United Kingdom
Ministry of Defence

Defence Public Key Infrastructure

X.509 Certificate Policy

Version 3.0

Date Issued: 8th October 2008
OID: 1.2.826.0.1310.100.3

CONFIDENTIALITY & COPYRIGHT NOTICES

a. This document is controlled and managed by the DPMA under the authority of the United Kingdom Ministry of Defence (MOD). Queries should be addressed to: -

Address	DES ISS Network Technical Authority Building 405 / E3 MoD Corsham Westwells Road Corsham Wiltshire SN13 9NR
Internet	http://www.mod.uk/pki
Intranet	http://www.mod.uk/DefenceInternet/MicroSite/DES/OurPublications/DefencePublicKeyInfrastructuredpkiPolicy.htm
Electronic Mail	dpki-dtag@mod.uk

b. The information contained in this document is intended for personnel charged with the management and operation of the Defence Public Key Infrastructure (DPKI) owned by the MOD.

c. © Crown Copyright 2008
The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material not being used in a derogatory manner or in a misleading context. The source of the material shall be acknowledged as Crown copyright and the title of the document shall be included when being reproduced as part of another publication or service.

DRCA KEY IDENTITY

Subject: UK Defence Root CA1, DPKI, MIL, GB

Issuer: Self Issued

Time Validity: 28 Mar 2008 to 28 Mar 2028

Serial Number: 47 EC BA B5

SHA1 Fingerprint: B7:7D:10:6B:84:4E:75:56:95:27:FF:BE:EA:12:AE:87:92:AB:7D:5F

MD5 Fingerprint: 82:DA:F9:D2:80:41:52:89:D1:0B:E3:22:81:7B:A2:9F

DOCUMENT INFORMATION

Document Title	Defence Public Key Infrastructure X.509 Certificate Policy
Object Identifier (OID)	1.2.826.0.1310.100.3
Issue Number	3.0
Issue Date	7th July 2008
Issued By	Defence Interoperable Network Services Authority Defence Equipment & Support \ Information Systems & Services Room 9, Building H21 JSU Corsham, Copenacre Site Park Lane Corsham Wiltshire SN13 9NR
Author(s)	DES ISS Sols-C4 TechArch Cons 1 (Peter Curran)

a. This document uses RFC 3647 (Certificate Policy and Certification Practices Framework) as a template. Some section titles have been amended to use terminology consistent with HMG practice, although section numbering is consistent with RFC 3647.

DOCUMENT HISTORY

Issue	Date	Details
0.1	23rd July 2004	Initial first draft.
1.0	21st April 2005	Issued version
1.5	11th November 2005	Issued version
2.1 draft-1 draft	5th March 2007	Incorporate comments from MOD – CertiPath policy mapping; include comments from DCL
3.0 draft-1	17 Jun 08	Draft release for DTAG comments
3.0 draft-2	7th July 2008	Draft incorporating comments from DTAG
3.0	8 Oct 08	Minor editorial amendments for release after DPMA approval.

REFERENCES

a.   The following documents contain information that has been required by reference or which otherwise describe or govern the Ministry of Defence Public Key Infrastructure operation.

JSP 440	The Defence Manual of Security
JSP 441	Defence Records Management
JSP 503	Business Continuity Management
JSP 457 Vol 2	The Defence Manual Of Interoperable Network and Enabling Services Volume 2 Enterprise Entity Identification
JSP 457 Vol 4	The Defence Manual Of Interoperable Network and Enabling Services Volume 3 Electronic Directory Services
JSP 457 Vol 5	The Defence Manual Of Interoperable Network and Enabling Services Volume 5 Public Key Infrastructure Technologies and X.509 Public-key Certificates
JSP 457 Vol 6	The Defence Manual Of Interoperable Network and Enabling Services Volume 6 Smart Tokens
JSP 541	MOD Information Security Alert Warning and Response Policy and Procedures Manual
IS1	HMG Infosec Standard No 1: Technical Risk Assessment
RFC 2510	C. Adams and S. Farrell. Internet X.509 Public Key Infrastructure Certificate Management Protocols (CMP), March 1999
RFC 3161	C. Adams et al. Internet X.509 Public Key Infrastructure Time Stamp Protocol, August 2001
RFC 3279	W. Polk et al. Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
RFC 3280	R. Housley et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
RFC 3447	J. Jonsson and B Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003
RFC 3647	S. Chokhani. Certificate Policy and Certification Practices Framework, November 2003
RFC 4630	R. Housley and S. Santesson, Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ISO 17799	International Standards Organisation Standard 17799 (Successor to British Standard BS7799-1)
FIPS 140-2	Security Requirements for Cryptographic Modules: FIPS 140-2 12-03-2002
FIPS 186-2	Digital Signature Standard: FIPS 186-2 27-01-2000

TABLE OF CONTENTS

1   INTRODUCTION

a.   This Defence Certificate Policy (DCP) defines the X.509 Certificate Policy for all certificates issued within the Defence Public Key Infrastructure (DPKI) for systems and networks operating at SECRET and below. Certificates identify an entity (a person, role or device) named in the certificate and state what the certificate (and corresponding public key) can be used for. The certificate binds an entity to a particular public key and in effect therein a particular public/private key pair.

1.1   Overview

a.   The MOD has established the DPKI Policy Management Authority (DPMA) to control the policies of the DPKI and to audit compliance with these policies. The role of the DPMA is detailed in section 1.3 of this policy. This Certificate Policy is the statement by the DPMA of the policies to be implemented and used within the DPKI, it may be supplemented by other more detailed policies that are subordinate to this policy. The manner in which this policy is maintained is defined in section 1.5.

b.   This document identifies the unified policy under which a Defence Certificate Management Authority (DCMA) and associated processes, operated by a MOD authorised element, is established and operates. The Defence Information Infrastructure (DII) Integrated Project Team (IPT), operating as directed by the DCMA, is responsible for delivery of the DPKI to the MOD. Any other body approved by the DPMA to deliver DPKI functionality shall comply with these policies.

c.   The DII IPT may use a Delivery Partner to deliver some aspects of certificate generation, revocation, storage, publishing and management.

d.   The DPMA will decide all trust relationships within the DPKI and is responsible for determining cross-certification and other relationships with external parties. The DCMA, through the Defence Root Certification Authority (DRCA), will provide the technical mechanisms to create cross-certification; the DII IPT will provide the technical infrastructure to support these trust relationships including cross-certification, mutual recognition and all other forms of interoperability of the DPKI with all internal and external parties.

e.   This document defines the creation and management of X.509 public key certificates for use in applications requiring communication between networked (and possibly stand-alone) computer-based systems. Such uses may include, but are not limited to, the following:

    i.   Authentication of users to applications and infrastructure

    ii.   Message signing and/or encryption

    iii.   Signing and/or encryption of electronic forms/files/contracts

    iv.   Authentication of infrastructure devices and services such as Routers, Web Servers, Firewalls, VPNs and Directories

    v.   Support for auditing and accountability

f.   MOD requires authentication, confidentiality, integrity, non-repudiation, and access control to support activities within and across the organisation. Public key certificates from the DPKI will complement and support existing security systems for MOD activities. Amongst other things, the reliability of a PKI depends on its secure and trustworthy operation, including equipment, facilities, personnel, procedures, a robust registration system and a trusted time source.

g.   Security management services provided by the DPKI shall include, but are not limited to the following:

    i.   Key generation, archival, recovery, and destruction

ii. Certificate generation, update, renewal, re-key, revocation, modification, distribution and archival

iii. Certificate Revocation List (CRL) generation, distribution and archival

iv. Online Certificate Status Check (OCSP) management and updating

v. Directory management of certificate related items

vi. Token initialisation, programming, management, and destruction

vii. System management functions (e.g., security audit, configuration management, archive, etc.)

h. The security of these services is ensured by defining requirements on PKI activities, including and not limited to the following:

i. Subscriber identification, authorisation and verification

ii. Control and operation of computer and cryptographic systems

iii. Usage of keys and public key certificates by Subscribers and Relying Parties

iv. Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met

i. If any part of the DPKI is used for financial purposes/considerations a review of the security services provided by the public key certificates, the potential value of transactions, and the risk associated with the applications shall be undertaken by the Relying Party. The applicability statements in this policy shall be considered minimum requirements; application/system accreditors may require higher levels of assurance than those specified in this Certificate Policy for these applications.

j. Certificates issued under this Defence Certificate Policy shall only be used for the purposes stated within this DCP, as limited by the key and policy information contained within the certificate, and by the community identified in this document. Use of certificates issued under this DCP for any other purposes or by and/or for any other individuals or organisations is strictly prohibited and is not supported under this DCP.

k. In compiling this DCP due regard has been paid to:

i. RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

ii. JSP 457 Volume 5 Public Key Infrastructure Technologies and X.509 Public-key Certificates.

1.1.1 Assurance Levels

a. This policy defines two assurance levels:

i. Medium Assurance Level – MAL (termed Medium in this policy)

ii. High Assurance Level – HAL (termed High in this policy)

b. Within each assurance level it is permitted to store private keys within an approved token (termed Hardware or Hard in this policy), or within a file or other similar container (termed Software or Soft in this policy).

c. The choice of assurance level and key storage mechanisms should be determined by the user (for example, an IPT or application designer) in agreement with a security accreditor. Guidance on the selection of assurance levels and key storage is given in JSP 457 vol 5.

1.2 Document name and identification

a. This document is referred to as the "Defence Public Key Infrastructure X.509 Certificate Policy Version 3".

b.   The registered Object Identifier (OID) of this Certificate Policy document is
      1.2.826.0.1310.100.3.

1.2.1 Object Identifiers

a.   This document describes multiple policies that are applicable to Subscribers of the DPKI.
      Each CA server and Subscriber shall indicate the policy being asserted in its certificates by
      including one or more OIDs in the *certificatePolicy* field within each certificate. All OIDs are
      assigned within the arc registered to the MOD[1], and assigned to the DPMA for use by the
      DPKI[2].

b.   The OIDs to be used are:

Policy	Assigned OID
Medium Soft Person	1.2.826.0.1310.100.3.1.0
Medium Soft Role	1.2.826.0.1310.100.3.1.1
Medium Soft Device	1.2.826.0.1310.100.3.1.2
Medium Soft Admin[3]	1.2.826.0.1310.100.3.1.3
Medium Hard Person	1.2.826.0.1310.100.3.1.10
Medium Hard Role	1.2.826.0.1310.100.3.1.11
Medium Hard Device	1.2.826.0.1310.100.3.1.12
Medium Hard Admin	1.2.826.0.1310.100.3.1.13
ACP145	1.2.826.0.1310.100.3.1.20
High Soft Person	1.2.826.0.1310.100.3.2.0
High Soft Role	1.2.826.0.1310.100.3.2.1
High Soft Device	1.2.826.0.1310.100.3.2.2
High Soft Admin	1.2.826.0.1310.100.3.2.3
High Hard Person	1.2.826.0.1310.100.3.2.10
High Hard Role	1.2.826.0.1310.100.3.2.11
High Hard Device	1.2.826.0.1310.100.3.2.12
High Hard Admin	1.2.826.0.1310.100.3.2.13

c.   It is explicitly prohibited to assert any policy OID not listed above within any certificate.

1.3   DPKI participants

a.   This section describes the identity or types of entities that fill the roles of participants within
      the DPKI, along with a brief description of their roles and/or responsibilities. A detailed
      description of some of these bodies, along with their terms of reference, is contained in *DPKI
      Programme Board: Management Structure Terms of Reference.* The relationship between

---

[1] See JSP 457 volume 2.
[2] OID assignment within the arc managed by the DPMA is described in the *DPKI Interface Specification.*
[3] Entities of type 'Admin' are PKI Roles, as defined elsewhere in the policy.

these participants is illustrated below:
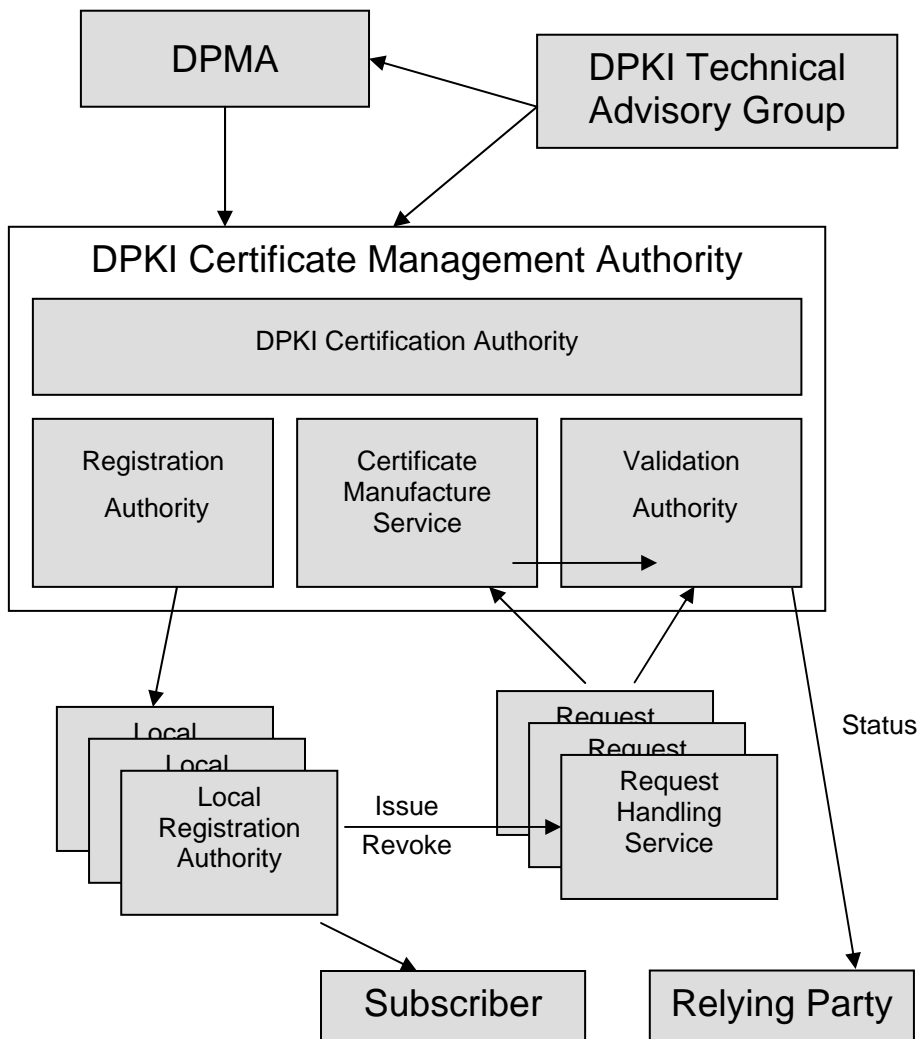
1.3.1 DPKI Policy Management Authority (DPMA)

a. The role of the DPMA is as the executive agent for the development and operation of the Defence PKI. Its primary focus is to establish and maintain a desired level of trust when providing PKI services to MOD users and when defining the rules for interoperation with other PKIs.

b. The DPMA has responsibility for approving:

   i. DPKI Policies.

   ii. DPKI policy and process changes requested by MOD Services, Agencies or the DII Delivery Partner.

   iii. Mutually agreed terms and conditions of a mode of PKI interoperability *(and as advised by DCMA or DTAG direct the suspension or termination of such PKI interoperability when necessary.)*

   iv. Exemptions with respect to the conditions for becoming a member of the Defence PKI or for cross-certification.

   v. Operational standards and guidelines to be followed by the DRCA and CAs operating within the MOD.

   vi. Certification Authorities as members of the Defence PKI, or conversely their disassociation.

vii.   Authority to issue, downgrade or revoke cross-certificates.

viii.   Plans for the implementation of accepted changes.

ix.   Maintaining a DPKI Compliance Audit Process and Programme.

c.   The composition of the DPMA and its Terms of Reference (TOR) is described in *DPKI Programme Board: Management Structure Terms of Reference.*

1.3.2 DPKI Technical Advisory Group (DTAG)

a.   The role of the DTAG is to support the DPMA by providing coherence in all the technical aspects of the DPKI Programme.

b.   The DTAG is responsible for:

i.   Advising the DPMA on the technical policy and issues relating to the coherent implementation, operation and security of the Defence PKI.

ii.   Establishing DTAG sub Working Groups to resolve specific technical and security issues of relevance to the DTAG.

iii.   Making technical recommendations, through the DPMA and DCMA, to MOD Programme and Project Managers and MOD Information System Accreditation Authorities regarding the appropriate use of certificates associated with the DPKI.

iv.   Reviewing and evaluating the following from a technical perspective, making recommendations to the DPMA and DCMA:

- Certificate Policies.

- Proposed policy and process changes as requested by MOD Services, Agencies or the DII Delivery Partner.

- Implementation of change *(and Plans).*

- Non-MOD policies for adoption within the MOD (for example, in cases where the process of "policy mapping" is being considered).

- Results of compliance audits.

c.   The composition of the DTAG and its TOR is described in *DPKI Programme Board: Management Structure Terms of Reference.*

1.3.3 DPKI Certificate Management Authority

a.   The aim of the DCMA is to support the DPMA by managing, using authority delegated by the Defence PKI Programme Board (DPKIPB) (through its DPMA Function), the overall processes of issuance and revocation of certificates used within the DPKI.

b.   The DCMA is responsible for:

i.   Acting as the overall MOD Certificate Management Authority.

ii.   Advising the DPMA on certification, registration, certificate manufacture and validation matters.

iii.   Submitting CPS(s) to the DPMA for approval.

iv.   Reviewing and evaluating the following from an operations perspective, making recommendations to the DPMA and DTAG:

- Proposed policy and process changes as requested by MOD Services, Agencies or the DII Delivery Partner.

- Implementation of change *(and Plans).*

- Non-MOD policies for adoption within the MOD (for example, in cases where the process of "policy mapping" is being considered).

- Results of compliance audits to determine that DPKI participants are adequately meeting the stipulations of the approved CPS documents.

    v.   Supervising the:

- Registration Authority Services.
- Certificate Manufacture Service.
- Validation Authority Service.

    vi.   Making operational recommendations to MOD Programme and Project Managers and MOD Information System Accreditation Authorities regarding the appropriateness of certificates associated with the Defence Certificate Policy for specific applications.

c.   The term DCMA is used to include the functions and responsibilities of the Certification Authority, Certificate Manufacture Service, Registration Authority and Validation Authority. It is used within this policy document to describe functions or responsibilities that may apply to one or all of these entities.

d.   The composition of the DCMA and its Terms of Reference (TOR) is described in *DPKI Programme Board: Management Structure Terms of Reference*.

