CabinetOffice

HMG Certificate Policies

Version 1.0

October 2004

csia

Central Sponsor for Information Assurance

Contents

1 Introduction

1.1 Overview

1.1.1 This document contains the four certificate policies listed below:

a. Level 2 Digital Signature Policy;

b. Level 3 Digital Signature Policy;

c. Level 2 Confidentiality Policy; and

d. Level 3 Confidentiality Policy.

1.1.2 This document details the minimum standards required for each Certificate Policy. Individual Certification Authorities (CAs) may exceed the specifications in the Certificate Policy, subject to approval by the Policy Management Authority (PMA).

1.1.3 This document is Version 1.0 of Her Majesty's Government (HMG) Certificate Policies and has been approved by the PMA.

1.1.4 Separate documents for each policy are also available.

1.1.5

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
This policy states the minimum requirements necessary to support trust in an HMG Level 2 Digital Signature Certificate.	This policy states the minimum requirements necessary to support trust in an HMG Level 3 Digital Signature Certificate.	This policy states the minimum requirements necessary to support trust in an HMG Level 2 Confidentiality (Data Encryption) Certificate.	This policy states the minimum requirements necessary to support trust in an HMG Level 3 Confidentiality (Data Encryption) Certificate.

1.1.6

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The issue of a certificate to an individual signifies that the Registration Authority (RA) and Certification Authority (CA) have followed the procedures specified in Section 3.1 of this Certificate Policy, and that there is a level of assurance corresponding to Level 2 in the e-Government Security Framework that the name on the certificate is a valid representation of the identity of the individual.	The issue of a certificate to an individual signifies that the Registration Authority (RA) and Certification Authority (CA) have followed the procedures specified in Section 3.1 of this Certificate Policy, and that there is a level of assurance corresponding to Level 3 in the e-Government Security Framework that the name on the certificate is a valid representation of the identity of the individual.	The issue of a certificate to an individual signifies that the Registration Authority (RA) and Certification Authority (CA) have followed the procedures specified in Section 3.1 of this Certificate Policy, and that there is a level of assurance corresponding to Level 2 in the e-Government Security Framework that the name on the certificate is a valid representation of the identity of the individual.	The issue of a certificate to an individual signifies that the Registration Authority (RA) and Certification Authority (CA) have followed the procedures specified in Section 3.1 of this Certificate Policy, and that there is a level of assurance corresponding to Level 3 in the e-Government Security Framework that the name on the certificate is a valid representation of the identity of the individual.

1.1.7

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
A digital signature does not in itself convey any authorization to bind any person, perform an activity, or access any information. A digital signature does not make any representations about the content of the document or message to which it has been applied beyond the identity of the signer of the document or message, unless otherwise indicated (for example in a separate agreement relating to the service for which the certificate is being used).		n/a	n/a

1.1.8 This policy has been structured according to IETF RFC 2527[1]. The reader is referred to RFC 2527 for background information regarding the terms used in this policy. In addition to the structure of RFC 2527, this document contains a list of definitions (Appendix A), a list of references (Appendix B), and guidance on physical security requirements (Appendix C).

1.2 Identification

1.2.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
This document is referred to as the "HMG Level 2 Digital Signature Certificate Policy" and contains the certificate policy for digital signatures at an equivalent level of assurance to Level 2 in the e-Government Security Framework.	This document is referred to as the "HMG Level 3 Digital Signature Certificate Policy" and contains the certificate policy for digital signatures at an equivalent level of assurance to Level 3 in the e-Government Security Framework.	This document is referred to as the "HMG Level 2 Confidentiality Certificate Policy" and contains the certificate policy for confidentiality (via data encryption) at an equivalent level of assurance to Level 2 in the e-Government Security Framework.	This document is referred to as the "HMG Level 3 Confidentiality Certificate Policy" and contains the certificate policy for confidentiality (via data encryption) at an equivalent level of assurance to Level 3 in the e-Government Security Framework.

1.2.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The Object Identifier (OID) of this Certificate Policy is 1.2.826.0.1316.2.0.1.2.0.	The Object Identifier (OID) of this Certificate Policy is 1.2.826.0.1316.2.0.1.3.0.	The Object Identifier (OID) of this Certificate Policy is 1.2.826.0.1316.2.0.1.2.1.	The Object Identifier (OID) of this Certificate Policy is 1.2.826.0.1316.2.0.1.3.1.

[1] http://www.ietf.org/rfc/rfc2527.txt

1.3 Community and Applicability

1.3.1 Certification authorities

1.3.1.1 The organizations entitled to apply to become Certification Authorities within the HMG PKI ('*Eligible Certification Authorities*') are all UK public sector bodies, including:

a. HMG Departments and Executive Agencies;

b. local authorities;

c. NHS bodies;

d. education authorities, schools, colleges and universities;

e. the police; and

f. other public sector bodies, as listed in Schedule 1 of the Freedom of Information Act 2000.

1.3.1.2 Membership of the HMG PKI is subject to approval by the Policy Management Authority (PMA), which it may grant or withhold in its absolute discretion and without giving any reason for its decision. The criteria which will be applied, together with their relative weighting, are contained in the PMA internal policy document.

1.3.1.3 While a department or other public authority may use a contractor to provide CA services, the public authority itself must remain responsible and accountable to the PMA and to the Relying Party for the operation of its CA.

1.3.2 Registration authorities

1.3.2.1 The Eligible Certification Authorities can be Registration Authorities within the HMG PKI.

1.3.2.2 While a CA may use a contractor to provide RA services, the CA remains responsible and accountable to the PMA and to the Relying Party for the operation of its RA.

1.3.2.3 An RA may perform duties on behalf of more than one CA, providing that in doing so it satisfies all the requirements of this Certificate Policy.

1.3.3 End entities

1.3.3.1 The following entities may be Subscribers to the HMG PKI:

a. the Eligible Certification Authorities;

b. entities working as agents of the Eligible Certification Authorities – these entities may only be Subscribers to the HMG PKI when explicitly authorised by the PMA (unless the entities are also covered by a.); and

c. entities working, or conducting business, with any of the Eligible Certification Authorities – these entities may only be Subscribers to the HMG PKI when explicitly authorised by the PMA (unless the entities are also covered by a.).

1.3.3.2 The following end entities may be Subjects in the HMG PKI:

a. employees of Subscriber organizations;

b. individuals who act as Subscriber entities; and

c. computer applications and devices (e.g. workstations, guards, firewalls, routers, in-line network encryptors, trusted servers, and other infrastructure components), in the control of Subscribers. These components must be represented by humans, who shall be known as *Representatives* of the components and shall accept the certificate and be responsible for the correct protection and use of the Private Key.

1.3.4 Applicability

1.3.4.1 Certificates issued under this Certificate Policy shall only be used for transactions related to legitimate business:

a. with Eligible Certification Authorities; or

b. by Eligible Certification Authorities.

1.3.4.2

Level 2 Digital Signature Policy	**Level 3 Digital Signature Policy**	**Level 2 Confidentiality Policy**	**Level 3 Confidentiality Policy**
Certificates issued under this Certificate Policy may be used only to provide digital signatures and may not be used for services providing confidentiality via data encryption.		Certificates issued under this Certificate Policy may be used only to provide confidentiality via data encryption and may not be used for digital signature services.	

1.3.4.3

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Certificates for digital signatures issued under this Certificate Policy shall be used for applications and services that have a registration and authentication or trust requirement up to Level 2, as defined in the latest release of the “e-Government Registration and Authentication Strategy Framework Policy and Guidelines” or the latest release of the “e-Government Trust Services Strategy Framework Policy and Guidelines”.	Certificates for digital signatures issued under this Certificate Policy shall be used for applications and services that have a registration and authentication or trust requirement up to Level 3, as defined in the latest release of the “e-Government Registration and Authentication Strategy Framework Policy and Guidelines” or the latest release of the “e-Government Trust Services Strategy Framework Policy and Guidelines”.	Certificates for confidentiality (via data encryption) issued under this Certificate Policy shall be used for data that has a confidentiality requirement of up to Level 2 as defined in the latest release of the “e-Government Confidentiality Strategy Framework Policy and Guidelines”.	Certificates for confidentiality (via data encryption) issued under this Certificate Policy shall be used for data that has a confidentiality requirement of up to Level 3 as defined in the latest release of the “e-Government Confidentiality Strategy Framework Policy and Guidelines”. They may also be used for encrypting RESTRICTED information.

1.4 Contact Details

1.4.1 Specification administration organization

1.4.1.1 The HMG PKI Policy Management Authority (PMA) is responsible for the definition, publication, revision and interpretation of this policy.

1.4.2 Contact person

1.4.2.1 Questions and comments regarding this Certificate Policy should be addressed to the Central Sponsor for Information Assurance (CSIA) within the Cabinet Office (csia@cabinet-office.x.gsi.gov.uk).

1.4.3 Person determining Certification Practice Statement (CPS) suitability for the policy

1.4.3.1 The Chairman of the PMA has overall responsibility for determining the suitability of a CPS, Subscriber Agreement and Relying Party Agreement for this policy.

INTENTIONALLY BLANK

2 General Provisions

2.1 Obligations

2.1.1 CA obligations

2.1.1.1 A CA that issues certificates according to the policy defined in this document shall use reasonable skill in its activities as a CA, and shall take reasonable care to:

a. comply with the latest version of the policies of the PMA as notified to the CA from time to time, provided they do not reduce the trust a Relying Party is able to place in a certificate issued under this Certificate Policy;

b. produce a CPS conformant to this Certificate Policy;

c. conform to procedures and practices defined in the CPS;

d. ensure that all RAs that perform registration activities for the CA in connection with certificates issued under this policy understand and comply with this policy and the CA's CPS;

e. produce certificates correctly, maintaining evidence that due diligence was exercised in validating the information contained in the certificate;

f. issue certificates, or a decision not to issue certificates, to authorized applicants in a timely manner;

g. not cross-certify using this Certificate Policy with any other CA that is not already a member of the HMG PKI, unless authorized by the PMA[2];

h. establish that any CA with whom it cross-certifies complies at all times with all Certificate Policies that are mutually recognized under the cross certification agreement;

[2] Normally this cross-certification would be performed by the HMG Root.

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
i. n/a		ensure that any confidentiality Private Keys escrowed are held securely and protected in accordance with Section 6.2.3;	

j. ensure that Subscribers are notified at the outset of their obligations, as described in Section 2.1.3, and from time to time of any changes to their obligations, and of the implications of not complying with these obligations;

k. ensure that each Subscriber signs a Subscriber Agreement and that the CA retains each signed agreement and delivers it to the PMA on demand;

l. manage suspected and actual key compromise, suspending or revoking certificates as appropriate, as covered in Section 4.4;

m. publish all certificates and all CRLs and ARLs in a publicly available location and in a timely manner (in accordance with Sections 2.6.1 and 4.4 of this policy);

n. publish this Certificate Policy in a publicly available location (as described in Section 2.6.1);

o. give notice of any changes to this Certificate Policy (other than those concerning only formatting and the correction of minor typographic errors) to all holders of any certificates it has issued under this policy;

p. make available the CPS when necessary for audit (as described in Section 2.6.1); and

q. ensure that appropriate contractual relationships are in place, with any third party service providers (e.g. RAs, repository providers) to ensure that the CA and the third party service providers comply fully with this Certificate Policy; these contractual relationships shall include:

1. obligations of each party;
2. liabilities of each party;
3. financial responsibilities, including fiduciary relationships;
4. dispute resolution provisions; and
5. compliance and audit provisions.

2.1.1.2 A CA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 2.7.5.

2.1.2 RA obligations

2.1.2.1 An RA that undertakes the registration for certificates according to the policy defined in this document shall:

a. conform to practices and procedures defined in a CPS (either generated by the RA or the CA) conformant to this Certificate Policy;

b. validate and verify the identity of applicants, as covered in Section 3.1;

c. ensure that Subscribers understand their obligations, as described in Section 2.1.3, and understand the implications of not complying with these obligations;

2.1.2.2 An RA who is found to have acted in a manner inconsistent with these obligations shall be subject to action as described in Section 2.7.5.

2.1.3 Subscriber obligations

2.1.3.1 Prior to applying for or being issued with a certificate by a CA, a Subscriber shall read and sign a Subscriber Agreement by which they agree to be bound by the terms of this Certificate Policy.

2.1.3.2 The Subscriber Agreement shall clearly state that the Subscriber shall:

a. provide accurate information at registration and at all subsequent communications with any member of the HMG PKI;

b. ensure that key pair generation, if not performed at CA or RA premises, is performed in a trusted environment;

c. prove possession of the Private Key in accordance with the Registration procedure, as defined in Section 3.1.7;

d. protect the Private Key at all times, in accordance with this policy;

e. ensure that the Private Key is only accessible by the Subject of the certificate, that the Private Key remains in the personal control of the Subject of the certificate at all times, and that no one other than the Subject has access to the Private Key at any time;

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
f. ensure that the number of number of copies of the Private Key is kept to the minimum needed for business purposes, that these copies are only accessible by the Subject of the certificate, and that they are protected using security measures that are at least as strong as those that protect the original key;	not attempt to duplicate or backup the Private Key;	ensure that the number of copies of the Private Key is kept to the minimum needed for business purposes, and that the copies of the Private Key are protected using security measures that are at least as strong as those that protect the original key;	

g. ensure that the Subject of the certificate does not disclose the activation data protecting the Private Key to any person at any time;

h. ensure that certificates are used in accordance with this Certificate Policy at all times;

i. notify the Registration Authority in the event of any change to, or inaccuracy in, information given at registration time;

j. notify either the CA or RA in the event of suspected compromise of the Private Key or the activation data protecting the Private Key;

k. ensure that the certificate is not used by the Subject after it has expired or been revoked, or while it is suspended;

l. not tamper with, or attempt to reverse engineer, any aspect of the technical implementation of the HMG PKI;

m. not apply (whether to a CA or to any other person whatsoever) for any other certificate using the same key pair that has been generated in the registration for a certificate under this policy;

n. agree to the terms in the Relying Party Agreement in force at the time the Relying Party relies on the certificate; and

o. ensure that any correspondence using the certificate clearly instructs the Relying Party to read, accept and agree to the Relying Party Agreement before relying on the certificate, and to warn the Relying Party that it is deemed to have accepted and agreed to the Relying Party Agreement if it relies on the certificate - this correspondence should use a direct link to the published Relying Party Agreement where possible.

2.1.3.3 Guidance shall be given by the CA to Subscribers, through the Subscribers Agreement or otherwise, regarding the mechanisms by which they shall adhere to their obligations. This guidance shall include, but shall not be limited to, guidance relating to Paragraphs 2.1.3.2b, d, e, f, g, h, j and Paragraph 2.3.1.2c.

2.1.3.4 A Subscriber is responsible and liable for the acts and omissions of its officers, directors, employees, agents and contractors in connection with any application for a certificate or key, and their use, storage, security and destruction, as if those acts and omissions were the Subscriber's.

2.1.3.5 If an authorized entity (as defined in Section 4.4.3 or 4.4.7) reasonably suspects a Subscriber of having acted in a manner inconsistent with these obligations, an authorized entity (as defined in Section 4.4.3 or 4.4.7) may request suspension or revocation of the Subscriber’s certificate(s), as described in Section 4.4.

