NHS Connecting for Health	**NHS Level 1 - Issuing Authority Base Certificate Policy**			
	Programme	NPFIT	**Document Record ID Key**	
	Sub-Prog / Project	Infrastructure	NPFIT-FNT-TO-INFR-0056.01	
	Prog. Director	Chris Wilber	Version	2.0
	Owner	James Wood	Status	APPROVED
	Author	Trustis Limited/Mark Penny	Version Date	10th November, 2011

NHS Level 1 Issuing Authority

Base Certificate Policy

Amendment History:

Version	Date	Amendment History
0.1	20th October 2006	First draft for comment
0.2	23 November 2006	Amendment to text in section 2.3 to align with NHS Root CA CP
0.3	4th. January 2007	Comments received from Malcolm McKeating and clarification of organisations as Subscribers.
0.4	13th February 2007	Revision to include End Point Authentication Certificates as a separate entity.
0.5	3rd August 2007	Revised following legal review.
0.6	3st1 August 2007	Revised following further input from DLA
0.7	25th July 2008	Owner change
1.0	28th October 2008	Extension to cover all Level 1 Issuing Authorities
1.1	3rd November 2008	Changes arising from QA
1.2	24th November 2008	Minor corrections
1.3	5th June, 2009	Updated with new document reference number
1.4	November, 2009	Further updates by Trustis in light of Certificate Manufacturer review
1.5	6th May, 2011	Annual review and update
1.6	1st June, 2011	Update following Certificate Manufacturer and NHS PKI Policy Management Authority review
1.7	23rd September, 2011	Further update following management decision to progress with CA Key Changeover option for extending the NHS PKI Service
2.0	10th November, 2011	Document approved by PMA

Forecast Changes:

Anticipated Change	When
Annual Review	November, 2012

Reviewers:

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
PMA Members				

Approvals:

This document must be approved by the following:

Name	Signature	Title / Responsibility	Date	Version
James Wood (for and on behalf of the PMA)		Head of Infrastructure Security		2.0
Alistair Donaldson (for and on behalf of the PMA)		Digital Information and Health Policy Directorate		2.0

Distribution:

NHS PKI Policy Management Authority, Department of Health Informatics Directorate, Spine Service Provider, Local Service Providers, NHS organisations, NHS suppliers.

This policy will also be made available from both the N3 and Internet facing Connecting for Health web sites.

NWW: http://nww.connectingforhealth.nhs.uk/infrasec/nhspki/docs

WWW: TBD

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in FileCM is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number/URL	Title	Version
1	http://intranet.connectingforhealth.nhs.uk/departments/npo/glossary/glossary (internal) http://www.connectingforhealth.nhs.uk/factsandfiction/acronyms (external)	Online 'Glossary of Terms'.	N/A
2	http://nww.connectingforhealth.nhs.uk/infrasec/nhspki/glossary (N3 connection required)	PKI 'Glossary of Terms'	N/A
3	NPFIT-FNT-TO-INFR-0054.01	Certificate Policy for NHS Root Certification Authority	2.0
4	NPFIT-FNT-TO-INFR-0055.01	NHS Root Certificate Authority PKI Disclosure Statement	2.0
5	NPFIT-FNT-TO-INFR-0053.01	Authentication PKI Disclosure Statement	2.0
6	NPFIT-FNT-TO-INFR-0057.01	Content Commitment PKI Disclosure Statement	2.0
7	NPFIT-FNT-TO-INFR-0059.01	Endpoint Authentication PKI Disclosure Statement	2.0
8	RFC 3647 (http://www.ietf.org/rfc/rfc3647.txt)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	N/A
9	RFC 3280 (http://www.ietf.org/rfc/rfc3280.txt)	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	N/A
10	http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/$file/authentication.htm	Registration and Authentication - e-Government Strategy Framework Policy and Guidelines	3.0 (September 2002)
11	NPFIT-FNT-TO-IG-IGCOM-0170.04	NHS CFH Contractor Security Policy	5
12	http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc	Information Governance Statement of Compliance (IGSoC)	N/A

Ref no	Doc Reference Number/URL	Title	Version
13	RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt)	Key words for use in RFCs to Indicate Requirement Levels	N/A
14	http://nww.connectingforhealth.nhs.uk/infrasec/nhspki/docs	NHS PKI Repository	N/A
15	NPFIT-FNT-TO-IG-PRJMGT-0093.05	IG Audit and Alerts Gold Standard	2.0
16	http://www.ietf.org/rfc/rfc2986.txt	PKCS #10: Certification Request Syntax Specification	1.7
17	http://csrc.nist.gov/groups/STM/cmvp/index.html	FIPS140-2: Security Requirements for Cryptographic Modules	N/A
18	http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/infoclassifications.doc	Guidance for the Classification Marking of NHS Information	N/A
19	http://www.legislation.gov.uk/ukpga/1998/29/contents	UK Data Protection Act (1998)	N/A
20	http://nww.connectingforhealth.nhs.uk/iim/ra	Registration Authority guidance web pages	N/A
21	http://nww.connectingforhealth.nhs.uk/iim/documents/raopprocess.pdf	RA Operational Process & Guidance	3.1
22	http://nww.connectingforhealth.nhs.uk/iim/documents/ra01parta.doc	RA01 Registration Form	1.2
23	RFC 4210 (http://www.ietf.org/rfc/rfc4210.txt)	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)	N/A
24	RFC 3447 (http://www.ietf.org/rfc/rfc3447.txt)	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1	2.1
25	http://www.legislation.gov.uk/ukpga/1986/45/contents	Insolvency Act 1986	N/A
26	http://www.legislation.gov.uk/ukpga/1999/31/contents	Contracts (Rights of 3rd Parties) Act 1999	N/A
27	http://nww.connectingforhealth.nhs.uk/iim/calendra/training/regusergui de.pdf	5592 2008-A RA User Guide	Issue 2

Glossary of Terms:

List any new terms created in this document. Mail the NPO Quality Manager to have these included in the master glossary above [1].

Term	Acronym	Definition

Contents

0 About this Document 15
0.1 Purpose 15
0.2 Audience 15
0.3 Content 16
1 Introduction 17
1.1 Overview 17
1.2 Document name and identification 17
1.3 PKI participants 18
1.3.1 Certification authorities 19
1.3.2 Registration authorities 21
1.3.3 Subscribers 21
1.3.4 Subjects 22
1.3.5 Relying parties 22
1.4 Certificate usage 23
1.4.1 Appropriate certificate uses 23
1.4.2 Prohibited certificate uses 23
1.5 Policy administration 23
1.5.1 Organization administering the document 23
1.5.2 Contact person 23
1.6 Person determining CPS suitability for the policy 23
1.6.1 CPS approval procedures 23
1.7 Definitions and acronyms 23
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 24
2.1 Repositories 24
2.2 Publication of certification information 24
2.3 Time or frequency of publication 24
2.4 Access controls on repositories 24
3 IDENTIFICATION AND AUTHENTICATION 25
3.1 Naming 25
3.1.1 Types of names 25
3.1.2 Need for names to be meaningful 25
3.1.3 Anonymity or pseudonymity of subjects 25
3.1.4 Rules for interpreting various name forms 25

3.1.5 Uniqueness of names 26
3.1.6 Recognition, authentication, and role of trademarks 26
3.2 Initial identity validation 26
3.2.1 Method to prove possession of private key 26
3.2.2 Authentication of organization identity 27
3.2.3 Authentication of individual identity 27
3.2.4 Non-verified subject information 28
3.2.5 Validation of authority 28
3.2.6 Criteria for interoperation 28
3.3 Identification and authentication for re-key requests 28
3.3.1 Identification and authentication for routine re-key 28
3.3.2 Identification and authentication for re-key after revocation 29
3.4 Identification and authentication for revocation request 29
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 30
4.1 Certificate Application....30
4.1.1 Who can submit a certificate application 30
4.1.2 Enrolment process and responsibilities 30
4.2 Certificate application processing....31
4.2.1 Performing identification and authentication functions 31
4.2.2 Approval or rejection of certificate applications 31
4.2.3 Time to process certificate applications 31
4.3 Certificate issuance 31
4.3.1 CA actions during certificate issuance 31
4.3.2 Notification to subscriber by the CA of issuance of certificate 31
4.4 Certificate acceptance....31
4.4.1 Conduct constituting certificate acceptance 31
4.4.2 Publication of the certificate by the CA 32
4.4.3 Notification of certificate issuance by the CA to other entities 32
4.5 Key pair and certificate usage 33
4.5.1 Subscriber private key and certificate usage 33
4.5.2 Relying party public key and certificate usage 33
4.6 Certificate renewal....33
4.6.1 Circumstance for certificate renewal 33
4.6.2 Who may request renewal 33

4.6.3 Processing certificate renewal requests 34
4.6.4 Notification of new certificate issuance to subscriber 34
4.6.5 Conduct constituting acceptance of a renewal certificate 34
4.6.6 Publication of the renewal certificate by the CA 34
4.6.7 Notification of certificate issuance by the CA to other entities 34
4.7 Certificate re-key 34
4.7.1 Circumstance for certificate re-key 34
4.7.2 Who may request certification of a new public key 34
4.7.3 Processing certificate re-keying requests 34
4.7.4 Notification of new certificate issuance to subscriber 35
4.7.5 Conduct constituting acceptance of a re-keyed Certificate 35
4.7.6 Publication of the re-keyed certificate by the CA 35
4.7.7 Notification of certificate issuance by the CA to other entities 35
4.8 Certificate modification 35
4.8.1 Circumstance for certificate modification 35
4.8.2 Who may request certificate modification 35
4.8.3 Processing certificate modification requests 35
4.8.4 Notification of new certificate issuance to subscriber 35
4.8.5 Conduct constituting acceptance of modified certificate 35
4.8.6 Publication of the modified certificate by the CA 35
4.8.7 Notification of certificate issuance by the CA to other entities 35
4.9 Certificate revocation and suspension 36
4.9.1 Circumstances for revocation 36
4.9.2 Who can request revocation 36
4.9.3 Procedure for revocation request 37
4.9.4 Revocation request grace period 37
4.9.5 Time within which CA must process the revocation request 37
4.9.6 Revocation checking requirement for relying parties 38
4.9.7 CRL issuance frequency (if applicable) 38
4.9.8 Maximum latency for CRLs (if applicable) 38
4.9.9 On-line revocation/status checking availability 38
4.9.10 On-line revocation checking requirements 38
4.9.11 Other forms of revocation advertisements available 38
4.9.12 Special requirements re key compromise 39