1.3.4 DPKI Certification Authority

a.   The term CA – Certification Authority – used within this policy refers to the DPKI certificate issuing authority – a functional component of the DCMA. It should not be confused with the common use of the term 'CA' to refer to a server that actually issues certificates – this device is termed a 'CA server' within this policy.

b.   The DPKI Certification Authority (CA) is responsible for issuing certificates to DPKI Subscribers, in accordance with this Defence Certificate Policy and approved Certification Practice Statements that define the implementation of this policy.

c.   The DPKI CA is responsible for developing, and submitting for approval by the DPMA, Certification Practice Statements (CPSs) that describe the implementation of this Defence Certificate Policy. The CPSs shall include at least:

    i.   One or more CPSs describing the operation of the Defence Root CA (DRCA) servers (DRCA CPS).

    ii.   A CPS describing the operation of the CA servers and ancillary systems to be implemented by the DII IPT (DII CPS).

    iii.   CPSs describing the operation of CA servers and ancillary systems to be implemented by the MOD separately to the DII.

    iv.   A CPS describing the operation of the registration process to be implemented by the MOD (Registration CPS).

d.   In order to minimise possible security implications, the DPMA may direct that a PKI Disclosure Statement (PDS) containing the key information of relevance to Subscribers and Relying Parties should be published, in place of the full CPS. The DPMA shall approve all PDSs.

e.   The CA is the issuing authority for all certificates used within the DPKI, technical implementation of the processes involved in issuing and revoking certificates may be wholly, or partly, delegated to the DII IPT.

1.3.5 Certificate Manufacture Service

a.   The Certificate Manufacture Service (CMS) is a service provided by the DII IPT for the management of certificates. The main activities performed by the CMS are:

      i.   Respond to a correctly authorised request for a certificate issue by creating a certificate in accordance with the appropriate Certificate Profile, containing the public key, subject identity and other information notified in the request.

      ii.   Publishing newly issued certificates in the DPKI Repository and making these available to the Registration Authority, Subscribers and Relying Parties.

      iii.   Responding to a correctly authorised revocation request by publishing details of the revoked certificate to the DPKI Repository; revocation status information will be provided to the Validation Authority.

      iv.   Operate a Key Recovery Service to support the lifecycle management of confidentiality certificates.

b.   The implementation of these services is described in the DII CPS.

c.   The CMS is implemented by the instantiation of one or more CA servers, which are delegated subordinated authority for issuing DPKI certificates by the DRCA.

1.3.6 Registration Authority

a.   The Registration Authority (RA) has the authority, delegated by the DPKI CA, to perform the registration service. This service will include:

      i.   Correct identification of all certificate recipients prior to issuance, in accordance with the general policy defined in this Certificate Policy and the specific procedures described in the Registration CPS.

      ii.   Verification of key-pair ownership.

      iii.   Submission of a signed certificate request to the CMS for action.

      iv.   Distribution and initialisation of smartcards containing personal certificates and keying material to individuals on successful completion of the certificate request.

      v.   Maintenance of a suitable audit mechanism to demonstrate compliance with the Certificate Policy and Registration CPS.

      vi.   Submitting certificate revocation requests to the CMS and subsequently managing the destruction or recycling of smartcards containing revoked keys and certificates.

b.   The Registration Authority is responsible for production of one or more Registration CPSs, on behalf of the DPKI CA, that describe the implementation of this Certificate Policy. The CPSs shall be submitted to the DPMA for approval.

1.3.7 Validation Authority

a.   The Validation Authority (VA) is a service delivered by the DII IPT to provide real-time certificate status information to DPKI Relying Parties using the Online Certificate Status Protocol (OCSP). Certificate status information is provided by the CMS and is updated following the authorised revocation of a certificate.

b.   The operation of the Validation Authority, in accordance with this policy, is described within the DII CPS.

c.   The technical components used to provide the VA service (e.g. OCSP servers, responders) that are assigned a private signing key for the purpose of authenticating a revocation statement are termed VA servers in this document[4].

1.3.8 Local Registration Authority

a.   A Local Registration Authority (LRA) operates under the delegated authority of the RA to support the registration process for a specific location, project or class of subscriber.

---

[4] Note that untrusted OCSP responders that are not assigned a private key to authenticate a revocation statement are excluded from this definition.

b.	All LRA procedures will be compliant with the appropriate Registration CPS.

c.	The MOD may operate one or more LRAs.

d.	The DII IPT may operate one or more LRAs to support internal operation of the DII – for the purposes of registration of certificates for PKI administration roles, TLS/SSL certificates for servers, code signing certificates and any other purpose identified by the DII IPT and approved by the DPMA

1.3.9 Request Handling Service

a.	The Request Handling Service is the service provided, and operated, by the DII IPT to support:

  i.	Creation and authentication of certificate issue requests

  ii.	Formatting, initialisation and loading (personalisation) of smartcards and other agreed devices holding Subscriber key-pairs and certificates

  iii.	Creation and authentication of revocation requests

b.	Operation of this service will be compliant with the appropriate Registration CPS.

1.3.10 Subscribers

a.	A Subscriber is the entity whose name appears as the subject in a certificate, and who asserts that the use of the key and certificate are in accordance with this policy. The targeted DPKI Subscribers include but are not limited to the following categories of entities:

  i.	MOD service and civilian personnel and eligible contractors.

  ii.	Personnel of, and approved contractors to, other UK government departments.

  iii.	MOD approved Foreign Government and Foreign organisation personnel, and eligible contractors.

  iv.	Devices (e.g. Workstations, Firewalls, Routers, Trusted Servers and other infrastructure components). These components may be operated by the MOD or third parties on behalf of the MOD, for example the DII Delivery Partner.

  v.	Organisational roles associated with individuals, groups of individuals or organisational entities.

b.	CA servers are technically subscribers to the DPKI. In this document, the term Subscriber refers only to those entities who receive certificates for uses other than signing and issuing certificates.

1.3.11 Relying Party

a.	A Relying Party (RP) is an entity that relies on the validity of the binding of a Subscriber's name to a public key to verify the integrity of a digitally signed object, to identify the creator of a digitally signed object, or to establish confidential communication with the holder of the certificate.

b.	Relying Parties may be Subscribers within the DPKI. A non-Subscriber shall only be a Relying Party if an explicit agreement exists with the MOD that creates such a relationship.

c.	A RP shall validate the status of all certificates in the certificate validation path, including verification of revocation status for all certificates, using the current revocation status information prior to their reliance. A certificate or revocation information must not be trusted if it is found to be invalid for any reason, or cannot be accessed, processed or authenticated.

d.	A RP shall use information in the certificate (such as certificate policy identifiers or key usage statements) to determine the suitability of the certificate for a particular use.

1.3.12 DPKI Technical Infrastructure

a.   The DPKI will be implemented using a number of components, including:

    i.   Defence Root CA servers (DRCA)

    ii.   Subordinate CA servers

    iii.   Registration servers

    iv.   Repository

    v.   OCSP responders

    vi.   Smartcard management systems

    vii.   Backups and alternatives to all of the above.

b.   All technical components of the DPKI shall be operated in accordance with this DCP as amplified by the appropriate Certification Practice Statements.

1.4   Certificate usage

a.   The DPKI supports the following services:

    i.   Authentication

    ii.   Integrity

    iii.   Non-repudiation

    iv.   Confidentiality

    v.   Other services as agreed by the DPMA

b.   The confidentiality service is expressly limited to support for privacy within MOD security domains at HMG Infosec Standard 1 (IS1) Impact Level 2 and for confidentiality outside MOD security domains at Impact Level 3. Guidance on the use of DPKI encryption services is given in JSP 457 vol 5 – applications that require confidentiality services at Impact Level 3, or above, should contact the DPMA.

c.   The authentication service is primarily intended to provide authentication to services operating within an MOD security domain. It is permitted to use this service, in conjunction with other elements, to authenticate a person to a MOD security domain. The MAL based service is limited to supporting Impact Level 3; HAL is limited to Impact Level 4. Logon to a MOD security domain, where reliance is placed on a DPKI credential, requires specific approval by the DPMA and agreement with a security accreditor.

d.   These core mechanisms are intended to support the long-term integrity of application data, but may not by themselves provide a complete solution for all circumstances. Subscribers and Relying Parties should identify additional application measures to satisfy their requirements.

1.4.1   Appropriate certificate uses

a.   DPKI certificates and associated keys shall only be used for authorised MOD business transactions covering the following:

    i.   Digital Signing (E-mail, Documents, Contracts) and/or Digital Signature checking.

    ii.   Authentication (e.g. via a Digital Signature).

    iii.   Confidentiality (via Encryption) for messaging, data transmission or secure data storage at an IS1 impact level no higher than Impact Level 3.

    iv.   Authentication and data separation using Transport Layer Security[5] (TLS) at an IS1 impact level no higher than Impact Level 3[6].

---

[5] All policies relating to TLS apply equally to Secure Sockets Layer version 3.0 (SSL 3.0).

     v.   Code Signing (e.g. Java applets, system upgrade patches or drivers).

     vi.   Specific requirements for VPNs and IPsec at an IS1 impact level no higher than Impact Level 3[7].

b.   The DCMA shall state this requirement in its CPSs and impose a requirement on Subscribers and Relying Parties to abide by this limitation.

1.4.2 Prohibited certificate uses

a.   Any uses other than those listed in Section 1.4.1 are prohibited. Any additional requirements and requests should be brought to the attention of the DPMA for consideration.

1.5 Policy administration

1.5.1 Organisation administering this document

The DPMA is responsible for the definition, revision and promulgation of this policy. The DPMA may delegate authorities in appropriate MOD policies and instructions.

1.5.2 Point of Contact

a.   Questions and comments regarding this DCP should be directed to:

Address	DES ISS Network Technical Authority Building 405 / E3 MoD Corsham Westwells Road Corsham Wiltshire SN13 9NR
Internet	http://www.mod.uk/pki
Intranet	http://www.mod.uk/DefenceInternet/MicroSite/DES/OurPublications/DefencePublicKeyInfrastructuredpkiPolicy.htm
Electronic Mail	dpki-dtag@.mod.uk

1.5.3 Person(s) determining CPS suitability to the DPKI CP

a.   The DPMA has responsibility for approving a CPS. Queries should be directed to the Point of Contact listed in Section 1.5.2 above.

b.   In each case, the determination of suitability shall be based on an independent compliance analyst's results and recommendations. The compliance analyst shall be from an organisation that is independent from the entity being audited. The compliance analyst shall not be the author of the subject CPS. The DPMA shall determine whether a compliance analyst meets these requirements.

1.5.4 CPS approval procedures

a.   The procedure for submitting CPS approval requests to the DPMA and the overall approval process is detailed in JSP 457 vol 5.

1.5.5 Waivers

a.   There shall be no waivers to this Certificate Policy.

---

[6] Support for TLS/SSL by the DPKI is dependant on compliance with CESG Manual T, as amplified by JSP 440 Part 8, when used at IS1 Impact Level 3.
[7] Support for IPsec by the DPKI is dependant on compliance with CESG Manual V, as amplified by JSP 440 Part 8, when used at IS1 Impact Level 3.

1.6 Definition of Terms

a. See Annexe A.

1.7 Acronyms

a. See Annexe B.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

a. The DPKI repository is used to store all certificates, ARLs/CRLs, CPSs, PDSs and policy statements (collectively, PKI objects) produced by the DPKI.

b. The location of any publication will be one that provides access to Subscribers and Relying Parties in accordance with a designated MOD accreditor's security requirements.

c. The repository shall not represent a single point of failure to the DPKI and as such shall provide multiple points of presence for each Relying Party to retrieve certificates and CRL information. At least one repository access point shall be available to each Subscriber and Relying Party at all times, subject to underlying network connectivity.

2.2 Publication of certification information

a. The DCMA shall ensure that this Defence Certificate Policy and the certificate status information are made available to all Subscribers and Relying Parties, either directly or through an online repository.

b. The repository may only be populated by authorised DPKI representatives. Mandatory information for inclusion in the repository includes:

   i. Issued encryption public key certificates that assert this Policy

   ii. Issued signing public key certificates that assert this Policy

   iii. CA certificates for each CA server certificate signing key

   iv. Certificate Revocation Lists

   v. A copy of this Policy.

c. Additionally, the DCMA shall provide an online repository that is available to Subscribers with certificates asserting this Policy that includes sections of the CPS that describes Subscriber duties and responsibilities, or a PDS as directed by the DPMA.

2.3 Time or frequency of publication

a. All information to be published in the repository shall be published promptly after such information becomes available to the DCMA. The DCMA shall specify in its CPS time limits within which it will publish various types of information. The minimum performance standards for this are defined in section 4 of this policy.

2.4 Access controls on repositories

a. The DCMA shall protect any repository information not intended for public dissemination or modification, as defined by the CPS and local security controls.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

a. Each Entity shall have a genuine, unambiguous, clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subject name field in accordance with RFC 3280 as amended by RFC 4630.

b. The DN shall be in the form of a X.501 *UTF8String* or *PrintableString* and shall not be a null entry.

c. Optionally, each Entity may use one or more alternative names via the *subjectAltName* certificate extension field, which shall also be in accordance with RFC3280, as amended by RFC 4630.

3.1.2 Need for names to be meaningful

a. In general certificate Subject and Issuer names shall be meaningful, using commonly understood semantics to identify the person or object to which they are assigned.

b. For Subject names:

    i. Signing and encryption certificates issued to individuals will use the Enterprise Directory Person object as the DN (ref. JSP 457 vol 4).

    ii. Signing and encryption certificates issued to organisational roles will use the Enterprise Directory Role object as the DN (ref. JSP 457 vol 4).

    iii. PKI role[8] certificates may use either the Enterprise Directory Person or Role object as the DN.

    iv. Server certificates for TLS/SSL shall use the device naming convention defined in JSP 457 vol 2 for the DN and an approved Fully Qualified Domain Name (FQDN) within the *subjectAltName* field.

    v. CA server certificates shall use the device naming convention defined in JSP 457 vol 2

c. For Issuer names:

    i. CA server certificates shall use the device naming convention defined in JSP 457 vol 2

d. The Registration Authority shall ensure that an affiliation exists between the Subscriber and any organisation that is identified by any component of any name in its certificate.

e. A CA server asserting this policy shall only sign certificates with Subject names from within a namespace approved by the DPMA. In the case where one DPKI CA server certifies a subordinate DPKI CA server, the certifying DPKI CA server shall impose restrictions on the name space authorised in the subordinate DPKI CA server, which are at least as restrictive as its own name constraints.

f. When technical means exist for imposing these constraints (such as the *nameConstraints* certificate extension), they shall be used. Otherwise, these constraints shall be imposed procedurally or contractually.

3.1.3 Anonymity or pseudonymity of Subscribers

a. Certificates issued to CA servers shall not contain anonymous or pseudonymous identities.

---

[8] PKI role certificates are for internal use within the operation of the PKI, examples include RA Operators and CA server administrators.

b. Certificates that contain a Subject name that is a pseudonym shall contain a unique reference that identifies the natural person, who controls the private key that corresponds to the public key within the certificate. There is no requirement for the reference to be meaningful to a Relying Party or for multiple certificates associated with the same natural person to contain the same reference number[9].

c. Organisation role names are defined as pseudonymous.

d. The DCMA shall not issue anonymous Subscriber certificates without the express consent of the DPMA.

3.1.4 Rules for interpreting various name forms

a. Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7).

b. All name forms used within the DPKI shall be approved by the DPMA.

3.1.5 Uniqueness of names

a. All distinguished names shall be unique within the DPKI, for all time. Names shall not be re-used for another end entity after a different end entity's certificate expires or is revoked; however, names can be re-used to re-issue a certificate to the same end entity.

b. Uniqueness of names may be established by a combination of Subject and *subjectAltName* when assigned to organisational role certificates. Note that the end entity corresponding to an organisational role is that role, not the natural person occupying the role from time-to-time.

c. Name uniqueness across the DPKI shall be enforced. Wherever practical, X.501 DNs allocated from the appropriate MOD naming authority shall be used, and the DCMA shall enforce name uniqueness policy within the X.500 name space that it has been authorised to use.

d. When other name forms are used (e.g., IP addresses, FQDNs), they too must be allocated such that name uniqueness across the MOD is ensured. The DCMA shall document in its CPSs what name forms will be used, how the CA and RA/LRAs will interact with MOD naming authorities, and how they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (for human entities this uniqueness is supported by the PUID/PUID Name mechanism[10]).

3.1.6 Recognition, authentication, and role of trademarks

a. If a person claims that a certificate contains a trademark for which they are the registered proprietor, and the DCMA is reasonably satisfied that the proper use of the certificate will infringe that registered trade mark, the DCMA shall immediately revoke the certificate. The MOD assumes no responsibility for this type of coincidence.

b. There is no obligation for the DCMA to investigate whether a certificate application contains a registered trademark. However, the DCMA should not issue a certificate where it reasonably suspects that the proper use of the certificate is likely to infringe a registered trademark.

c. Intellectual Property Rights (IPR) for trademarks is described in Section 9.

---

[9] Approved mechanisms for creating references are given in the DPKI Interface Specification. The database containing the association between a reference and a natural person may be protectively marked, but the reference value is not.
[10] See JSP 457 vol 2.

3.1.7 Name claim dispute resolution procedure

a.   The DCMA shall investigate and correct, if necessary, any name collisions brought to its attention, relating to certificates issued by the DCMA. If appropriate, the DCMA shall coordinate with, and defer to, the appropriate naming authority.

b.   The DCMA shall have and follow a name claim dispute resolution procedure with providers of repository services, if external to the DPKI.

3.2   Initial identity validation

3.2.1 Method to prove possession of private key

a.   In all cases where the Subscriber generates keys, the Subscriber shall prove to the DCMA that it is in possession of the private key that corresponds to the public key in the certificate request. For signature keys this may be done by signing the request using the appropriate private key. Other key possession mechanisms may be approved by the DPMA.

b.   In the case of a key being generated directly on the Subscriber's token, or in a key generator that subsequently transfers the key to the Subscriber's token, then it may be assumed that the Subscriber is in possession of the private key at the time of generation or transfer.