2.1.3.6 Subscribers shall indemnify the HMG PKI Authorities in accordance with Paragraph 2.3.1.1.

2.1.4 Relying party obligations

2.1.4.1 Relying Parties shall use the HMG PKI, and rely on a certificate that has been issued under this Certificate Policy if (and only if):

a. the certificate has been used for the purpose for which it has been issued, as described in this Certificate Policy;

b. the Relying Party has verified the validity of the digital certificate, using procedures described in the X.509 standard;

c. the Relying Party has established trust in the certificate by verifying the certificate path to a trust point, in accordance with the guidelines set by the X.509 standard and as stated in Section 4.4.11;

d. the Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate;

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
e. the Relying Party has verified that the digital signature has been generated using the Private Key; and		n/a	n/a
f. the Relying Party preserves the original signed data for as long as it may be necessary to verify the signature on that data.		n/a	n/a

2.1.4.2 Guidance shall be given by the CA to Relying Parties, through the Relying Party Agreement or otherwise, regarding the mechanisms by which they shall adhere to their obligations. This guidance shall include, but shall not be limited to, guidance relating to Paragraphs 2.1.4.1a, b, c, e and f.

2.1.4.3 Relying parties shall indemnify the HMG PKI Authorities in accordance with Paragraph 2.3.1.3.

2.1.5 Repository obligations

2.1.5.1 Repositories that operate certificate status services, publish certificates or publish Certificate Revocation Lists in relation to the Certificate Policy defined in this document shall:

a. publish all certificates as soon as they are received, within normal business hours (at the time of receipt);

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
b. publish all certificate revocation information, including suspension information, as soon as it is received, within normal business hours, and conformant to Section 4.4 of this policy;	publish all certificate revocation information, including suspension information, as soon as it is received, whether inside or outside normal business hours (i.e. 24x7x365), and conformant to Section 4.4 of this policy – in very restricted circumstances, the PMA may authorize a CA to publish ARLs within normal business hours only;	publish all certificate revocation information, including suspension information, as soon as it is received, within normal business hours, and conformant to Section 4.4 of this policy;	publish all certificate revocation information, including suspension information, as soon as it is received, whether inside or outside normal business hours (i.e. 24x7x365), and conformant to Section 4.4 of this policy – in very restricted circumstances, the PMA may authorize a CA to publish ARLs within normal business hours only;

c. operate all certificate status services in accordance with Section 4.4 of this policy;

d. enable access to published information by all those authorized to do so, as described in Section 2.6; and

e. provide sufficient security to protect published repository information, as defined in Section 2.6.

2.1.5.2 A repository which is found to have acted in a manner inconsistent with these obligations shall be subject to action as described in Section 2.7.5.

2.2 Liability

2.2.1 This Section 2.2 restricts the liability of the HMG PKI Authorities to End Entities. The liability of the HMG PKI Authorities to each other is governed by agreements between them.

2.2.2 Except as expressly stated in this Section 2.2, this section covers the liability of the HMG PKI Authorities to any person for loss, damage, liabilities and expenses (including legal costs and expenses) of any kind which are suffered or incurred by any person, however they may be caused - even if they are caused by the HMG PKI Authorities' negligence or breach of this policy. As exceptions, the HMG PKI Authorities do not exclude any liability which they would otherwise have for either (1) any personal injury resulting from negligence, whether or not it results in death, or (2) fraud by the HMG PKI Authorities.

2.2.3 The HMG PKI Authorities make no representations other than those expressly stated in this policy, and any which would otherwise be implied by law, custom, course of dealings or circumstances are excluded. By using or relying on a certificate issued under this policy, an End Entity accepts and agrees that it has not relied on any other representation.

2.2.4 No warranties, conditions or other terms other than those expressly stated in this policy are incorporated in any agreement based on this policy and made between any of the HMG PKI Authorities and an End Entity, unless they are expressly stated to be part of that agreement.

2.2.5 An HMG PKI Authority shall have no liability or obligation whatsoever for the acts, omissions or representations of any other HMG PKI Authority.

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

2.2.7 The HMG PKI 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.

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

2.2.9 The HMG PKI Authorities shall have no liability whatsoever for any loss, damage, liability or expense which is not, in the ordinary course of things, the natural consequence of the claimant's reliance on a certificate issued by a CA under this policy and the Authority's breach of this policy.

2.2.10 The HMG PKI 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 a CA.

2.2.11 The HMG PKI Authorities shall have no liability whatsoever in relation to any decision not to issue a certificate under this policy to any person.

2.2.12 The HMG PKI Authorities shall have no liability whatsoever in relation to the suspension or revocation of a certificate issued under this policy if it is suspended or revoked in accordance with this policy.

2.2.13 The HMG PKI Authorities shall have no liability whatsoever in relation to either (1) a certificate issued under this policy, or (2) the associated public/private key pairs, to any person who has not used them strictly in accordance with this policy and any agreements pertaining to their use.

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

2.2.15 The HMG PKI Authorities shall have no liability whatsoever in relation to any reliance on either (1) a certificate issued under this policy, or (2) the associated public/private key pairs, if at any time these are relied on the certificate is identified in the relevant published CRL/ARL as having been suspended or revoked.

2.2.16 The HMG PKI Authorities shall have no liability whatsoever in relation to any reliance on either (1) a certificate issued under this policy, or (2) the associated public/private key pairs, if at any time these are relied on the issuing CA would have published the suspension or revocation of the certificate in a CRL/ARL in accordance with this policy, 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 policy).

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

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

2.2.19 The HMG PKI Authorities shall have no liability whatsoever for any loss, damage, liability or expense (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.

2.2.20

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The total aggregate liability of the HMG PKI Authorities in connection with a transaction in which either (1) a certificate issued under this policy, or (2) the associated public/private key pairs, have been relied on, is limited to £10,000. If two HMG PKI Authorities would otherwise be liable for more than this – 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.	The total aggregate liability of the HMG PKI Authorities in connection with a transaction in which either (1) a certificate issued under this policy, or (2) the associated public/private key pairs, have been relied on, is limited to £250,000. If two HMG PKI Authorities would otherwise be liable for more than this – 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.	The total aggregate liability of the HMG PKI Authorities in connection with a transaction in which either (1) a certificate issued under this policy, or (2) the associated public/private key pairs, have been relied on, is limited to £10,000. If two HMG PKI Authorities would otherwise be liable for more than this – 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.	The total aggregate liability of the HMG PKI Authorities in connection with a transaction in which either (1) a certificate issued under this policy, or (2) the associated public/private key pairs, have been relied on, is limited to £250,000. If two HMG PKI Authorities would otherwise be liable for more than this – 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.

2.2.21

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The total aggregate liability of the HMG PKI Authorities to each End Entity in respect of all claims notified by that End Entity during any one calendar year (running from 1 January to 31 December) is limited to £50,000. If two HMG PKI Authorities would otherwise be liable for more than this – either individually or collectively – they are only liable to pay this between them.	The total aggregate liability of the HMG PKI Authorities to each End Entity in respect of all claims notified by that End Entity during any one calendar year (running from 1 January to 31 December) is limited to £1,000,000. If two HMG PKI Authorities would otherwise be liable for more than this – either individually or collectively – they are only liable to pay this between them.	The total aggregate liability of the HMG PKI Authorities to each End Entity in respect of all claims notified by that End Entity during any one calendar year (running from 1 January to 31 December) is limited to £50,000. If two HMG PKI Authorities would otherwise be liable for more than this – either individually or collectively – they are only liable to pay this between them.	The total aggregate liability of the HMG PKI Authorities to each End Entity in respect of all claims notified by that End Entity during any one calendar year (running from 1 January to 31 December) is limited to £1,000,000. If two HMG PKI Authorities would otherwise be liable for more than this – either individually or collectively – they are only liable to pay this between them.

2.2.22

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The total aggregate liability of the HMG PKI Authorities to all claimants in respect of all claims notified during any one calendar year (running from 1 January to 31 December) is limited to £1,000,000. Their liability for each claim shall be apportioned pro rata according to the value of each claim.	The total aggregate liability of the HMG PKI Authorities to all claimants in respect of all claims notified during any one calendar year (running from 1 January to 31 December) is limited to £10,000,000. Their liability for each claim shall be apportioned pro rata according to the value of each claim.	The total aggregate liability of the HMG PKI Authorities to all claimants in respect of all claims notified during any one calendar year (running from 1 January to 31 December) is limited to £1,000,000. Their liability for each claim shall be apportioned pro rata according to the value of each claim.	The total aggregate liability of the HMG PKI Authorities to all claimants in respect of all claims notified during any one calendar year (running from 1 January to 31 December) is limited to £10,000,000. Their liability for each claim shall be apportioned pro rata according to the value of each claim.

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

2.2.24 Subscriber Agreements shall require Subscribers to compensate a Relying Party which suffers or incurs loss, damage, liabilities or expenses as a result of the Subscriber's breach of this Certificate Policy or its negligence (including the Subscriber's failure to keep its Private Key private), and to indemnify the HMG PKI Authorities against any loss, damage, liability and expense of any kind (including legal costs and expenses) suffered or incurred by them in connection with any claim brought against them by the Relying Party. The Subscriber Agreement may additionally require the Subscriber to acknowledge that when the replacement of a Subscriber's keys is required in such circumstances, then the Subscriber is liable for the cost of replacing such keys and certificates.

2.2.25 Relying Parties shall, and Relying Party Agreements shall require them to, acknowledge that they shall bear the consequences if they fail to perform the Relying Party obligations described in Section 2.1.4 of this policy, and that, if they abide by those obligations, they will have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a certificate but they are solely responsible for their decision.

2.2.26

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
n/a		The HMG PKI Authorities do not provide key escrow or recovery services. Subscribers must make their own provisions for the backup of Private Keys.	

2.2.27 This Section 2.2 is subject to the express terms of this policy and any relevant agreement with an End Entity.

2.3 Financial Responsibility

2.3.1 Indemnification by Subscribers and Relying Parties

2.3.1.1 A Subscriber shall indemnify the HMG PKI Authorities against all loss, damage, liability and expenses of any kind (including legal costs and expenses) that they incur as a result of any breach of this Certificate Policy by the Subscriber.

2.3.1.2 Subscribers shall, and Subscriber Agreements shall require Subscribers to, indemnify the HMG PKI Authorities against any loss, damage and expenses of any kind (including legal costs and expenses) that they may incur as a result of or arising from:

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

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

c. 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 Certificate Policy and the guidance provided by the CA, as specified in Paragraph 2.1.3.3;

d. 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;

e. any unauthorised or unlawful use of a certificate by a Subscriber, its servants, agents, employees or contractors; or

f. any breach of this Certificate Policy by the Subscriber, the Subject or the Representative.

2.3.1.3 Relying Party Agreements shall require Relying Parties to indemnify the HMG PKI Authorities against any loss, damage and expenses of any kind (including legal costs and expenses) that they may incur as a result of:

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

b. the Relying Party’s reliance on a certificate that is not reasonable under the circumstances (for example, through relying on a certificate with an inappropriate level of assurance for the transaction concerned; it is up to Relying Parties to determine the appropriate level of assurance required for a particular transaction, in accordance with the e-Government Security Framework);

c. the Relying Party’s failure to check, in an appropriate manner, the status of each certificate to determine if the certificate is expired, suspended or revoked; or

d. any breach of this Certificate Policy by the Relying Party.

2.3.2 Fiduciary relationships

2.3.2.1 Issuance of certificates under this Certificate Policy does not make any of the HMG PKI Authorities a representative of Subscribers or Relying Parties (whether as an agent, fiduciary, trustee or in any other way whatsoever).

2.3.2.2 Issuance of certificates under this Certificate Policy does not make a Registration Authority (RA) an agent for a Certification Authority (CA) (whether as an agent, fiduciary, trustee or in any other way whatsoever).

2.3.3 Administrative processes

2.3.3.1 CAs shall ensure that they have sufficient financial resources to maintain their operations and perform their duties as defined in this Certificate Policy. The PMA internal policy document specifies criteria with which the PMA will determine the level of financial resources required.

2.4 Interpretation and Enforcement

2.4.1 Governing law

2.4.1.1 The enforceability, construction, interpretation and validity of this policy shall be governed by English Law. A CA must ensure that any agreements entered into by that CA are also governed by English Law.

2.4.2 Severability, survival, merger and notice

2.4.2.1 In the event that any part of this Certificate Policy is found to be unenforceable or invalid pursuant to the applicable law, that part will be enforced to the maximum extent possible so as to give effect to its intention, and the remaining terms and conditions will continue in full force and with full effect.

2.4.2.2 If a CA, RA or Subscribers undergoes a merger or takeover, such that the binding between the certificate and the Private Key becomes invalid, it shall immediately notify the issuing CA and the certificate shall be revoked, as described in Section 4.4.2.

2.4.2.3 Each CA shall ensure that any agreements it enters into contain appropriate provisions governing severability, survival, merger and notice as applicable.

2.4.3 Dispute resolution procedures

2.4.3.1 Any dispute arising out of, or relating to, this Certificate Policy should be resolved using an appropriate dispute settlement mechanism in accordance with this policy. In this Section 2.4.3, 'parties' means the persons between whom the dispute has arisen.

2.4.3.2 For at least one week, the parties shall use reasonable endeavours to resolve the dispute by negotiation before proceeding to mediation.

2.4.3.3 If the dispute is not resolved by negotiation, for at least one week the parties shall use reasonable endeavours to resolve the dispute by mediation, using an independent mediator. The mediator must be reasonably acceptable to the parties, but a party shall not unreasonably withhold its consent.

2.4.3.4 If the dispute is not resolved by mediation, the parties shall refer the dispute to arbitration in accordance with the Arbitration Act 1996.

2.4.3.5 If the dispute concerns key or certificate management the mediator and arbitrator shall be appointed by the PMA.

2.4.3.6 A dispute related to key and certificate management within a department or single organisation belonging to the HMG PKI is to be resolved, where appropriate, by the appropriate departmental or organisational authority in conjunction with the Issuing CA. If necessary, the dispute will be escalated to the PMA (for example, if the department itself is one of the parties in dispute).

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

2.4.3.8 Each CA must ensure that any agreement it enters into provides appropriate dispute resolution procedures equivalent to these.

2.5 Fees

2.5.1 The charging of fees is subject to appropriate legislative authority and policy. Notice of any fee charged to a Subscriber must be brought to the attention of that Entity before the validity period of the certificate comes into effect. Notice of any fee charged to a Relying Party must be brought to the attention of that Entity before the Entity relies on the certificate.

2.6 Publication and Repository

2.6.1 Publication of CA information

2.6.1.1 A CA that issues certificates according to the policy defined in this document shall:

a. ensure that this Certificate Policy is digitally signed by a member of the HMG PKI approved by the PMA, and publish the location of the digitally signed Certificate Policy;

b. ensure that the CPS is digitally signed by a member of the HMG PKI approved by the PMA and make available the digitally signed CPS when necessary for audit, inspection, accreditation or cross-certification;

c. publish certificates, including a reference within the certificate to a website where CA information is located;

d. publish certificate status information;

e. ensure that only authorized representatives of the CA can publish the information defined in Paragraphs a to d; and

f. ensure that this Certificate Policy and the certificate status information are made available to all Subscribers and Relying Parties, either directly or in agreement with a repository.

2.6.2 Frequency of publication

2.6.2.1 Certificates shall be published on issuance, before the Subscriber receives the certificate. This Certificate Policy must be published immediately within normal business hours, on issuance, and when any updates are made.

2.6.2.2 Certificate Revocation Lists (CRLs) must be issued daily, even if there is no change to the certificate status information, or more frequently when end entity certificates are suspended or revoked as a result of a suspected or actual compromise, and in accordance with Section 4.4.10 of this document.

2.6.2.3 Authority Revocation Lists (ARLs) must be issued monthly, even if there is no change to the certificate status information, or more frequently when CA certificates are suspended or revoked as a result of a suspected or actual compromise, and in accordance with Section 4.4.10 of this document.