4.9.13 Circumstances for suspension 39
4.9.14 Who can request suspension 39
4.9.15 Procedure for suspension request 39
4.9.16 Limits on suspension period 39
4.10 Certificate status services 40
4.10.1 Operational characteristics 40
4.10.2 Service availability 40
4.10.3 Optional features 40
4.11 End of subscription....40
4.12 Key escrow and recovery 40
4.12.1 Key escrow and recovery policy and practices 40
4.12.2 Session key encapsulation and recovery policy and practices 40
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 41
5.1 Physical controls 41
5.1.1 Site location and construction 41
5.1.2 Physical access 42
5.1.3 Power and air conditioning 42
5.1.4 Water exposures 42
5.1.5 Fire prevention and protection 42
5.1.6 Media storage 42
5.1.7 Waste disposal 42
5.1.8 Off-site backup 42
5.2 Procedural controls 43
5.2.1 Trusted roles 43
5.2.2 Number of persons required per task 43
5.2.3 Identification and authentication for each role 43
5.2.4 Roles requiring separation of duties 44
5.3 Personnel controls....44
5.3.1 Qualifications, experience, and clearance requirements 44
5.3.2 Background check procedures 45
5.3.3 Training requirements 45
5.3.4 Retraining frequency and requirements 45
5.3.5 Job rotation frequency and sequence 45
5.3.6 Sanctions for unauthorized actions 45

5.3.7 Independent contractor requirements 45
5.3.8 Documentation supplied to personnel 45
5.4 Audit logging procedures....45
5.4.1 Types of events recorded 45
5.4.2 Frequency of processing log 46
5.4.3 Retention period for audit log 47
5.4.4 Protection of audit log 47
5.4.5 Audit log backup procedures 47
5.4.6 Audit collection system (internal vs. external) 47
5.4.7 Notification to event-causing subject 47
5.4.8 Vulnerability assessments 47
5.5 Records archival....48
5.5.1 Types of records archived 48
5.5.2 Retention period for archive 48
5.5.3 Protection of archive 48
5.5.4 Archive backup procedures 48
5.5.5 Requirements for time-stamping of records 49
5.5.6 Archive collection system (internal or external) 49
5.5.7 Procedures to obtain and verify archive information 49
5.6 Key changeover 49
5.7 Compromise and disaster recovery....50
5.7.1 Incident and compromise handling procedures 50
5.7.2 Computing resources, software, and/or data are corrupted 51
5.7.3 Entity private key compromise procedures 51
5.7.4 Business continuity capabilities after a disaster 51
5.8 CA or RA termination 51
6 TECHNICAL SECURITY CONTROLS 53
6.1 Key pair generation and installation 53
6.1.1 Key pair generation 53
6.1.2 Private key delivery to subscriber 53
6.1.3 Public key delivery to certificate issuer 54
6.1.4 CA public key delivery to relying parties 54
6.1.5 Key sizes 54
6.1.6 Public key parameters generation and quality checking 54

6.1.7 Key usage purposes (as per X.509 v3 key usage field) 55
6.2 Private Key Protection and Cryptographic Module Engineering Controls....55
6.2.1 Cryptographic module standards and controls 55
6.2.2 Private key (n out of m) multi-person control 55
6.2.3 Private key escrow 55
6.2.4 Private key backup 55
6.2.5 Private key archival 56
6.2.6 Private key transfer into or from a cryptographic module 56
6.2.7 Private key storage on cryptographic module 56
6.2.8 Method of activating private key 56
6.2.9 Method of deactivating private key 57
6.2.10 Method of destroying private key 57
6.2.11 Cryptographic Module Rating 57
6.3 Other aspects of key pair management.....57
6.3.1 Public key archival 57
6.3.2 Certificate operational periods and key pair usage periods 57
6.4 Activation data.....58
6.4.1 Activation data generation and installation 58
6.4.2 Activation data protection 58
6.4.3 Other aspects of activation data 58
6.5 Computer security controls.....58
6.5.1 Specific computer security technical requirements 58
6.5.2 Computer security rating 59
6.6 Life cycle technical controls.....59
6.6.1 System development controls 59
6.6.2 Security management controls 59
6.6.3 Life cycle security controls 59
6.7 Network security controls 60
6.8 Time-stamping.....60
7 CERTIFICATE, CRL, AND OCSP PROFILES 61
7.1 Certificate profile 61
7.1.1 Version number(s) 61
7.1.2 Certificate extensions 61
7.1.3 Algorithm object identifiers 61

7.1.4 Name forms 61
7.1.5 Name constraints 61
7.1.6 Certificate policy object identifier 62
7.1.7 Usage of Policy Constraints extension 62
7.1.8 Policy qualifiers syntax and semantics 62
7.1.9 Processing semantics for the critical Certificate Policies extension 62
7.2 CRL profile 62
7.2.1 Version number(s) 62
7.2.2 CRL and CRL entry extensions 62
7.3 OCSP profile 62
7.3.1 Version number(s) 62
7.3.2 OCSP extensions 62
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 63
8.1 Frequency or circumstances of assessment 63
8.2 Identity/qualifications of assessor 63
8.3 Assessor's relationship to assessed entity 63
8.4 Topics covered by assessment 63
8.5 Actions taken as a result of deficiency 64
8.6 Communication of results 64
9 OTHER BUSINESS AND LEGAL MATTERS 65
9.1 Fees 65
9.1.1 Certificate issuance or renewal fees 65
9.1.2 Certificate access fees 65
9.1.3 Revocation or status information access fees 65
9.1.4 Fees for other services 65
9.1.5 Refund policy 65
9.2 Financial responsibility 65
9.2.1 Insurance coverage 65
9.2.2 Other assets 66
9.2.3 Insurance or warranty coverage for end-entities 66
9.3 Confidentiality of business information 66
9.3.1 Scope of confidential information 66
9.3.2 Information not within the scope of confidential information 66
9.3.3 Responsibility to protect confidential information 66

9.4 Privacy of personal information 67
9.4.1 Privacy plan 67
9.4.2 Information treated as private 67
9.4.3 Information not deemed private 67
9.4.4 Responsibility to protect private information 67
9.4.5 Notice and consent to use private information 67
9.4.6 Disclosure pursuant to judicial or administrative process 68
9.4.7 Other information disclosure circumstances 68
9.5 Intellectual property rights 68
9.6 Representations and warranties 68
9.7 Disclaimers of warranties 68
9.8 Limitations of liability 69
9.9 Indemnities 70
9.10 Term and termination 70
9.10.1 Term 70
9.10.2 Termination 70
9.10.3 Effect of termination and survival 71
9.11 Individual notices and communications with participants 71
9.11.1 Subscribers 71
9.11.2 Issuing Authority 72
9.11.3 Notification 72
9.12 Amendments 72
9.12.1 Procedure for amendment 72
9.12.2 Notification mechanism and period 73
9.12.3 Circumstances under which OID must be changed 73
9.13 Dispute resolution provisions 73
9.14 Governing law 74
9.15 Compliance with applicable law 74
9.16 Miscellaneous provisions 74
9.16.1 Entire agreement 74
9.16.2 Assignment 74
9.16.3 Severability 74
9.16.4 Enforcement (attorneys' fees and waiver of rights) 75
9.16.5 Force Majeure 75

9.17 Other provisions 75
9.17.1 Certificate Policy Content 75
9.17.2 Third party rights 75

0 About this Document

0.1 Purpose

The purpose of this document is to provide the base policy under which Level 1 Issuing Authorities are operated and how they support the requirement that certificates will be issued subject to the security controls required by HMG Authentication Framework Level 3 [10].

This policy is produced to the standard defined by IETF RFC 3647 [8].

Certificates issued from the NHS PKI Level 1 Issuing Authorities may be used for a wide range of purposes. Where an Issuing Authority mandates specific constraints and controls, for example limits on use of Certificates, these will be specified in the PKI Disclosure Statement (PDS) for a set or class of certificates issued. Therefore this Base Certificate Policy must be read in conjunction with a relevant PDS as it is the pairing of these two documents that comprise the full Certificate Policy (CP) for any Certificate.

The Certificate Policy describes the standards and services associated with the operation of the NHS PKI. It also defines the obligations and responsibilities associated with digital certificates issued by the NHS PKI Level 1 Issuing Authorities.

0.2 Audience

This document has been written for:

- All NHS PKI Participants.
- All Subscribers to and the Subjects of digital certificates and all Relying Parties for digital certificates, including both natural persons, and computer devices or applications (via the responsible person for that application).

This document is to be made available to the specified community. Publication more widely is permitted. It shall be published in conjunction with all associated PKI Disclosure Statements.