3.2.2 Authentication of organisation identity

a.   Authentication of a civil or military body shall include the organisation name, address, and documentation of the existence of the organisation. This documentation shall be based on the charter or Terms of Reference for the organisation which shall have the approval of the appropriate superior body. The DCMA shall verify this information, in addition to the authenticity of the requesting representative, and the representative's authorisation to act in the name of the organisation.

b.   The DCMA shall keep a record of the type and details of identification used.

3.2.3 Authentication of individual identity

3.2.3.1   Authentication of Person Identity

a.   The DCMA shall ensure that the Subscriber's identity and public key information are bound adequately prior to requesting/issuing a certificate. The DCMA shall specify in its Registration CPS the procedures to be followed to provide identification of individuals and the generation of an auditable record of this process. At a minimum the auditable record shall include:

    i.   Identity of the person performing the identification;

    ii.   The mechanism used to perform the identification, along with serial numbers or other unique identifiers for documents used to support identification.

    iii.   The date and time of the identity verification.

b.   An approved authentication mechanism shall be employed every time a certificate is issued.

c.   The RA shall compare the identity of the individual with two pieces of original identification e.g. passport or driving licence. Where the applicant is a MOD employee or contractor, at least one of these shall be MOD identification containing a photograph.

d.   The RA shall establish that an applicant for a MAL certificate intended for use in the RESTRICTED domain has a valid and current Baseline Personnel Security Standard check (BS). The RA shall establish that an applicant for a MAL certificate intended for use in the SECRET domain, or a HAL certificate for use in any domain, has a valid and current Security Check (SC).

e.   Additionally, the process documentation shall include a declaration of identity. The declaration shall be signed with a handwritten signature or, if a good fingerprint or other

adequate biometric is collected and can be linked to the subscriber identity, a digital signature can be used[11]. Either type of signature shall be applied in the presence of the person performing the identity authentication.

3.2.3.2 Authentication of Existing Subscriber Identity

a.   In some circumstances, detailed elsewhere in this DCP, it is necessary to establish the identity of an existing Subscriber (for example, during certificate re-key or modification). A Subscriber shall authenticate their identity to the RA using a digital signature or other technical mechanism (e.g. client-side TLS authentication) in order to prove their identity, and their status as a Subscriber.

3.2.3.3 Authentication of Sponsor Identity

a.   A Sponsor acts on behalf of another entity and will assume all the responsibilities associated with the entity, as if the Sponsor was the entity.

b.   A Sponsor shall be an existing Subscriber. A Sponsor shall authenticate their identity to the RA using a digital signature or other technical mechanism (e.g. client-side TLS authentication) in order to prove their identity, and their status as a Subscriber.

c.   A MAL Subscriber shall not act as a Sponsor for a certificate request that will be issued under the HAL policy. A HAL Subscriber may act as a Sponsor for certificate requests issued under either the MAL or HAL policies.

d.   The RA/LRA shall keep a record of the type and details of identification used.

3.2.3.4 Authentication of Role Identity

a.   A request for a certificate to be allocated to an organisational role identity shall be made by a Sponsor. A Sponsor shall be an individual who currently occupies the role, or is the designated administrator for a multi-user role, who is deemed accountable and responsible for that role entity.

b.   Identification and authentication of the Sponsor shall follow the procedures established by this policy in 3.2.3.3. The RA shall additionally verify the individual authority to act on behalf of the role.

c.   The RA/LRA shall keep a record of the type and details of identification used.

3.2.3.5 Authentication of Devices or Applications

a.   A request for a device or application to be an end entity shall be made by a Sponsor. A Sponsor shall be an individual or organisational role to whom the device or application is attributable for the purposes of accountability and responsibility. Where an organisational role acts as a Sponsor, the current Sponsor of that role shall be accountable as an individual.

b.   Identification and authentication of the Sponsor shall follow the procedures established by this policy in 3.2.3.3. The RA shall also verify the individual authority to act on behalf of that device or application.

c.   The RA/LRA shall keep a record of the type and details of identification used.

3.2.4 Non-verified Subscriber information

a.   All Subscriber information shall be verified. Non-verified Subscriber information shall not be included in certificates.

---

[11] The terms "good" and "adequate" are used advisedly, pending further guidance on the use of biometric identification from CSIA.

3.2.5 Validation of authority

a.   Certificates that contain explicit or implicit organisation affiliations shall be issued only after ascertaining that the Subscriber or Sponsor has the authorisation to act on behalf of the organisation in the implied capacity. Examples of these include organisation/group and role certificates, and CA/RA server certificates.

3.2.6 Criteria for interoperation

a.   This Defence Certificate Policy shall form a basis for assessing interoperability with the DPKI. Where interoperation with a PKI that does not implement this DCP is required, the DPMA shall establish that equivalent requirements and constraints exist for the uniqueness of names and the establishment of identity.

b.   For cross certification, the DPMA shall validate the external organisation representative's authorisation to act in the name of the external organisation.

3.3   Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

a.   To maintain assurance provided to a Relying Party that a unique binding between a key and its named Subscriber is valid, a Subscriber shall periodically obtain new keys *and* re-establish its identity.

b.   A request for re-key may only be made by the entity (or Sponsor acting on its behalf) in whose name the certificate has been issued.

c.   The entity (or its Sponsor) should use its existing credentials, to authenticate themselves to the RA in accordance with the appropriate policy in 3.2.3.

d.   For HAL, verification and validation of identity to the same standard as initial registration shall always be required.

e.   For MAL, routine re-key may be automated: In this case possession of an existing certificate and proof of possession of the associated private key is accepted as identification. Section 4.6.7 identifies the maximum number of times this may be performed before re-registration is required.

f.   For CA servers, request for re-key shall always be made by the Sponsor for the device, and will normally require approval by the DPMA of the continuing operation of the CA server[12]. The DCMA shall describe the process and authentication requirements in the relevant CPS.

g.   The entity/Sponsor shall prove possession of its current private key by using that private key to sign a value and providing that value to the DCMA. The issuing RA will then validate the signature using the party's public key. Where possible, the RA should use the party's public key certificate as stored within the repository.

3.3.2 Identification and authentication for re-key after revocation

a.   Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key, the DCMA shall authenticate a re-key in the same manner as for initial registration. Any change in the information contained in a certificate shall be verified by the RA before that certificate is issued.

3.4   Identification and authentication for revocation request

a.   The list of entities that can request revocation is described in Section 4.9.2. The DCMA shall authenticate a request for revocation of a certificate. Revocation requests may be

---

[12] Note that all CA servers require approval by the DPMA for their establishment and continuing operation. This process requires evidence of accreditation, as well as an approved CPS that describes the operation of the CA server (see 4.1).

authenticated using the public key of the certificate to be revoked, regardless of whether or not the associated private key has been compromised.

b.   When the requester of revocation is the Subscriber, other methods may be used to authenticate revocation requests, such as communication with the Subscriber providing reasonable assurance that the person or organisation requesting revocation is, in fact, the Subscriber. The DCMA shall establish, and make publicly available, the process by which it addresses such revocation requests and the means by which it will establish the validity of the request.

c.   The DRCA shall only accept revocation requests that are authenticated using the digital signature of the device Sponsor where revocation of a CA server or CA cross certificate is requested. This process shall be described in the DRCA CPS.

d.   Requests for revocation of certificates shall be included in the accounting log, as described in Section 5.4.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

a. It is the aim of this Policy to identify the minimum requirements and procedures that are necessary to support trust in the DPKI, and to minimise imposition of specific implementation requirements on the DCMA, Subscribers, and Relying Parties. The relationships within the DPKI should be clearly understood, and are described in Section 1.3 of this policy. Authority for approving the issue of a certificate rests with the MOD and is delegated to the Registration Authority, who may in turn delegate some part of this authority to a Local Registration Authority. The Certificate Manufacture Service is responsible for responding to authorised Certificate Requests in a timely manner.

b. All aspects of the certificate life-cycle processes shall be documented in the appropriate Certification Practice Statement. In particular, there may be multiple CPSs for use by LRAs to support varying local and/or security requirements. This policy identifies minimum standards to be met by CPSs – these standards may be exceeded to suit local requirements. In all cases secure mechanisms to establish and maintain authentication, non-repudiation, integrity and confidentiality shall be used commensurate with the assurance level of the keys and certificates being managed.

4.1 Certificate Application

a. An entity requesting a certificate is an Applicant. The Applicant could be a person or a Sponsor acting on behalf of a person, organisational role or device. Where the terms Applicant or Subscriber are used in this section it may be assumed that this applies equally to a Sponsor, unless it is clear from the context that this is not intended.

b. A valid application for a certificate does not oblige the DCMA to authorise the issue of a certificate.

c. Generally, an RA/LRA will register the Applicant of a certificate, but if the CA server issues certificates directly (for example to an operator of a CA server), the CA shall verify the identity of the Applicant in the same way as an RA, as described in Section 3.

d. The DII IPT may establish one or more LRAs to support the registration of certificates for internal operations within the DPKI or the DII. Such LRAs shall operate under a CPS approved by the DPMA and are deemed to receive delegated authority to perform their functions from the Registration Authority.

e. Applications for CA certificates, for instantiation or renewal of a CA server, shall be submitted to the DPMA accompanied with a CA Certification Practice Statement detailing the operation of the CA server and showing compliance with this policy.[13]

4.1.1 Enrolment process and responsibilities

a. Upon receiving a request from an Applicant, the RA/LRA shall:

    i. Verify the identity of the Applicant.

    ii. Verify the authority of the Applicant.

    iii. Verify the accuracy of the information provided by the Applicant.

b. It is the responsibility of the RA/LRA to verify that the information is correct and accurate and comes from an appropriate and authoritative source[14].

---

[13] There will also be a requirement for other documentation for security accreditation purposes, which is beyond the scope of this policy.

[14] If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a RA/LRA shall be protected from unauthorised modification.

c. RA/LRAs shall verify all authorisations and other attribute information received from an Applicant. Information regarding attributes shall be verified via those offices or roles that have authority to assign the information or attribute.

d. In the circumstance where a request is received as a Certificate Request (e.g., PKCS#10), the integrity of this request shall be tested by the RA/LRA.

e. On completion of the validation process, the RA/LRA shall create a Certificate Request, or utilise the one provided by the Applicant. This request shall be either:

    i. Signed by the RA/LRA using a signing key previously allocated to the RA/LRA by the DCMA or,

    ii. Submitted to the CMS within a secure session (e.g. TLS) where the RA/LRA endpoint is authenticated using DPKI credentials previously allocated to the RA/LRA for this purpose.

f. This authentication attests that the request is correct, authentic and authorised by the DCMA and is the authority for the CMS to process the request and issue a certificate.

4.1.2 Who can submit a certificate application

a. DPKI Subscribers include, but are not limited to, the following categories of entities:

    i. MOD service and civilian personnel.

    ii. MOD contractors.

    iii. Devices (e.g. Workstations, Firewalls, Routers, Trusted Servers and other infrastructure components).[15]

    iv. Organisational roles.

b. A Sponsor always acts on behalf of a device or organisation role (see Section 3.2).

c. The following entities may be eligible as DPKI Subscribers, but shall apply through a DPMA approved MOD Sponsor:

    i. Personnel and approved contractors to other UK government departments.

    ii. Personnel of List X companies not directly contracted to MOD.

    iii. Foreign Government and Foreign organisation personnel and eligible contractors.

4.2 Certificate application processing

a. It is the responsibility of the RA/LRA to verify that the information in certificate applications is accurate. Registration CPSs shall specify procedures to verify information in certificate applications.

4.2.1 Performing identification and authentication functions

a. The identification and authentication of the Applicant shall be conducted by the RA or LRA.

b. Where the Applicant is a Sponsor acting on behalf of a CA server, identification and authentication of the Sponsor shall be performed by the trusted roles with responsibility for this function, as identified in the appropriate CPS. DPMA approval for instantiation, or continued operation, of a CA server shall state the DN of the server and the Sponsor and this identity shall be established and authenticated by the trusted roles.

4.2.2 Approval or rejection of certificate applications

a. The certificate application may be rejected for various reasons, such as inaccurate information or lack of mission need to provide a certificate to the applicant. The RA/LRA may

---

[15] These components may be operated by MOD or third parties on behalf of the MOD, for example the DII Delivery Partner.

reject a certificate application. The RA/LRA shall work with the appropriate parties to resolve the problem; final arbitration rests with the DPMA.

b.   A certificate application shall not be considered accepted until the RA/LRA has issued an authenticated Certificate Request and this has been received by the CMS.

4.2.3 Time to process certificate applications

a.   The Registration Authority may define minimum performance standards in its CPS. These may be exceeded as deemed appropriate by LRAs; where performance standards are established these shall be documented in the appropriate LRA CPS.

4.3   Certificate issuance

a.   All certificates are issued under the authority of the DPKI Certification Authority, who may delegate this authority to subordinate authorities. In general, that part of the authority relating to determining which entities may receive a certificate is delegated to the Registration Authority, that part relating to the issuance of certificates is delegated to the Certificate Manufacture Service.

4.3.1 CMS actions during certificate issuance

a.   On receipt of a Certificate Request from an authorised RA/LRA, the CMS shall:

   i.   Authenticate the requesting RA/LRA and verify the integrity of the request.

   ii.   Verify that the RA/LRA has authority to request issuance of the class of certificate or key usage.

   iii. Verify that the RA/LRA has authority to request a certificate that may be issued to the Subscriber within the namespace constraints imposed by the CPS.

   iv.   Validate that, where values to include within the certificate are contained within the request, these are consistent with the values permitted by the appropriate certificate profile and as defined by the appropriate CPS or notified by the DPMA.

   v.   Create the certificate in a timely manner and publish the result in the Repository.

   vi.   Notify the requesting RA/LRA that the certificate has been issued (this may be accomplished by providing a copy of the issued certificate or an indication of its location within the Repository).

b.   For CA server certificates the CMS shall verify all fields within the certificate prior to its publication and/or transmission to the Sponsor.

c.   A full accounting log shall be maintained of all CMS actions, including the basis on which verification of authority is determined.

d.   The CMS is entitled to reject any request that cannot be authenticated, the integrity of which cannot be demonstrated or is not authorised within the limits of certificate type, key usage or namespace constraints. Such a rejection shall be indicated to the requesting RA/LRA in a timely manner, along with an explanatory statement of the reason for rejection.

4.3.2 Notification to subscriber by the CA of issuance of certificate

a.   The RA/LRA is responsible for notifying the Subscriber that a certificate has been issued. The process for this should be described in the Registration CPS.

b.   Where a certificate is issued to a CA server the process for notifying the Subject CA server shall be described in the CPS of the Issuer CA server.

4.4   Certificate acceptance

a.   A certificate is deemed to be accepted when it is delivered to the Subscriber by the RA/LRA.

b.   In the case of Person and/or Role certificates, issued in conjunction with a smartcard or other token, the certificate is deemed to be delivered at the point where the token is loaded with the certificate and associated private key. In the case of a re-key onto an existing token, certificate acceptance is deemed at the point where the token is loaded with the new certificate.

c.   In the case of device/server certificates (e.g. TLS/SSL certificates) acceptance is deemed at the point at which the certificate is downloaded from the RA/LRA or issuing CA server.

d.   In the case where the Subscriber is responsible for key generation, prior to requesting a certificate, Subscriber responsibilities commence at the time of key generation. Subscriber responsibilities to the DPKI may, in some circumstances, commence at the time of certificate acceptance – for example, if a smartcard is pre-loaded with keys and certificates prior to issue to a user.

e.   In the case of a CA server, acceptance is deemed at the point at which the certificate is delivered to the server. In all the cases (instantiation and re-key) the DPMA shall be notified when a CA server certificate has been issued and accepted.

4.4.1 Conduct constituting certificate acceptance

a.   No stipulation.

4.4.2 Publication of the certificate by the CA

a.   The DCMA shall publish the certificate into the repository in a timely manner, following its creation. This task should be performed by the CMS.

4.4.3 Notification of certificate issuance by the CA to other Entities

a.   In all the cases the DPMA shall be notified when a CA server certificate has been issued and accepted.

4.5   Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

a.   The Subscriber shall use the private key for transactions relating to authorised MOD business covering the certificate uses stated in Section 1.4.1 only. The use of the private key shall be further limited in accordance with the key usage extension in the associated certificate.

b.   The Subscriber shall not use a private key after the associated certificate has been revoked or has expired.

c.   If the extended key usage extension is present and implies any limitation on the use of the private key, those constraints shall also be observed. For example, the OCSP Validation Authority private key shall be used only for signing OCSP responses.

d.   Subscribers shall protect their private keys from access by other parties.

e.   CA servers shall limit the use of their private keys to those activities explicitly stated within the approved CPS that describes their operation.

4.5.2 Relying party public key and certificate usage

a.   Relying Parties shall ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension, if the extension is present.

b.   If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be observed.

4.6 Certificate renewal

a. Except as noted below, the DPKI does not support certificate renewal – the issuance of a new certificate containing an existing public key. New key pairs shall be generated whenever a certificate is issued, except where modification is permitted (see 4.8).

b. Where CA server certificates are issued to a CA server that is external to the DPKI for the purposes of cross-certification the use of certificate renewal is permitted. The circumstances of such renewal shall be described within a Cross-Certification Agreement, or other similar document, that is approved by the DPMA and the equivalent body representing the external PKI.

4.6.1 Circumstances for certificate renewal

a. A new cross-certificate may be issued to an external CA server, provided that:

  i. The DPMA has authorised the issuance

  ii. The private key of the external CA server is not expired, revoked or compromised

  iii. The Subject name and other identifying attributes are unchanged

b. The expiry date of the new certificate shall not exceed the lifetime of the corresponding private key.

c. The expiry date of the new certificate shall not exceed the expiry date of any Cross-Certification Agreement.

4.6.2 Who may request renewal

a. Renewal may be requested by any of the parties to the Cross-Certification Agreement.

4.6.3 Processing certificate renewal requests

a. The DRCA shall define the process for renewal of a cross-certificate in its CPS. In general it is a requirement that the process described in 3.3 be followed for identification and authentication.