2.6.3 Access controls

2.6.3.1 CAs shall ensure that sufficient controls are in place to prevent unauthorized addition, deletion or modification of repository entries.

2.6.3.2 No additional access control mechanisms are necessary to protect the Certificate Policy.

2.6.4 Repositories

2.6.4.1 Repository obligations are described in Section 2.1.5.

2.7 Compliance Audit

2.7.1 Frequency of entity compliance audit

2.7.1.1 The frequency and extent of audits are to be determined by the HMG PMA on a case-by-case basis, according to the guidelines specified in the PMA internal policy. The HMG PKI PMA shall have the free and unrestricted right to audit and inspect the premises, staff, documents and data of any HMG PKI CA/ RA for the purposes of evaluating that CA/RA's compliance with the terms of this Certificate Policy.

2.7.1.2 The PMA, at its discretion, may request a Certification or Registration Authority to have an audit by an agency external to the department at any time.

2.7.1.3 The CA/RA must certify annually to the PMA that they have at all times during the period in question complied with the requirements of this policy. The CA/RA must also provide to the PMA details of any periods of non-compliance and explain the reasons why the CA/RA has not complied with this Certificate Policy.

2.7.2 Identity/qualifications of the Auditor

2.7.2.1 The auditor acts as agent for the HMG PMA and shall be selected by the PMA, and shall have such qualifications as accord with best commercial practice or as required by law. This shall include significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software.

2.7.3 Auditor's relationship to audited party

2.7.3.1 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.

2.7.4 Topics covered by audit

2.7.4.1 The audit must cover whether:

a. the Certification Practice Statement (CPS) outlines, in sufficient detail, the technical, procedural and personnel policies and practices of the CA/RA which meet the requirements of all the certificate policies supported by the CA/RA;

b. the CA implements and complies with the technical, procedural and personnel practices and policies outlined in the CPS; and

c. an RA, if used, implements and complies with the technical, procedural and personnel practices and policies set out by the CA in the CPS.

2.7.4.2 The topics covered by a compliance audit consist of the following:

a. physical security;

b. documentation and process;

c. vetting of operational personnel;

d. technical security measures; and

e. privacy, including compliance with Data Protection laws.

2.7.4.3 A Certification or Registration Authority shall be given advance notice (of not less than 10 working days) of the aspects of the PKI that will be audited for any given inspection.

2.7.4.4 The Certification or Registration Authority shall co-operate with the auditor and shall afford the auditor all reasonable assistance and access to the Authority's premises, staff, documentation and data.

2.7.5 Actions taken as a result of deficiency

2.7.5.1 If irregularities are found by the PMA, the CA/RA shall be informed in writing immediately. The CA/RA must submit a report to the auditor or directly to the PMA, as determined by the PMA, as to any remedial action the CA/RA 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 PMA as appropriate. The PMA shall be kept informed by the CA/RA at all times.

2.7.5.2 Remedial action may include suspension or revocation of the CA/RA certificate, as defined in Section 4.4.

2.7.5.3 Where a CA/RA fails to take appropriate action in response to the identified deficiencies, the PMA shall be informed and shall take the appropriate action, according to the severity of the deficiencies which shall include:

a. noting the deficiencies but allowing the CA/RA to continue operations until the next planned, or newly scheduled, inspection;

b. suspending the CA/RA's certificate; or

c. revoking the CA/RA's certificate.

2.7.6 Communication of results

2.7.6.1 Audit results are to be treated as confidential information. Unless otherwise specified in an applicable contract, they shall be treated in accordance with Section 2.8.

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

2.8.1.1 All CAs, RAs and repositories within the HMG PKI shall implement and maintain a privacy policy, which shall be in accordance with the Data Protection Act 1998 and the Freedom of Information Act 2000.

2.8.1.2 The following information shall be kept confidential, subject to Section 2.8.2:

a. all applications made by potential Subscribers to a CA (whether successful or otherwise);

b. all records of CA activities and events;

c. Private Keys;

d. transactional records;

e. audit trail records and reports;

f. contingency planning and disaster recovery plans; and

g. security measures.

2.8.1.3 Inspection information is considered confidential and must not be disclosed to anyone for any purpose other than inspection purposes or where required by law.

2.8.1.4 Any requests for the disclosure of information must be made in writing, signed and delivered to the CA.

2.8.2 Types of information not considered confidential

2.8.2.1 Certificates, CRLs and ARLs, and personal or corporate information appearing on them are not considered confidential and are therefore deemed to be in the public domain.

2.8.3 Disclosure of certificate revocation/suspension information

2.8.3.1 Policy relating to disclosure of certificate revocation/suspension information is covered in Sections 2.8.2 and 4.4.4.

2.8.4 Release to law enforcement officials

2.8.4.1 Privacy rights will be respected subject to the applicable laws.

2.8.5 Release as part of civil discovery

2.8.5.1 Privacy rights will be respected subject to the applicable laws.

2.8.6 Disclosure upon owner's request

2.8.6.1 Privacy rights will be respected subject to the applicable laws.

2.8.7 Other information release circumstances

2.8.7.1 No stipulation.

2.9 Intellectual Property Rights

2.9.1 All Intellectual Property Rights in certificates, OIDs, directories and all documents comprising the HMG PKI (including but not limited to this Certificate Policy) belong to and will remain the property of the Crown, with the exception of any items specifically mentioned in this Section 2.9 of the Certificate Policy.

2.9.2 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 HMG PKI documentation, the HMG PKI and its component CAs and RAs are not infringing any third party intellectual property rights.

2.9.3

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The IPR for a digital signature key pair belongs to the entity that generated the key pair, i.e. the subject of the certificate.		The IPR for a confidentiality key pair belongs to the entity that generated the key pair, i.e. the Subscriber, CA or RA.	

INTENTIONALLY BLANK

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

3.1.1.1 Each certificate issued under this policy must have a non-null X.501 Distinguished Name (DN) in the certificate subject name field, in accordance with the IETF RFC 3280. An alternative name may be use in addition, using the `SubjectAlternateName` field, also in accordance with IETF RFC 3280.

3.1.1.2 Names shall be defined in accordance with HMG naming policy and shall be genuine, unique and unambiguous.

3.1.1.3 If the certificate is issued to a non-human subject, it is necessary to include directly in the certificate the name of a person responsible for the correct use of the certificate.

3.1.2 Need for names to be meaningful

3.1.2.1 Certificate Subject and Issuer names shall be meaningful, using commonly understood semantics to identify the person or object to which they are assigned. Typically this means initials and surname for person, with additional information in order to be unique.

3.1.2.2 Each DN shall have a common name (CN) which may not be unique but shall represent the Subscriber and the subject in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process.

3.1.3 Rules for interpreting various name forms

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

3.1.3.2 HMG PKI certificate naming shall conform to HMG naming policy and shall be approved by the PMA.

3.1.4 Uniqueness of names

3.1.4.1 All distinguished names shall be unique across the HMG PKI, for all time. Names shall not be re-used for another end entity after an end entity's certificate expires or is revoked; names can be re-used to re-issue a certificate to the same end entity.

3.1.4.2 CAs and RAs shall enforce uniqueness within the X.500 name space from which they have been authorized to issue names.

3.1.5 Name claim dispute resolution procedure

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

3.1.5.2 Each CA shall have and follow a name claim dispute resolution procedure with providers of repository services, if external to the CA.

3.1.5.3 If the Root CA is not able to correct a name collision brought to its attention, it shall be resolved by the PMA.

3.1.6 Recognition, authentication and role of trademarks

3.1.6.1 If a person claims that a certificate contains a trademark for which they are the registered proprietor, and the issuing CA is reasonably satisfied that the proper use of the certificate would infringe that registered trade mark, the CA shall immediately suspend or revoke the certificate.

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

3.1.7 Method to prove possession of Private Key

3.1.7.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Subscribers must prove to the RA, as part of the registration process, possession of the Private Key corresponding to the public key contained in the certificate request.		n/a	

3.1.7.2

<table>
<tr><th>Level 2 Digital Signature Policy</th><th>Level 3 Digital Signature Policy</th><th>Level 2 Confidentiality Policy</th><th>Level 3 Confidentiality Policy</th></tr>
<tr><td colspan="2">Proof of possession of the Private Key shall be achieved by signing the certificate request using a recognized standard protocol, as determined by the PMA (e.g. PKCS#10).</td><td colspan="2">n/a</td></tr>
</table>

3.1.8 Authentication of organization identity

3.1.8.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Authentication of the identity of an organization, for the purposes of issuance of a digital signature end-entity certificate shall conform to the Level 2 requirements as specified in “HMG’s minimum requirements for the verification of the identity of organisations”.	Authentication of the identity of an organization, for the purposes of issuance of a digital signature end-entity certificate shall conform to the Level 3 requirements as specified in “HMG’s minimum requirements for the verification of the identity of organisations”.	Authentication of the identity of an organization, for the purposes of issuance of a confidentiality end-entity certificate shall either conform to the Level 2 requirements as specified in “HMG’s minimum requirements for the verification of the identity of organisations” or be verified by the use of a digital signature bound to that organization by a certificate issued according to the HMG Level 2 Digital Signature Certificate Policy.	Authentication of the identity of an organization, for the purposes of issuance of a confidentiality end-entity certificate shall either conform to the Level 3 requirements as specified in “HMG’s minimum requirements for the verification of the identity of organisations” or be verified by the use of a digital signature bound to that organization by a certificate issued according to the HMG Level 3 Digital Signature Certificate Policy.

3.1.8.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Authentication of the identity of an organization that shall act as a CA or RA shall conform to the Level 3 requirements as specified in "HMG's minimum requirements for the verification of the identity of organisations".	Authentication of the identity of an organization that shall act as a CA or RA shall conform to the Level 3 requirements as specified in "HMG's minimum requirements for the verification of the identity of organisations". An additional check shall be made that the individuals involved appear in an appropriate personnel register[3].	Authentication of the identity of an organization that shall act as a CA or RA shall conform to the Level 3 requirements as specified in "HMG's minimum requirements for the verification of the identity of organisations".	Authentication of the identity of an organization that shall act as a CA or RA shall conform to the Level 3 requirements as specified in "HMG's minimum requirements for the verification of the identity of organisations". An additional check shall be made that the individuals involved appear in an appropriate personnel register[3].

[3] The personnel register refers to an official staff list for the organisation against which the individual(s) concerned can be checked.

3.1.9 Authentication of individual identity

3.1.9.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Authentication of the identity of an individual for the purposes of issuance of a digital signature end-entity certificate shall conform to the Level 2 requirements as specified in “HMG’s minimum requirements for the verification of the identity of individuals”. Additionally, the process documentation shall include a declaration of identity which shall be signed with a handwritten signature by the certificate applicant in the presence of the authorized person performing the identity authentication.	Authentication of the identity of an individual for the purposes of issuance of a digital signature end-entity certificate shall conform to the Level 3 requirements as specified in “HMG’s minimum requirements for the verification of the identity of individuals”. Additionally, the process documentation shall include a declaration of identity which shall be signed with a handwritten signature by the certificate applicant in the presence of the authorized person performing the identity authentication. An additional check shall be made of the individual against a personnel register.	Authentication of the identity of an individual for the purposes of issuance of a confidentiality end-entity certificate shall conform to the Level 2 requirements as specified in “HMG’s minimum requirements for the verification of the identity of individuals” or be verified by the use of a digital signature bound to that individual by an HMG Level 2 (or Level 3) certificate.	Authentication of the identity of an individual for the purposes of issuance of a confidentiality end-entity certificate shall conform to the Level 3 requirements as specified in “HMG’s minimum requirements for the verification of the identity of individuals” with an additional check to cross reference the individual against a personnel register. Alternatively, the individual could be verified by the use of a digital signature bound to that individual by an HMG Level 3 certificate.

3.1.10 Authentication of device identity

3.1.10.1 Authentication of the identity of a device or application shall be verified using appropriate documentation.

3.1.10.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The Representative of the device or application shall authenticate themselves, either as defined in Paragraph 3.1.8.1 or by using a digital signature corresponding to an HMG Level 2 (or Level 3) certificate.	The Representative of the device or application shall authenticate themselves, either as defined in Paragraph 3.1.8.1 or by using a digital signature corresponding to an HMG Level 3 certificate.	The Representative of the device or application shall authenticate themselves, either as defined in Paragraph 3.1.8.1 or by using a digital signature corresponding to an HMG Level 2 (or Level 3) certificate.	The Representative of the device or application shall authenticate themselves, either as defined in Paragraph 3.1.8.1 or by using a digital signature corresponding to an HMG Level 3 certificate.

3.2 Routine Rekey

3.2.1 A request for rekey may only be made by the Subject in whose name the certificate has been issued. This applies to certificates that have been issued to CAs, RAs and end-entities.

3.2.2 All requests for rekey must be authenticated by the CA, and the subsequent response must be authenticated by the Subject. This may be done by an on-line method in accordance with a standard protocol such as PKCS#10, as determined by the PMA. An Entity requesting digital signature rekey may authenticate the request for rekey by signing using its valid digital signature Private Key. An Entity requesting a confidentiality rekey can authenticate by correctly decrypting a challenge using its current confidentiality Private Key. If the Private Key has expired the request for rekey must be authenticated in the same manner as the initial registration.

3.2.3 A maximum of two consecutive on-line rekeys may take place between rekeys that shall be authenticated in the same manner as for initial registration.

3.3 Rekey after Revocation

3.3.1 Where the information contained in a certificate has changed or there is a known or suspected compromise of the Private Key, a CA or RA must authenticate a rekey in the same manner as for initial registration. Any change in the information contained in a certificate must be verified by the CA or the RA authorized to act on behalf of that CA before that certificate is issued.

3.4 Revocation Request

3.4.1 The list of entities that can request revocation is described in Section 4.4.3. A CA, or an RA acting on its behalf, must authenticate a request for revocation of a certificate. Requests to revoke a certificate may be authenticated using that certificate's associated public key, regardless of whether or not the Private Key has been compromised.

3.4.2 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 assurances that the person or organisation requesting revocation is, in fact, the Subscriber. A CA must 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.

3.4.3 Requests for revocation of certificates must be logged, as described in Section 4.5.

INTENTIONALLY BLANK

4 Operational Requirements

4.1 Certificate Application

4.1.1 Overview

4.1.1.1 All requests for certificates, where the CA is on-line, shall be accompanied by a digitally signed authorization from an authorized RA. This authorization may take the form of a digitally signed certificate request.

4.1.1.2 Bulk (i.e. more than five) requests for certificates shall be accompanied by two digitally signed authorizations from separate personnel within an authorized RA.

4.1.1.3 An application for a certificate does not oblige a CA to issue a certificate. A CA may decline to issue a certificate under this Certificate Policy in its absolute discretion and it is not obliged to give any reason for doing so.

4.1.1.4 All procedures for certificate application shall be documented in the CPS.

4.1.1.5 The following types of certificate can be applied for according to this Certificate Policy:

a. end-entity certificates;

b. CA certificates;

c. CA cross-certificates; and

d. RA certificates.

4.1.1.6 All Subscriber, RA and CA certificate applicants shall undergo a registration process which, prior to certificate issuance, will:

a. establish and prove the identity of the subject and of the Subscriber according to the registration procedures described in Section 3.1;

b. require proof of authorization to have a certificate;

c. require Subscriber applicants to verify the accuracy of information submitted in certificate requests;

d. require Subscriber applicants to read, understand and sign the Subscriber's Agreement;

e. require RA and CA applicants to agree and sign a Service Agreement with the CA;

f. submit a signed certificate request to the CA using a recognized standard protocol (e.g. PKCS#10), as approved by the PMA; and

g. require the applicant, where they have generated the key pair themselves, to prove possession of the Private Key corresponding to the public key contained in the certificate request, as described in Section 3.1.7.