0.3 Content

This document comprises the following sections/topics:

- Section 0 – About This Document.
- Section 1 – Introduction.
- Section 2 – Publication and Repository Responsibilities.
- Section 3 – Identification and Authentication.
- Section 4 – Certificate Life-Cycle Operational Requirements.
- Section 5 – Facility, Management and Operational Controls.
- Section 6 – Technical Security Controls.
- Section 7 - Certificate, CRL and OCSP Profiles.
- Section 8 – Compliance Audit and Other Assessments.
- Section 9 – Other Business and Legal Matters.

1 Introduction

1.1 Overview

This Certificate Policy (CP) is a named set of rules that indicates the applicability of Certificates issued by the level 1 Certificate Authority operated on behalf of NHS Connecting for Health by its nominated Certificate Manufacturers. The responsibility for this Certificate Policy lies with the NHS CFH Policy Management Authority (PMA) and any queries regarding the content of this Certificate Policy should be directed to the PMA.

Explanations of the various terms used throughout this document can be found at the websites listed in the 'Related Documents' section above.([1], [2])

This Certificate Policy is structured according to the guidelines provided by IETF RFC 3647 [8] with extensions and modifications defined where appropriate.

The Issuing Authority which controls the NHS PKI Level 0 Root Issuing Authority has made its own stipulations regarding operational standards, Participants, further restrictions on usage of Certificates, additional liability provisions, etc. These stipulations are contained in the document "Certificate Policy for NHS Root Certification Authority" (NPFIT-FNT-TO-INFR-0054.01) [3]

This Policy defines a Public Key Infrastructure and specifies:

- Who can participate in the Public Key Infrastructure defined by this Certificate Policy
- The primary rights, obligations and liabilities of the parties governed by this Certificate Policy.
- The purposes for which Certificates issued under this Certificate Policy may be used.
- Minimum requirements to be observed in the Issuance, management, usage and reliance upon Certificates.

This Certificate Policy (CP) is concerned with the production of certificates by the NHS Level 1 CAs for issuance to the NHS user community (both NHS organisations and non NHS organisations supporting the health care delivery process) for use with CRS, CRS compliant applications and any other application deemed acceptable by the PMA. The audience for this CP is therefore any user who is a Subject, Subscriber or Relying Party, plus the representatives of service providers to the NHS where appropriate.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.2 Document name and identification

The Policy Management Authority and Issuing Authority (see Section 2.1 of the relevant PKI Disclosure Statement) control this Policy document. The NHS Issuing Authority is responsible for the management and maintenance of this CP and may

devolve this role to subcontractors, as authorised by the Policy Management Authority.

The Object Identifier (OID) assigned to Certificates depends upon permitted usage and is given in section 2.12 of the PKI Disclosure Statement associated with the relevant class of certificates.

1.3 PKI participants

An Issuing Authority has an obligation to operate a PKI in accordance with the Certificate Policies it defines and publishes. The Issuing Authority does not however have to conduct all aspects of PKI operations itself. There are sets of functions that can be logically and conveniently grouped and delegated. This allows PKI services to align with business models, including the outsourcing of some or all of the PKI services to Participants.

There is not necessarily a one-to-one correlation between roles and Participants. Any Participant may perform one or more roles in any particular PKI. Each Participant operates to fulfil clearly defined roles. Typically these roles are:

- Policy Management Authority
- Trust Service Providers,
  - NHS Issuing Authority.
  - Certificate Manufacturer; see section 2.17 of the PKI Disclosure Statements.
  - Registration Authority; see section 2.13 of the PKI Disclosure Statements.
  - Repository; see section 2.14 of the PKI Disclosure Statements.
- End Entities,
  - Subscribers and Subjects; see section 2.15 of the PKI Disclosure Statements.
  - Relying Parties; see section 2.16 of the PKI Disclosure Statements.

Under this scheme, End-Entities only have a business relationship with the Issuing Authority. These relationships are defined by the Subscriber Agreements and Relying Party Agreements between the End-Entities and the Issuing Authority. In all matters, the End-Entity relationship is with the Issuing Authority.

Subjects may hold Certificates on behalf of Subscribers. In all cases however, the business relationship with the Issuing Authority is held by the Subscriber.

The requirements placed upon Participants providing Trust Services which support the Issuing Authority are controlled by the provisions of this Certificate Policy and any contractual arrangements between them and the Issuing Authority.

The NHS Issuing Authority is responsible for compliance with this Certificate Policy. It may refer matters to the Policy Management Authority which has overall and final control over the content of the Certificate Policy and related documentation.

These relationships are illustrated diagrammatically in Figure 1.

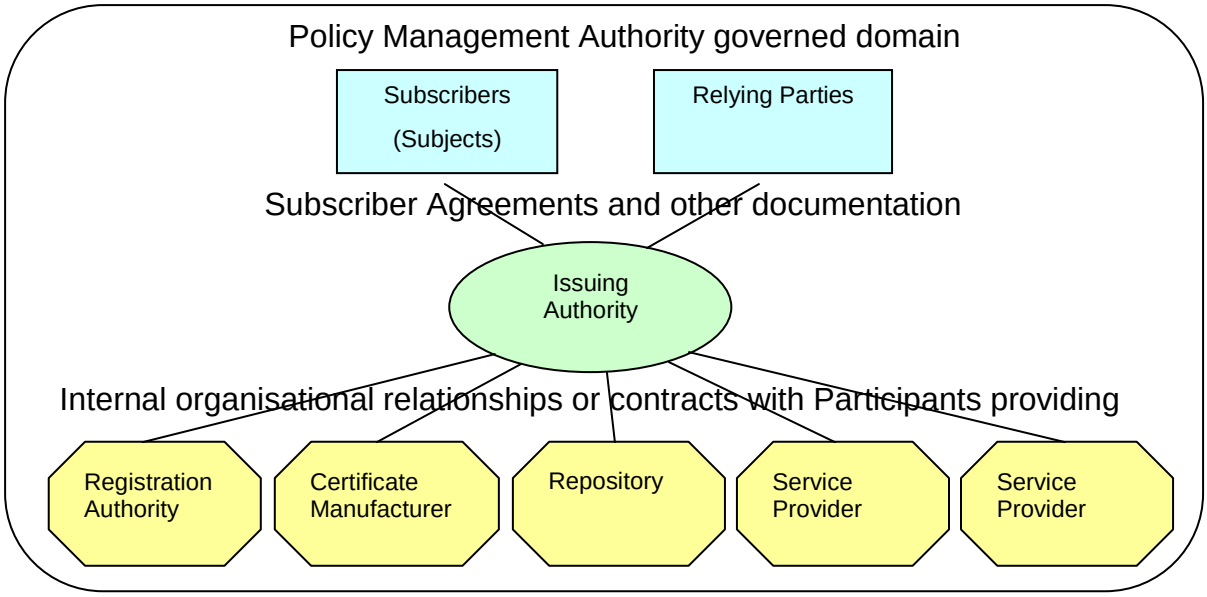

Figure 1. Roles & Business Relationships

These roles, that collectively comprise the PKI community governed by this Certificate Policy, are described in the remainder of Section 1.3. These descriptions are illustrative. The specific roles and obligations for Participants are defined elsewhere in this Certificate Policy.

1.3.1 Certification authorities

RFC 3647 [8] defines Certification Authorities as the entities that Issue Certificates. Within the scope of model outlined above the Certification Authority consists of the two elements described in 1.3.1.1 and 1.3.1.2.

1.3.1.1 Issuing Authority

By definition, an Issuing Authority is the entity listed in the Issuer field of a Certificate. The Issuing Authority has the ultimate responsibility for deciding who may be issued with a Certificate carrying its name as the Issuer and is the only entity with which End-Entities have any form of direct or indirect contractual relationship. Whether its PKI services are provided by internal resources or are contracted out to external Participants, the provisions of this Policy apply. The Certificate Policy may be complemented by a contract between the Issuing Authority and Participants providing services.

For the benefit of Subscribers and Relying Parties, the Issuing Authority publishes a summary of important provisions that form a part of this Certificate Policy, together with any further provisions affecting Subscribers and Relying Parties, in a document

known as a PKI Disclosure Statement. These provisions typically include, but are not limited to the following:

- Policy Management Authority & Issuing Authority Contact Information.
- Certificate Type, validation procedures and usage.
- Reliance Limits.
- Obligations of Subscribers.
- Certificate Status checking obligations of Relying Parties.
- Limited Warranty & Disclaimer/Limitation of Liability.
- Applicable Agreements, Certificate Policy.
- Privacy Policy.
- Refund Policy.
- Applicable Law & Dispute Resolution.
- CA & Repository Licences Trust Marks & Audit.
- Identification of this Certificate Policy.
- Approved Registration Authorities.
- Approved Repositories.
- Eligible Subscribers.
- Eligible Relying Parties.
- Certificate Status Information.

Issuing Authorities may require that all Certificates issued by it under this Certificate Policy contain a reference to where the PKI Disclosure Statements and this Certificate Policy document are published. Where no reference is contained within the certificate, the relevant documents can be located at [14].

1.3.1.2 Certificate Manufacturer

The Certificate Manufacturer provides Certificate management operational services for the Issuing Authority.

The Certificate Manufacturer is approved by the Issuing Authority to manage Certificates on behalf of the Issuing Authority or other Participants in the PKI governed by this Certificate Policy. It has no authority to make decisions on the Issuance of Certificates or other aspects of certificate management; it operates under the direct control of the Issuing Authority.

The Certificate Manufacturer must demonstrate compliance with this Certificate Policy. Compliance may be demonstrated via a Certification Practice Statement. This does not override the requirement for Participants providing trust services to adhere to the NHS CFH Contractor Security Policy [11]. Where the Certification Practice Statement exists and is complemented by additional supporting documentation, it is

referred to generically in the Certificate Policy with the term ‘Certificate Manufacturer Procedures’.