4.6.4 Notification to subscriber by the CA of issuance of new certificate

a. The DPMA shall notify the PMA of the external PKI of the issuance of a new certificate.

4.6.5 Conduct constituting certificate acceptance

a. See 4.4.

4.6.6 Publication of the renewal certificate by the CA

a. The DRCA shall describe within its CPS the mechanism used to publish the renewed certificate following issuance.

4.6.7 Notification of certificate issuance by the CA to other Entities

a. The DPMA shall be notified when a cross-certificate has been renewed.

4.7 Certificate re-key

a. Certificate re-key occurs when a new key-pair is created for an existing Subscriber, where this new key-pair is intended to replace an existing key-pair for which the Subscriber has previously received a certificate.

b. In principle, the new certificate will be identical to the original, apart from the serial number, validity period and public key value. However, using the re-key procedure, it is permitted by

this policy to make other changes to the certificate that may be deemed necessary at the time of issue[16].

4.7.1 Circumstance for certificate re-key

a. Certificate re-key will normally be required prior to the expiry of the certificate supporting an existing key-pair: This is deemed a routine re-key. The time period before expiry at which a re-key should occur should be stipulated in the CPS of the RA/LRA issuing the original certificate. In the absence of such a stipulation, a re-key may be requested at any time prior to the expiry of an existing certificate.

b. It is permitted to automate the routine re-key process (see 3.3.1). The maximum number of automated re-key events permitted is:

	MAL Soft	MAL Hard	HAL
Person certificates	0	2	0
Role certificates	0	2	0
Device certificates	2	2	0

c. Certificate re-key will normally be required following a certificate revocation, unless such a revocation is performed because the certificate (and therefore the associated key-pair) is no longer required. The procedure for requesting a re-key following revocation is not the same as that required for routine re-key – RA/LRA CPSs shall specify a separate process for re-key following revocation, with due regard being given to the circumstances of revocation. Normally, such a request should be treated as a new Subscriber request.

4.7.2 Who may request certification of a new public key

a. Any existing Subscriber is entitled to request a routine re-key prior to the expiry of an existing certificate. A trusted software agent, such as the DII Smart Card Management System, may act on behalf of the Subscriber or Sponsor for such a request.

b. The Sponsor of a CA server certificate may request a re-key, but only with the authorisation of the DPMA for the continued operation of the CA server.

c. A request for a re-key following the expiry of an existing certificate shall be treated as a new Subscriber request and follow the procedures outlined in Section 4.1.

d. A request by an existing subscriber for re-key following revocation is permitted, but this will normally be treated as a new Subscriber request and follow the procedures outlined in Section 4.1.

4.7.3 Processing routine re-keying requests

a. RA/LRAs should:

    i. Verify that the Subscriber (or Sponsor) retains possession of the smartcard or other token (if applicable) and can demonstrate continued access to, and operation of the current private key.

    ii. Enforce the identification requirements given in section 3.3 and as stipulated in the CPS of the RA/LRA.

    iii. Verify that the authority of the Subscriber to hold the certificate is still in existence.

b. Once the RA/LRA is satisfied that the request for routine re-key is permissible, then the re-key may proceed. This should follow the same processes for key generation, request processing and submission to the CMS as described in Section 4.2 and 4.3.

---

[16] In particular, a different CA server could be used for issuance, global changes to policy OIDs or other matters that apply to the class of certificate could be made during re-key.

c.   The original certificate may be revoked once the new certificate has been issued. This revocation may be delayed to suit the requirements of the Subscriber – this should be detailed in the Registration CPS. Where the original private key has been irrevocably put beyond further use[17] there is no requirement to revoke the original certificate – this circumstance shall never apply to a key that has been, or is capable of being, copied, backed-up or stored in a retrieval system.

d.   In the circumstance where a CA server is to be re-keyed, approval of the DPMA for continued operation must be confirmed. Under no circumstance shall a certificate supporting an old CA server key be revoked without the express instruction of the DPMA.

4.7.4   Notification of new certificate issuance to subscriber

a.   The RA/LRA is responsible for notifying the Subscriber that a certificate has been issued. The process for this should be described in the Registration CPS.

b.   Where a certificate is issued to a CA server the process for notifying the Subject CA server shall be described in the CPS of the Issuer CA server.

4.7.5   Conduct constituting acceptance of a re-keyed certificate

a.   See 4.4.

4.7.6   Publication of the re-keyed certificate by the CA

a.   The DCMA shall publish the certificate into the repository in a timely manner, following its creation; this task should be performed by the CMS.

4.7.7   Notification of certificate issuance by the CA to other Entities

a.   In all the cases the DPMA shall be notified when a CA server certificate has been issued and accepted.

4.8   Certificate modification

a.   Certificate modification occurs when changes other than the public key are required to an existing Subscriber certificate. It is not permitted to use certificate modification as a means of renewal. RA/LRAs may support certificate modification if they deem it necessary – this shall be documented in the appropriate CPS if it is to be supported.

b.   In general, RA/LRAs should consider issuing a new certificate using the re-key procedure if more than 75% of the certificate lifetime has been expended.

4.8.1   Circumstance for certificate modification

a.   A certificate modification may be required for a number of reasons, including:

   i.   Following a change of name by a Subscriber (e.g., marriage) that results in a new DN.

   ii.   Following a change in the Electronic Unit Name (EUN) component of the name of an organisational role that results in a new DN.

   iii.   Following a change in policy OIDs or policy constraints.

   iv.   For a CA certificate following a change in namespace constraints.

b.   A RA/LRA that supports certificate modification should specify the circumstances under which a modification is permissible in its CPS.

---

[17] E.g., where the key storage area of a smartcard or other token has been overwritten with a new key, or zeroised using an approved method.

4.8.2 Who may request certificate modification

a. An existing Subscriber may request modification of its certificate.

b. A Sponsor may request modification of any certificate that it is the sponsor for.

c. The Registration Authority may request modification of any existing certificate – this will normally be done when some significant change is required for all certificates of a particular type.

4.8.3 Processing certificate modification requests

a. RA/LRAs should:

    i. Verify that the Subscriber (or Sponsor) retains possession of the smartcard or other token (if applicable) and can demonstrate continued access to, and operation of the private key.

    ii. Repeat the identification requirements stipulated in Section 3.2 to a degree to be stipulated in the CPS of the RA/LRA.

    iii. Verify that the authority of the Subscriber to hold the certificate is still in existence.

    iv. Verify that the requested modifications are permitted by the Registration Authority.

b. Once the RA/LRA is satisfied that the request for modification is permissible, then the modification may proceed. This should follow the same processes for request processing and submission to the CMS as described in Section 4.2 and 4.3.

c. The original certificate may be revoked, but this is not required and the RA/LRA may stipulate within their CPS the circumstances in which the original certificate may be retained.

4.8.4 Notification of new certificate issuance to Subscriber

a. The RA/LRA is responsible for notifying the Subscriber that a certificate has been issued. The process for this should be described in the Registration CPS.

b. Where a certificate is issued to a CA server the process for notifying the Subject CA server shall be described in the CPS of the Issuer CA server.

4.8.5 Conduct constituting acceptance of modified certificate

a. See 4.4.

4.8.6 Publication of the modified certificate by the CA

a. The DCMA will publish the certificate into the repository in a timely manner, following its creation; this task will be performed by the CMS.

4.8.7 Notification of certificate issuance by the CA to other Entities

a. In all the cases the DPMA shall be notified when a CA server certificate has been issued and accepted.

4.9 Certificate revocation and suspension

a. A certificate may be revoked prior to its expiry. A decision to revoke a certificate is made by the Registration Authority who is responsible for sending a revocation request to the CMS for action. Initiation of the revocation process need not originate from the RA, but the RA shall authorise the request. Creation and publication of CRLs, updating of OCSP responders and management of the certificate within the repository are the responsibility of the CMS and/or the VA.

4.9.1 Circumstances for revocation

a.   A certificate issued to a Subscriber shall be revoked by the Registration Authority:

    i.   Upon suspected or known compromise of the private key.

    ii.   Upon suspected or known loss or compromise of the media holding the private key.

    iii.   Following termination of affiliation or employment with a MOD civil or military body.

    iv.   Upon decommissioning a device.

    v.   Following determination that registration information was invalid.

b.   A certificate issued to a Subscriber may be revoked by the Registration Authority:

    i.   Upon termination of the need for a certificate.

    ii.   When a certificate has been replaced following re-key or modification.

c.   This DCP does not require the revocation of a certificate where the private key associated with the certificate has been destroyed, or rendered beyond further use (for example, by destruction of a hardware token or overwriting of a key store). This statement can never be applied to a key that has been, or is capable of being, copied, backed-up or stored in a key retrieval system.

d.   In the case were the private key of a CA server is known, or suspected to be, compromised the decision to revoke the certificate of the CA server shall be made by the DPMA.

e.   The DCMA, at its discretion, may revoke a certificate when a Subscriber or CA server fails to comply with obligations set out in this policy, the relevant CPS, or any other agreement or applicable law.

f.   Where a non-MOD CA is cross-certified with the DPKI, the DPMA shall revoke a cross-certificate:

    i.   When any of the information in the External CA certificate changes.

    ii.   Upon suspected or known compromise of the External CA private key.

    iii.   Upon suspected or known compromise of the media holding the cross-certified External CA private key.

    iv.   When the External CA certificate is revoked.

g.   The DPMA, at its discretion, may direct the revocation of a cross-certificate when an external PKI fails to comply with obligations set out in its CP, CPS, any agreement or any applicable law.

4.9.2 Who can request revocation

a.   All requests for revocation should be forwarded through the Registration Authority or an LRA, who provide the interface into the CMS.

b.   The revocation of a certificate may be requested by:

    i.   The Subscriber.

    ii.   The Sponsor who made the application for the certificate.

    iii.   The relevant Security Officer (if applicable).

    iv.   Personnel or Human Resources department.

    v.   An RA/LRA for any certificate issued at their request.

    vi.   The DPMA for any certificate.

c.   The revocation of a cross-certificate shall only be requested by:

i.   The External PMA on whose behalf the cross-certificate was issued.

ii.   The DPMA (or delegated authority).

iii.   The JSyCC in its role as the relevant Security Officer.

4.9.3   Procedure for revocation request

a.   Following the decision to revoke a certificate, the RA/LRA is responsible for generating a Revocation Request. This request should be either:

i.   Signed by the RA/LRA using a signing key previously allocated to the RA/LRA by the DCMA or,

ii.   Submitted to the CMS within a secure session (e.g. TLS) where the RA/LRA endpoint is authenticated using DPKI credentials previously allocated to the RA/LRA for this purpose.

b.   This signature attests that the request is correct, authentic and authorised by the DCMA. This signature is the authority for the CMS to process the request and revoke a certificate.

c.   Prior to issuing a Revocation Request the RA/LRA shall satisfy itself:

i.   That the request for revocation is made by an authorised source.

ii.   That the certificate to be revoked is unambiguously identified.

iii.   That the reason specified for revocation is one of those given in Section 4.9.1.

d.   The RA/LRA shall record full details of all requests for revocation it receives, including those it may reject. The accounting log shall include at least:

i.   The source of the request.

ii.   The date/time of the request being received.

iii.   The mechanisms used to determine that the request is acceptable.

iv.   The reasons for rejection, if applicable.

v.   The reason for the request.

vi.   Confirmation that the key store of any token used to store a private key associated with a certificate has been zeroised, if this is possible.

vii.   The date/time of the Revocation Request being transmitted to the CMS.

e.   The RA/LRA CPS shall fully document the revocation procedure and should identify a target time interval to create a Revocation Request.

4.9.4   Revocation request grace period

a.   This DCP does not define a permitted grace period. Following discovery of a certain or potential compromise of a Subscriber private key, or the loss of a cryptographic token used to store a private key, a Subscriber or Sponsor shall report this to the RA/LRA. Such a report may be made directly, or via an appropriate security officer. The report shall be made as soon as practicably possible.

b.   For all certificates a revocation request shall be made immediately upon discovery of the loss or potential compromise.

4.9.5   Time within which the CMS must process the revocation request

a.   The CMS shall process 99% of Revocation Requests within 15 minutes of receipt. Processing is completed when the current revocation status of a certificate is available for publication in a CRL, or notification to the DPKI Validation Authority.

b.   The service for processing Revocation Requests and subsequently updating OCSP and CRL information shall be available at all times (subject to the availability of the underlying infrastructure).

4.9.6 Revocation checking requirement for relying parties

a.   It is incumbent on a Relying Party to verify the status of any certificate that it wishes to use. This should be done using the DPKI Validation Authority (VA) service. In exceptional circumstances the DPMA may authorise the use of a current CRL.

b.   A current CRL is defined as the most recent relevant CRL published to the Repository by the CMS.

c.   If it is not possible to determine the current revocation status of a certificate, because the OCSP service is unavailable or the current CRL is not accessible, then the Relying Party may choose to accept the certificate if it is in all other respects valid. However, the MOD accepts no liability if such an action is taken.

4.9.7 CRL issuance frequency

a.   The DRCA shall publish an ARL at intervals of approximately 30 days, and indicate the lifetime of each ARL to be 90 days from the date of issuance.

b.   At intervals, the CMS shall publish to the repository a CRL for each CA server. Each CRL shall state a lifetime not to exceed 24 hours from the time of issuance. Where a CRL is the means of communicating revocation status to the Validation Authority, then each CA server shall publish its CRL at intervals not to exceed 1 hour. Where other means exist to communicate revocation status to the VA (or where the CA server has been exceptionally excused from supplying revocation information to the VA), then the CRL publishing interval shall not exceed 12 hours.

c.   Details of the CRL issuance frequency, CRL lifetimes and availability of revocation status information via the VA, shall be stated in the relevant CPS. The information stated in the CPS (or associated PDS) should be sufficient to permit a Relying Party to determine the timeliness of the revocation status information available from the CA server.

4.9.8 Maximum latency for CRLs

a.   The CRL shall be published on generation.

4.9.9 On-line revocation/status checking availability

a.   The normal mechanism for checking the revocation status of a certificate within the DPKI is using the OCSP service provided by the Validation Authority (VA).

b.   To support this, a VA service shall be available within the DPKI at all times (subject to the availability of the underlying infrastructure).

c.   In exceptional circumstances, a Relying Party may routinely use CRLs to determine status information. This is subject to authorisation by the DPMA.

4.9.10 On-line revocation checking requirements

a.   Following the revocation of a certificate, the CMS shall notify the VA of the changed status of the certificate. The worst case latency between the completion of revocation processing and the availability of updated revocation information from the VA shall not exceed 1 hour.

b.   The interface requirements (including OCSP options) for the VA are specified in the DPKI Profile and Interface Specification.

4.9.11 Other forms of revocation advertisements available

a.   No stipulation.

4.9.12 Special requirements re key compromise

a.   No stipulation.

4.9.13 Circumstances for suspension

a.   The DPKI does not support suspension of certificates. Once a certificate has been revoked that fact shall continue to be published on the appropriate CRL until after the expiry of the certificate. The VA shall continue to indicate a revoked status until after the expiry of the certificate.

4.9.14 Who can request suspension

a.   No stipulation.

4.9.15 Procedure for suspension request

a.   No stipulation.

4.9.16 Limits on suspension period

a.   No stipulation.

4.10   Certificate status services

a.   The DPKI offers the On-line Certificate Status Protocol (OCSP) as defined in RFC 2560 to provide on-line access to the current revocation status of all certificates used in the DPKI. This is the primary means of checking the revocation status of a certificate. To support this, the DCMA will deploy an OCSP service as part of the VA. All Relying Parties are expected to use systems and software compatible with OCSP to ensure access to up-to-date status information.

4.10.1 Operational characteristics

a.   No stipulation.

4.10.2 Service availability

a.   The OCSP service shall be available to all users at all times (subject to the availability of the underlying networks).

4.10.3 Optional features

a.   The DPMA intends to explore the future deployment of the Certificate Validation Status Protocol, or its successor, as an additional on-line service for the DPKI.

4.11   End of subscription

a.   Once a subscription has ended, the supporting certificate may be revoked in accordance with the procedures at Section 4.9. Where the provisions stated in 4.9.1c apply, then revocation may not be required.

b.   All smartcards and other tokens shall be retrieved and zeroized and either recycled or destroyed in accordance with the appropriate local SyOps.

c.   Where the subscription of a CA server has ended then all valid certificates associated with the CA server shall be revoked. This action shall only be taken at the express direction of the DPMA.

4.12   Key escrow and recovery

a.   Under no circumstances is a private key that is used for a signing service to be placed into a Key Recovery System. To this end it is forbidden under this policy to issue a certificate to support a key-pair that is intended for use in both signing and encryption operations without

the explicit approval of the DPMA. The DPMA has approved the issuance of certificates that support both signing and encryption to TLS/SSL servers, where this is deemed necessary.

4.12.1 Key escrow and recovery policy and practices

a. When a key-pair is generated with the exclusive purpose of supporting the encryption of data, or key material or to support key agreement, then the private key shall be copied to an approved Key Recovery System. This is a critical requirement for business continuity/disaster recovery purposes: a technical issue that prevents such a Key Recovery System from being operated shall be reported to the DPMA.

b. The DPMA shall publish a Key Recovery Policy (KRP) that shall stipulate the policies of the DPKI relating to the storage and recovery of private keys that have been stored within a Key Recovery System in accordance with 4.12.1.a. The KRP shall be compliant with this DCP, where any policies stated in the KRP conflict with those stated in this DCP, then this DCP shall be overarching.

c. The DCMA shall publish a Key Recovery Practice Statement (KRPS) that shall describe the KRP-compliant practices and related processes of the DCMA in its implementation of a Key Recovery System. The KRPS shall be subject to an audit to ensure that the practices it describes are compliant with the policies stated in the KRP.

4.12.2 Session key encapsulation and recovery policy and practices

a. The DPKI does not support the recovery of session keys, except indirectly as a result of the recovery of an encryption private key, as described in 4.12.1. There is no requirement to prepare, encapsulate or store session keys to support their direct recovery by any means. When products are used, or intended to be used, that provide mechanisms to facilitate the recovery of session keys then the approval of the DPMA shall be sought prior to such a product being used in conjunction with the DPKI.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

a. The policies described in this section are abstracted from JSP 440 Issue 3.6. However, JSP 440 will continue to evolve as threats change. Policies in the latest version of JSP 440 will always take precedence if they are found to be different from those in this document.