4.1.1.7 Generally an RA will register the applicant of a certificate, but if the CA issues certificates directly (for example to an Operator of the CA), the CA must verify the identity of the applicant in the same way as an RA, as described in Section 3.

4.1.2 CA cross-certificate

4.1.2.1 Initial cross-certification with this Certificate Policy shall only be done by the HMG Root Authority and shall require authorization from the PMA. CAs underneath the HMG Root Authority shall only cross-certify with this Certificate Policy where the HMG Root Authority has already established a cross certification relationship. CAs underneath the HMG Root Authority may initiate cross-certification relationships with their own non-HMG certificate policies.

4.1.2.2 All CA cross-certificate applicants shall undergo an application process and, prior to certificate issuance, will submit to the PMA:

a. organisation information;

b. certification practice statement (CPS) and relevant certificate policies;

c. information regarding the PKI architecture, including information regarding existing trust relationships of the applicant;

d. information regarding the directory architecture;

e. information regarding the technical configuration and implementation of the PKI;

f. information on auditing practices and a copy of the most recent audit; and

g. information regarding the required trust relationship, including:

1. any proposed legal or service level agreements pertinent to the trust relationship; and
2. the required policy mappings to be put into place.

4.1.2.3 Cross-certification will require a detailed policy mapping assessment to be made and an external audit report to be produced confirming the adherence of the applicant to their certificate policy. A contract or Memorandum of Understanding (MoU) will be agreed and signed by the applicant and the CA. In addition to the signature of the contract or MoU, all CA cross-certificate applicants shall undergo an organizational registration process which, prior to the issuance of the cross-certificate, will:

a. establish and prove the identity of the Representative of the applicant organization according to the registration procedures described in Section 3.1;

b. establish and prove the identity of the applicant organization, according to the registration procedures described in Section 3.1;

c. submit a cross-certificate request to the CA using a recognized standard protocol (e.g. PKCS#10); and

d. require the applicant to prove possession of the Private Key corresponding to the public key contained in the certificate request, as described in Section 3.1.7.

4.2 Certificate Issuance

4.2.1 The issuance and publication of a certificate by a CA indicates approval of the certificate application by the CA to the level appropriate to the certificate.

4.2.2 Where the CA is on-line, the CA shall check the RA signature of the certificate request against a known list of authorized RAs.

4.2.3 The Subscriber will be informed that the certificate has been created, and will either be provided with the certificate directly or informed as to a location where they can obtain the certificate.

4.2.4 The CA must ensure that delivery of the trust point to Subscribers is achieved in a secure way, as detailed in Section 6.1.4.

4.3 Certificate Acceptance and Usage

4.3.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The following two events shall constitute an automatic acceptance of the certificate: a. the Subscriber has signed the Subscriber Agreement; and b. the Subject has proved possession of the Private Key associated with the Public Key contained in the certificate request, as specified in Section 3.1.7.		The following two events shall constitute an automatic acceptance of the certificate: a. the Subscriber has signed the Subscriber Agreement; and b. the Subscriber has received, or generated, the key pair.	

4.3.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Private keys shall be used with appropriately evaluated products, as specified in the Level 2 requirements in the latest release of the "e-Government Strategy Framework Policy and Guidelines: Assurance".	Private keys shall be used with appropriately evaluated products, as specified in the Level 3 requirements in the latest release of the "e-Government Strategy Framework Policy and Guidelines: Assurance".	Private keys shall be used with appropriately evaluated products, as specified in the Level 2 requirements in the latest release of the "e-Government Strategy Framework Policy and Guidelines: Assurance".	Private keys shall be used with appropriately evaluated products, as specified in the Level 3 requirements in the latest release of the "e-Government Strategy Framework Policy and Guidelines: Assurance".

4.4 Certificate Suspension and Revocation

4.4.1 Overview

4.4.1.1 If a certificate is reasonably suspected to be compromised it shall immediately (as per Section 4.4.5.1) be suspended and an investigation shall be invoked to determine the actual status of the certificate. In the event that compromise is confirmed, the certificate shall be immediately revoked (as per Section 4.4.5.1). If the investigation confirms that the suspicions of compromise are groundless, the certificate shall be un-suspended.

4.4.1.2 If requested by the Subscriber, a CA may revoke a certificate immediately on suspicion of compromise.

4.4.1.3 A CA may revoke a certificate immediately, without first suspending the certificate, if it can immediately be confirmed that the certificate has been compromised.

4.4.2 Circumstances for revocation

4.4.2.1 A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid by one of the entities listed in Section 4.4.3. Examples of circumstances that invalidate the binding are:

a. known compromise of the Private Key due to theft, loss, disclosure, modification or other compromise;

b. any misuse of keys and certificates;

c. known compromise of the media holding the Private Key;

d. information contained in the certificate changes;

e. a change in role (for example terminating employment with the employing organization) such that the certificate is no longer valid or authorized;

f. the determination by the CA or RA that the certificate was not properly issued in accordance with this Certificate Policy; and

g. it becomes apparent that any of the information submitted during registration is false.

4.4.2.2 A certificate shall be revoked when any of the following conditions is true:

a. a properly formatted request for revocation is received from an authorized party (as described in Section 4.4.3);

b. the registered proprietor of a registered trademark claims that a certificate infringes that trademark; or

c. an investigation into a suspended certificate has concluded that the certificate should be revoked.

4.4.2.3 A CA can revoke, at its discretion, if:

a. the Subscriber fails to abide by the Subscriber's agreement or does not comply with this Certificate Policy; or

b. the Subscriber or subject undergoes a change in role such that the certificate is no longer required.

4.4.3 Who can request revocation

4.4.3.1 The following entities can request revocation:

a. the Subscriber of the certificate (or Representative in the case of an application or device certificate);

b. RA personnel for certificates that have been issued by that RA;

c. CA personnel for certificates that have been issued by that CA; and

d. the PMA for any certificate.

4.4.4 Procedure for revocation request

4.4.4.1 Revocation requests must be authenticated, accountable and auditable.

4.4.4.2 Each CA shall describe the procedure for revocation in the CPS, which shall include:

a. an identification of the certificate to be revoked;

b. a clear statement of the reasons for revocation; and

c. the authentication of the requester of the revocation, as described in Section 3.4.

4.4.4.3 When revoking a certificate, checks will be made to verify that the certificate has not been used to re-issue replacement certificates (as specified in Sections 3.2 and 4.7); if the certificate has been used for certificate issuance after an actual or suspected compromise, these additional certificates shall also be revoked.

4.4.4.4 Once a revocation request has been received and authenticated, the certificate will be revoked and the revocation shall be published in the relevant CRL or ARL and made available to all Relying Parties. A CRL or ARL shall be published, even if an on-line status checking mechanism is additionally used.

4.4.5 Revocation request grace period

4.4.5.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
There is no grace period for revocation under this policy; CAs shall revoke certificates immediately upon receipt of a proper revocation request, within normal business hours.	There is no grace period for revocation under this policy; CAs shall revoke certificates immediately upon receipt of a proper revocation request. Revocation shall occur immediately, whether inside or outside normal business hours (i.e. 24x7x365). In very restricted circumstances, the PMA may authorize a CA to publish ARLs within normal business hours only.	There is no grace period for revocation under this policy; CAs shall revoke certificates immediately upon receipt of a proper revocation request, within normal business hours.	There is no grace period for revocation under this policy; CAs shall revoke certificates immediately upon receipt of a proper revocation request. Revocation shall occur immediately, whether inside or outside normal business hours (i.e. 24x7x365). In very restricted circumstances, the PMA may authorize a CA to publish ARLs within normal business hours only.

4.4.6 Circumstances for suspension

4.4.6.1 If a CA suspects, for whatever reason, that a certificate should be revoked for one of the circumstances described in Section 4.4.2, the CA shall immediately suspend the suspected certificate.

4.4.6.2 If a CA or RA certificate has been suspended due to reasons of suspected or actual compromise, fraud or misuse, the PMA shall be informed immediately. The PMA, or the CA on its behalf, shall conduct a thorough investigation, after which the PMA shall decide whether to:

a. restore the suspended certificate; or

b. revoke the suspended certificate.

4.4.6.3 If any certificate has been suspended or revoked for any reason, as described in Section 4.4.2, the PMA shall be informed as part of a regular (e.g. monthly, quarterly, etc.) reporting activity.

4.4.7 Who can request suspension

4.4.7.1 The following entities can request suspension:

a. RA personnel for certificates that have been issued by that RA;

b. CA personnel for certificates that have been issued by that CA; and

c. the PMA for any certificate.

4.4.8 Procedure for suspension request

4.4.8.1 Suspension requests must be authenticated, accountable and auditable.

4.4.8.2 Each CA shall describe the procedure for suspension in the CPS, which shall include:

a. an identification of the certificate to be suspended;

b. a clear statement of the reasons for suspension; and

c. the authentication of the requester of the suspension, as described in Section 3.4.

4.4.8.3 Once a suspension request has been received and authenticated, the certificate will be suspended and the suspension shall be published in the relevant CRL or ARL.

4.4.8.4 Un-suspension requests must be authenticated, accountable and auditable. Requests for un-suspension shall be made using an out-of-band method to the issuing CA and shall be accompanied by an explanation detailing the justification for un-suspension. The CA shall verify that there is no risk that the certificate has been compromised before proceeding with the un-suspension process.

4.4.9 Limits on suspension period

4.4.9.1 There is no limit on the period for which a certificate can be suspended.

4.4.10 CRL issuance frequency

4.4.10.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
ARLs shall be issued monthly, or immediately after revocation, subject to normal business hours. ARLs shall be issued each month, even if there has been no change since the previous month.	ARLs shall be issued monthly, or immediately after revocation at any time whether inside or outside business hours (i.e. 24x7x365). In very restricted circumstances, the PMA may authorize a CA to publish ARLs within normal business hours only. ARLs shall be issued each month, even if there has been no change since the previous month.	ARLs shall be issued monthly, or immediately after revocation, subject to normal business hours. ARLs shall be issued each month, even if there has been no change since the previous month.	ARLs shall be issued monthly, or immediately after revocation at any time whether inside or outside business hours (i.e. 24x7x365). In very restricted circumstances, the PMA may authorize a CA to publish ARLs within normal business hours only. ARLs shall be issued each month, even if there has been no change since the previous month.

4.4.10.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
CRLs shall be issued daily or immediately after revocation, subject to normal business hours. CRLs shall be issued each day, even if there has been no change since the previous day.	CRLs shall be issued daily or immediately after revocation at any time whether inside or outside business hours (i.e. 24x7x365). CRLs shall be issued each day, even if there has been no change since the previous day.	CRLs shall be issued daily or immediately after revocation, subject to normal business hours. CRLs shall be issued each day, even if there has been no change since the previous day.	CRLs shall be issued daily or immediately after revocation at any time whether inside or outside business hours (i.e. 24x7x365). CRLs shall be issued each day, even if there has been no change since the previous day.

4.4.10.3 If a revoked certificate expires, it may be removed from subsequent versions of the CRL or ARL, provided that the certificate has appeared in at least one CRL or ARL.

4.4.10.4 CAs shall use reasonable efforts to make CRLs and ARLs accessible to Relying Parties.

4.4.10.5 ARLs and CRLs shall continue to be available to Relying Parties for at least a year after publication, to enable the status of a certificate at the time it was used to be determined.

4.4.11 CRL checking requirements

4.4.11.1 Relying parties must check revocation status of any certificates on which they wish to rely, either by accessing the relevant CRLs and ARLs from the published source at the time of certificate validation, or through an on-line certificate status checking protocol such as OCSP.

4.4.11.2 Relying parties must check the authenticity and integrity of the CRL or ARL by:

a. verifying that the CRL or ARL has been digitally signed using the Private Key corresponding with the digital certificate purported to have been used;

b. verifying the validity of the digital certificate, using procedures described in the X.509 standard; and

c. establishing trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 standard.

4.4.11.3 If practical, the Relying Party shall check the subsequent CRL or ARL issued after the digital signature has been created to verify the on-going validity of the certificate that has been used.

4.4.11.4 If a CRL or ARL is temporarily not available, a certificate has no status or value until the CRL or ARL becomes available once more. The Relying Party can make an informed decision as to whether to reject the certificate, or whether to accept the increased risk, responsibility and consequences of accepting the certificate.

4.4.12 On-line revocation/status checking availability

4.4.12.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
CA and Relying Party client software may optionally support on-line status checking.	CA and Relying Party client software may optionally support on-line status checking. On-line status checking, if provided, shall be available at all times, whether inside or outside normal business hours (i.e. 24x7x365).	CA and Relying Party client software may optionally support on-line status checking.	CA and Relying Party client software may optionally support on-line status checking. On-line status checking, if provided, shall be available at all times, whether inside or outside normal business hours (i.e. 24x7x365).

4.4.13 On-line revocation checking requirements

4.4.13.1 An OCSP service must perform the same level of checks as to the status of the certificate as that which would be achieved by checking the published ARL or CRL and the same conditions apply.

4.4.14 Other forms of revocation advertisements available

4.4.14.1 Other forms of revocation advertisements may be used provided the following requirements are met:

a. the procedures shall be fully described in the CPS;

b. the method shall provide authentication and integrity services to the same level as provided by the CRL/ARL or OCSP approach; and

c. the same time constraints as apply as to the CRL/ARL or OCSP approach.

4.4.15 Checking requirements for other forms of revocation advertisements

4.4.15.1 Another revocation advertisement service must perform the same level of checks as to the status of the certificate as that which would be achieved by checking the published ARL or CRL and the same conditions apply.

4.4.16 Special requirements re key compromise

4.4.16.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
A Certificate holder shall inform the issuing RA or CA immediately, within the normal business hours of the CA, if there are reasonable grounds to suspect that the confidentiality of the Private Key has been compromised.	A Certificate holder shall inform the issuing RA or CA immediately, whether inside or outside normal business hours, if there are reasonable grounds to suspect that the confidentiality of the Private Key has been compromised.	A Certificate holder shall inform the issuing RA or CA immediately, within the normal business hours of the CA, if there are reasonable grounds to suspect that the confidentiality of the Private Key has been compromised.	A Certificate holder shall inform the issuing RA or CA immediately, whether inside or outside normal business hours, if there are reasonable grounds to suspect that the confidentiality of the Private Key has been compromised.

4.4.16.2 If a CA key is compromised, or is suspected of compromise, the CA must immediately notify all parties to which it has issued certificates.

4.4.16.3 A CA must ensure that its CPS contains provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

4.5.1.1 As a minimum, the following events shall be recorded in the audit log[4]:

a. any logon or logoff attempts by RA or CA operators;

b. messages received from any source requesting RA/CA action (e.g. certificate requests, certificate revocation requests, etc.);

c. actions taken in response to requests;

[4] The term ‘audit log’ as used in this document refers to the data that is collected in preparation for an audit, rather than the log of the audit process itself. This use of terminology is compatible with RFC2527 and BS ISO/IEC 17799. This data is sometimes referred to as ‘accounting logs’.

d. physical access to, loading, zeroizing, transferring keys to or from, backing up, acquiring or destroying cryptographic modules;

e. receipt, servicing (e.g. keying or other cryptologic manipulations), and shipping hardware cryptographic modules;

f. publishing of any material to a repository;

g. anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages;

h. any known or suspected violations of physical security, suspected or known attempts to attach the CA or RA equipment;

i. server installation, access or modification;

j. system start-up and shutdown;

k. RA/CA application start-up and shutdown;

l. CA equipment access (e.g. room access);

m. file manipulation and account management;

n. any use of the CA signing key;

o. checks made during the registration process; and

p. personnel changes.