Approved Certificate Manufacturers are specified in section 2.17 of the PKI Disclosure Statements [5, 6, 7]

1.3.2 Registration authorities

The Registration Authorities of the Issuing Authority are responsible for ensuring the eligibility of applicants to be issued with Certificates for use with NHS CRS applications and NHS CRS conformant applications from the level 1 Certificate Authorities operating under this Policy, together with the accuracy and integrity of required information presented by applicants. Registration Authorities are an integral function of the Issuing Authority and their role is to process and approve requests from applicants for the Issue of Certificates or for their Revocation, Suspension, Renewal or Re-Key as detailed elsewhere in this Certificate Policy.

For the aspects of PKI operations governed by this CP, multiple Registration Authorities as defined by the Issuing Authority are permitted. Registration Authorities must demonstrate compliance with this Certificate Policy. Compliance is documented and controlled via adherence to the procedures described in the latest versions of the NHS documents available from the ‘Registration Authority’ web site run by NHS CFH [20]

The Issuing Authority has approved the Registration Authorities listed in section 2.13 of the PKI Disclosure Statements for Authentication and Content Commitment Certificates governed by this Certificate Policy [5, 6, 7]. The Issuing Authority is the sole Registration Authority for End Point Authentication Certificates.

1.3.3 Subscribers

A Subscriber is either:

- The organisation that has contracted for the National Care Records Service (NCRS) and has, via an authorised signatory completed the NHS Connecting for Health Information Governance Statement of Compliance (IGSoC) [12]. It is the Subscriber that contracts with an Issuing Authority for the Issuance of Certificates to Subjects on behalf of the organisation. The Subscriber may in some instances also be the Subject; e.g. computer end point devices. The Subject bears responsibility for the use of the Private Key associated with the Certificate; or
- The Service Provider organisation that is making an application for an End Point Authentication Certificate for use by an approved service from either the Service Provider or an NHS organisation contracted to the Service Provider.

Certificate applicants, eligible to be authorised by the Registration Authority as Subjects, are identified in section 2.15 of the PKI Disclosure Statements [5, 6, 7].

1.3.4 Subjects

The Subject is the entity that is identified in the 'subject' field of the Certificate. The authorised Subscriber will accept the terms and conditions on behalf of the Subject that is identified in the Certificate. The Subject must be under the jurisdiction and control of the Subscriber and comply with all relevant aspects of this Certificate Policy and other agreements and obligations undertaken by the Subscriber. In all cases the Subscriber is responsible for compliance with the Certificate Policy and all other obligations applicable to it and the Subject.

1.3.5 Relying parties

A Relying Party is an End-Entity that does not necessarily hold a Certificate but even so, may rely on a Certificate and/or Digital Signatures created using that Certificate.

Eligible Relying-Parties for Certificates Issued under this Certificate Policy are specified in Section 2.16 of the PKI Disclosure Statements [5, 6, 7].

1.3.6 Other participants

1.3.6.1 Policy Management Authority

The Policy Management Authority has ultimate responsibility for governance and control over the Issuance, management and usage of Certificates Issued under this Certificate Policy. Simply stated, the Policy Management Authority is the entity that sets the rules under which the PKI is to be operated.

The Policy Management Authority can be either a governing body or a designee thereof that is tasked with defining the Certificate Policy in a manner that supports and reflects the needs of the underlying relationships and transactions to be supported by a PKI.

The Policy Management Authority is identified in Section 2.1 of the PKI Disclosure Statements [5, 6, 7].

1.3.6.2 Repository

A Repository is a Participant organisation that holds data in support of PKI operations. This includes policy and related documentation, Certificates and Certificate Status information.

The Repository provides a community-wide accessible mechanism by which primarily Subscribers and Relying Parties can obtain and validate information on Certificates Issued under this Certificate Policy.

The Issuing Authority has approved the Repositories identified in section 2.14 of PKI Disclosure Statements to provide these services [5, 6, 7]. The Repository can be located at [14].

1.4 Certificate usage

Certificate usage is defined by the Certificate Profile. Certificate Profiles must be approved by the Policy Management Authority.

1.4.1 Appropriate certificate uses

The categories of transactions, applications or purposes for which Certificates are issued under this policy and may be used are defined in Section 2.2 of the PKI Disclosure Statements [5, 6, 7].

1.4.2 Prohibited certificate uses

All other application use and any other usage categories for Certificates Issued under this Certificate Policy is prohibited as described in Section 2.2 of the PKI Disclosure Statements [5, 6, 7].

1.5 Policy administration

1.5.1 Organization administering the document

The Policy Management Authority, responsible for approving rights, obligations, liabilities and all other terms and conditions contained in this Certificate Policy, is listed in Section 2.1 of the PKI Disclosure Statements [5, 6, 7].

1.5.2 Contact person

Either of the mailboxes listed in Section 2.1 of the PKI Disclosure Statements [5, 6, 7] should be used in the first instance when raising queries regarding the contents of this Certificate Policy.

1.6 Person determining CPS suitability for the policy

The Policy Management Authority determines the suitability of any Certification Practice Statement operating under this Certificate Policy.

In the first instance, the Issuing Authority must be contacted regarding the inclusion of additional Certification Authorities to operate within this PKI or interoperation with other PKIs.

Contact details are provided in Section 2.1 of the PKI Disclosure Statements [5, 6, 7].

1.6.1 CPS approval procedures

The CPS and other Certificate Manufacturer Procedures are reviewed by the Policy Management Authority.

1.7 Definitions and acronyms

A definition of the terms used in this Certificate Policy can be found in the online ‘Glossary of Terms’ [1] and the online ‘PKI Glossary of Terms’ [2]

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

An information Repository shall be made available under the terms of this Certificate Policy. The Issuing Authority is the entity with overall responsibility for the operation of a Repository which it may delegate to Participants providing trust services.

2.2 Publication of certification information

The Issuing Authority shall ensure the following items are published for all Participants of this PKI via the Repository [14] or an equivalent mechanism:

- This Certificate Policy with its associated PKI Disclosure Statements.
- Any supporting policy documents and agreements.
- The Information that will allow the authenticity of the Issuing Authority's Certificate to be verified.
- All CA-Certificates of Certificate Authorities Issued by the Issuing Authority (including those for sub-ordinate and superior Certificate Authorities, and Cross-certificates for cross certified PKI's i.e. other PKI regimes whose certificates and underlying processes are recognised by the NHS, and vice versa).
- Certificate Status Information for Certificates Issued under this Certificate Policy.

The location of, (or mechanism to obtain access to) this Certificate Policy may be provided in Certificates Issued under this Certificate Policy.
Paper copies of documentation published in the Repository will be made available on request (a charge may be made). Application should be made to the Issuing Authority.

2.3 Time or frequency of publication

Information as listed in 2.2 shall be published promptly upon its creation, with the exception that if CRLs are used to provide Revocation information, they shall be published according to sections 4.9.7 and 4.9.8 of this Certificate Policy.

2.4 Access controls on repositories

The Repository must make available the information specified above. However the Repository may control access to information and restrict access to those Participants with specific need for the information.

The Repository shall not prevent access by Participants where required by this Certificate Policy.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Each Subject must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Certificate 'Subject' field of Certificates Issued under this Certificate Policy and in accordance with IETF PKIX RFC 3280 [9]. Each Entity may, in addition, use an alternative name via the 'Subject Alternative Name' field, which must also be in accordance with IETF PKIX RFC 3280 [9]. The 'Subject Alternative Name' field must not be marked critical. Where use of the 'Subject Alternative Name' field is made, all aspects of the alternate name form must be verified at the time of registration.

3.1.2 Need for names to be meaningful

The contents of each Certificate 'Subject' name field must have an association with the authenticated name of the Subject. This association may be direct, or where the natural identity of a Subject is required to be hidden, may be recorded elsewhere by the Registration Authority. The Relative Distinguished Name (RDN) may also identify an organisational position or role or link to a Subscriber (if different from the Subject) provided that a person responsible for the oversight of that role is recorded.

A Certificate Issued for a device or application must include within the DN the name of the person or organisation acting as Subscriber for that device or application.

3.1.3 Anonymity or pseudonymity of subjects

The anonymity or pseudonymity of Subjects is not permitted under this Certificate Policy, unless this is explicitly requested by the Issuing Authority responsible for this Certificate Policy. Where permitted, the Registration Authorities operating under this Certificate Policy must record the authenticated real identity of the Subject with the anonymised or pseudonymised Subject name.

3.1.4 Rules for interpreting various name forms

The inclusion of Common Name in a Distinguished Name is mandatory. All other fields that may be included are optional. Their interpretation for any entity shall be as follows:

Element	Description
Common Name	Where the Subject is a natural person, Common name may consist of a pseudonym established to hide the natural identity of the Subject. In this case, the fact that the Common name is a pseudonym must be made obvious, either by the style of the pseudonym or by explicit indication in Common Name. Where this hiding is not required, Common name shall consist of the given name, middle name or middle initial (if the Subject has a middle name), and the family name of the Subject, in that

Element	Description
	order, separated by space characters. Where the Subject is a device or application, Common name shall consist of sufficient information to uniquely identify the Subject. These name forms may be followed by any other optional information required for identification or for uniqueness of RDN.
Street address	The physical location where the Subscriber resides or conducts business or where the entity can receive paper mail.
Locality name	The city or town or other recognised locality where the entity resides or conducts business.
Country name	The country where the entity resides or conducts business.
Organization name	An organisation with which the entity has a significant relationship. The organisation name serves only as an additional identifier of the entity and does not imply employment or any authority to act on behalf of the organisation unless the Certificate and/or its policy specifically provide otherwise.
SubjectAlternative Name	Specified only in accordance with IETF PKIX RFC 3280 [9]. Where this specifies an email address, it is the electronic mail address at which the entity can receive electronic mail via the Internet.