5.1 Physical controls

a. Physical security requirements for the DPKI technical infrastructure shall be implemented in accordance with JSP 440 Part 7.

5.1.1 Site location and construction

a. Any building intended to house a DPKI Root CA server, or its backup, shall satisfy the requirements for a MOD Class 4 building. Within such a building, the equipment shall be located within a Strong Room that is protected by a Class 4 lock.

b. Any building intended to house a DPKI CA server shall satisfy at least the requirements for a MOD Class 3 building that has an approved Intruder Detection System (IDS). Within such a building, the equipment shall be located within a Secure Room that is protected by a Class 3 lock.

c. Any building intended to house a VA server shall satisfy at least the requirements for a MOD Class 3 building that has an approved Intruder Detection System (IDS). Within such a building, the equipment shall be located within a Secure Room that is protected by a Class 3 lock.

d. DPKI registration terminals and similar equipment shall be located within a Class 2 building or better, located within a Locked Room equipped with a Class 1 lock or better.

5.1.2 Physical access

a.   DPKI CA server and VA server sites shall implement an access control mechanism to limit and control physical access:

    i.   There shall be a clearly defined perimeter through which all entry and exit is controlled.

    ii.   Access shall be restricted to those persons authorised to access the area.

    iii.   A log of visitors entering and leaving the controlled area shall be maintained.

b.   All sensitive material shall be adequately secured when not in use. For LRA sites and similar locations that are not contained within a Secure Room, all sensitive material shall be stored in an approved Class 3 security container. Security accreditation documentation should identify the arrangements for securing sensitive material, such material includes:

    i.   Hardware Security Modules (HSMs), other cryptographic hardware and tokens.

    ii.   Tokens containing operator private keys.

    iii.   System software and backups.

5.1.3 Power and air conditioning

a.   Adequate power, backup power and air conditioning to operate equipment within agreed SLAs should be provided at each location.

5.1.4 Water exposures

a.   Adequate protection to protect against water exposure shall be provided.

5.1.5 Fire prevention and protection

a.   All DPKI technical infrastructure shall be located in areas protected by a fire detection system. CA servers should be protected by a fire suppression system.

5.1.6 Media storage

a.   All storage media used by the DPKI technical infrastructure shall be protected from physical access by unauthorised entities and environmental threats such as temperature, humidity and magnetism.

b.   Media that contains accounting, archival or backup information shall be stored in a location separate to a CA server.

5.1.7 Waste disposal

a.   All media used for the storage of information such as keys, activation data, accounting data or CA server files shall be handled in accordance with the procedures given in JSP 440 Part 8 and as agreed with the system accreditor.

5.1.8 Off-site backup

a.   To safeguard business continuity it is essential that full system backups are performed at regular intervals, to be defined in the appropriate CPS. An off-site backup permitting recovery to an acceptable level shall be made at regular intervals. The storage and handling of off-site backups shall be of the same quality as that for the main site.

5.2 Procedural controls

5.2.1 Trusted roles

a.   A trusted role is one whose incumbent performs a specific function that is important for the security or continued operation of the system. The functions performed are an important

source of trust in the PKI, and as such these roles shall be performed by a trustworthy person with appropriate security clearance.

b. Certain tasks performed by trusted roles require a higher degree of assurance – these are designated 'Sensitive Tasks'. Such tasks shall be split across multiple people so that malicious or inappropriate activity requires collusion.

5.2.1.1   CA server trusted roles

a. The DCMA shall ensure a separation of duties for critical CA server functions to prevent one person from maliciously using the CA server system without detection. Each user's system access is to be limited to those actions for which he or she is required to perform in fulfilling his or her responsibilities. The DCMA shall assign distinct PKI roles, distinguishing between day-to-day operation of the CA server, the management and audit of those operations and the management of substantial changes to requirements on the system including its policies, procedures or personnel.

b. The division of responsibilities between the roles, and the identification of Sensitive Tasks, shall be defined in the appropriate CPS.

c. Only those personnel assigned trusted roles shall have access to the functions that control the CA server operation.

5.2.1.2   RA/LRA trusted roles

a. Much of the integrity of the PKI is dependant on the correct performance of the registration function, in particular the binding of identification and key. The RA shall ensure that RA/LRA personnel are fully aware of their responsibilities in this matter. To assist in the correct functioning of the registration process the RA/LRA shall publish in its CPS precise instructions for the registration process.

b. RA operators are in possession of the credentials to authorise the issue of a certificate and should be fully aware not only of the security implications of this duty, but also the potential financial liability that may be incurred.

c. The RA/LRA should identify, in its CPS, the trusted roles that are required and define Sensitive Tasks that may be undertaken. Under no circumstances is it permitted for the operator and audit function to be performed by the same person.

5.2.1.3   Key Recovery Service trusted roles

a. The DPMA shall describe in its Key Recovery Policy (KRP) the nature and scope of trusted roles associated with key recovery and management. The roles identified in the KRP should require similar processes to those defined for CA server trusted roles.

5.2.1.4   Other trusted roles

a. The Sponsor of a device or a Subscriber external to the MOD is responsible to the DCMA for providing valid information to the registration process, and where applicable ensuring that the Subscriber is aware of their responsibilities.

5.2.1.5   VA server trusted roles

a. The operator of a VA server is responsible for ensuring the correct and secure operation of the device and for ensuring that only authorised and correctly authenticated data is made available via the VA server.

5.2.2 Number of persons required per task

a. In general, when a higher level of assurance is required, an N of M mechanism shall be used for sensitive tasks conducted by CA and VA servers:

    i. Key generation for CA and VA servers

    ii.   Activation of CA and VA server signing keys

    iii.   Backup of CA and VA server keys

    iv.   Signing of CA server certificates

    v.   Signing of OCSP signing certificates employed by VA servers

b.   Sensitive Tasks shall be identified in the appropriate CPS. Minimum stipulations for critical operational roles are given below for CA server and RA/LRA functions. See also section 6.2.2 for further stipulations regarding private key management.

c.   Minimum number of persons required for CA and VA server Sensitive Tasks:

CA server	VA server	DRCA
2		3

d.   Minimum number of persons required for RA/LRA Sensitive Tasks:

MAL	HAL
Single person	2

5.2.3 Identification and authentication for each role

a.   At a minimum, users shall identify themselves within a particular role using a role specific username and password. This mechanism should be capable of identifying the person assuming the role – this information shall be retained within the accounting log. It is a fundamental requirement of the audit system that any actions performed by a trusted role shall be identified against an individual.

b.   Where possible, it is recommended that use of a digital signature be made to authenticate actions performed by a role and that authenticated logon using a smartcard and a public key operation be used. The private key associated with these actions should be stored on a smartcard or other approved hardware token. The token shall be carefully controlled and protectively marked at a level that is agreed with the system accreditor.

c.   The mechanisms to be used shall be fully documented in the appropriate CPS.

5.2.4 Roles requiring separation of duties

a.   In addition to the stipulations given in this section, it is emphasised that it is forbidden for any person responsible for an operational role to also undertake an audit role on the same system.

b.   A person undertaking a RA/LRA trusted role shall not undertake a trusted role for a CA or VA server.

5.3 Personnel controls

a.   JSP 440 Part 6 defines the overarching policy for personnel security controls.

b.   All personnel responsible for operation of the DPKI shall sign an appropriate SyOPs.

5.3.1 Qualifications, experience, and clearance requirements

a.   Personnel engaged in the operation of the DPKI shall be suitably qualified and trained. The DCMA is to identify specific requirements, as appropriate.

b.   In general, it is expected that all personnel engaged on the operation of the DPKI will be cleared to SC level (iaw JSP 440 Part 6 section 2).

5.3.2 Background check procedures

a. See JSP 440 Part 6.

5.3.3 Training requirements

a. The DCMA shall ensure that all personnel performing operational or audit duties within the DPKI receive comprehensive training, to include:

   i. DPKI security principles and mechanisms.

   ii. Software operation and usage.

   iii. DPKI duties and responsibilities for the role.

   iv. Disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

a. DPKI personnel should be retrained, as required, when changes to the infrastructure or policies occur. This requirement may be waived at the discretion of the DCMA. Refresher training may be required at intervals.

5.3.5 Job rotation frequency and sequence

a. The DCMA shall ensure that changes in staffing have no impact on the operational effectiveness or security of the DPKI.

5.3.6 Sanctions for unauthorised actions

a. If an unauthorised action takes place then appropriate action shall be taken by the DCMA to ensure disciplinary or other actions are taken. In cases where an unauthorised action brings into question the security of the system or its processes then the procedures given in JSP 440 should be followed.

5.3.7 Independent contractor requirements

a. Policies in this section apply equally to MOD personnel and contractors. See JSP 440 for additional guidance on the difference between List X and non-List X company contractors.

5.3.8 Documentation supplied to personnel

a. Personnel engaged on duties within the DPKI need to have access to all relevant policies, practice statements and other operational instructions and guides as appropriate. Where documentation is protectively marked it shall be treated in accordance with standard procedures laid down in JSP 440.

5.4 Accounting log procedures

a. The terminology used in this DCP is derived from that defined in CESG Infosec Memorandum 22: *Protective Monitoring*. In summary, the collection of raw data concerning the operation of the DPKI is 'accounting', it is stored in an 'accounting log'. Subsequently the accounting log may be used during the process of 'audit'. Reports and other data relating to an audit are stored in an 'audit log'. Where the term 'accounting log' is used in the singular, the plural may be inferred.

b. Accounting logs shall be generated for all events relating to the security of the DPKI. Where possible, accounting logs shall be automatically collected; where this is not possible a logbook, paper form or other suitable mechanism shall be employed. All accounting logs, both electronic and non-electronic, shall be retained and made available for the audit process. All accounting mechanisms provided by CA/VA/RA systems shall at all times be enabled.

5.4.1 Types of events recorded

a.   As a minimum, the following security events shall be recorded in the accounting log:

Event	CA server	VA server	RA system
Accounting System			
Any changes to accounting parameters, e.g. types of event logged	X	X	X
Any attempt to delete or modify accounting logs	X	X	X
Obtaining a third-party time stamp	X	X	X
Identity Proofing			
Successful and unsuccessful attempts to assume a role	X	X	X
The value of *maximum number of authentication attempts* is changed	X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum number of authentication attempts* during user login	X	X	X
Unlocking an account that has been locked as a result of unsuccessful authentication attempts	X	X	X
Change of the type of an authenticator, e.g. from a password to smartcard	X	X	X
Local Data Entry			
All security-relevant data that is entered in the system	X	X	X
Remote Data Entry			
All security-relevant messages that are received by the system	X	X	X
Data Export and Output			
All successful and unsuccessful requests for sensitive and security-relative information	X	X	X
Key Generation			
Generation of a key (excluding session and on-time use symmetric keys)	X	X	X
Private Key Load and Storage			
The loading of a private key, including activation of an HSM partition containing a private key	X	X	X
All access to Subscriber private keys retained for key recovery purposes	X	N/A	N/A
Trusted Public Key Entry, Deletion and Storage			
All changes to trusted public keys, including additions and deletions	X	X	X
Secret Key Storage			
The manual entry of secret keys used for authentication	X	X	X
Private and Secret Key Export			
The export of private and secret keys (excluding session keys)	X	X	X
Certificate Issuance			
All certificate issuance requests sent and received	X	N/A	X
All certificate issuance requests processed (successful and unsuccessfully)	X	N/A	N/A
Certificate Revocation			
All certificate revocation requests sent and received	X	N/A	X
All certificate revocation requests processed	X	N/A	N/A
Configuration			
Any security-relevant changes to the configuration of the device, e.g. patches, configuration settings	X	X	X
Account Administration			
Roles and users added or deleted	X	X	X
Access control privileges of an account or role are changed	X	X	X
Certificate Profile Management			
All changes to the certificate profiles	X	N/A	N/A
Validation Authority Management			
All changes to VA server profile or configuration, including changes to certificate profile	X	X	N/A
Certificate Revocation List Profile Management			
All changes to the certificate revocation list profile	X	N/A	N/A

Event	CA server	VA server	RA system
Miscellaneous			
Appointment of an individual to a trusted role	X	X	X
Designation of personnel for multi-person control	X	X	X
Installation of the operating system	X	X	X
Installation of the PKI application	X	X	X
Installation of hardware cryptographic modules	X	X	X
Removal of hardware cryptographic modules	X	X	X
Destruction of cryptographic modules	X	X	X
System startup	X	X	X
Logon attempts to PKI application	X	X	X
Receipt of hardware/software	X	X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Backup of the internal CA database	X	N/A	N/A
Restoration from backup of the internal CA database	X	N/A	N/A
File manipulation (e.g. creation, renaming, modification)	X	N/A	N/A
Posting of any material to a PKI repository	X	N/A	N/A
Access to the internal CA database	X	X	N/A
All certificate compromise notification requests	X	N/A	X
Loading tokens with certificates	X	N/A	X
Shipment of tokens	X	N/A	X
Zeroizing of tokens	X	N/A	X
Re-key of the component	X	X	X
Configuration Changes			
Hardware	X	X	N/A
Software	X	X	X
Operating system	X	X	X
Patches	X	X	X
Security profiles	X	X	X
Physical Access/Site Security			
Personnel access to room holding component	X	X	N/A
Access to the component	X	X	N/A
Known or suspected violations of physical security	X	X	X
Anomolies			
Software error conditions	X	X	X
Software integrity check failures	X	X	X
Receipt of improper messages	X	X	X
Misrouted messages	X	X	X
Network attacks (suspected or confirmed)	X	X	X
Equipment failure	X	X	X
Electrical power outages	X	X	N/A
Uninterruptible Power Supply (UPS) failures	X	X	N/A
Obvious and significant network service or access failures	X	X	N/A
Violations of security policy	X	X	X
Violations of CPS	X	X	X
Resetting operating system clock	X	X	X

b.   For each event, the following information shall be recorded:

  i.   Type of event.

  ii.   Date and time of event.

  iii.   Identity of entity causing event and that of those handling it.

  iv.   The success or failure (along with reason for failure) of the event.

5.4.2 Frequency of processing log

a.   For MAL related processes and events the log shall be reviewed at least 6 times per year, with at least 25% of the security accounting data generated since the last review being examined.

b.   For HAL related processes and events the log shall be reviewed at least 12 times per year, with at least 33% of the security accounting data generated since the last review being examined.

c.   The periodic reviews described above shall be focused on identifying security-related events. A log of the audit results shall be generated and made available to the DCMA.

5.4.3 Retention period for accounting log

a.   The information generated on DCMA equipment shall be retained on that equipment until the information is archived. Deletion of the accounting log following archive should be supervised by a security or audit officer whose role is not a DPKI operational role. Accounting log data shall be available for at least two months or until reviewed, then may be archived in accordance with the procedures in 5.4.5.

5.4.4 Protection of accounting log

a.   Accounting logs shall be immutable-append-only[18] for any person or system process except as noted below. Where accounting logs are maintained manually (e.g., site access logs) then these should be operated in a manner that is tamper-evident.

b.   The DCMA shall define in its CPSs a mechanism to ensure that only specifically authorised personnel may archive or delete accounting logs. The deletion of an accounting log (following archival, or for any other reason) is an event that shall be recorded in the accounting log.

c.   All accounting logs that are archived shall be digitally signed to protect their integrity and identify the archiver; for manual logs an equivalent mechanism should be adopted.

d.   Archived accounting logs shall be stored in a location separate to the source of the accounting data. Storage within the same site is permitted, provided that the storage location is physically separate to the operational system (e.g., a different room or building).

e.   Accounting logs should attract the same protective marking as their source system and shall be handled accordingly.

5.4.5 Accounting log backup procedures

a.   Accounting logs shall be archived and should be removed to an offsite location (see 5.4.4.d) at an interval not to exceed 2 months. Where accounting logs are included in system backups the process of recovering from a backup should be designed to avoid loss of later accounting data where possible.

5.4.6 Audit collection system (internal vs. external)

a.   The accounting log collection procedure may or may not be external to the CA, VA or RA systems. Accounting process shall commence at system startup and cease only at system shutdown. Should it become apparent that an automated accounting system has failed, then all operations shall be suspended until the problem is remedied.

5.4.7 Notification to event-causing subject

a.   There is no requirement for the subject of an event to be notified.

---

[18] I.e. it can be added to, but not changed or deleted.

5.4.8 Vulnerability assessments

a. CPSs and other security documentation shall reflect the assessment of vulnerability for any site or system, as agreed with the system security accreditor. Further guidance is given in JSP 440.

5.5 Records archival

5.5.1 Types of records archived

a. CA, VA and RA archive records shall be sufficiently detailed to establish the proper operation of the appropriate system, or the validity of any certificate (including those revoked or expired) issued by the CA.

Data to be Archived	CA	VA	RA
Certification Practice Statement	X	X	X
Contractual obligations	X	X	X
System and equipment configuration	X	X	X
Certificate requests	X	-	X
Revocation requests	X	-	X
Subscriber identity authentication data (Section 3.2.3)	X	-	X
Documentation of acceptance and receipt of certificates	X	-	X
Documentation of receipt of tokens	X	-	X
All certificates issued or published	X	-	-
Record of re-key	X	X	X
All ARLs and CRLs issued and/or published	X	-	-
All audit logs	X	X	X
Other data or applications to verify archive contents	X	X	X
Documentation required by compliance auditors	X	X	X
Accreditation documents and certificates	X	X	X

5.5.2 Retention period for archive

a. The retention period for archived material shall be no longer than 25 years. The actual period for retention shall be determined by the DPMA in accordance with JSP 441.

5.5.3 Protection of archive

a. Archives should be managed in accordance with JSP 440 Part 8 and JSP 441.

5.5.4 Archive backup procedures

a. Archives should be managed in accordance with JSP 440 Part 8 and JSP 441.

5.5.5 Requirements for time-stamping of records

a. Wherever practical, a trusted source of system time should be used. See Section 6.8.

5.5.6 Archive collection system (internal or external)

a. No stipulation.

5.5.7 Procedures to obtain and verify archive information

a. CPSs should identify the mechanisms for obtaining archived information.

b. Whenever practicable, a digital signature shall be used to affirm the integrity and authenticity of archival records.