4.5.1.2 For each event, the following information shall be recorded:

a. type of event;

b. date and time of the event;

c. message source, destination and contents, where relevant;

d. success or failure indication, where relevant; and

e. the identity of the entity that caused the event.

4.5.1.3 Private keys shall not under any circumstances be recorded in the audit log.

4.5.1.4 Each CA and RA shall enable any accounting or audit capability of the underlying OS on which software relating to this PKI operates.

4.5.2 Frequency of processing log

4.5.2.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The audit log must be reviewed weekly in order to verify that: a. the log has not been tampered with; b. the logging is working correctly; and c. no anomalies have been detected (by briefly scanning each entry).	The audit log must be reviewed daily in order to verify that: a. the log has not been tampered with; b. the logging is working correctly; and c. no anomalies have been detected (by briefly scanning each entry).	The audit log must be reviewed weekly in order to verify that: a. the log has not been tampered with; b. the logging is working correctly; and c. no anomalies have been detected (by briefly scanning each entry).	The audit log must be reviewed daily in order to verify that: a. the log has not been tampered with; b. the logging is working correctly; and c. no anomalies have been detected (by briefly scanning each entry).

4.5.2.2 The audit log may be reviewed less frequently if compensated by enhanced personnel and physical security measures, and if specifically approved in writing by the PMA.

4.5.2.3 A more detailed study of each suspect entry shall be undertaken if any anomalies are detected in the initial review.

4.5.2.4 All actions taken shall be documented.

4.5.3 Retention period for audit log

4.5.3.1 Each CA shall retain a copy of the audit log on-site for at least 2 months; after this period the audit log shall be archived as described in Section 4.6.

4.5.4 Protection of audit log

4.5.4.1 Access to the audit log shall be read-only and shall be limited to the system security officer (SSO), the system administrator and, during an audit, the auditor. Protection mechanisms shall be put into place to enforce this.

4.5.5 Audit log backup procedures

4.5.5.1 Audit logs shall be backed up daily, or whenever activity has taken place at the CA in the event of infrequent use, as part of the same schedule as the regular backup of the CA database.

4.5.5.2 If audit logs are held in a physical form, they shall also be backed up daily, or whenever activity has taken place at the CA in the event of infrequent use, through photocopy or other means.

4.5.5.3 Incremental backups are permitted; a maximum of ten incremental backups may be taken before a full backup is required.

4.5.5.4 All audit log backups, whether electronic or physical, shall be held in a separate site at least 25 kilometers from the primary copy of the audit logs. The security of the audit log backup shall be at least as strong as for the primary copy of the audit logs.

4.5.6 Audit collection system

4.5.6.1 The CA audit collection system shall be documented in the CPS.

4.5.7 Notification to event-causing subject

4.5.7.1 A person causing an audit event will not be notified separately that information concerning the audit event and that person will be retained.

4.5.8 Vulnerability assessments

4.5.8.1 Events in the audit process are logged, in part, to monitor system vulnerabilities. The CA must ensure that a vulnerability assessment is performed prior to live operation. This vulnerability assessment shall be reviewed and revised in the event that security issues are identified in the examination of these monitored events.

4.6 Records Archival

4.6.1 Types of event recorded

4.6.1.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The events and accompanying data described in Section 4.5.1 shall be recorded in the archive. All issued CRLs and ARLs shall be archived. Digital Signature Private Keys shall not be recorded in the archive.		The events and accompanying data described in Section 4.5.1 shall be recorded in the archive. All issued CRLs and ARLs shall be archived. Confidentiality Private Keys may be archived by the RA, CA or the Subscriber.	

4.6.2 Retention period for archive

4.6.2.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Archive records shall be kept for a period of at least seven years without any loss of data. Applications necessary to read these archives must be maintained for at least the applicable retention period above.	Archive records shall be kept for a period of at least 25 years without any loss of data. Applications necessary to read these archives must be maintained for at least the applicable retention period above.	Archive records shall be kept for a period of at least seven years without any loss of data. Applications necessary to read these archives must be maintained for at least the applicable retention period above.	Archive records shall be kept for a period of at least 25 years without any loss of data. Applications necessary to read these archives must be maintained for at least the applicable retention period above.

4.6.3 Protection of archive

4.6.3.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Protection shall either be physical security alone, or a combination of physical security and cryptographic protection. The archive shall also be protected from environmental factors such as temperature, humidity and magnetism.		Protection shall either be physical security alone, or a combination of physical security and cryptographic protection. If confidentiality Private Keys are archived, cryptographic protection appropriate for a Level 2 confidentiality requirement shall be used. The archive shall also be protected from environmental factors such as temperature, humidity and magnetism.	Protection shall either be physical security alone, or a combination of physical security and cryptographic protection. If confidentiality Private Keys are archived, cryptographic protection appropriate for a Level 3 confidentiality requirement shall be used. The archive shall also be protected from environmental factors such as temperature, humidity and magnetism.

4.6.3.2 The archive shall only be accessible to, and accessed by, authorized personnel. No user shall be able to write to, modify, or delete the archive.

4.6.4 Archive backup procedures

4.6.4.1 The archive shall be backed up in a second physical location at a distance of at least 25 kilometres from the main archive. Protection shall be to the same level as required at the primary site.

4.6.5 Requirements for time-stamping of records

4.6.5.1 It shall be possible to verify the date and time, in hours, minutes and seconds, of every electronic record. It shall be possible to verify the date and time, in hours and minutes, of every non-electronic record.

4.6.5.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The system clocks on all platforms associated with the issuing of certificates, CRLs or ARLs at RAs and CAs shall be synchronized to within an accuracy of ten seconds.	The system clocks on all platforms associated with the issuing of certificates, CRLs or ARLs at RAs and CAs shall be synchronized to within an accuracy of ten seconds, preferably taking the source from the British MSF Time Signal Transmitter, transmitted by the National Physics Laboratory at Rugby.	The system clocks on all platforms associated with the issuing of certificates, CRLs or ARLs at RAs and CAs shall be synchronized to within an accuracy of ten seconds.	The system clocks on all platforms associated with the issuing of certificates, CRLs or ARLs at RAs and CAs shall be synchronized to within an accuracy of ten seconds, preferably taking the source from the British MSF Time Signal Transmitter, transmitted by the National Physics Laboratory at Rugby.

4.6.6 Archive collection system

4.6.6.1 The CA and RA archive collection system shall be documented in the CPS.

4.6.7 Procedures to obtain and verify archive information

4.6.7.1 CAs and RAs shall ensure that the integrity of backups is verified at least every 6 months. The integrity of archived material that is stored off-site shall be verified at least annually. The procedures for verification shall be stated in the CPS.

4.7 Key Changeover

4.7.1 A Subscriber may only apply to renew his or her key pair within a period of time determined by the CA, prior to the expiration of one of the keys, provided the previous certificate has not been revoked. A Subscriber, the CA, or the RA may initiate this key changeover process. Automated key changeover is permitted. A CA must ensure that the details of this process are indicated in its CPS.

4.7.2 Where a Subscriber's certificate has been revoked as a result of non-compliance, the CA must verify that any reasons for non-compliance have been addressed to its satisfaction prior to certificate re-issuance.

4.7.3 Keys shall not be renewed using keys that have already expired. Subscribers without valid keys must be re-authenticated by the CA or RA in the same manner as the initial registration.

4.7.4 CAs shall not issue certificates that extend beyond the expiry dates of their own certificates and public keys.

4.7.5

<table>
<tr><th>Level 2 Digital Signature Policy</th><th>Level 3 Digital Signature Policy</th><th>Level 2 Confidentiality Policy</th><th>Level 3 Confidentiality Policy</th></tr>
<tr><td colspan="2">On key changeover a new key-pair shall be generated and a new certificate published. The old digital signature key remains valid for verifying signatures produced prior to changeover.</td><td colspan="2">On key changeover a new key-pair shall be generated and a new certificate published. The old confidentiality key remains valid for decrypting documents that have been encrypted prior to changeover.</td></tr>
</table>

4.8 Compromise and Disaster Recovery

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

4.8.1.1 In the event of a disaster, where a CA installation is damaged and becomes inoperative, that CA installation shall preferably be rolled back and recovered to a known state with priority given to:

a. the availability of all previously issued CRLs and ARLs; and

b. the ability to revoke certificates.

4.8.1.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
If the CA cannot re-establish revocation capabilities within one week, it must report its keys as potentially compromised, to be suspended if necessary. The PMA may grant extensions to CAs on a case-by-case basis.	If the CA cannot re-establish revocation capabilities within one day, it must report its keys as potentially compromised, to be suspended if necessary. The PMA may grant extensions to CAs on a case-by-case basis.	If the CA cannot re-establish revocation capabilities within one week, it must report its keys as potentially compromised, to be suspended if necessary. The PMA may grant extensions to CAs on a case-by-case basis.	If the CA cannot re-establish revocation capabilities within one day, it must report its keys as potentially compromised, to be suspended if necessary. The PMA may grant extensions to CAs on a case-by-case basis.

4.8.1.3 If all copies of the CA signature key are destroyed, the PMA shall revoke the CA certificate and all subordinate certificates. The CA installation shall be rebuilt from the start, by re-establishing the CA equipment and, where necessary, re-issuing the CA certificate, all cross-certificates, and all subordinate certificates.

4.8.1.4 If a certificate between the CA certificate and the HMG Root Authority certificate is revoked, the CA shall notify all end entities and subordinate CAs of this fact.

4.8.1.5 A report of the disaster event shall be made by the CA and made available to the PMA. This report shall include

a. an assessment of the impact of this disaster;

b. an assessment of whether and to what degree compromise of the confidentiality, integrity of availability of confidential information (as defined in Section 2.8.1) has taken place;

c. a description of the actions taken to restore the CA;

d. a description of the results of those actions; and

e. a description of the level of service that has been restored, including the time at which the service was restored.

4.8.2 Entity or CA public key is revoked

4.8.2.1 In the event of the need for revocation of a CA's certificate, the CA must immediately notify:

a. the PMA;

b. all CAs to whom it has issued certificates;

c. all of its RAs;

d. all Subscribers to whom it has issued certificates; and

e. all Representatives.

4.8.2.2 The CA must also:

a. publish the certificate serial number on an appropriate CRL or ARL; and

b. revoke all cross-certificates signed with the revoked certificate if the revoked certificate has, or is suspected to have, been compromised.

4.8.2.3 After addressing the factors that led to revocation, the CA may, if necessary and with the approval of the PMA:

a. generate a new CA signing key pair; and

b. re-issue certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

4.8.2.4 Revocation issues associated with other types of certificate are described in Section 4.4.

4.8.3 Entity or CA key is compromised

4.8.3.1 In the event of a compromise of the Private Key of a CA, the certificate shall be revoked in accordance with Section 4.4.4 of this policy and the revocation reported in accordance with Section 4.8.2 or this policy.

4.8.3.2 Compromise issues associated with other types of certificate are described in Section 4.4.

4.8.4 Secure facility after a natural or other type of disaster

4.8.4.1 A CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the CA, a CA must ensure that any agreement with the repository provider includes the requirement that a disaster recovery plan be established, tested and documented by the repository.

4.8.4.2 In developing disaster recovery plans, priority shall be given to:

a. the availability of all previously issued CRLs and ARLs; and

b. the ability to revoke certificates.

4.9 CA Termination

4.9.1 Prior to termination, CAs shall provide archived data to a PMA approved archival facility.

4.9.2 In the event that a CA ceases operation, it must notify its Subscribers in writing at least one month before termination of operations and arrange for the continued retention of the CA's keys and information. It must also notify in writing at least one month before termination of operations, all CA's with whom it is cross-certified.

4.9.3 In the event of a change in management of a CA's operations, the CA must notify in writing all Entities for which it has issued certificates and CA's with whom it has cross-certified.

4.9.4 The CA archives should be retained in the manner and for the time indicated in Section 4.6.2.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site location and construction

5.1.1.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
As a minimum, the location and construction of the facility that will house RA and CA equipment and operational procedures shall be equivalent to that required to protect material with an HMG Protective Marking of RESTRICTED. Appendix C contains guidance on these requirements.	As a minimum, the location and construction of the facility that will house RA and CA equipment and operational procedures shall be equivalent to that required to protect material with an HMG Protective Marking of CONFIDENTIAL. Appendix C contains guidance on these requirements.	As a minimum, the location and construction of the facility that will house RA and CA equipment and operational procedures shall be equivalent to that required to protect material with an HMG Protective Marking of RESTRICTED. Appendix C contains guidance on these requirements.	As a minimum, the location and construction of the facility that will house RA and CA equipment and operational procedures shall be equivalent to that required to protect material with an HMG Protective Marking of CONFIDENTIAL. Appendix C contains guidance on these requirements.

5.1.2 Physical access

5.1.2.1 Physical access requirements are covered by the site location and construction policy statements in Section 5.1.1 of this document. Typically, this includes the following:

a. a CA shall permit entry to its secure operating area only to authorised personnel, and to visitors under the constant supervision of an authorised person; and

b. the number of personnel authorised to enter the area shall be kept to a minimum and a log shall be maintained of all visitor accesses.

5.1.3 Power and air conditioning

5.1.3.1 No stipulation.

5.1.4 Water exposures

5.1.4.1 No stipulation.

5.1.5 Fire prevention and protection

5.1.5.1 No stipulation.

5.1.6 Media storage

5.1.6.1 All magnetic and optical media containing CA and RA information, including backup media, shall be stored in containers, cabinets or safes with fire protection capabilities, and shall be located in a secure storage area. The containers, cabinets or safes shall conform to LPS1183-4 or equivalent, with a Resistance Grade as specified by the PMA.

5.1.7 Waste disposal

5.1.7.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Paper documents and magnetic or optical media containing the CA or RA Private Key, or commercially sensitive or confidential information, shall be securely disposed of such that: a. the disposal is witnessed and recorded; and b. reconstitution is unlikely.	Paper documents and magnetic or optical media containing the CA or RA Private Key, or commercially sensitive or confidential information, shall be securely disposed of such that: a. the disposal is witnessed and recorded; b. retrieval or reconstitution is unlikely; and c. attempted retrieval or reconstitution is likely to be detected.	Paper documents and magnetic or optical media containing the CA or RA Private Key, or commercially sensitive or confidential information, shall be securely disposed of such that: a. the disposal is witnessed and recorded; and b. reconstitution is unlikely.	Paper documents and magnetic or optical media containing the CA or RA Private Key, or commercially sensitive or confidential information, shall be securely disposed of such that: a. the disposal is witnessed and recorded; b. retrieval or reconstitution is unlikely; and c. attempted retrieval or reconstitution is likely to be detected.

5.1.8 Off-site backup

5.1.8.1 Off site storage may be used for the storage and retention of backup software and data.

5.1.8.2 Where used, off site storage shall:

a. be available to authorised personnel during the hours of operation of the CA, for the purpose of retrieving software and data; and

b. have appropriate levels of security in place, equivalent to the main CA site.

5.2 Procedural Controls

5.2.1 Trusted roles

5.2.1.1 A CA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection. Each user's system access is to be limited to those actions for which they are required to perform in fulfilling their responsibilities.

5.2.1.2 At a minimum, the following roles shall be established:

a. CA or RA System Administrator;

b. CA or RA Operator;

c. System Auditor; and

d. System Security Officer (SSO).

5.2.1.3 The CA or RA Administrator is responsible for system administration, including configuration changes and management of user accounts.

5.2.1.4 The CA or RA Operator has responsibility for day to day operation of the facility (e.g. generation of certificates, publication of CRLs/ARLs, etc.).

