service Desk, giving reasons for why it has ceased to be a DCCKI Authorised Subscriber;

(b) update its list of DCCKI Authorised Subscribers; and

(c) revoke all DCCKI Certificates that have been Issued to that Party or RDP, in accordance with this DCCKI RAPP.

ANNEX A – FORM TEMPLATES

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

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

A1. DCCKI SRO NOMINATION FORM

A2. DCCKI ARO NOMINATION FORM

A3. DCCKI AUTHORISED SUBSCRIBER APPLICATION FORM

A4. DCCKI CERTIFICATE SIGNING REQUEST REJECTION FORM

A5. ADMINISTRATION USER CREDENTIALS REQUEST FORM

A6. DCCKI CERTIFICATE REVOCATION REQUEST FORM

ANNEX B DEFINED TERMS

In this DCCKI RAPP, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of this document.

Definitions for this DCCKI RAPP

Administration User Credentials Request	means a request submitted by a DCCKI ARO for the provision of Smart Card Tokens, usernames and single use passwords to be utilised by User Personnel nominated to be an Administration User.
Authorised Responsible Officer	has the meaning given to that expression in the SMKI RAPP.
Authenticate	has the meaning given to that term in the DCCKI Certificate Policy.
CISO	means chief information security officer
DCCKI Authorised Responsible Officer (DCCKI ARO)	means an individual that has successfully completed the process for becoming a DCCKI ARO on behalf of a party or RDP in accordance with this DCCKI RAPP.
DCCKI ARO Nomination Form	means the form of that name as provided via the DCC Website which shall be used by Parties and RDPs wishing to nominate individuals to act as a DCCKI ARO on their behalf.
DCCKI Authorised Subscriber Application	means a request to become a DCCKI Authorised Subscriber submitted by a Party or RDP in accordance with the procedures set out in the DCCKI RAPP.

DCCKICA Systems	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Certificate Revocation Request	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Certificate Signing Request Rejection Form	means the form of that name as set out in Annex A (A6) to the DCCKI RAPP and used by the DCCKI Registration Authority to inform a DCCKI Authorised Subscriber for the reasons for rejection of a DCCKI Certificate Signing Request or DCCKI Certificate Application.
DCCKI Registration Authority Manager	means an individual who acts on behalf of the DCCKI Registration Authority to perform tasks relating to the management of the DCCKI Registration Authority, as set out in the DCCKI RAPP.
DCCKI Registration Authority Personnel	means those persons who are engaged by DCC, in so far as such persons carry out functions of the DCCKI Registration Authority as set out in the DCCKI RAPP.
DCCKI Senior Responsible Officer (DCCKI SRO)	means an individual that has successfully completed the process for becoming a DCCKI SRO on behalf of a Party or RDP in accordance with this DCCKI RAPP.
DCCKI SRO Nomination Form	means the form of that name as provided via the DCC Website which shall be used by Parties and RDPs wishing to nominate individuals to act as a DCCKI SRO on their behalf.
EII DCCKICA	has the meaning given to that expression in the DCCKI Certificate Policy.
EII DCCKICA Private Key	has the meaning given to that expression in the DCCKI Certificate Policy.
Personnel Credentials Interface	means the interface that allows for the activation of user accounts, the submission of Personnel Authentication Certificate Applications, and the provision of Personnel Authentication Certificates to persons.
Root DCCKICA	has the meaning given to that expression in the DCCKI Certificate Policy.
Root DCCKICA Private Key	has the meaning given to that expression in the DCCKI Certificate Policy.
Smart Card Token	a physical security device used to assist authentication of User Personnel
Senior Responsible Officer (SRO)	has the meaning given to that expression in the SMKI RAPP.
SMKI Registration Authority	has the meaning given to that expression in the SMKI RAPP.

UI DCCKICA	has the meaning given to that expression in the DCCKI Certificate Policy.

UI DCCKICA Private Key	has the meaning given to that expression in the DCCKI Certificate Policy.