5.6 Key changeover

a. No stipulations.

5.7 Compromise and disaster recovery

a. General guidance on business continuity planning is contained in JSP 503. JSP 440 contains specific guidance on disaster recovery for CIS as well as incident handling and reporting procedures.

5.7.1 Incident and compromise handling procedures

a. Each CPS shall specify the incident handling processes for the appropriate component. These should be compliant with JSP 440 Part 8 and JSP 541.

b. If an actual or suspected compromise of the private key assigned to a CA server or RA server occurs, this is to be reported immediately to the JSyCC via the WARP process defined in JSP 541. Incident handling processes shall identify immediate response actions for compromise of CA server and RA server keys.

c. The DPMA shall notify the PMAs of external PKIs that have a trust relationship with the DPKI if a CA server or RA server key is compromised.

5.7.2 Computing resources, software, and/or data are corrupted

a. The CMS shall maintain a complete backup of CMS technical components to permit reconstruction of any component or system following data corruption through accidental or malicious means.

5.7.3 Entity private key compromise procedures

a. In the event of a compromise of the DPKI Root CA key the certificate supporting the compromised key shall be removed from all systems, a new key generated and distributed to all DPKI components, Subscribers and Relying Parties. Such an action will automatically remove trust from all certificates in the DPKI and the disaster recovery plan should identify priorities for recreation of all trust links within the DPKI and re-key of all certificates.

b. In the event of the compromise of a CA server key the superior CA shall immediately revoke the appropriate certificate and publish this fact through the most expeditious route. Disaster recovery plans should identify the priorities for recreation of trust links and re-key of all effected certificates.

c. In the event of the compromise of a RA server key the issuing CA shall immediately revoke the appropriate certificate and publish this fact through the most expeditious route. Disaster recovery plans should identify a process to determine certificates that may be at risk.

d. In the event of the compromise of a Subscriber key the associated certificate should be revoked by the issuing CA server as soon as possible. If required the revoked certificate should be re-issued using the procedures described in Section 4.

5.7.4 Business continuity capabilities after a disaster

a. The DCMA is responsible for disaster recovery and business continuity planning. Disaster recovery plans shall be submitted to the DPMA for approval.

b. JSP 503 provides recommended intervals for testing and exercising disaster recovery plans, as well as mechanisms for testing compliance with business continuity measures. The DCMA shall indicate in its planning how these recommendations are to be implemented for the DPKI.

5.8 CA or RA termination

a. The DPMA shall be notified of any intention to terminate the operations of any CA server or RA server. At least 30 days notice should be given of termination, and a full service is to be maintained during this notice period.

b.   At the termination of service all keys, audit logs and other archived material shall be retained. All private keys, and their back-ups, shall be destroyed.

c.   A CA server shall not be permitted to terminate until it can demonstrate that all certificates in issue have either been revoked or replaced with an equivalent certificate issued by an alternative CA server. Wherever possible, all certificates issued by the CA server should be revoked and that fact published on at least 2 consecutive CRLs, prior to cessation of service.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

a. The following table identifies the minimum requirements for key-pair generation for use by entities recognised by this DCP:

Entity	Cryptographic Module Requirements	Hardware/ Software	Entropy Source
Defence Root CA server	CAPS or FIPS 140-2 Level 3	Hardware	Approved
CA server	CAPS or FIPS 140-2 Level 3	Hardware	Approved
RA systems	CAPS or FIPS 140-2 Level 2	Hardware	Approved
VA server	CAPS or FIPS 140-2 Level 2	Hardware	Approved
High Assurance Level Hard	CAPS or FIPS 140-2 Level 2	Hardware	Approved
High Assurance Level Soft	CAPS or FIPS 140-2 Level 1	Software	Approved
Medium Assurance Level Hard	CAPS or FIPS 140-2 Level 2	Hardware	Internal
Medium Assurance Level Soft	FIPS 140-2 Level 1	Software	Internal

b. Entropy sources for cryptographic modules providing key generation shall be approved by the DPMA on a case-by-case basis, when indicated as 'Approved' in the table above.

c. Where a CESG Assisted Products Scheme (CAPS) cryptographic module is required, the DPMA shall determine if a FIPS 140-2 module may be used as an alternative. The table above identifies the FIPS 140-2 modules that may be acceptable as alternatives to CAPS. Details of module selection shall be documented within the appropriate CPS.

6.1.2 Private Key delivery to subscriber

a. CA servers shall always generate their own key-pairs.

b. Where a CA server or RA generates a key-pair on behalf of a Subscriber, then these shall be delivered to the Subscriber by a secure means. Specific requirements for this are given in 6.1.2.1 and 6.1.2.2. The CA server or RA shall maintain a log of all keys generated on behalf of Subscribers, including a record of delivery and acknowledgement of receipt.

6.1.2.1 High Hard and Medium Hard Subscribers

a. The mechanism for delivering pre-keyed smartcards/tokens to the Subscriber shall ensure the correct smartcard/token and associated activation/access codes are delivered to the correct Subscriber. Where a password or PIN must be delivered to activate the device, the delivery mechanism shall ensure that only the generator and Subscriber are aware of the value.

b. The DCMA shall retain a record of the delivery of all smartcards/tokens and their associated activation password/PIN.

6.1.2.2 High Soft and Medium Soft Subscribers

a. The mechanism for delivering key-pairs shall ensure the confidentiality of the key values at all times. Key-pairs shall be delivered using PKCS#12 or PKCS#8 formatted files, which shall be encrypted using an approved symmetric encryption algorithm (see 6.1.5.a). The encryption key (or password used to generate the encryption key) to provide access to a file

containing a private key shall be distributed to the Subscriber securely, not using the same path as that used for the key delivery.

b. The DCMA shall retain a record of the delivery of all keys and their associated encryption key/password.

c. These requirements shall apply to delivery of keys following generation, and to delivery of keys recovered from a Key Recovery Database.

6.1.3   Public key delivery to certificate issuer

a. Public keys shall be delivered to the CMS using a mechanism that binds the verified identity of the Subscriber and the public key being certified. The mechanisms approved for this purpose are Certificate Management Protocol (CMP) certificate request (RFC 2510) and PKCS#10. These mechanisms shall always include proof of possession of the associated private key.

b. Within the DPKI, initial registration (and other subsequent operations for HAL) is always made by an RA/LRA. Certificate requests shall always be authenticated by the RA/LRA to authorise the request (See 4.1.1).

c. Where key-pairs are generated by an entity other than the Subscriber (e.g. RA or CA servers) then the appropriate CMP processes should be used.

6.1.4   CA public key delivery to relying parties

a. Trusted CA certificates for the DRCA, and any directly trusted Intermediate CAs, shall be delivered to Relying Parties by a secure mechanism. Publication of trusted CA certificates via the DII system directory may accomplish this objective for most systems. However, the requirements for devices such as routers and firewalls may differ and a secure out-of-band distribution mechanism should be adopted. The mechanisms used shall be fully described in the appropriate CPS.

b. The DCMA shall arrange that the public key fingerprints of trusted CA servers be published on the Defence Intranet web sites and other locations that may be considered appropriate.

6.1.5   Key sizes

a. The following key sizes should be used. A larger key size may be specified if required, but this is subject to DPMA approval.

	Subscribers	CA servers
MAL	1024 bit RSA	2048 bit RSA
HAL	2048 bit RSA	
Hashing	SHA-1	SHA-1
Symmetric Encryption	3-key (168 bit) Triple DES or AES128	3-key (168 bit) Triple DES or AES128

b. A DRCA shall use a 2048 bit RSA key.

6.1.6   Public key parameters generation and quality checking

a. Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptoalgorithm in which the parameters are used. For RSA this is ANSI X9.31-1998, FIPS 186-2 or FIPS 186-3.

b. In some circumstances it is specified that approved entropy sources shall be used for the key generation process (see 6.1.1).

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

a. For all assurance levels, key usage as asserted in the appropriate certificate shall be for signing or encryption, but not both. The only exception to this policy is for keys associated with the use of a TLS/SSL server that may be used for both signing and encryption, but only for use by the TLS/SSL protocol in conjunction with the TLS/SSL cipher suites defined in JSP 440: Annex B to Part 8, Section 5, Chapter 7.

b. The X.509 *keyUsage* field (and associated *extendedKeyUsage* field) shall fully state the intended purposes of the key, and the DCMA shall not issue certificates that specify both signing and encryption for the same key (except as noted above).

c. Where certificates, intended for the purpose of signing, are issued to a natural person and state their certificate policy as either High Hard Person/Role or Medium Hard Person/Role the non-repudiation bit shall be set in the *keyUsage* field.

d. Where certificates, intended for the purpose of signing, are issued to a natural person and state their certificate policy as either High Soft Person/Role or Medium Soft Person/Role the non-repudiation bit shall be set in the *keyUsage* field if the key pair was generated by the Subscriber. If the key pair was generated by a CA server or RA, then the non-repudiation bit shall not be set.

e. CA server certificates shall set the *cRLSign* and *certSign* bits in the *keyUsage* field.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

a. All hardware cryptographic modules used within the DPKI shall meet minimum standards, identified and approved by the DPMA. The preference is for products accredited via the CESG Assisted Products Scheme (CAPS), but currently products identified as FIPS 140-2 (*Security Requirements for Cryptographic Modules)* evaluated (at various levels) have been approved, pending the availability of CAPS products.

b. All software cryptographic modules used within the DPKI shall meet minimum standards, identified and approved by the DPMA. The preference is for products accredited via the CAPS, but products certified to FIPS 140-2 at Level 1 or higher are permitted in the absence of a suitable CAPS product. All software cryptographic modules shall be approved by the DPMA, in general the requirement is for support within an evaluated operating system at EAL3 (or higher).

c. CA and RA server cryptographic module minimum standards:

RA	CA server	DRCA	OCSP Responder
CAPS or FIPS 140-2 Level 2	CAPS or FIPS 140-2 Level 3	CAPS or FIPS 140-2 Level 3	CAPS or FIPS 140-2 Level 2

d. Subscriber cryptographic module minimum standards:

HAL/MAL Soft	HAL/MAL Hard
CAPS or FIPS 140-2 Level 1	CAPS or FIPS 140-2 Level 2

e. All cryptographic modules shall be operated in such a manner that the private key is never output in plaintext. No private key shall ever appear unencrypted outside of the module.

6.2.2 Private Key (n out of m) multi-person control

a. Section 5.2.2 identifies the number of persons required to provide certain trusted roles. These roles extend to control over the private key used by specific critical infrastructure components. In the circumstances where multi-person (n of m) controls are stipulated, n and m will always be 2 or more, as stipulated in other parts of this document. The actual value of n should be agreed with an accreditor and documented in the appropriate CPS. Access to the private key shall be divided between n authentication components, stored on appropriate approved hardware tokens – there may be multiple copies of the authentication components. Procedures shall require n persons to load the key into the HSM prior to use.

b. Where access to a private key has been divided in the manner described above, the authentication components for each key shall be stored in separate locations to prevent unauthorised combination of the components. In general, for a CA or RA server, storage in separate security containers within the same secure location is acceptable.

c. The names of all persons able to control the operation of the equipment or provide access to private key authentication components shall be recorded and available for audit purposes.

6.2.3 Private Key escrow

a. Under no circumstances is it permitted that a key used for non-repudiation services be held in trust by a third party. For practical purposes, this stipulation applies to all keys intended for signing purposes used by any human Subscriber.

b. To support business continuity requirements it is necessary to provide a key recovery mechanism to support encryption services. Keys intended for either data or key decryption purposes may be held in trust by the CMS. The mechanism for this should be described in the DII CPS and should be fully compliant with requirements stated in JSP 440.

c. Where encryption keys are held in trust, they shall be retained for subsequent recovery operations, see Section 4.1.12.

6.2.4 Private Key backup

a. The general principle adopted within the DPKI is to balance the technical requirements of non-repudiation with those of good business continuity practice. To this end, it is not permitted to make backup copies of Subscriber signing keys that are stored on smartcards or other approved hardware tokens. Signing keys stored under software control may be backed-up, subject to certain limitations. Signing keys used by infrastructure components, such as CA, RA and VA servers shall always be backed-up.

b. HAL/MAL Soft Subscriber signing private keys may be backed up. At all times, such keys shall remain encrypted as required elsewhere in this policy. Activation data shall remain within the sole control of the Subscriber at all times.

c. HAL/MAL Soft Subscriber signing keys may be copied from the protected operating system key store to a suitable transfer medium solely for the purpose of transferring the keys from one computer to another. The key shall be stored on the transfer medium in an encrypted file; only the Subscriber shall have knowledge of the decryption key. The transfer medium should be protectively marked and handled in accordance with the instructions contained in JSP 440.

d. Signing keys stored in devices, such as web servers or routers, will normally be stored under software control. To ensure business continuity these keys should be backed-up; no more than two backups containing the private key shall be retained, and these should be stored at separate locations. Backups of the private key, or system backups containing the private key, shall be protected from unauthorised access.

e. Signing keys used by the DPKI technical infrastructure shall be backed up and protected by a suitable mechanism. Generally, either the private key, or access to the private key, should be split between a number of approved hardware storage devices (e.g. smartcards) – using

the same n of m principles used to provide access control. The individual components should not be stored together, but spread across multiple locations.

6.2.5 Private Key archival

a.   See 6.2.3 and 6.2.4.

6.2.6 Private Key transfer into or from a cryptographic module

a.   For hardware cryptographic modules key generation will take place within the module. Transfer into and out of hardware cryptographic modules, where permitted, should use the same mechanisms defined above for backup. The general principle that must be asserted is that a private key shall never exist outside of a cryptographic module in an un-encrypted state; storage of a key or part of a key within an approved smartcard or other hardware token provides the required level of protection.

b.   Where key-pairs are generated outside of a software cryptographic module and transferred in, this should follow the same principles.

6.2.7 Private Key storage on cryptographic module

a.   All cryptographic modules approved for use within the DPKI provide an adequate level of protection for the storage of the private key.

6.2.8 Method of activating private key

a.   Activation of the private key within a cryptographic module should always be protected by a suitable authentication mechanism. Such mechanisms include:

   i.   Password

   ii.   Personal Identification Number (PIN)

   iii. Biometric

b.   See 6.4.1 for requirements governing the quality of these mechanisms.

c.   Activation data shall be passed to the subscriber through a secure means. Entry of the activation data should be protected from disclosure.

6.2.9 Method of deactivating private key

a.   Cryptographic modules that have been activated shall not be left unattended at any time without deactivation. Deactivation may be achieved using a software command, physical removal from a card reader or similar, or a passive timeout. Hardware cryptographic modules shall always be removed from the system when not in use.

6.2.10 Method of destroying private key

a.   Private keys shall be destroyed when no longer required (including lifetime expiry and revocation). For software cryptographic modules this shall be performed by overwriting the data using an approved wiping mechanism. For hardware cryptographic modules a 'zeroising' mechanism shall be used.

b.   Under certain circumstances physical destruction of smartcards that are no longer required, or have reached the end of their useful life, may be required. JSP 457 vol 6 contains guidance on the lifecycle management of smartcards.

6.2.11 Cryptographic Module Rating

a.   See 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

a. Public keys are archived as part of the certificate archive process.

6.3.2 Certificate operational periods and key pair usage periods

a. In order to promote interoperability between DII systems and MOD systems that may be outside the DII the DPKI policy is that key and certificate lifetimes shall be harmonised. The lifetime of a key pair is the same as that indicated in the certificate that binds the public key. The maximum lifetime of keys and certificates used within the DPKI are:

CA & RA servers	Validation Authority servers	DRCA
10 years	1 year	20 years

HAL/MAL Soft Subscribers	HAL/MAL Hard Subscribers	PKI Roles
1 year	3 Years	1 year

b. Subject to approval by the DPMA, shorter lifetimes may be specified to suit the requirements of an application or service.

6.4 Activation data

6.4.1 Activation data generation and installation

a. Access to private keys within cryptographic modules is protected by activation data. Section 6.2.8 identifies three permitted mechanisms for activation data. Where non-biometric mechanisms are adopted an approved password or PIN generator shall be used.

b. PINs shall be a minimum of 6 digits in length.

c. Passwords shall be random strings, not based on a dictionary word and not personally related to the Subscriber.

d. Support for biometric authentication/activation is under consideration by the DPMA and further guidance on appropriate mechanism and usage will be promulgated via JSP 457 vol 6.

e. Where the activation data is not generated by the Subscriber directly, the activation data shall be notified to the Subscriber using a secure mechanism that guards against disclosure to unauthorised persons. Protective marking of the activation data should be considered by the system owner or security accreditor, in accordance with the requirements given in JSP 440.

f. The Subscriber agreement shall include instructions to the Subscriber on the correct handling and protection of activation data.

6.4.2 Activation data protection

a. Activation data for cryptographic modules shall be treated in the same manner as long-term system access passwords. Instructions for management of this class of data are given in JSP 440 Part 8.

6.4.3 Other aspects of activation data

a.   Where a certificate re-key is performed in conjunction with an existing cryptographic module the activation data shall be changed at the same time.

6.5   Computer security controls

6.5.1 Specific computer security technical requirements

a.   CA, RA and OCSP server equipment shall utilise an approved operating system evaluated to EAL 4 where possible; this should be operated in an evaluated configuration. Server equipment shall be configured so as to remove or deactivate all accounts and services that are not required for the operation of the DPKI service.

6.5.2 Computer security rating

a.   Protective marking and system security status shall be established in accordance with JSP 440 and agreed with the accreditor.

6.6   Life cycle technical controls

6.6.1 System development controls

a.   No stipulation.

6.6.2 Security management controls

a.   CA, RA and OCSP server equipment shall be dedicated to a single task to support the DPKI. Formal configuration management controls shall be implemented throughout the life of the equipment.

b.   All equipment used within the DPKI shall be routinely swept for viruses and other malware in accordance with the guidance in JSP 440 Part 8.

6.6.3 Life cycle security controls

a.   All equipment used within the DPKI shall be procured, delivered and commissioned in a manner designed to reduce the risk of a compromise of the integrity of the DPKI.

b.   Equipment update or repair shall be conducted in a manner compatible with the above objective.