5.2.1.5 The System Auditor has responsibility for auditing the operation of the CA or RA, as described in Section 4.5 of this Certificate Policy.

5.2.1.6 The System Security Officer (SSO) has overall responsibility for system security, including the review of audit logs and taking the appropriate corrective action.

5.2.2 Number of persons required per task

5.2.2.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Separate individuals should fill each of the three roles: System Administrator, Operator and SSO. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However, if staffing levels do not permit this: a. a single individual may assume the roles of the System Administrator and Operator; and b. the SSO shall always remain separate from the System Administrator, in order to provide an independent review of the audit log.	Separate individuals shall fill each of the three roles: System Administrator, Operator and SSO. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation.	Separate individuals shall fill each of the three roles: System Administrator, Operator and SSO. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However, if staffing levels do not permit this: a. a single individual may assume the roles of the System Administrator and Operator; and b. the SSO shall always remain separate from the System Administrator, in order to provide an independent review of the audit log.	Separate individuals shall fill each of the three roles: System Administrator, Operator and SSO. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation.

5.2.2.2 A CA must ensure that no single individual may gain direct access to CA Private Keys.

5.2.2.3 At a minimum two individuals, using a split-knowledge technique such as twin passwords, must perform any CA system start-up, CA system shutdown, key backup or key recovery operation.

5.2.2.4 Two individuals are required for submission of bulk certificate requests from an RA, as described in Section 4.1.

5.2.3 Identification and authentication for each role

5.2.3.1 When accessing RA or CA systems, all RA and CA personnel shall authenticate themselves using a trusted token such as a smart card, which meets a sufficient level of trust as defined in the PMA internal policy. In very restricted circumstances, where there are increased physical and personnel security measures, the PMA may authorize an RA or CA to allow personnel to authenticate themselves using other mechanisms.

5.2.3.2 All RA and CA personnel must have their identity and authorization verified (as specified in Section 5.3 of this Certificate Policy) before they are:

a. included in the access list for the CA site;

b. included in the access list for physical access to the CA system;

c. given a certificate for the performance of their CA role; and

d. given an account on the PKI system.

5.2.3.3 Each of these certificates and accounts (with the exception of CA signing certificates) must:

a. be directly attributable to an individual;

b. not be shared; and

c. be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

5.2.3.4

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
CA operations must be secured, using mechanisms such as token-based strong authentication and encryption conforming to IAG Level-3, when accessed across a shared network.	CA operations must not be accessed across a shared network.	CA operations must be secured, using mechanisms such as token-based strong authentication and encryption conforming to IAG Level-3, when accessed across a shared network.	CA operations must not be accessed across a shared network.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

5.3.1.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
All CA personnel shall have a clearance of at least Basic Check (BC) or equivalent. Maintenance personnel for the CA shall either have a Basic Check (BC) or shall be escorted at all times when on site.	All CA personnel shall have a clearance of at least Security Check (SC) or equivalent. Maintenance personnel for the CA shall either have a Security Check (SC) or shall be escorted at all times when on site.	All CA personnel shall have a clearance of at least Basic Check (BC) or equivalent. Maintenance personnel for the CA shall either have a Basic Check (BC) or shall be escorted at all times when on site.	All CA personnel shall have a clearance of at least Security Check (SC) or equivalent. Maintenance personnel for the CA shall either have a Security Check (SC) or shall be escorted at all times when on site.

5.3.2 Background check procedures

5.3.2.1 Checks appropriate to the clearance level defined in 5.3.1 shall be carried out according to local policy.

5.3.3 Training requirements

5.3.3.1 Appropriate training shall be provided for all personnel, and a training plan shall be produced.

5.3.3.2 Training shall cover the following aspects:

a. PKI concepts;

b. an explanation of the risks associated with the PKI;

c. the use and operation of the CA software;

d. documented CA procedures;

e. computer security awareness and procedures;

f. how to explain to Subscribers the responsibilities adhering to the possession, use and operation of their key pairs; and

g. the meaning and effect of this Certificate Policy and the relevant CPS.

5.3.4 Retraining frequency and requirements

5.3.4.1 Any significant change in CA operation shall have a training plan. The execution of the training plan shall be documented.

5.3.5 Job rotation frequency and sequence

5.3.5.1 Job rotation frequency and sequence shall be described in the CPS.

5.3.6 Sanctions for unauthorized actions

5.3.6.1 Appropriate disciplinary actions shall be undertaken if this policy is violated.

5.3.7 Contracting personnel requirements

5.3.7.1 Requirements for contractors and other non-HMG staff are the same as for HMG employees, as specified in Sections 5.3.1 through 5.3.6.

5.3.7.2 PKI service providers who provide services to HMG shall establish procedures to ensure that any subcontractors perform in accordance with this policy and the relevant CPS.

5.3.8 Documentation supplied to personnel

5.3.8.1 Personnel must be supplied with sufficient documentation and training in order to perform their job responsibilities competently and satisfactorily.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

6.1.1.1 The HMG Root Authority private signing key shall be generated by CESG, using imported CESG-generated entropy to seed the random number generator.

6.1.1.2 All other CA and RA private signature keys may be generated by the CA or RA itself, or may be generated by CESG and imported to the CA or RA.

6.1.1.3

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
All CA and RA key pairs shall be generated using equipment that has been evaluated according to FIPS140 to a level approved by the PMA, or evaluated to CWA 14167-2. If the CA or RA is connected to a network, key pair generation must be performed in hardware.	All CA and RA key pairs shall be generated using equipment that has been evaluated according to FIPS140 to a level approved by the PMA, or evaluated to CWA 14167-2:2002. If an RA is connected to a network, key pair generation must be performed in hardware.	All CA and RA key pairs shall be generated using equipment that has been evaluated according to FIPS140 to a level approved by the PMA, or evaluated to CWA 14167-2. If the CA or RA is connected to a network, key pair generation must be performed in hardware.	CA and RA key pairs used for certificate or CRL/ARL signing shall be generated using equipment that has been evaluated according to FIPS140 to a level approved by the PMA, or evaluated to CWA 14167-2. CA and RA key pairs used for key or data confidentiality shall be generated using equipment that has been CAPS-approved to BASELINE grade. If an RA is connected to a network, key pair generation must be performed in hardware.

6.1.1.4

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Subscribers' private signature keys shall always be generated by the subject themselves and may be generated using software using a PMA-approved algorithm. Random input from the subject such as typing using a keyboard or moving the mouse for a period of time, or a source of random entropy approved by the PMA, is required to seed the random number generation.	Subscribers' private signature keys shall always be generated by the subject themselves and shall be generated on a secure token, as defined in Section 6.1.8. Random input from the subject such as typing using a keyboard or moving the mouse for a period of time, or a source of random entropy approved by the PMA, is required to seed the random number generation.	Subscribers' confidentiality key pairs shall be generated by the Subscriber, RA or CA using equipment that has been evaluated according to FIPS140, to a level approved by the PMA.	Subscribers' confidentiality key pairs shall be generated by the Subscriber, RA or CA using equipment that has been CAPS-approved to BASELINE grade.

6.1.2 Private key delivery to entity

6.1.2.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Digital Signature Private Key delivery to Subscribers is not applicable as Subscribers shall always generate key pairs themselves.		If the key pair has been generated by the CA or RA, confidentiality Private Keys shall be delivered to end entities either by an on-line transaction in accordance with RFC 2510 encrypted using a public key from an HMG Level 2 certificate, or by an accountable out-of-band method approved by the PMA.	If the key pair has been generated by the CA or RA, confidentiality Private Keys shall be delivered to end entities either by an on-line transaction in accordance with RFC 2510 encrypted using a public key from an HMG Level 3 certificate, or by an accountable out-of-band method approved by the PMA.

6.1.2.2 If a Private Key is delivered to a CA it will be divided into two or more parts, with each part delivered by separate personnel. The Private Key components may be sent by registered post, or, if applicable, delivered manually.

6.1.3 Public key delivery to certificate issuer

6.1.3.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Delivery of digital signature public keys shall be achieved with a certificate request using a recognized standard protocol (e.g. PKCS#10).		If confidentiality key pairs are generated by the Subscriber, delivery of public keys shall be achieved with a certificate request using a recognized standard protocol (e.g. PKCS#10).	

6.1.4 CA public key delivery to users

6.1.4.1 The delivery of the CA public key to end entities must be performed in a secure manner in order to guarantee the integrity of the public key, such as:

a. manual delivery;

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
b. secure on-line delivery of the trust point which has been encrypted using a public key from an HMG Level 2 (or Level 3) certificate;	secure on-line delivery of the trust point which has been encrypted using a public key from an HMG Level 3 certificate;	secure on-line delivery of the trust point which has been encrypted using a public key from an HMG Level 2 (or Level 3) certificate;	secure on-line delivery of the trust point which has been encrypted using a public key from an HMG Level 3 certificate;

c. delivery using secure internal systems; or

d. on-line delivery of the public key using an out-of-band method to verify the integrity of the public key using a PMA-approved hash function.

6.1.5 Key size

6.1.5.1 The RSA key length shall be at least 1024 bits.

6.1.5.2 The DSA key length shall be 1024 bits.

6.1.6 Public key parameters generation

6.1.6.1 A CA must generate parameters in accordance with HMG cryptographic policy, as approved by the PMA, on a case-by-case basis.

6.1.7 Parameter quality checking

6.1.7.1 The quality of the parameters will be verified in accordance with HMG cryptographic policy, as approved by the PMA, on a case-by-case basis.

6.1.8 Hardware/software key generation

6.1.8.1 CA and RA keys shall be generated by an approved process seeded from an approved entropy source. Both process and entropy source shall be approved by the PMA on a case-by-case basis.

6.1.8.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Keys generated by the Subscriber may be generated in software, but must be generated either offline or on a secure network that meets the Level-2 requirements specified in the latest release of the “e-Government Strategy Framework Policy and Guidelines: Network Defence”.	Keys generated by the Subscriber shall be generated on a secure hardware token that has been evaluated according to FIPS140 to a level approved by the PMA, or to EAL4+ according to CWA 14169:2002.	Keys generated by the Subscriber, or on behalf of the Subscriber by the CA or RA, may be generated in either hardware or software that has been evaluated according to FIPS140, to a level approved by the PMA.	Keys generated by the Subscriber, or on behalf of the Subscriber by the CA or RA, shall be generated in either hardware or software, using equipment that has been CAPS-approved to BASELINE grade.

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

6.1.9.1

<table>
<tr><th>Level 2 Digital Signature Policy</th><th>Level 3 Digital Signature Policy</th><th>Level 2 Confidentiality Policy</th><th>Level 3 Confidentiality Policy</th></tr>
<tr><td colspan="2">End entity keys may be used only for authentication and message integrity and may not be used for confidentiality purposes. CA signing keys are the only keys permitted to be used for signing certificates and CRLs/ARLs.</td><td colspan="2">End entity keys may be used only for confidentiality and may not be used to provide authentication and message integrity services. CA signing keys are the only keys permitted to be used for signing certificates and CRLs/ARLs.</td></tr>
</table>

6.1.9.2 The certificate KeyUsage field must be used in accordance with PKIX-1 Certificate and CRL Profile.

6.1.9.3

<table>
<tr><th>Level 2 Digital Signature Policy</th><th>Level 3 Digital Signature Policy</th><th>Level 2 Confidentiality Policy</th><th>Level 3 Confidentiality Policy</th></tr>
<tr><td colspan="2">The following KeyUsage values must be present in digital signature certificates: Digital Signature and Non-Repudiation. CA certificates may omit the Digital Signature and Non-Repudiation KeyUsage values. Furthermore, the following KeyUsage values must not be present in digital signature certificates: keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, or decipherOnly.</td><td colspan="2">At least one of the following KeyUsage values must be present in confidentiality certificates: keyEncipherment, dataEncipherment. Furthermore, the following KeyUsage values must not be present in confidentiality certificates: Digital Signature and Non-Repudiation.</td></tr>
</table>

6.1.9.4

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
The presence of the Non-Repudiation bit signifies that the certificate may be used as a component of a non-repudation service, up to Level 2, as defined in the latest release of the “e-Government Trust Services Strategy Framework Policy and Guidelines”. However, the act of signing a document does not, in itself, provide a non-repudiation service.	The presence of the Non-Repudiation bit signifies that the certificate may be used as a component of a non-repudation service, up to Level 3, as defined in the latest release of the “e-Government Trust Services Strategy Framework Policy and Guidelines”. However, the act of signing a document does not, in itself, provide a non-repudiation service.	n/a	

6.1.9.5 The following additional values must be present in CA certificate-signing certificates: Key Cert Sign, and CRL Sign. These values must not be present in end-entity certificates.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

6.2.1.1 CA and RA keys must be stored within a hardware module assured to EAL4. All CA and RA cryptographic operations must be performed within this hardware module.

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

6.2.2.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Private Keys need not be under “n out of m” multi-person control. However, CAs shall maintain a policy of no lone physical access to the CA’s Private Key by individuals, with some operations requiring two personnel (as described in Section 5.2).	CA Private Keys shall be under “n out of m” multi-person control, where both n and m are 2 or greater.	Private Keys need not be under “n out of m” multi-person control. However, CAs shall maintain a policy of no lone physical access to the CA’s Private Key by individuals, with some operations requiring two personnel (as described in Section 5.2).	CA Private Keys shall be under “n out of m” multi-person control, where both n and m are 2 or greater.

6.2.3 Private key escrow

6.2.3.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Digital Signature Private Keys shall not be escrowed.		Confidentiality Private Keys may be escrowed and any recovery of an escrowed key will occur under the key recovery policy described in Paragraphs 6.2.3.2 and 6.2.3.4. The level of protection of the escrow data shall be equivalent to that required for protection of data with a Level 3 confidentiality requirement as defined in the latest release of the "e-Government confidentiality strategy framework policy and guidelines".	Confidentiality Private Keys may be escrowed and any recovery of an escrowed key will occur under the key recovery policy described in Paragraphs 6.2.3.2 and 6.2.3.4. Escrowed keys may not be stored on any network. The level of physical protection of the escrow data shall be equivalent to that required for protection of data with a protective marking of CONFIDENTIAL. Appendix C contains guidance on these requirements.

6.2.3.2 The following entities can request the recovery of an escrowed Private Key:

a. the Subject of the certificate;

b. an authorized individual belonging to the Subscriber organization; and

c. a nominated individual or organization identified by the Subscriber on issuance of the certificate.

6.2.3.3 Privacy rights will be respected subject to the applicable laws, as stated in Paragraphs 2.8.4.1 and 2.8.5.1.

6.2.3.4 When key recovery is requested the individual, and if necessary the relevant organization, shall be authenticated to the CA using the same mechanisms for authentication as required for the original issue and described in Sections 3.1.8 and 3.1.9.

6.2.4 Private key backup

6.2.4.1 Backup CA Private Keys shall be stored in encrypted form. CA database backups shall be maintained in secure storage, where the security of the backup site shall be at least as secure as the security of the main CA database. CA database backups shall be stored at a distance of at least 25 kilometers from the main CA database.

6.2.4.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
A Subscriber may optionally back up their Private Key. The copy of the Private Key shall only be accessible by the certificate subject and shall be kept at least as secure as the primary copy.	A Subscriber shall not back up their Private Key.	A Subscriber may optionally back up their Private Key. The copy of the Private Key shall be kept at least as secure as the primary copy.	

6.2.5 Private key archival

6.2.5.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Digital Signature Private Keys shall not be archived.		Confidentiality Private Keys may be archived by the CA and the level of physical and cryptographic protection of such an archive shall be as defined in Section 4.6	

6.2.6 Private key entry into cryptographic module

6.2.6.1 When a Private Key is not generated within a cryptographic module, it shall be delivered to the module in a secure manner, either using PKIX compliant key management protocol or in a manner approved by the PMA.