3.1.5 Uniqueness of names

Distinguished names must be unique for Certificate Authorities and all Subjects under the jurisdiction of an Issuing Authority. For each Subject any other optional information may be appended to the Distinguished Name as required for identification or to ensure its uniqueness.

3.1.6 Recognition, authentication, and role of trademarks

Neither the Policy Management Authority nor the Issuing Authority is liable for the inclusion of trademarks, trade names or other information under restricted use. Subscriber Agreements shall require Subjects to warrant legitimacy of their registration details provided to the Issuing Authority as part of the Registration process.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The Registration and/or Issuance process shall involve a stage in which the applicant demonstrates possession of the Private Key. Technical means employed to ensure possession of Private Keys will be PKCS#10 [16], other equivalent cryptographic mechanism, or a process specifically approved by the Issuing Authority.

3.2.2 Authentication of organization identity

Authentication of the NHS organisation as defined in the current version of the document “Registration Authorities Operational Process & Guidance" [21] must be performed as described by a Superior Registration Authority. Where the organisation is the Certificate ‘Subject’, or where the organisation is a component of the distinguished name of the Certificate ‘Subject’ the identity of the organisation must be established to a level of Beyond Reasonable Doubt.

Authentication processes must include face-to-face authentication with an authorised representative of the organisation, as nominated or other form of direct registration by a representative of the organisation. Where the latter is the case, the identity of the representative must be authenticated and their authority to represent the organisation must be validated.

Specific requirements for authentication of organisation identity are provided in Section 2.2 of the PKI Disclosure Statements [5, 6, 7] or other community-wide accessible document. The Registration Authority shall define and document the mechanisms used to support the level of authentication assurance.

The Registration Authority shall verify that each Certificate applicant has a right to obtain that Certificate and, if the Certificate identifies that the Subject (including the Subscriber as Subject) has particular attributes or privileges, that they are valid.

3.2.3 Authentication of individual identity

The authentication of Registration Authority Operators must at a minimum satisfy the specific criteria for authentication specified in the PKI Disclosure Statements [5, 6, 7] and be performed in accordance with the procedures defined in the document “Registration Authorities Operational Process & Guidance" [21]. Additionally the Issuing Authority shall undertake face-to-face authentication of one or more initial Registration Authority Administrators. An authenticated and nominated Registration Authority Administrator may undertake face-to-face authentication of subsequent Registration Authority Administrators.

Authentication processes for Certificate applicants may include face-to-face authentication. Individual identity may be authenticated by remote means, provided that the criterion of beyond reasonable doubt assurance is satisfied.

Any specific additional requirements for authentication of individual identity are provided in the document “Registration Authorities Operational Process & Guidance" [21] and described in Section 2.2 of the PKI Disclosure Statements [5, 6, 7]. The Registration Authority shall define and document the mechanisms used to support the level of authentication assurance.

The Registration Authority shall verify that each Certificate applicant has a right to obtain that Certificate and, if the Certificate identifies that the Subject has particular attributes or privileges, that they are valid.

The PMA may specify additional requirements for any Subject.

3.2.4 Non-verified subject information

Use of non-verified information may be included in Certificates governed by this Certificate Policy.

Where non-verified information is incorporated in a Certificate these sources of information must be detailed in the “Registration Authorities Operational Process & Guidance" [21] and approved by the Issuing Authority.

3.2.5 Validation of authority

Validation of authority (i.e. the determination of whether a Subject has specific rights, entitlements, or permissions, including the permission to act on behalf of an organisation to obtain a Certificate) is the responsibility of the Registration Authorities. Validation procedures shall be conducted as described in the Issuing Authority document “Registration Authorities Operational Process & Guidance" [21] Details of validation procedures may be published to Participants.

3.2.6 Criteria for interoperation

The criteria by which another Certification Authority wishing to operate within, or interoperate with the PKI governed by this Certificate Policy is defined by the Policy Management Authority. The Policy Management Authority will also determine whether any specific Certification Authority is approved for interoperation.

The Policy Management Authority operates formal mechanisms for approval of interoperation with other trust infrastructures. This requires but is not limited to:

- Provision of a Certificate Policy which at a minimum is equivalent to NHS Level 1 CA requirements.
- A Certification Practice Statement that demonstrates compliance with the corresponding Certificate Policy.
- Evidence of operational compliance with the CPS and CP, e.g. via independent audit.

Requests for interoperation must be directed in the first instance to the Issuing Authority, whose contact details are given in Section 2.1 of the PKI Disclosure Statements [5, 6, 7]**.**

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-key of Certificates governed by this Certificate Policy prior to any revocation or expiry is permitted.

Re-key requests from Subscribers and any Subject shall at a minimum, incorporate mechanisms for Authentication that fulfil initial authentication requirements. Proof of possession of a valid Certificate via Authentication (by making use of the associated ‘private key’) is permitted.

3.3.2 Identification and authentication for re-key after revocation

Re-Key after Revocation requests to the Registration Authorities, must at a minimum include the identification and Authentication of the requester to at least the Authentication standards defined in the governing Certificate Policy. This by definition is an issuance of a new Certificate.

3.4 Identification and authentication for revocation request

Revocation requests must at a minimum include the identification and authentication of the requester and sufficient information to uniquely identify the Certificate to be Revoked. Valid proof of possession of the Certificate to be Revoked (via use of the associated 'private key') is permitted as Authentication.

The risk for fraudulent misuse of the Private Key associated with the Certificate to be Revoked must be recognised. Where reliable authentication of the Revocation request is not possible or even omitted, either the Issuing Authority or Registration Authority acting on its behalf, is authorised to conduct Revocation. In such cases the Issuing Authority or Registration Authority shall seek confirmation of the request to the greatest extent possible by practical means, prior to Revocation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate applications may be made by the following:

- A Subscriber.
- A representative of a Subject acting on behalf of the Subject.
- A Registration Authority (including approved operators, Vettors, Sponsors and Pre-Authorisation managers).

Certificate applicants must comply with the procedures described in this document. Eligible Subjects are specified in Section 2.15 of the PKI Disclosure Statements [5, 6, 7].

An application for a Certificate does not oblige an Issuing Authority to Issue a Certificate.

4.1.2 Enrolment process and responsibilities

A range of enrolment processes are permitted.

The Issuing Authority in its document “Registration Authorities Operational Process & Guidance" [21] defines the specific processes associated with a particular enrolment mechanism.

In all cases enrolment processes shall include:-

- Provision of accurate information in support of authentication (and validation of a Subject or representative of an organisation if applicable).
- Proof of possession of the Private Key.
- Acceptance of the RA01 User Registration form [21] or the equivalent ‘on-line’ form by the Subscriber.

Compliance with this Certificate Policy and obligations of Subscribers and Subjects are defined in Section 2.4 of the relevant PKI Disclosure Statement [5, 6, 7].

4.1.2.1 Registration Authorities and their Representatives

Enrolment of RAs and their representatives, including managers is undertaken once the RA organisation has been approved by either a superior RA or the Issuing Authority.

Issuance of Certificates to RA Operators, Vettors and Pre-Authorisation managers shall be conducted by the Issuing Authority via security devices which are managed and maintained under the direct control of the Issuing Authority or by specifically nominated and duly authenticated representatives of the Registration Authority. See section 3.2.3.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Issuing Authority or an approved Registration Authority acting on its behalf is permitted to conduct authentication of Subscribers and Subjects.

4.2.2 Approval or rejection of certificate applications

The Issuing Authority or Registration Authority acting on its behalf will either approve or reject a Certificate application.

Where an application fails to achieve the specified authentication requirements or the level of assurance of authentication cannot be met a Certificate application will be rejected.

Where approved, the Certificate application will be digitally signed for processing by the Certificate Manufacturer.

Where a Certificate application is rejected, the reasons for rejection may be given to the prospective applicant in accordance with the Issuing Authority “Registration Authorities Operational Process & Guidance" [21].

4.2.3 Time to process certificate applications

Within 5 days of submission of the certificate application to the RA.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificates shall be Issued by the Certificate Manufacturer only in response to a properly constructed, signed and validated Certificate request from the relevant Registration Authority. Only an approved Registration Authority system can communicate with the associated Certificate Manufacturer to submit a Certificate request.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Certificate Manufacturer (i.e. Certificate Authority) does not communicate with the Subscriber or Subject regarding Certificate Issuance. The Registration Authority is responsible for such notification where applicable.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

A Subject shall explicitly indicate acceptance of a Certificate to the Issuing Authority, or Registration Authority acting on its behalf, this may be via technical or procedural processes.

Collection of a Certificate via on line authentication by the Subscriber or Subject constitutes acceptance of the Certificate.

Acceptance of tokens, smart cards or similar devices which possess Private Keys constitutes acceptance of the associated Certificate.

Use of a private-key for an activity or transaction approved under this Certificate Policy constitutes acceptance of the associated Certificate.

The Issuing Authority shall ensure that the Subscriber (or its authorised representative), during application for or delivery of a Certificate, is provided with the details of terms and conditions stipulated in the governing Certificate Policy, associated Subscriber Agreement and any other applicable contractual commitments.

The Subject must, acknowledge that it agrees to the terms and conditions stipulated in the Certificate Policy and the associated RA01 Registration form [22] or the 'online' version of same and any other applicable contractual commitments prior to first use of the Certificate.

The authorised representative of the Subscriber (which may be the Subject) may give this acknowledgement on behalf of a Subject or device requesting and collecting a Certificate.

The Issuing Authority shall undertake to clearly inform the Subject or Subscribers representative that by accepting a Certificate Issued under this Certificate Policy, a Subject agrees to, and certifies, that at the time of Certificate acceptance and throughout the operational period of the Certificate, until notified otherwise by the Subscriber:

- No unauthorised person has ever had access to the Subject's Private Key; and
- All information given by the Subject to the Issuing Authority or Registration Authority is true and accurate.