6.7   Network security controls

a.   CA, RA and VA servers shall be located within MOD networks in a manner that affords sufficient protection, given the risk assessment conducted during the accreditation process. Generally, it is anticipated that adequate screening and access control will be provided using suitable approved firewalls and similar systems.

b.   As most equipment will be connected to general purpose networks, a thorough risk assessment should be conducted to ensure that appropriate additional screening and other controls are provided. CA servers and VA servers shall be hosted on dedicated networks, with interconnection to other networks protected by suitable approved firewall products.

6.8   Time-stamping

a.   The DPKI does not support or provide a Time Stamping Service, as defined in RFC 3161 *Time Stamp Protocol.*

b.   Where time is a part of any operation (e.g. a digital signature) then it shall be derived from an authorised and trusted source. Where this policy requires time to be incorporated in accounting and other records then this implies the use of such a time source.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

a. Full details of certificate profiles are contained in the *Defence PKI Interface Specification* document.

b. The certificate profiles defined in the DPKI Interface Specification are the only ones approved for use with the DPKI. Any variation to the profiles, or a requirement for additional profiles, shall be approved by the DPMA and documented in the appropriate CPS. Such approval has been extended for internal certificates to support infrastructure services, as specified in the DPKI Interface Specification.

7.1.1 Version number(s)

a. The DPKI only uses X.509 version 3 public key certificates. This policy does not currently support the use of X.509 attribute certificates, although such support may be added in the future by the DPMA.

7.1.2 Certificate extensions

a. The rules for inclusion, assignment of values and criticality of extensions are defined in the profiles. Any variation to these shall be approved by the DPMA.

b. It is permitted to include additional attributes, such as access control information, within the *subjectDirectoryAttributes* extension of a certificate. Any usage of this field shall be documented in the appropriate CPS.

7.1.3 Algorithm object identifiers

a. Certificates under this policy will use the following OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption*	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
*This algorithm may only be used with prior approval of the DPMA. Examples of usage are documented in the DPKI Interface Specification.	

b. Certificates under this policy will use the following OIDs for identifying the algorithm for which the subject key was generated:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

c. The DPKI shall only certify public keys associated with the cryptographic algorithms identified above, and shall only use the signature algorithms identified above to sign certificates, CRLs and any other DPKI product.

7.1.4 Name forms

a. All certificates used within the DPKI shall include a Subject name, containing a Distinguished Name (DN) conformant with X.501. The approved formats for this are defined in the DPKI Interface Specification.

b. Some applications may require alternative name forms (e.g., email addresses). These may be placed in the *subjectAltName* extension field and permitted formats are defined in the DPKI Interface Specification.

7.1.5 Name constraints

a. All subordinate CA server certificates shall impose name constraints as defined by the DCMA and approved by the DPMA. CA servers may enforce path length constraints, as determined by the DPMA.

b. Where cross-certificates are used to support external interoperability name constraints shall be included in each cross-certificate. The DPKI Interface Specification defines which name constraints should be used.

7.1.6 Certificate policy object identifier

a. Certificates issued under this policy should assert a policy OID appropriate to the level of assurance, key storage mechanism and the entity type:

Policy	Assigned OID
Medium Soft Person	1.2.826.0.1310.100.3.1.0
Medium Soft Role	1.2.826.0.1310.100.3.1.1
Medium Soft Device	1.2.826.0.1310.100.3.1.2
Medium Soft Admin	1.2.826.0.1310.100.3.1.3
Medium Hard Person	1.2.826.0.1310.100.3.1.10
Medium Hard Role	1.2.826.0.1310.100.3.1.11
Medium Hard Device	1.2.826.0.1310.100.3.1.12
Medium Hard Admin	1.2.826.0.1310.100.3.1.13
ACP145	1.2.826.0.1310.100.3.1.20
High Soft Person	1.2.826.0.1310.100.3.2.0
High Soft Role	1.2.826.0.1310.100.3.2.1
High Soft Device	1.2.826.0.1310.100.3.2.2
High Soft Admin	1.2.826.0.1310.100.3.2.3
High Hard Person	1.2.826.0.1310.100.3.2.10
High Hard Role	1.2.826.0.1310.100.3.2.11
High Hard Device	1.2.826.0.1310.100.3.2.12
High Hard Admin	1.2.826.0.1310.100.3.2.13

b. MAL end entity certificates should normally assert a single policy OID; where a HAL policy is asserted, the corresponding MAL policy should also be asserted to support interoperability.

c. CA servers shall assert all policy OIDs for which they are authoritative (i.e. for which they may issue certificates), as defined by the approved CPS.

d. The requirements of cross-certificates for asserting policy, and for policy mapping, are defined in the DPKI Interface Specification.

7.1.7 Usage of Policy Constraints extension

a. See the DPKI Interface Specification for details of policy constraint usage for CA and cross-certificates.

7.1.8 Policy qualifiers syntax and semantics

a. See the DPKI Interface Specification.

7.1.9 Processing semantics for the critical Certificate Policies Extension

a. This policy requires that the *certificatePolicies* extension be marked critical. Relying Parties should be aware that they may use a certificate in an inappropriate manner if this extension is ignored by none compliant software.

7.2 CRL profile

a. Full details of the CRL profiles are contained in the *Defence PKI Interface Specification* document.

b.   The CRL profiles defined in the DPKI Interface Specification are the only ones approved for use with the DPKI. Any variation to the profiles, or a requirement for additional profiles, shall be approved by the DPMA.

7.2.1 Version number(s)

a.   The DPKI only uses X.509 version 2 certificate revocation lists.

7.2.2 CRL and CRL entry extensions

a.   The rules for inclusion, assignment of values and criticality of extensions are defined in the profiles. Any variation to these shall be approved by the DPMA.

7.3   OCSP profile

7.3.1 Version number(s)

a.   The DPKI uses OCSP version 1 as defined in RFC 2560.

7.3.2 OCSP extensions

a.   Appropriate extensions from RFC 2560 may be used in OCSP requests and responses, as detailed in the DPKI Interface Specification.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

a. The frequency and extent of audits are to be determined by the DPMA on a case-by-case basis. The DPMA shall have the free and unrestricted right to audit and inspect the premises, staff, documents and data of any component of the DPKI for the purposes of evaluating that component's compliance with the terms of this Defence Certificate Policy.

b. The DPMA, at its discretion, may request any part of the DCMA to have an audit by an agency external to the department at any time.

c. The DCMA shall, on an annual basis, either (i) certify to the DPMA that it has at all times during the period in question complied with the requirements of this policy, or (ii) provide to the DPMA details of any periods of non-compliance and explain the reasons why the DCMA has not complied with the DCP.

8.2 Identity/qualifications of assessor

a. The auditor/assessor shall have such qualifications that accord with best commercial practice or as required by law.

b. In addition, any person or entity, either internal or external to MOD, undertaking a compliance inspection shall possess significant experience with PKI and cryptographic technologies as well as the operation of relevant DPKI software.

c. The DPMA is responsible for ensuring that an appropriate person or organisation performs the compliance audit or inspection.

8.3 Assessor's relationship to assessed entity

a. Aside from the audit function, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest. Should at any time in the future a potential conflict of interest arise, then this matter shall be reported to the DPMA for advice/action.

8.4 Topics covered by assessment

a. The audit should assess that:

   i. The CPS in use by the DPKI component describes, in sufficient detail, the technical, procedural and personnel policies and practices of the component and that such practices meet the requirements of this Defence Certificate Policy.

   ii. The DPKI component implements and complies with the technical, procedural and personnel practices and policies described in the CPS.

b. The topics covered by a compliance and/or conformance audit should include:

   i. Physical security

   ii. Documentation and process

   iii. Vetting of operational personnel

   iv. Technical security measures

   v. Privacy, including compliance with Data Protection laws

c. The DCMA, and if appropriate the DPKI component, shall be given advance notice (of not less than 10 working days) of the aspects of the DPKI that will be audited for any given inspection.

d. The DCMA shall co-operate with the auditor and shall afford the auditor all reasonable assistance and access to premises, staff, documentation and data. The DCMA shall provide

a full text version of the appropriate CPS, when necessary, for the purposes of any audit, inspection, accreditation, or cross-certification.

8.5   Actions taken as a result of deficiency

a.   If irregularities are found by the audit, the DPMA and DCMA shall be informed in writing immediately. The DCMA shall submit a report to the auditor or directly to the DPMA, as determined by the DPMA, as to any remedial action the DCMA will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor, or by the DPMA as appropriate. The DPMA shall be kept informed by the DCMA at all times.

b.   Remedial action may include suspension or revocation of CA or RA/LRA certificates, as defined in Section 4.9.

c.   Where a DPKI component fails to take appropriate action in response to the identified deficiencies, the DPMA shall be informed and shall take the appropriate action, according to the severity of the deficiencies which shall include:

    i.   Noting the deficiencies but allowing the DPKI component to continue operations until the next planned, or newly scheduled, inspection

    ii.   Allow the DPKI component to continue operations for a maximum of thirty days pending correction of any problems prior to revocation

    iii.   Revoking the DPKI component's certificate

d.   The inspection results for external PKI systems shall be submitted to the DPMA. Where the PMA of a cross-certified PKI fails to take appropriate action to correct irregularities, the DPMA may revoke the external PKI's cross-certificate with the DPKI Defence Root CA.

8.6   Communication of results

a.   Audit results are to be treated as confidential information. Unless otherwise specified in an applicable contract, they shall be treated in accordance with Section 9.3.

b.   External PKIs cross-certified with the DPKI Defence Root CA shall provide the DPMA with a copy of the results of the compliance inspection. The DPMA shall provide the DPKI compliance audit results to the PMA of cross-certified PKIs if required by the cross-certification agreement. These results shall remain confidential.

c.   The method and detail of notification of inspection results to PKIs cross-certified with the DPKI shall be defined within the cross-certification agreement between the two parties.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

a. The charging of fees is subject to appropriate legislative authority and policy.

b. The DPKI Authorities will ensure that any applicable fees and charging structures relating to the DPKI will be published.

c. Notice of any fee to be charged to a Subscriber shall be brought to the attention of that Subscriber before the validity period of the certificate comes into effect. Notice of any fee to be charged to a Relying Party shall be brought to the attention of that Relying Party before the Relying Party relies on the certificate.

9.2 Financial Responsibility

a. No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope

a. Business information used in connection with this DCP may be confidential and any such confidential information shall be kept confidential[19].

b. The treatment of protectively marked business information is subject to the requirements of the MoD Security Policies.

c. The following information shall be regarded as confidential:

   i. All applications made by potential Subscribers to the DCMA (whether successful or otherwise).

   ii. Personal information supplied during registration.

   iii. All records of DCMA activities and events.

   iv. Private keys.

   v. Transactional records.

   vi. Records relating to the management of certificates.

   vii. Audit trail records, reports and data.

   viii. Contingency planning, disaster recovery plans and security measures.

d. The following information shall not be regarded as confidential, and shall not therefore contain any confidential information:

   i. Certificates;

   ii. CRLs.

9.3.2 Duty to protect Confidential Information

a. All participants shall have a duty to protect all confidential information in their possession, custody or control. Confidential information shall not be used or disclosed without the consent of the owner, except where required by law.[20]

b. Any request for the disclosure of information shall be made in writing, signed and delivered to the DCMA. The disclosure of information will be subject to the requirements of the MoD Security Policies; JSP 440, Part 9 provides guidance on the procedures to be adopted.

---

[19] i.e. information which is subject to obligations of confidentiality. This should not be confused with protectively marked information, which is to be dealt with as provided in paragraph b of Section 9.3.1.
[20] JSP 440 provides guidance.

c.   Audit information shall be protectively marked and, save as provided by law, shall not be disclosed to anyone for any purpose except to the duly authorised Audit Authority for audit purposes and the appropriate MoD Security Authority.

d.   Save as provided by law, information relating to the DCMA's management of a Subscriber's certificate may only be disclosed to the Subscriber, the duly authorised Audit Authority for audit purposes or the relevant MoD Security Authority.

9.4   Privacy of Personal Information

a.   Personal information used in connection with this DCP shall be dealt with in accordance with the Data Protection Act 1998 and the Human Rights Act 1998.

b.   The DCMA and repositories within the DPKI shall implement and maintain a privacy policy, in accordance with the Data Protection Act 1998, the Human Rights Act 1998 and the Freedom of Information Act 2000.

c.   A certificate will contain such personal information as is relevant and necessary to effect secure transactions using the certificate. Such information may include, the following concerning a Subscriber:

i.   Subscriber name

ii.   Subscriber organisation

iii.   Subscriber e-mail address

iv.   Person Unique Identifier

d.   Certificates, CRLs and repositories shall not contain any further personal information. If it is necessary to include any further personal information in a certificate or repository to enable the DPKI to operate, it will be necessary to obtain the consent of that person to the inclusion or use of any such further personal information. JSP 440, Part 9 provides guidance on the procedures to be adopted.

e.   All participants shall have a duty to protect all personal information in their possession, custody or control. Personal information shall not be used or disclosed without the consent of the owner or as required by law.[21]

9.5   Intellectual Property Rights (IPR)

b.   Subject to any existing rights of third parties and as otherwise provided in this Section 9.5, all Intellectual Property Rights, including any database rights and copyright in all certificates, OIDs, repositories and documents (electronic or otherwise) comprising the DPKI (including but not limited to this DCP) belong to and are and will remain the property of the Crown.

c.   No certificate, OID, repository or document shall be copied, used or dealt with otherwise than as provided for in this DCP.

d.   A certificate applicant retains all rights it has (if any) in any trademark, service mark or trade name contained in any certificate application and Distinguished Name with any certificate issued to the certificate applicant. The applicant warrants that in receiving and processing the applicant's application, and in issuing any certificate or DPKI documentation, the DPKI Authorities, the DCMA and their component parts are not infringing any third party intellectual property rights.

e.   Where the DPKI relies upon any pre-existing third party proprietary information, the Crown will be granted a perpetual irrevocable royalty free licence to use or have used any such information for DPKI purposes.

---

[21] JSP 440 provides guidance.

9.6　Representations and Warranties

a.　In issuing certificates to Subscribers under this DCP the DPKI Authorities will comply with the policies set out in this DCP.

b.　The DPKI Authorities make no representation other than that expressly stated in paragraph a of this Section 9.6 of this DCP and any representations which would otherwise be implied by law, custom, course of dealings or circumstances are hereby excluded.

c.　By using or relying on a certificate issued under this DCP, an End Entity accepts and agrees that it has not relied on any other representation.

9.7　Disclaimer of Warranties

a.　Certificates issued under this DCP will be issued in accordance with the policies set out in this DCP.

b.　The DPKI Authorities make no warranty other than that expressly stated in paragraph a of this Section 9.7 of this DCP and any warranties which would otherwise be implied by law, custom, course of dealings or circumstances are hereby excluded.

c.　By using or relying on a certificate issued under this DCP, an End Entity accepts and agrees that it has not relied on any other warranty.

d.　No representations or warranties except those expressly stated in paragraph a. of each of Sections 9.6 and 9.7 of this DCP shall be incorporated in any agreement made between any of the DPKI Authorities and an End Entity.

9.8　Limitations of Liability

a.　This Section 9.8 limits the liability of the DPKI Authorities to Subscribers and Relying Parties (End Entities). The liability of the DPKI Authorities to each other is governed by agreements between them.

b.　This Section 9 specifies the total liability of the DPKI Authorities for all losses, damages, costs and expenses (including legal costs and expenses) of any kind which are suffered or incurred by any person, however they may be caused, including those caused by negligence on the part of the DPKI Authorities or breach of this DCP. This Section 9 does not exclude any liability which the DPKI Authorities would otherwise have for any personal injury resulting from negligence, whether or not it results in death, or from fraud by the DPKI Authorities.

c.　A DPKI Authority shall have no liability or obligation whatsoever for the acts, omissions or representations of any other DPKI Authority.

d.　The DPKI Authorities shall have no liability whatsoever for any loss, damage, costs or expenses (including legal costs and expenses) which is not the direct result of both (1) the claimant's reliance on a certificate issued by the DCMA under this DCP, and (2) the negligent failure of the DPKI Authorities to follow the policies described in this DCP.

e.　The DPKI Authorities shall have no liability whatsoever for any loss or damage which is indirect, incidental, consequential or special, or for any aggravated, exemplary or punitive damages.

f.　The DPKI Authorities shall have no liability whatsoever for any loss of business, income, profit or anticipated savings, or for any damage to reputation.

g.　The DPKI Authorities shall have no liability whatsoever for any loss, damage, costs or expenses which are not, in the ordinary course of things, the natural consequence of the claimant's reliance on a certificate issued by the DCMA under this DCP and a DPKI Authority's breach of this DCP.

h.　The DPKI Authorities shall have no liability whatsoever in relation to any decision to allow, or not to allow, any body, authority or person to cross-certify with the DRCA.

i.   The DPKI Authorities shall have no liability whatsoever in relation to any decision not to issue a certificate under this DCP to any entity.

j.   The DPKI Authorities shall have no liability whatsoever in relation to the revocation of a certificate issued under this DCP if it is revoked in accordance with this DCP.

k.   The DPKI Authorities shall have no liability whatsoever in relation to either (1) a certificate issued under this DCP, or (2) the associated public/private key pairs, to any entity which has not used them strictly in accordance with this DCP and any agreements pertaining to their use.

l.   The DPKI Authorities shall have no liability whatsoever in relation to any reliance on either (1) a certificate issued under this DCP, or (2) the associated public/private key pairs, if at the time these are relied on the certificate has expired.

m.   The DPKI Authorities shall have no liability whatsoever in relation to any reliance on either (1) a certificate issued under this DCP, or (2) the associated public/private key pairs, if at the time these are relied on the certificate is identified in the latest revocation information.

n.   The DPKI Authorities shall have no liability whatsoever in relation to any reliance on either (1) a certificate issued under this DCP, or (2) the associated public/private key pairs, if at the time these are relied on the DCMA should have published the revocation of the certificate in accordance with this DCP, but has not done so due to reasons beyond its reasonable control (including the failure of any person to provide any relevant information in accordance with this DCP).

o.   The DPKI Authorities shall have no liability whatsoever in relation to any person's reliance on either (1) a certificate issued under this DCP, or (2) the associated public/private key pairs, unless that person has complied fully with this DCP and the Relying Party Agreement.

p.   The DPKI Authorities shall have no liability whatsoever in relation to any person's reliance on either (1) a certificate issued under this DCP, or (2) the associated public/private key pairs, unless the Subject of that certificate and the Subscriber have both complied fully with this DCP and the Subscriber Agreement.

q.   The DPKI Authorities shall have no liability whatsoever for any loss, damage, costs or expenses (including legal costs and expenses) which would not have arisen if the Relying Party had done what a reasonable person would have done in the circumstances.

r.   The DPKI Authorities shall have no liability whatsoever for any loss, damage, costs or expenses (including legal costs and expenses) resulting from the reliance of a Relying Party of a body which has cross-certified with the DRCA upon a certificate issued under this DCP or upon the associated public/private key pairs.

s.   The total aggregate liability of the DPKI Authorities in connection with a transaction in which either (1) a certificate issued under this DCP, or (2) the associated public/private key pairs, have been relied on, is limited to £1,000. If two or more DPKI Authorities would otherwise be liable for more than this amount, either individually or collectively, they are only liable to pay this amount between them. For these purposes, a series of connected transactions is deemed to be a single transaction.

t.   The total aggregate liability of the DPKI Authorities to each End Entity in respect of all claims notified by that End Entity during any one calendar year (running from 1st January to 31st December) is limited to £10,000. If two or more DPKI Authorities would otherwise be liable for more than this amount, either individually or collectively, they are only liable to pay this amount between them.

u.   The total aggregate liability of the DPKI Authorities to all claimants in respect of all claims notified during any one calendar year (running from 1st January to 31st December) is limited to £100,000. Their liability for each claim shall be apportioned pro rata according to the value of each claim.