6.2.7 Method of activating Private Key

6.2.7.1 The cryptographic module shall require the successful completion of an authentication process, which may involve the use of a password or digital credentials, before activating the Private Key. A deactivated key shall be kept encrypted, or otherwise secured within the cryptographic module, to prevent unauthorised access.

6.2.8 Method of deactivating Private Key

6.2.8.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
When keys are deactivated they shall be cleared from memory by overwriting with random data before the memory is de-allocated. Any disk space where keys were stored shall be over-written before the space is released to the operating system. The cryptographic module shall automatically deactivate the Private Key after a pre-set period of inactivity.	End entity Private Keys shall be held within the secure token and shall not be held directly in memory. When CA Private Keys held in memory are deactivated, they shall be cleared from memory by overwriting with random data before the memory is de-allocated. Any disk space where keys were stored shall be over-written before the space is released to the operating system. The cryptographic module shall automatically deactivate the Private Key after a pre-set period of inactivity.	When keys are deactivated they shall be cleared from memory by overwriting with random data before the memory is de-allocated. Any disk space where keys were stored shall be over-written before the space is released to the operating system. The cryptographic module shall automatically deactivate the Private Key after a pre-set period of inactivity.	

6.2.9 Method of destroying Private Key

6.2.9.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Upon termination of use of a Private Key, all copies of the Private Key in computer memory and shared disk space must be securely destroyed by over-writing. The method of over-writing must be approved by the PMA.	End-entity Private Keys and CA keys stored in tokens shall be destroyed through destruction of the token, by disintegration, incineration, pulverisation, shredding or melting. CA Private Keys stored in memory shall be destroyed by over-writing. The method of over-writing must be approved by the PMA. When disks are disposed of that have held CA Private Keys, they must by purged in accordance with HMG Infosec Standard Number 5, or destroyed by disintegration, incineration, pulverisation, shredding or melting.	Upon termination of use of a Private Key, all copies of the Private Key in computer memory and shared disk space must be securely destroyed by over-writing. The method of over-writing must be approved by the PMA.	Upon termination of use of a Private Key, all copies of the Private Key in computer memory and shared disk space must be securely destroyed by over-writing. The method of over-writing must be approved by the PMA. When disks are disposed of that have held Private Keys, they must by purged in accordance with HMG Infosec Standard Number 5, or destroyed by disintegration, incineration, pulverisation, shredding or melting.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

6.3.1.1 CAs shall archive their public keys in accordance with the requirements of Section 4.6.

6.3.2 Usage periods for the public and Private Keys

6.3.2.1 The usage period for CA private and public keys shall not be more than 10 years.

6.3.2.2 The usage period for end-entity private and public keys shall not be more than 1 year, unless explicitly approved by the PMA.

6.4 Activation Data

6.4.1 Activation data generation and installation

6.4.1.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Any activation data shall be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected, commensurate with the protection of Level 2 information, as defined by the latest release of the "e-Government Security Framework". Where passwords are used, an entity must have the capability to change its password at any time.	Any activation data shall be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected, commensurate with the protection of Level 3 information, as defined by the latest release of the "e-Government Security Framework". Where passwords are used, an entity must have the capability to change its password at any time.	Any activation data shall be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected, commensurate with the protection of Level 2 information, as defined by the latest release of the "e-Government Security Framework". Where passwords are used, an entity must have the capability to change its password at any time.	Any activation data shall be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected, commensurate with the protection of Level 3 information, as defined by the latest release of the "e-Government Security Framework". Where passwords are used, an entity must have the capability to change its password at any time.

6.4.2 Activation data protection

6.4.2.1 Data used for Entity initialization must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

6.4.2.2 The Private Keys of Entities must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The level of protection must be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism should include a facility to temporarily lock the account after a predetermined number of login attempts.

6.4.3 Other aspects of activation data

6.4.3.1 No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

6.5.1.1 Access controls shall be implemented to prevent unauthorized access to CA data and functionality. Each CA server shall include the following functionality:

a. access control to CA services and PKI roles, ensuring that authenticated users can access only the services to which they are entitled;

b. enforced separation of duties for PKI roles;

c. identification and authentication of PKI roles and associated identities, via a trusted path;

d. object re-use control, key obfuscation (e.g. Private Key storage in non-contiguous memory locations) or separation for CA random access memory;

e. use of cryptography for session communication and database security;

f. archival of CA and End-Entity history and audit data;

g. audit of security related events;

h. self-test of security related CA services; and

i. recovery mechanisms for keys and the CA system.

6.5.1.2 This functionality may be provided by the operating system, or through a combination of operating system, CA software, procedural and physical safeguards.

6.5.2 Computer security rating

6.5.2.1 The cryptographic functionality of the CA and RA shall have been successfully evaluated by CESG as meeting appropriate HMG standards.

6.5.2.2 The CA software shall be certified under the Common Criteria or ITSEC to a level equivalent to Common Criteria EAL 3 or higher.

6.6 Life Cycle Security Controls

6.6.1 System development controls

6.6.1.1 CA operational software shall be developed in a controlled environment, under a recognized quality management system (e.g. ISO 9000-3:1997 or similar).

6.6.2 Security management controls

6.6.2.1 System security management shall be controlled by the privileges assigned to system accounts and by the trusted roles described in Section 5.2.1, according to appropriate standards (e.g. ISO 17799-1:2000 or similar).

6.6.2.2 The configuration of the CA system as well as any modifications and upgrades must be documented and controlled. A formal configuration management methodology must be used for installation, ongoing maintenance and evolution of the CA system. No upgrades shall be permitted without prior offline testing and assessment, and regular backups must be taken. The CA software, when first loaded, must provide a method for the CA to verify that the software on the system:

a. originated from the software developer;

b. has not been modified prior to installation; and

c. is the version intended for use.

6.6.2.3 Any CA installation shall be subject to an IT Health Check, carried out by CESG or a CHECK-approved supplier.

6.6.2.4 The CA shall conduct a failure impact analysis in order to demonstrate security resilience. The CA shall provide a mechanism to periodically verify the integrity of the software. These mechanisms shall be documented in the CPS.

6.6.2.5 Subscribers shall use security access controls provided by the underlying operating system to ensure that only the subject and authorised users (e.g. administrators) may access Private Key files.

6.6.3 Life cycle security ratings

6.6.3.1 No stipulation.

6.7 Network Security Controls

6.7.1 The HMG Root Authority is the trust point for HMG and shall not be connected to a network.

6.7.2

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
Other CAs may be connected to a network to enable the publication of certificates and revocation data. However, the CA server shall be protected from attack through any open or general purpose network with which it is connected, using mechanisms at least as strong as those specified in the Level 3 requirements in the latest release of the "e-Government Strategy Framework Policy and Guidelines: Network Defence".	CAs shall not be connected to a network.	Other CAs may be connected to a network to enable the publication of certificates and revocation data. However, the CA server shall be protected from attack through any open or general purpose network with which it is connected, using mechanisms at least as strong as those specified in the Level 3 requirements in the latest release of the "e-Government Strategy Framework Policy and Guidelines: Network Defence".	CAs shall not be connected to a network.

6.7.3

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
RA software shall be protected from attack through any open or general purpose network with which it is connected, using mechanisms at least as strong as those specified in the Level 2 requirements in the latest release of the “e-Government Strategy Framework Policy and Guidelines: Network Defence”.	RA software shall be protected from attack through any open or general purpose network with which it is connected, using mechanisms at least as strong as those specified in the Level 3 requirements in the latest release of the “e-Government Strategy Framework Policy and Guidelines: Network Defence”.	RA software shall be protected from attack through any open or general purpose network with which it is connected, using mechanisms at least as strong as those specified in the Level 2 requirements in the latest release of the “e-Government Strategy Framework Policy and Guidelines: Network Defence”.	RA software shall be protected from attack through any open or general purpose network with which it is connected, using mechanisms at least as strong as those specified in the Level 3 requirements in the latest release of the “e-Government Strategy Framework Policy and Guidelines: Network Defence”.

6.7.4 Subscribers shall ensure that suitable network protection is provided for networks holding Private Keys or applications using PKI cryptography. This shall include:

a. a properly configured firewall;

b. an effective configuration management process and routine inspections to ensure that cross-domain services and interfaces are limited to those necessary to meet the connection’s business objectives;

c. import restrictions such that imported objects are limited to information object types reasonably required to meet business needs. An anti-virus strategy with timely updates should be implemented; and

d. security awareness training shall be provided to users.

6.8 Cryptographic Module Engineering Controls

6.8.1 Cryptographic module engineering controls are covered in Section 6.2.1 of this Certificate Policy.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number(s)

7.1.1.1 The version number shall be v3 (value number 2), as defined in RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

7.1.2 Certificate extensions

7.1.2.1 The use of certificate extensions shall comply with the specifications in RFC 3280.

7.1.2.2 Certification Authorities shall define, populate and make non-critical the following extensions for all certificates generated:

a. `AuthorityKeyIdentifier`, using one of the two methods specified in RFC 3280;

b. `SubjectKeyIdentifier`, using one of the two methods specified in RFC 3280; and

c. `CRLDistributionPoints`.

7.1.2.3 Certification Authorities shall define, populate and make critical the following extension for all certificates generated:

a. `KeyUsage`, using the values specified in Section 6.1.9.

7.1.2.4 Certification Authorities shall define and populate the following extension for all certificates generated:

a. `CertificatePolicies`, using the values specified in Section 7.1.6 and including the `UserNotice` qualifier field, which shall include a reference to the Relying Party Agreement; the value `anyPolicy` shall not be present on end entity certificates. The `UserNotice` qualifier field should only be included in end entity certificates and certificates issued to CAs outside the HMG PKI (cross certificates). Policy qualifiers shall be limited to those defined in RFC 3280. The use of the `CPSPointer` qualifier is optional.

This extension may be critical.

7.1.2.5 Certification Authorities shall define, populate and make critical the following extension for certificates issued to CAs within the HMG PKI:

a. `BasicConstraints`, where the value of `cA` shall be true.

7.1.2.6 Certification Authorities shall define and populate the following extension for certificates issued to CAs within the HMG PKI:

a. `PolicyConstraints`, where the `RequireExplicitPolicy` field shall be defined with value `0` (zero) and the `inhibitPolicyMapping` field shall be undefined.

This extension may be critical.

7.1.2.7 Certification Authorities shall define, populate and make critical the following extensions for all cross-certificates (i.e. certificates issued to CAs outside the HMG PKI):

a. `BasicConstraints`, where the value of `cA` shall be true; and

b. `PolicyConstraints`, where the `RequireExplicitPolicy` field shall be defined with value `0` (zero) and the `inhibitPolicyMapping` field shall be defined with value `0` (zero). In certain circumstances, such as cross-certifying with a bridge architecture, the inhibitPolicyMapping field may be defined with a value greater than 0 (zero). This must be approved by the PMA.

7.1.2.8 Certification Authorities shall define, populate and make non-critical the following extension for all cross-certificates (i.e. certificates issued to CAs outside the HMG PKI):

a. `PolicyMappings`.

7.1.2.9 Certification Authorities may define and populate the following extensions:

a. `PrivateKeyUsagePeriod`;

b. `SubjectAlternativeName`;

c. `IssuerAlternativeName`;

d. `SubjectDirectoryAttributes`;

e. `BasicConstraints` (for end entity certificates, where the value of `cA` shall be false);

f. `NameConstraints`, according to HMG naming policy;

g. `ExtKeyUsage`;

h. `FreshestCRL`;

i. `AuthorityInformationAccess`; and

j. `SubjectInformationAccess`.

If defined, these extensions shall be non-critical.

7.1.2.10 Certification Authorities may define and populate the `InhibitAnyPolicy` extension. If defined, this extension shall be critical.

7.1.2.11 The CPS must define the use of any extensions supported by the CA, its RAs and end entities.

7.1.3 Algorithm object identifiers

7.1.3.1 Entities may use, for signing and verification, the following algorithms:

a. DSA with SHA-1 (ID DSA with SHA-1): OID 1.2.840.10040.4.3, Issuing Authority X9-57; or

b. RSA 1024, RSA 2048 and SHA-1 (ID SHA-1 with RSA Encryption): OID 1.2.840.113549.1.1.5, Issuing Authority RSADSI.

7.1.3.2 Entities may use, for confidentiality, the following algorithm:

a. RSA 1024, RSA 2048 (ID RSA Encryption): OID 1.2.840.113549.1.1.1, Issuing Authority RSADSI.

7.1.4 Name forms

7.1.4.1 All distinguished names must be in the form of an X.501 `PrintableString`.

7.1.5 Name constraints

7.1.5.1 Subject and issuer distinguished names must comply with PKIX standards and must be present in all certificates. All names must comply with HMG naming policy.

7.1.5.2 Unique identifiers (`IssuerUniqueID` and `SubjectUniqueID`) shall not be defined.

7.1.6 Certificate policy Object Identifier

7.1.6.1

Level 2 Digital Signature Policy	Level 3 Digital Signature Policy	Level 2 Confidentiality Policy	Level 3 Confidentiality Policy
All certificates must contain the Policy OID for the HMG Level 2 Digital Signature Policy (OID 1.2.826.0.1316.2.0.1.2.0).	All certificates must contain the Policy OID for the HMG Level 2 Digital Signature Policy (OID 1.2.826.0.1316.2.0.1.2.0) and the HMG Level 3 Digital Signature Policy (OID 1.2.826.0.1316.2.0.1.3.0).	All certificates must contain the Policy OID for the HMG Level 2 Confidentiality Policy (OID 1.2.826.0.1316.2.0.1.2.1).	All certificates must contain the Policy OID for the HMG Level 2 Confidentiality Policy (OID 1.2.826.0.1316.2.0.1.2.1) and the HMG Level 3 Confidentiality Policy (OID 1.2.826.0.1316.2.0.1.3.1).

7.1.7 Usage of Policy Constraints extension

7.1.7.1 All cross-certificates (i.e. certificates issued by CAs to other CAs outside the HMG PKI) shall define and populate the Policy Constraints extension with the following attributes: `inhibitPolicyMapping` and `requireExplicitPolicy`.

7.1.8 Policy qualifiers syntax and semantics

7.1.8.1 The `UserNotice` qualifier field shall include a reference to the Relying Party Agreement.

7.1.9 Processing semantics for the critical certificate policy extension

7.1.9.1 Critical extensions shall be interpreted as defined in PKIX RFC 3280.

7.2 CRL Profile

7.2.1 Version number(s)

7.2.1.1 The version number shall be 2 (two), as defined in RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

7.2.2 CRL and CRL entry extensions

7.2.2.1 All entity PKI software must correctly process all CRL extensions identified in the PKIX Certificate and CRL profile. The CPS must define the use of any extensions supported by the CA, its RAs and end entities.

INTENTIONALLY BLANK

8 Specification Administration

8.1 Specification Change Procedures

8.1.1 The following aspects of this Certificate Policy can change without notification and without requiring a new Object Identifier to be allocated:

a. formatting; and

b. correction of minor typographic errors.

8.1.2 The following aspects of this Certificate Policy can change with notification but without requiring a new Object Identifier to be allocated:

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

8.1.3 The following aspects of this Certificate Policy cannot be changed, unless a new certificate policy with a new Object Identifier is created:

a. any aspect that lowers, or could be perceived to lower, the fundamental trust that can be placed in the certificate.