The above stipulations may be integrated with the Certificate application process and any smart card or token delivery process as appropriate.

4.4.2 Publication of the certificate by the CA

The Certificate Manufacturer (i.e. Certificate Authority) places the Issued Certificate in a Repository or other location as specified by the Issuing Authority. This repository may be subject to access restrictions.

Further "publication" of the Certificate is permitted. Details of approved Repositories are provided in Section 2.14 of the PKI Disclosure Statements. [5, 6, 7]

4.4.3 Notification of certificate issuance by the CA to other entities

The Certificate Manufacturer (i.e. Certificate Authority) does not directly inform any other participants of the Issuance of a Certificate.

Notification of Certificate Issuance, by inclusion into a directory or other mechanism for Certificate Discovery is permitted.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subjects and Subscriber's representatives must ensure that use of the Private Key associated with the Certificate is consistent with the usage restrictions in the Certificate as stipulated in sections 1.4.1 and 1.4.2 of this policy and as otherwise published by the Issuing Authority.

4.5.2 Relying party public key and certificate usage

A Relying Party may only rely on a Subject's Public Key and Certificate for the specific functions stipulated and published by the Issuing Authority. Where PKIs interoperate, this must be through the terms and conditions as stipulated and published in an interoperability agreement, or similarly named document.

Relying Parties must satisfy the requirements for reliance on a Certificate defined in Section 2.5 of the PKI Disclosure Statements. [5, 6, 7]

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificates may, subject to approval by the Issuing Authority, be Renewed at any time during their Operational Period, in accordance with the procedures described in the current version of the document "Registration Authorities Operational Process & Guidance" [21]. Without prejudice to Section 3.3, renewal of Expired, Revoked or Suspended Certificates is not permitted.

Renewal requests from Subscribers and Subjects shall at a minimum, incorporate mechanisms for Authentication that fulfil initial authentication requirements. Proof of possession of a valid Certificate as authentication is permitted.

Subject Certificates - Following the initial issuance, re-key is required for every subsequent issuance.

4.6.2 Who may request renewal

Renewal applications may be made by:

- A Subject holding the Certificate.
- A Sponsor acting on behalf of a Subject holding the Certificate.
- An RA.
- Automatically by the Certificate Manufacturer (provided standing orders for renewal have been contractually agreed upon with the Certificate Manufacturer).

4.6.3 Processing certificate renewal requests

The Issuing Authority or Registration Authority acting on its behalf will either approve or reject an application for Certificate Renewal.

Certificate renewals are automatically processed by the Certificate Manufacturer (i.e. Certificate Authority) in response to a properly constructed and signed Certificate request from the relevant Registration Authority.

Extension of validity of a Key Pair beyond the initial validity period of Key Pair, as defined by the Expiry Date field of the Issued Certificate is not permitted.

4.6.4 Notification of new certificate issuance to subscriber

As specified in Section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

As specified in Section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

As specified in Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

As specified in Section 4.4.3.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Re-Key of Certificates is permitted at any time during their Operational Period. Re-Key of Expired, Revoked or Suspended Certificates is not permitted.

4.7.2 Who may request certification of a new public key

Re-Key requests may be made by:

- A Subject or Subscriber's representative holding the Certificate.
- A Sponsor acting on behalf of a Subject holding the Certificate.

4.7.3 Processing certificate re-keying requests

The Issuing Authority or Registration Authority acting on its behalf will either approve or reject an application for Re-Key of a Certificate.

Certificate Re-Key requests are automatically processed by the Certificate Manufacturer (i.e. Certificate Authority) in response to a properly constructed and signed Certificate request from the relevant Registration Authority.

4.7.4 Notification of new certificate issuance to subscriber

As specified in Section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

Acceptance of a Re-Keyed Certificate is the same as that for Issued Certificates. See Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

As specified in Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

As specified in Section 4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Certificate modification is not permitted. Changes to Certificates must be enacted via Issuance of a new Certificate or one of the approved processes specified in this Certificate Policy.

4.8.2 Who may request certificate modification

See Section 4.8.1.

4.8.3 Processing certificate modification requests

See Section 4.8.1.

4.8.4 Notification of new certificate issuance to subscriber

See Section 4.8.1.

4.8.5 Conduct constituting acceptance of modified certificate

See Section 4.8.1.

4.8.6 Publication of the modified certificate by the CA

See Section 4.8.1.

4.8.7 Notification of certificate issuance by the CA to other entities

See Section 4.8.1.

4.9 Certificate revocation and suspension

Certificate Status Information services shall identify all Revoked and/or Suspended Certificates; at least until their assigned validity period expires.

Upon Revocation or Suspension of a Subject's Certificate, the Issuing Authority shall undertake to inform the Subject or Subscriber's representative.

4.9.1 Circumstances for revocation

The circumstances under which Certificate Revocation may be requested (and carried out) is defined by the Issuing Authority and published as appropriate in the current version of the document "Registration Authorities Operational Process & Guidance" [21]. The Registration Authority is responsible for the implementation of the decision of the Issuing Authority.

Registration Authorities must conduct verification of Revocation and Suspension Requests in accordance with this Certificate Policy. See Section 3.4

A Certificate must be Revoked:

- When any of the information in the Certificate is known or suspected to be inaccurate.
- Upon suspected or known compromise of the Private Key associated with the Certificate.
- Upon suspected or known compromise of the media holding the Private Key associated with the Certificate.
- When the Subject withdraws from or is no longer eligible to participate in the Public Key Infrastructure governed by this Certificate Policy.

The Issuing Authority or any Registration Authority acting on its behalf may Revoke a Certificate when an Entity fails to comply with its obligations set out in this Certificate Policy, any additional published documents defining practices to be followed by the entity, any other relevant agreement or any applicable law.

4.9.2 Who can request revocation

The Revocation of a Certificate may be requested by any entity, provided they are authenticated according to section 3.4 of this Certificate Policy.

The Revocation request must present a valid circumstance for Revocation as outlined in section 4.9.1 of this Policy.

Approval of a Revocation request may only be granted by:

- The Policy Management Authority.
- The Issuing Authority.
- An Approved Registration Authority.
- Authorised Registration Authority Operators.

4.9.3 Procedure for revocation request

Revocation must be requested promptly after detection of a compromise or any other event giving cause for Revocation.

A Revocation request may be generated in the following ways, in order of preference:

- Electronically by a digitally signed message.
- By personal representation to the Issuing Authority or a Registration Authority.
- By a signed fax message.
- Electronically by a non-signed message.
- By telephone call to the Issuing Authority or a Registration Authority.

Certificate Revocation requests will be received by the Registration Authority which must:

- Conduct authentication of the requestor.
- Validate the reason for the request.
- Ensure sufficient information to uniquely identify the Certificate which is the subject of the request.

The risk for fraudulent misuse of the Private Key associated with the Certificate to be Revoked must be recognised. Where reliable authentication of the Revocation request is not possible or even omitted, either the Issuing Authority or any Registration Authority acting on its behalf, is authorised to conduct Revocation. In such cases the Issuing Authority or Registration Authority shall seek confirmation of the request to the greatest extent possible by practical means, prior to Revocation. Processes may involve additional checking and information gathering to allow the Issuing Authority or its representative to achieve a satisfactory level of assurance of the validity of the request.

Certificate Revocations are automatically processed by the Certificate Manufacturer (i.e. Certificate Authority) in response to a properly constructed and signed Revocation instruction from the relevant Registration Authority.

4.9.4 Revocation request grace period

None. If the Revocation request is approved, it must be enacted as soon as practicable and reflected in the next scheduled publication of Certificate Status Information.

4.9.5 Time within which CA must process the revocation request

The time to process a Certificate Revocation request is made up of two elements:

- The time for the Certificate Revocation request to be validated, approved and action taken by the Registration Authority. This time is not constrained but the Registration Authority must take all reasonable steps to conduct the Revocation procedure expeditiously.
- The time taken for the Certificate Manufacturer to respond to the authorised Certificate Revocation request. The Certificate Manufacturer must respond promptly to duly authorised Revocation requests. The maximum time taken for this element is determined by the Issuing Authority in its contract with the Certificate Manufacturer.

4.9.6 Revocation checking requirement for relying parties

The mechanisms, if any, that a Relying Party may use (or where defined in Section 2.5 of the PKI Disclosure Statements) in order to check the Certificate Status Information of the Certificate upon which they wish to rely, must be via a Certificate Revocation List or equivalent on-line protocol that permits authenticity and integrity of the Status Information to be verified. Specific mechanisms will be defined in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

4.9.7 CRL issuance frequency (if applicable)

The frequency of CRL Issuance is defined in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency of CRL Issuance shall be defined in the contract between the Issuing Authority and the Certificate Manufacturer and published by the Issuing Authority.

4.9.9 On-line revocation/status checking availability

The availability of on-line Certificate Status checking is published by the Issuing Authority in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

4.9.10 On-line revocation checking requirements

The requirements on Relying Parties to perform on-line Certificate Status checking are defined in Section 2.5 of the PKI Disclosure Statements [5, 6, 7].

4.9.11 Other forms of revocation advertisements available

Where applicable, the availability of other forms of Revocation advertisement is published by the Issuing Authority in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

4.9.12 Special requirements re key compromise

In the event of the compromise, or suspected compromise, of any Entity's Private Key, an Entity must notify the Issuing Authority or Registration Authority immediately and must indicate the nature and circumstances of the compromise, to the fullest extent known.