9.9 Indemnities

9.9.1 Subscriber Indemnities

a. External Subscribers shall and Subscriber Agreements shall require external Subscribers to compensate a Relying Party which suffers or incurs loss, damage, liability, costs or expenses as a result of the Subscriber's breach of this DCP or its negligence (including the Subscriber's failure to keep its Private Key private) and to indemnify the DPKI Authorities against all and any loss, damage, liability, costs and expenses of any kind (including legal costs and expenses) suffered or incurred by them in connection with any claim brought against them by a Relying Party.

b. External Subscribers shall, and Subscriber Agreements shall require external Subscribers to, indemnify the DPKI Authorities against any loss, damage, liability, costs and expenses of any kind (including legal costs and expenses) that they incur as a result of or arising from:-

    i. any false, inaccurate or misleading information supplied by the Subscriber or its servants, employees, agents or contractors;

    ii. any failure of the Subscriber to disclose any material fact, or any misrepresentation of any material fact;

    iii. failure by the Subscriber to adequately protect the Subscriber's Private Key, to use a trustworthy system to ensure the protection of the Private Key, or to take adequate precautions to prevent the compromise, loss, disclosure, modification or unauthorised use of the Subscriber's Private Key – each Subscriber should take precautions appropriate to the level of threat facing that Subscriber and should comply with the requirements of this DCP and the guidance provided by the DPMA, as specified in this DCP;

    iv. the Subscriber contravening any applicable laws in the UK and/or the Subscriber's country or territory (if not the UK), including but not limited to those relating to intellectual property rights, use of computer systems, and data protection;

    v. any unauthorised or unlawful use of the Subscriber's Private Key or a certificate by a Subscriber, its servants, agents, employees or contractors;

    vi. any breach of this DCP by a Subscriber, a Subject or a Sponsor.

c. Subscriber Agreements may require an external Subscriber to acknowledge that when the replacement of a Subscriber's Private Keys is required, the Subscriber shall be liable for the cost of replacing such keys and the related certificates.

9.9.2 Relying Party Indemnities

a. External Relying Parties shall and Relying Party Agreements shall require external Relying Parties to indemnify the DPKI Authorities against all and any loss, damage, liability, costs and expenses of any kind (including legal costs and expenses) that they incur as a result of:

    i. the Relying Party's failure to perform the obligations of a Relying Party;

    ii. the Relying Party's reliance on a certificate for a purpose excluded by that certificate or where it is not reasonable to rely upon the certificate in the circumstances, for example, by relying on a certificate with an inappropriate level of assurance for the transaction concerned. Relying Parties shall determine the appropriate level of assurance required for a particular transaction, in accordance with the e-Government Security Framework;

    iii. the Relying Party's failure to check, in an appropriate manner, the status of each certificate to determine if the certificate has expired or been revoked;

    iv. any breach of this DCP by the Relying Party.

9.10 Term and Termination

9.10.1 Term

a. This DCP shall remain effective until the DPKI is terminated or the end of the archive period for the last expired or revoked certificate which asserts this DCP.

9.10.2 Termination

a. This DCP may only be terminated or withdrawn by the DPMA.

9.10.3 Effects of Termination

a. No further certificates may be issued under this DCP.

b. The provisions of Sections 9.3, 9.4, 9.5, 9.8 and 9.9 of this DCP and any related agreements shall survive termination of this DCP.

c. A new Defence PKI X.509 Certificate Policy will only become effective when it has been approved by the DPMA.

9.11 Individual Notices and Communications with Participants

a. No stipulation.

9.12 Amendments

9.12.1 Procedure for amendments

9.12.1.1 Amendments without notification

a. The following amendments may be made by the DPKI Authorities to this DCP without notification to affected parties and without the requirement for a new Object Identifier to be allocated:

    i. spelling/punctuation/grammar;

    ii. formatting;

    iii. correction of minor typographical errors;

    iv. amendments to the annexes.

9.12.1.2 Amendments with notification

a. Amendments to the following aspects of this DCP may be made with notification to affected parties in accordance with Section 9.12.2 but without the requirement for a new Object Identifier to be allocated:

    i. Any aspect that does not lower, and cannot be perceived to lower, the fundamental trust that can be placed in a certificate.

b. Prior to approving any such amendments to this DCP, the DPMA shall notify the DCMA and all CAs that are directly cross-certified with the DRCA.

9.12.1.3 Amendments requiring a new Certificate Policy

a. Amendments to the following aspects of this DCP may not be made, unless a new certificate policy with a new Object Identifier is created:

    i. Amendments which the DPMA determines would cause significant changes to the DCP.

9.12.2 Notification mechanism and period

a.   The DPMA shall publish a notice containing the proposed amendments on the DPMA Web site inviting comments on the proposed amendments and stating the final date for receipt of comments. The DPMA shall notify, in writing, all CAs that are directly cross-certified with the DRCA of any proposed amendments to this DCP, the final date for receipt of comments and the proposed effective date for such amendments.

b.   The comment period shall be 30 days unless otherwise specified. The comment period shall be defined in the notification.

c.   Written and signed comments on the proposed amendments shall be directed to the DPMA. Decisions with respect to the proposed amendments shall be made at the sole discretion of the DPMA.

d.   The DPMA shall determine the period of notification for approved amendments.

9.12.3 Circumstances in which a new OID must be issued

a.   in the circumstances specified in Section 9.12.1.3;

b.   where the DPMA otherwise determines that a new OID is required.

9.13   Dispute resolution provisions

a.   Any dispute arising out of or relating to this DCP shall be resolved using the appropriate dispute resolution procedure in accordance with this DCP.

b.   A dispute related to key and certificate management within the DPKI shall be resolved by the appropriate DPKI Authority in conjunction with the DPMA in accordance with any dispute resolution procedures determined by the DPMA.

c.   Any dispute related to key and certificate management between a DPKI Authority and a third party shall be resolved by negotiation if possible. A dispute not settled by negotiation shall be resolved through a mediator appointed by the DPMA. If the dispute is not resolved by mediation, the dispute shall be referred to arbitration in accordance with the Arbitration Act 1996, the arbitrator being appointed by the DPMA.

d.   Any other dispute in relation to this DCP shall be resolved if possible, by negotiation. A dispute not settled by negotiation shall be resolved through mediation. A dispute not resolved by mediation shall be referred to arbitration in accordance with the Arbitration Act 1996.

e.   No court proceedings shall be issued except in accordance with the Arbitration Act 1996.

f.   The DPKI Authorities shall ensure that any agreements entered into by them which incorporate the provisions of this DCP, including any cross-certification agreements, contain similar dispute resolution procedures.

9.14   Governing Law

a.   The construction, interpretation and validity of this DCP shall be governed by English Law. The DPKI Authorities shall ensure that any agreements entered into by them which incorporate the provisions of this DCP shall also be governed by English Law.

9.15   Compliance with Applicable Law

a.   All participants shall comply with all laws applicable to this DCP and to any agreements entered into by them which incorporate the provisions of this DCP.

9.16 Miscellaneous Provisions

9.16.1 Severability

a.   In the event that any part of this DCP is found to be invalid that part will be applied to the maximum extent possible so as to give effect to its intention and the remaining provisions will continue to be fully effective.

9.16.2 No Agency or Fiduciary Relationship

a.   In issuing any certificate under this DCP the DPKI Authorities will not become a representative of a Subscriber or a Relying Party (whether as an agent, fiduciary, trustee or in any other way whatsoever).

b.   In issuing any certificate under this DCP a Registration Authority (RA) will not become an agent of any other CA (whether as an agent, fiduciary, trustee or in any other way whatsoever).

9.16.3 No Third Party Rights

a.   Notwithstanding the Contract (Rights of Third Parties) Act 1999, this DCP does not confer on any person any right to enforce any term of this DCP, and the parties to any agreement which incorporates this DCP shall be entitled to exercise their rights (if any) to rescind, terminate or vary that agreement without reference to, or the consent of, any third party.

UK UNCLASSIFIED

ANNEXE A: DEFINITION OF TERMS

Access	Ability to make use of any information system (IS) resource.
Access control	Process of granting access to information system resources only to authorised users, programs, processes, or other systems.
Accreditation	Formal declaration by an authority that a system is approved to operate in a particular security Mode using a prescribed set of safeguards at an acceptable level of risk.
Accounting	The process of collecting and recording information about events.
Accounting Log	The repository for *accounting* information.
Applicant	The Subscriber is termed an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Approved	The default approval authority for anything related to the DPKI is the DPMA; other approval authorities are identified by name in DPKI documentation.
Archive	Long-term, physically separate storage.
ARL	Authority Revocation List – a file containing the serial numbers, and revocation date, of revoked CA certificates. (See *CRL*).
Asymmetric encryption	A cryptographic technique such that an object that has been encrypted using one key of a *key-pair* may only be decrypted with the other key of the *key-pair*.
Attribute Authority	An entity recognised by the DCMA as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit log	The repository for records produced as a result of an audit process.
Authentication	Verification of the identity claimed by an *entity*.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information. For an X.509 certificate the binding is between *subject* and *public key*.
Biometric	A physical or behavioural characteristic of a person.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

CA server	The equipment used in the process of issuing and revoking certificates. Part of the CA facility.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. It may also contain additional information that defines or constrains its usage.
Certificate chain	A series of *certificates* that are linked together such that the *subject* of *certificate* <u>n</u> is the *issuer* of the *certificate* <u>n+1</u>.
Certificate modification	The process of replacing an existing *certificate*, retaining the existing *public key*, subject and key usage but changing minor details within the certificate.
Certificate re-key	The process of replacing an existing *certificate* whilst creating a new *key-pair* such that the connection between old and new certificates is only the *subject* name.
Certificate renewal	The process of replacing an existing *certificate* whilst retaining the existing *public key* value and *subject* name and with an expiry date after that of the original certificate.
Certificate suspension	The process of temporarily *revoking* a *certificate.* The fact of suspension is published on a *CRL* or *ARL*.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorised persons, or a violation of the security policy of a system in which unauthorised intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorised entities or processes.
CRL	Certificate Revocation List – a file containing the serial numbers (and revocation date) of *revoked* CA and/or end-entity certificates. (See *ARL*).
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Crypto period	Time span during which each key setting remains in effect.
DCMA	Defence Certificate Management Authority. Body established to operate the DPKI, incorporating all Certification Authority and Registration Authority functions. The DCMA is subordinate to the DPMA.
Digital Signature	The *hash* of a data object encrypted using a *private key.* Where *non-repudiation* is required the *private key* should be under the sole control of a single *entity*.
DPKI	Defence Public Key Infrastructure
DPMA	Defence Policy Management Authority. Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.

DRCA	Defence Root Certification Authority
Dual-use certificate	A certificate that is intended for use with both *digital signature* and data encryption services.
End-entity	The final (lowest) object in a *chain* of certificates; a Subscriber to a PKI that is not a *CA*.
Entity	A single object.
Encryption certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Integrity	Protection against unauthorised modification or destruction of information.
Intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is located in the path between an *end-entity* certificate and a *trust anchor.*
Issuer	Identity of the CA that issues, or has issued, a *certificate.*
Hash	(Properly: hash result). The output of a *hash function.*
Hash function	An algorithm that computes a fixed size value based on a data object of arbitrary size.
Key-pair	Two mathematically related cryptographic keys used in conjunction with an *asymmetric encryption algorithm.*
Key escrow	The retention of the private component of the key pair associated with a subscriber's *encryption certificate* to support key recovery.
Key exchange	The process of exchanging *public keys* (and other information) in order to establish secure communication.
Key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Level 1 CA	A CA directly subordinate to the Root CA
Local Registration Authority (LRA)	A type of Registration Authority with responsibility for a local community.
Naming authority	An organisational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non-repudiation service	A security service that provides protection against false denial of involvement in a communication or other action.
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party, or through a CA that Relying Party trusts, or through the CA that issued the certificate whose revocation status is being sought.

Outside threat	An unauthorised entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Path	A series of *certificates* that are linked together such that (from the top of the path) each certificate *subject* is the *issuer* of the certificate immediately below it in the path. See also *certificate chain.*
Path discovery	The process of determining the list (*chain*) of *certificates* that lie between an *entity* certificate and a *trust anchor*. This *path* is influenced by the presence of multiple constraints indicated in the *certificate chain* or established by the *initial conditions* set in the *client*.
Path processing	*Path discovery* followed by *path validation* for a given *entity certificate*.
Path validation	The process of testing each *certificate* in a *path* to ensure that it has not expired or been *revoked*. The integrity of the issuing CA *digital signature* is also tested for each *certificate.*
Physically isolated network	A network that has no electronic connection to individuals outside a physically controlled space.
PKI Sponsor	Fills the role of a subscriber for non-human system components or organisations that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers as defined throughout this document.
Policy Management Authority (PMA)	See DPMA.
Privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key	One key of a *key-pair* that is used in association with an *asymmetric encryption algorithm*. Normally the value of a private key is known, or accessible, only to a small group of *entities* (often the group size is 1).
Public key	One key of a *key-pair* that is used in association with an asymmetric encryption algorithm. Normally the value of a public key is widely distributed.
Public Key Infrastructure (PKI)	Framework established to issue, distribute, maintain, and revoke public key certificates and their associated key-pairs.
PUID	Person Unique Identifier – a unique identifier that is permanently assigned to a MOD employee or contractor
PUID Name	A format for presenting the name of a MOD employee or contractor that is permanently unique; the PUID Name associated with a person may change over time but the PUID never changes.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects and subsequently issuing an authorised certificate request.
Registration information	Information, such as a subscriber's postal address, that is not included in a *certificate*, but that may be used by a CA/RA in certificate management.
Root CA	In a hierarchical PKI, the CA whose *public key* serves as the *trust anchor* for *subordinate CAs* and *end-entities*.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to

rely on them.

Repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
Revocation list	See *CRL* and *ARL*.
Revoke	The cancellation of a *certificate* prior to its expiry; certificates are self-revoking as they are cancelled once their expiry date has passed.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Server	A system entity that provides a service in response to requests from clients.
Signing (signature) certificate	A *certificate* that contains a *public key* intended for verifying *digital signatures* or *authenticating* the identity of an *entity*.
SSL	Secure Sockets Layer. Proprietary secure communications protocol widely used in COTS products. Version 3 of the protocol is a subset of TLS version 1.0.
Subject	The recipient of a *certificate*; the identity of the *entity* that knows the value of a *private key* that is from the same pair as the *public key* contained in a *certificate.*
Subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by a *superior CA*, and whose activities are constrained by that CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of a *subordinate CA*, and who constrains the activities of that CA.
System high	The highest security level supported by an information system.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
TLS	Transport Layer Security. Standardised secure communications protocol supporting application-to-application security.
Trust anchor	A public key that is known (*trusted*) by a *Relying Party*. The mechanism of *path discovery* establishes a *trusted* path between a *certificate* and a trust anchor. A common trust anchor is a *self-signed* (*root*) *certificate*.
Trust list	Collection of trusted *certificates* used by *relying parties* as *trust anchors* during *path processing*.
Trusted	A relationship between a *certificate* user and a *CA* in which the user acts according to the assumption that the *CA* creates only valid *certificates*.
Trusted certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. A *trust anchor* is contained in a trusted certificate.
Trusted time	A trusted source of time information within an information system.

Trusted timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorised individuals, each capable of detecting incorrect and/or unauthorised procedures with respect to the task being performed, and each familiar with established security and safety requirements.
Validation Authority (VA)	That part of the DCMA responsible for confirming the status of a certificate (via OCSP) or providing access to CRLs.
Zeroise	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

ANNEXE B: ACRONYMS

ARL	Authority Revocation List
CA	Certification Authority
CAPS	CESG Assisted Products Scheme
CIS	Communication and Information Systems
DCMA	Certificate Management Authority
DINSA	Defence Interoperable Network Services Authority
DPKIPB	Defence PKI Programme Board
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DCMA	Defence Certificate Management Authority
DCP	Defence Public Key Infrastructure X.509 Certificate Policy
D-H	Diffie-Hellman Key Exchange Algorithm
DII	Defence Information Infrastructure
DII(F)	Defence Information Infrastructure (Future)
DN	Distinguished Name
DPKI	Defence Public Key Infrastructure
DPMA	Defence Policy Management Authority
DRCA	Defence Root Certificate Authority
DTAG	DPKI Technical Advisory Group
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IETF	Internet Engineering Task Force
IPT	Integrated Project Team
JSP	Joint Services Publication
JSyCC	Joint Security Coordination Centre
LRA	Local Registration Authority
MOD	Ministry of Defence
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
RA	Registration Authority
RFC	Request For Comment
RP	Relying Party
RSA	Rivest, Shamir, Adleman (encryption algorithm)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UK	United Kingdom
VA	Validation Authority