8.2 Publication and Notification Policies

8.2.1 An electronic copy of this document, digitally signed by an authorized representative of the CA, is to be made available:

a. at the HMG PMA World Wide Web site, URL http://www.hmgpki.gov.uk/; and

b. via an e-mail request to csia@cabinet-office.x.gsi.gov.uk.

8.3 CPS Approval Procedures

8.3.1 A CA’s accreditation into the HMG PKI must be in accordance with procedures specified by the PMA.

8.3.2 Where a CPS contains information relevant to the security of a CA, all or part of the CPS need not be made publicly available.

INTENTIONALLY BLANK

A Definitions

A.1 This section defines the terms used in this Certificate Policy.

Term	Definition
Authority Revocation List (ARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock Private Keys for signing or decryption events).
Applicant	The Subscriber is sometimes also called an "applicant" after applying to a CA for a certificate, but before the certificate issuance procedure is completed.
Certification Authority (CA)	An authority trusted and authorised by the HMG PKI Root Authority (as indicated by the issue of a CA certificate to the authority concerned by the HMG PKI Root Authority) to issue and manage X.509 Public Key Certificates and ARLs or CRLs within the HMG PKI.
Certificate Policy (CP)	This set of rules governing the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates, and providing access to them, in accordance with specific requirements (e.g., requirements specified in this Certificate Policy, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	A list maintained by a CA of the certificates which it has issued that are revoked prior to their stated expiration date.
CONFIDENTIAL	A Government protective marking classification, as defined in HMG Security Policy.

Term	Definition
Confidential	A general term used to express the concept of secrecy.
Cross-Certificate	A certificate issued between two Certification Authorities used to establish and indicate a trust relationship between them.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using private/public key pairs and certificates such that the recipient of the message and signature can determine: (1) whether the transformation was created using the Private Key which complements the public key in the certificate; and (2) whether the message has been altered since the transformation was made.
Eligible Certification Authorities	The public sector bodies specifically listed in Paragraph 1.3.1.1 which, amongst other things, are eligible to apply to become Certification Authorities within the HMG PKI.
End Entities	Relying Parties, Subscribers, Subjects and Representatives.
Government	Her Majesty's Government.
HMG	Her Majesty's Government.
HMG PKI	The public key infrastructure created and operated by Her Majesty's Government.
HMG PKI Authorities	The following bodies and authorities, which are, or have been, involved in the creation and operation of the HMG PKI: Her Majesty's Government; the PMA; the CAs; the RAs; the Repositories; CESG; the officers, employees and agents of any of these to the extent they are acting as such.
HMG Root Authority	The Root Authority for the HMG PKI.

Term	**Definition**
Intellectual Property Rights (IPR)	Includes copyright works, databases, data, designs, discoveries, inventions, improvements, know-how, confidential information, all title, rights and interests to and in all of these or arising out of them (whether such rights exist, or are of a kind which exist, at the time of this agreement or whether they or that kind only come into existence afterwards), applications for and registrations of them and the rights in them, and the right to apply for any form of protection for any of these things and rights (whether such rights exist, or are of a kind which exist, at the time of this agreement or whether they or that kind only come into existence afterwards) In each case it includes the aforesaid title, rights and interests in every part of the world for their full term, including any renewals and extensions, the right to receive any income from them, and the right to sue in respect of any past, continuing or future infringement of any of them, and to claim and receive damages (or an account of profits) and interest in respect of any such infringement.
Normal business hours	There is no absolute definition of this term as it will depend on the working practices of the organisation concerned. However, when referred to in this document, normal business hours shall at least include the hours from 9.00 to 17.30.
OID	Object identifier.
Online Certificate Status Protocol (OCSP)	Protocol for determining the status of a certificate, as defined by the Internet Engineering Task Force (RFC 2560).
Policy Management Authority (PMA)	The body established to ensure that the use of PKI within HMG meets the relevant business and security requirements and conforms appropriately to HMG policy.
Private Key	The key which complements the key identified in the certificate (the Public Key).
Registration Authority (RA)	An entity that is responsible for identification and authentication of Certification Authorities, Subscribers and certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Term	**Definition**
Relying Party	An individual or an organisation, who acts in reliance on a certificate and digital signatures verified using that certificate.
Relying Party Agreement	The terms of an agreement between a Relying Party and the issuing CA, as published by the CA at the time of the Relying Party relying on the certificate, which impose obligations on the Relying Party and restrict the liability of the CA and other HMG PKI Authorities to the Relying Party.
Repository	A service which publishes certificates and/or ARLs and CRLs for access by Relying Parties.
RESTRICTED	A Government protective marking classification, as defined in HMG Security Policy.
Representative	The individual who accepts the certificate associated with computer applications and devices (e.g. workstations, guards, firewalls, routers, in-line network encryptors, trusted servers, and other infrastructure components) in the control of Subscribers which are Eligible Certification Authorities, and is responsible for the correct protection and use of the Private Key.
Revocation advertisement service	A service by which certificate revocation information is published for access by Relying Parties.

Term	Definition
Root Authority	The Certification Authority (CA) at the top of a CA hierarchy.
Subject	The Subject of the certificate is the entity to whom the certificate applies and is the individual that is authenticated by the Private Key[5]. In the case of computer applications and devices, the certificate applies to the application or device; the associated Representative is responsible for the correct protection and use of the Private Key.
Subscriber	The Subscriber is an entity who contracts with a CA for the issuance of certificates. The Subscriber bears ultimate responsibility for the use of the Private Key.
Subscriber Agreement	A binding written agreement between the CA and the Subscriber, entered into out-of-channel, under which the Subscriber undertakes certain obligations and liabilities to the CA in accordance with this Certificate Policy.

[5] In the case of certificates issued to an individual (e.g. acting in a self-employed capacity), the subscriber and subject will be the same entity. In other cases, such as certificates issued to employees, the subscriber and subject are different. The subscriber would be, for example, the employer; the subject would be the employee.

B References

B.1 This section lists the documents that are referred to in this Certificate Policy.

1. *“E-Government strategy framework policy and guidelines: Security”*, http://www.e-envoy.gov.uk/

2. *“E-Government strategy framework policy and guidelines: Registration and Authentication”*, http://www.e-envoy.gov.uk/

3. *“E-Government strategy framework policy and guidelines: Trust Services”*, http://www.e-envoy.gov.uk/

4. *“E-Government strategy framework policy and guidelines: Confidentiality”*, http://www.e-envoy.gov.uk/

5. *“E-Government strategy framework policy and guidelines: Network Defence”*, http://www.e-envoy.gov.uk/

6. *“E-Government strategy framework policy and guidelines: Assurance”*, http://www.e-envoy.gov.uk/

7. *“HMG's Minimum Requirements for the Verification of the Identity of Individuals”*, http://www.e-envoy.gov.uk/

8. *“HMG's Minimum Requirements for the Verification of the Identity of Organisations”*, http://www.e-envoy.gov.uk/

9. *“Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)”*, http://www.cenorm.be/

10. *“Secure Signature-Creation Devices EAL 4+”*, http://www.cenorm.be/

C Physical Security

C.1 Introduction

C.1.1 CA and RA facilities which issue (or process requests for) Level 2 certificates shall, as a minimum, be protected by physical security equivalent to that required to protect material with an HMG Protective Marking of RESTRICTED.

C.1.2 CA and RA facilities which issue (or process requests for) Level 3 certificates shall, as a minimum, be protected by physical security equivalent to that required to protect material with an HMG Protective Marking of CONFIDENTIAL.

C.1.3 All HMG PKI member organisations should conduct an assessment of the physical security of proposed CA (and RA) facilities, and implement any extra physical security measures accordingly.

C.1.4 Organisations which are bound by the HMG Manual of Protective Security (MPS)[6] should conduct this assessment using Supplement 16 of MPS ("Physical Security Assessment Process").

C.1.5 Organisations which are *not* bound by the MPS may conduct their assessment using MPS Supplement 16 if it is available to them. Otherwise, they should conduct the assessment using the "Physical Security Assessment Guide" (PSAG) contained in this Appendix[7].

C.1.6 The Certification Practice Statement (CPS) produced by an HMG PKI member organisation which owns CA (or RA) facilities should describe how the physical security requirements as stated above have been met, by reference to the specific physical security measures in place at the CA (or RA) facilities.

[6] Organisations handling protectively marked government material, including: the Home Civil Service; Diplomatic Service; Armed Forces; Police Services; UK Atomic Energy Authority; BNFL; NIREX; URENCO; employees of industrial, commercial and other firms engaged on government contracts involving protectively marked assets; departmental consultants; the Civil Aviation Authority; British Telecommunications PLC; MMO2; and the Bank of England.

[7] The PSAG is effectively a cut-down version of MPS Supplement 16, tailored for the use of organisations that are not familiar with the procedures (or special security products) for protecting HMG protectively marked information. One consequence of this is that the PSAG does not give extra credit for certain high-end security measures (such as SEAP-approved locks, perimeter fences or entry control systems), whereas Supplement 16 does. If an organisation uses such measures, but fails the PSAG self-assessment, it should contact the HMG PKI Policy Management Team (PMT) for advice.

C.2 Physical Security Assessment Guide (PSAG)

C.2.1 How to use this PSAG:

a. Work through the questionnaire below, noting your scores in the appropriate boxes.

b. Combine the scores in each box as indicated in the assessment sheet, to calculate a total value.

c. Compare this total value with those shown on the last page of this Appendix, to determine whether your existing physical security controls are adequate to house CA or RA facilities. If it is not, implement further security measures until your score exceeds the required score.

C.2.2 The minimum security requirements are as follows:

a. CA and RA facilities which issue (or process requests for) Level 3 certificates must:

1. Have a Total Security Score of at least **11**; AND

2. Have a Total Score *for Section 1* of at least **4**; AND

3. Have a Total Score *for Section 3* of at least **3**.

b. CA and RA facilities which issue (or process requests for) Level 2 certificates must:

1. Have a Total Security Score of at least **3**; AND

2. Have a Total Score *for Section 1* of at least **2**.

PSAG Questionnaire

1. Will your CA / RA facilities be housed in:
   (a) A *strongroom*, certified in accordance with British Standard BS EN 1143-1-1997?

   If YES, enter '**4**' in assessment box 1.

   (b) A *lockable room*, which will be locked when unattended?

   If YES, enter '**1**' in assessment box 1

   (c) Neither of the above?

   If YES, enter '**0**' in assessment box 1

2. Will the building housing your CA / RA facilities:
   (a) Be constructed of walls, floors and ceiling each constructed of reinforced concrete or concrete slabs, with a steel reinforced (wood faced with steel) door, and windows which offer substantial resistance to a physical attack (e.g. are covered by metal bars, grills or shutters?

   If YES, enter '**5**' in assessment box 2.

   (b) Be constructed of cavity walls of brick or block, or pre-cast or fabricated panels, or steel frame filled with glass?

   If YES, enter '**3**' in assessment box 2.

   (c) Be constructed of single-thickness brick or lightweight block?

   If YES, enter '**1**' in assessment box 2.

   (d) Be none of the above?

   If YES, enter '**0**' in assessment box 2.

3. Will the site, area, building or room(s) housing your CA / RA facilities have an access control system?

   If NO, enter '**0**' in assessment box 3.

   If YES, is the system:

   (a) Based on the use of a card or token in association with a unique Personal Identification Number (PIN)?

   If YES, enter '**4**' in assessment box 3.

   (b) A card-only system, or a card system with a PIN which is common to more than one user, or a PIN-only system which records the time and entry point for each transaction?

   If YES, enter '**3**' in assessment box 3.

   (c) Based on security guards, custodians, or receptionists verifying photographic passes belonging to users?

   If YES, enter '**2**' in assessment box 3.

   (d) Based on a locked door, which is opened by means of a mechanical or electronic Push Button Code Lock (PBCL) and/or the issue of keys to "authorised key users"?

   If YES, enter '**1**' in assessment box 3.

4. Are all visitors (other than those with an SC security clearance or above) to the site or building housing your CA / RA facilities:

   (a) Escorted at all times by a permanent member of staff?

   If YES, enter '**3**' in assessment box 4.

   (b) Issued with passes or badges identifying them as visitors?

   If YES, enter '**1**' in assessment box 4.

   (c) Neither of the above?

   If YES, enter '**0**' in assessment box 4.

5. Does the site or building housing your CA / RA facilities have an out-of-hours guard service?

   If NO, enter '**0**' in assessment box 5.

   If YES, does the guard service:

   (a) Undertake frequent random patrols inside the building housing your CA / RA facilities?

   If YES, enter '**5**' in assessment box 5.

   (b) Undertake infrequent random patrols inside the building housing your CA / RA facilities?

   If YES, enter '**4**' in assessment box 5.

   (c) Undertake only external patrols?

   If YES, enter '**3**' in assessment box 5.

   (d) Only provide a resident guard?

   If YES, enter '**2**' in assessment box 5.

   (e) Only provide a visiting guard?

   If YES, enter '**1**' in assessment box 5.

6. Does the building housing your CA / RA facilities have an Intrusion Detection System?

   If YES, enter '**1**' in assessment box 6.

   If NO, enter '**0**' in assessment box 6.

7. Is there some form of access control at the site perimeter?

   If NO, enter '**0**' in assessment box 7.

   If YES:

   (a) In addition to the access control procedures, is the building, area or site housing your CA / RA facilities surrounded by a welded-mesh anti-intruder fence at least 2.9m high, OR a palisade anti-intruder fence at least 3m high, OR an expanded metal (Expamet) fence with steel posts which is at least 2.9m high, OR a steel profile sheet fence (SPSF) at least 3m high, OR a solid, dense masonry wall at least 3m high with a minimum thickness of 100mm?

   If YES, enter '**2**' in assessment box 7.

   (b) In addition to the access control procedures, is the building, area or site housing your CA / RA facilities surrounded by a solid perimeter fence, wall or hedge that is at least 1.5m high?

   If YES, enter '**1**' in assessment box 7.

   (c) Does neither of the above statements apply?

   If YES, enter '**0**' in assessment box 7.

8. Are random entry and exit searches carried out?

   If YES, enter '**1**' in assessment box 8.

   If NO, enter '**0**' in assessment box 8.

9. Is an electronic PIDS (Perimeter Intruder Detection System) installed?

   If YES, enter '**2**' in assessment box 9.

   If NO, enter '**0**' in assessment box 9.

10. Is a perimeter CCTV system installed?

    If YES, enter '**2**' in assessment box 10.

    If NO, enter '**0**' in assessment box 10.

11. Is site perimeter lighting installed?

    If YES, enter '**2**' in assessment box 11.

    If NO, enter '**0**' in assessment box 11.

PSAG Assessment Sheet

Section 1

Assessment Box 1: Room Security □

Assessment Box 2: Building Security □

Total Score for Section 1: □ (= Box 1 + Box 2)

Section 2

□

Assessment Box 3: Access Control

□

Assessment Box 4: Visitor Control

□

Assessment Box 5: Guard Service

□

Assessment Box 6: IDS

□

Total Score for Section 2: (= Box 3 + Box 4 + Box 5 + Box 6)

Section 3

Assessment Box 7: Fence/Wall	□
Assessment Box 8: Searches	□
Assessment Box 9: PIDS	□
Assessment Box 10: CCTV	□
Assessment Box 11: Lighting	□

Total Score for Section 3:	□	(= Box 7 + Box 8 + Box 9 + Box 10 + Box 11)
Total Security Score:	□	(=Total of Sections 1, 2 and 3)

INTENTIONALLY BLANK

CSIA
Cabinet Office
Stockley House
130 Wilton Road
London SW1V 1LQ

Tel: 020 7276 3115
Fax: 020 7276 5096
e-mail: csia@cabinet-office.x.gsi.gov.uk
Website: http://www.cabinetoffice.gov.uk/csia