4.9.13 Circumstances for suspension

Certificate suspension is under the control of RAs. Suspension may be used in circumstances where there is no evidence or suspicion of private key compromise and where the use of the suspension facility is more efficient for RA operations than certificate revocation/renewal.

Detailed requirements are laid down in section 13.1 of the 'Registration Authority User Guide" [27].

Where there is any evidence or suspicion of any instance of private key compromise, the certificate(s) must be revoked see section 4.9.1.

4.9.14 Who can request suspension

One or more of the following parties can request suspension of a certificate:

- The Policy Management Authority.
- The Issuing Authority.
- A Registration Authority.
- A Certificate Holder in whose name the Certificate was issued.
- The Certificate Holder's Sponsor or someone in the Certificate Holder's organisation with managerial responsibility for the Certificate Holder or a designated security officer of the organisation.
- Trust Service Providers.
- Health care professional body or officer (such as Caldicott guardians, Medical Directors of NHS Trusts, or the General Medical Council).

All suspension requests must be authenticated. Detailed requirements are laid down in section 13.1 of the 'Registration Authority User Guide" [27].

4.9.15 Procedure for suspension request

Detailed requirements are laid down in section 13.1 of the 'Registration Authority User Guide" [27].

4.9.16 Limits on suspension period

There is no time limit on certificate suspension. Once suspended, certificates will remain suspended until the suspension on the certificate is removed, the certificate is revoked or its validity expires.

4.10 Certificate status services

4.10.1 Operational characteristics

The types of Certificate Status checking services made available to the Subscriber by the Repository are defined in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

4.10.2 Service availability

The availability of any Certificate Status checking services that are available to Relying Parties is, if applicable, published in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

4.10.3 Optional features

The optional features of any Certificate Status checking services that are available to the Relying Parties are, if applicable, published in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

4.11 End of subscription

Subscribers - At the end of a commercial arrangement or subscription, the relevant Certificates may either be Revoked or permitted to expire. The decision on which action to take is made by the Issuing Authority and implemented by the Registration Authority on a case by case basis and is communicated directly to the Subject concerned.

Service Termination - The actions to be taken in the event of the termination of the service will be defined in the contract between the Issuing Authority, the Certificate Manufacturer and any other Participants providing the Service.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Participants providing trusts services shall not offer or support any form of key escrow.

Subscribers may facilitate key recovery mechanisms locally for keys used for authentication or encryption services.

Key escrow or recovery is not permitted for keys used for signing or content commitment.

4.12.2 Session key encapsulation and recovery policy and practices

This Certificate Policy does not prescribe or control session key management for applications. Use of session key management is a matter for Subscribers.

The Issuing Authority does not offer or support any form of session key encapsulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Where “no stipulation” is stated in this section of the Certificate Policy it indicates there are no specific prescribed requirements for the controls, configuration or security requirements.

Where no prescribed requirement is stipulated, specific details on controls operated for components of the PKI infrastructure must be detailed in the Certification Practice Statement (CPS) and/or supporting documentation.

Controls must be approved by the Policy Management Authority (PMA).

5.1 Physical controls

5.1.1 Site location and construction

Sites where Certificate manufacture or time-stamping operations are carried out must:

- Satisfy at least the security requirements for a physical location which will be used to store sensitive information. These requirements are stipulated in the contract between the Certificate Manufacturer and the Issuing Authority.
- Be manually or electronically monitored for unauthorised intrusion at all times.
- Ensure unescorted access to the CA or time-stamping server is limited to those personnel identified on an access list.
- Ensure personnel not on the access list are properly escorted and supervised.
- Ensure a site access log is maintained and inspected periodically.
- Ensure all removable media and paper containing sensitive plain text information is stored in secure containers.

Under this Certificate Policy, the detailed functionality of a Registration Authority is described in the current document “Registration Authorities Operational Process & Guidance" [21] and as stipulated within relevant sections of the ‘Registration Authority Guidance’ web pages [20]. NHS Registration Authorities must comply with the security requirements specified in this document and on this web site.

In the case where the Registration Authority initialises and loads Certificates and Private Keys into stores or tokens, then the RA’s physical security controls shall be equivalent to those required for Certificate manufacture as described in this section. Subscriber key material must not be stored on RA workstations.

All Repository sites must be located in areas that satisfy the physical security controls as governed by the existing contractual arrangements between CFH and the Spine Service Provider i.e. adherence to the NHS CFH Contractor Security Policy [11] for both staff vetting and the maintenance and operation of secure processing facilities, including access and accompanied access to such facilities.

Where PINs, pass-phrases or passwords are recorded, they must be stored in a security container accessible only to authorised personnel.

5.1.2 Physical access

See section 5.1.1.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

Controls must be placed on all media used for the storage of information such as keys, activation data, confidential Subscriber information or CA data. Controls must be detailed in the Certification Practice Statement and/or supporting documentation.

5.1.7 Waste disposal

All media used for the storage of information such as keys, activation data, confidential Subscriber information or CA data is to be sanitised or destroyed before being released for disposal.

All documentation classified as ‘Confidential’ or equivalent shall be subject to a defined secure disposal procedure.

5.1.8 Off-site backup

Off site backup arrangements must be in place as required by the business continuity arrangements outlined in Section 5.7

Where data and facilities are removed from primary locations or in support of Business Continuity activities, controls must be applied which are at least comparable with those of the primary location.

5.2 Procedural controls

5.2.1 Trusted roles

A Participant providing Trust Services must ensure a separation of duties for critical functions to prevent a single person from maliciously using CA systems and supporting systems without detection.

The Certificate Manufacturer shall provide for the separation of distinct PKI personnel roles by named personnel, distinguishing between day-to-day operation of the CA system and the management and audit of those operations. To the greatest extent possible, differing levels of physical and systems access control based on roles and responsibilities must be employed to reflect the requirements of those roles and responsibilities. Controls must be detailed in the Certification Practice Statement and/or supporting documentation.

Registration Authorities must ensure that all Registration Authority personnel are adequately trained and understand their responsibility for the identification and authentication of prospective Subscribers and related Certificate management tasks. Registration Authorities shall document arrangements for trusted roles in the current document “Registration Authorities Operational Process & Guidance" [21]. Arrangements must be approved by the Issuing Authority or Auditors acting on its behalf.

A Registration Authority may permit all roles and duties for Registration Authority functions to be performed by one individual.

5.2.2 Number of persons required per task

Multi-user control is required for CA Key generation.

Multi-person controls must be established for the performance of critical functions associated with the build and management of CA systems, including the software controlling Certificate manufacturing operations.

All other duties associated with Certificate Manufacture or Participants providing other Trust Services may be performed by an individual operating alone, however, verification processes employed must provide for oversight of all activities performed by trusted role holders.

5.2.3 Identification and authentication for each role

All Participants providing Trust Services shall ensure personnel in trusted roles have their identity and authorisation verified before they are:

- Included in the access list for the Trust Service provider site.
- Included in the access list for physical access to the Trust Service provider systems.
- Given a credential for the performance of their Trust Service provider role.
- Given an access on Trust Service provider systems.

Credentials issued to personnel in trusted roles must be:

- Managed so that their use can be detected and monitored.
- Managed so that their use is restricted to actions authorised for that role through applicable technical and procedural controls.
- Maintained under a prescribed and documented security policy.

5.2.4 Roles requiring separation of duties

For the Certificate Manufacturer, roles requiring the separation of duties are not specifically prescribed. The assignment of duties among personnel shall maintain appropriate separation of duties so as not to compromise the security arrangements for the Certificate Manufacturing and other critical processes. The Certificate Manufacturer shall maintain records of role allocation.

Other Participants providing Trust Services shall maintain appropriate separation of duties so as not to compromise the security arrangements for critical processes. For NHS Registration Authorities, these requirements are detailed in the current document “Registration Authorities Operational Process & Guidance" [21].

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

A Participant providing Trust Services must ensure that all personnel performing duties with respect to its operation must:

- Be appointed in writing.
- Be bound by agreement to the terms and conditions of the position they are to fill.
- Have received training with respect to the duties they are to perform.
- Be bound by agreement not to disclose sensitive security-relevant information or Subscriber information and maintain required protection of personal information.
- Not be assigned duties that may cause a conflict of interest with their service provision duties.
- Not have been, as far as known, previously relieved of a past assignment for reasons of negligence or non-performance of duties.

The Issuing Authority for its Registration Authorities and other Trust Service Providers may also specify additional criteria for security clearance of personnel, such as requirements for citizenship, rank, qualifications, satisfactory credit check, and absence of a criminal record. For NHS Registration Authorities this will be described in the current version of the CFH document “Registration Authorities Operational Process & Guidance" [21]. For other Trust Service Providers these shall be stated in the Certification Practice Statement and/or supporting documentation.

5.3.2 Background check procedures

See Section 5.3.1.

5.3.3 Training requirements

See Section 5.3.1.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

A Participant providing Trust Services must ensure that contractor access to its facilities is in accordance with the NHS CFH Contractor Security Policy [11]. Individuals not security cleared must be under supervision by approved personnel at all times.

The actions of contracting staff are subject to the same audit arrangements and requirements as those of the personnel of the Participant providing Trust Services.

5.3.8 Documentation supplied to personnel

All personnel associated with Trust Service provision shall be provided access to all documentation relevant to their position. This will include the Certificate Policies and any associated Certification Practice Statements relevant to the service, together with any specific supporting documentation, statutes, policies or contracts relevant to the position and role of the personnel.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Certificate Manufacturer - Audit logs of all transactions relevant to Certificate creation, Certificate lifecycle management and the operation of trusted systems and services must be maintained to provide an audit trail. The event types are, at a minimum:

- Messages received from authorised sources requesting an action on the part of the CA.
- All actions taken in response to requests.

- Trusted system installation and any modifications.
- Receipt, servicing and shipping of hardware cryptographic modules.
- Creation and issuance of CRLs.
- All error conditions and anomalies associated with the operation of trusted systems and services.
- Any known or suspected violations of physical security.
- Any known or suspected violations of network and/or trusted system security.
- All CA and trusted application start-up and shutdown.
- All usage of the CA signing key.
- All personnel/role changes for trusted roles.
- All issuance records, including those approved by NHS CFH for End Point Registration Process and the daily DNS spreadsheets.

Issuing Authority – For the registration of End Point Certificates, the following information must be retained for audit purposes:

- All requests for End Point Registration approval from BT EPR team.
- All e-mails relating to the End Point Registration approval/rejection process.

Registration Authorities – Must record for audit purposes, at a minimum the event types listed below:

- Any log on/off attempts by RA operators.
- All messages from authorised sources requesting an action of the RA and the subsequent actions taken by the RA in response to such requests.
- All messages to the CA requesting an action of the CA and the subsequent action taken by the CA.
- All physical accesses to RA systems (including components) and RA locations
- RA application start-up and shut down.
- All use of the RA signing key(s).
- Any suspected or known violations of physical security.
- Any suspected or known violations of network and system security.
- All checks made for the registration of RA staff.
- All personnel/role changes for trusted roles.

5.4.2 Frequency of processing log

Participants providing Trust Services may review audit logs as appropriate to the items being recorded.

The Participant shall provide details of audit log processing in the records of role allocation in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

5.4.3 Retention period for audit log

Audit logs are to be retained for the following periods as described in the current version of the NHS CFH document ”IG Audit & Alerts Gold Standard” [15]:

- 3 Years on-line (Years 1 to 3) for those data items described in section 5.4.1, plus any other data items considered appropriate that are recorded in on-line systems. For those data items that are not captured on-line, the retention conditions described in the following bullet point shall apply for a period of 10 years (Years 1-10 inclusive).
- A further 7 years off-line, recoverable within 1 working day (Years 4 to 10 inclusive)
- A further 20 years off-line, recoverable within 1 working week (Years 11 to 30 inclusive) – slight change from 26 but in line with HSC 1999/053

5.4.4 Protection of audit log

The electronic audit log system must be securely managed in accordance with ISO 27002:2005 (“Code of Practice for Information Security Management”) and any subsequent revisions or standards that supersede it, as a minimum, and must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction.

5.4.5 Audit log backup procedures

Audit logs and audit summaries must be backed up or if in manual form, must be copied.

Such backups must be provided with the same level of security as the originals and must be commensurate with the data contained within them and the business continuity arrangements of the Trust Service Provider.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The events and any accompanying data as described in section 5.4.1 of this Certificate Policy are to be archived.

As a minimum the following data must be archived:

- Trust Service Provider key creation ceremony records.
- Trust Service Provider's policies and procedures.
- Contractual obligations – Certificate Manufacturer and RAs.
- System equipment and configuration – Certificate Manufacturer and RAs.
- Certificate requests – Certificate Manufacturer and RAs.
- Revocation requests – Certificate Manufacturer and RAs.
- Certificate suspension/removal of suspension requests - Certificate Manufacturer.
- Certificate Holder identity authentication and supporting evidence records - RA.
- Documentation of receipt and acceptance of Certificates - RA.
- Documentation of receipt of tokens - RA.
- All Certificates issued or published - Certificate Manufacturer.
- All CRLs issued and or published – Certificate Manufacturer, plus any other forms of Certificate Status Information.

Participants providing Trust Services may also be required to retain additional information to ensure compliance with this Certificate Policy and/or legal requirements.

Registration Authorities must retain records of information provided in support of Certificate application and Revocation or Suspension requests.

5.5.2 Retention period for archive

Archived information is to be retained in accordance with the requirements stated in section 5.4.3.

5.5.3 Protection of archive

Archives are to be protected from unauthorised viewing, modification, and deletion.

Archives are to be adequately protected from environmental threats such as temperature, humidity and magnetism.

Multiple copies of information may be archived.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Participants providing Trust Services shall comply with the confidentially requirements specified in this Certificate Policy (see section 9.3).

Records of individual transactions may be released upon request by any of the Participants involved in the transaction, or their recognised representatives.

Participants providing Trust Services shall ensure availability of their archives and that archived information is stored in a readable format during its retention period, even if the Trust Service Provider's operations are interrupted, suspended or terminated.

In the event that the services of a Participant providing Trust Services for or on behalf of the Issuing Authority are to be interrupted, suspended or terminated, the Issuing Authority shall ensure the continued availability of the archive. All requests for access to such archived information shall be sent to the Issuing Authority or to the entity identified by the Issuing Authority prior to terminating its service.

5.6 Key changeover

A Subject or Subscriber's representative may only renew or replace their Certificate and key pair prior to the expiration of the keys, provided that the current Certificate remains valid and has not been Revoked or Suspended. This key changeover may be initiated by one of the following:

- The Subject (or Subscriber's representative).
- The Sponsor.
- The Registration Authority.
- The Issuing Authority.

Automated notification of an impending required key changeover is permitted, but not required to be supported.

Subjects without valid keys must be re-authenticated in the same manner as for an initial registration.

Where a Subjects Certificate has been Revoked as a result of suspected or actual non-compliance, the Registration Authority or the Issuing Authority that intends to initiate the key changeover process must verify that the reasons for non-compliance have been satisfactorily addressed and resolved prior to Certificate Re-issuance.

Certificate Manufacturer (CA) and Issuing Authority (CA) - All CA signing keys shall be generated and a new CA-certificate corresponding to these keys shall be Issued at least three months prior to the expiration of the old CA-certificate.

After generation of the new Issuing Authority (CA) signing keys, the Issuing Authority shall cross certify according to the requirements for cross certification as approved by the Policy Management Authority and must include the following:

- The Issuing Authority holding the new private CA-key shall Issue one Certificate for the old public CA-certificate signed with the new private CA-key and;
- The Issuing Authority holding the old private CA-key shall Issue one Certificate for the new public CA-certificate signed with the old private CA-key.

All CA-certificates shall be made available in a repository accessible to all Participants in the PKI [14] and may be made available in other locations as required.

All copies of old Issuing Authority private CA-keys shall be:

- Destroyed such that the Private Keys cannot be retrieved; or
- Retained in a manner such that they are protected against being put back into use.

Either one of the above options must be taken following expiry of the associated CA Public Key Certificate

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

A business continuity plan shall be in place to protect critical Public Key Infrastructure processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all Issuing Authority services. Business continuity plans for Participants providing Trust Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Issuing Authority or Auditors acting on its behalf.

Participants providing Trust Services must provide evidence that such plans have been exercised.

In the case of compromise of a CA or CA-keys, the Issuing Authority shall as a minimum require the following:

- Immediately cause the suspension of the Certificate Status checking service for all Issued Certificates affected by a compromise, failure or disaster. This will stop any of these Certificates from being accepted by any Relying Party who follows proper Revocation checking procedures according to Section 2.5 of the relevant PKI Disclosure Statement [5, 6, 7].
- Suspension of any further Certificate Issuance from the affected CA.

The Policy Management Authority and/or Issuing Authority shall make any determination relating to Revocation of CA Certificates.

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

Participants providing Trust Services must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Business continuity plans for Participants providing Trust Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Issuing Authority or Auditors acting on its behalf.

5.7.3 Entity private key compromise procedures

See Section 5.7.1

5.7.4 Business continuity capabilities after a disaster

The business continuity plan for the Certificate Manufacture shall be designed to deal with any disruption to services and shall ensure managed, progressive recovery of components used to provide the service. A geographically separate alternative backup facility in order to maintain, at a minimum, for Certificate Status information must be made available.

Any backup facility used for relocation following a disaster shall maintain compliance with this Certificate Policy. The provisions of this Certificate Policy shall be maintained during any relocation/transition.

Registration Authorities deployment and configuration details vary. No specific business continuity requirements are defined. NHS Registration Authority business continuity arrangements must be approved by the Issuing Authority or Auditors acting on its behalf.

5.8 CA or RA termination

Termination of a CA is regarded as the situation where all service associated with an Issuing Authority is terminated permanently. It is not the case where the service or elements of the service is transferred, such as between or to Certificate Manufacturers or responsibility for Certificates is transferred between Issuing Authorities, even if there is a change of CA-Keys.

Certificate Manufacturer – The specific circumstance related to termination of a CA must be prescribed by the Issuing Authority. At a minimum the following actions shall be taken under the direction of the Issuing Authority:

- Inform both the Issuing Authority and Policy Management Authority for the governing Certificate Policy.
- Provide a notice period of 90 days.
- Revoke all relevant CA and Subscriber Certificates at the end of 90 days if required by the Issuing Authority.

- Arrange with a third party for the preservation and storage of records for the minimum period of time stipulated for the service being terminated but in any event not less than 7 years.

Registration Authority – Registration Authorities deployment and configuration details vary. At minimum the Registration Authority terminating service shall:

- Have all RA keys under their control Revoked.
- Have all RA Operator, Vettor and Pre-Authorisation manager Certificates Revoked.
- Ensure preservation and storage of records for the minimum period of time stipulated for the service being terminated but in any event not less than 7 years. Alternatively with the written approval of the Issuing Authority records may be transferred to another Participant providing Trust Services, e.g. a new or alternative Registration Authority.

Registration Authority termination arrangements must be approved by the Issuing Authority or Auditors acting on its behalf.

6 TECHNICAL SECURITY CONTROLS

Where “no stipulation” is stated in this section of the Certificate Policy it indicates there are no specific prescribed requirements for the controls, configuration or security requirements.

Specific details on technical controls operated for components of the PKI infrastructure must be detailed in the Certification Practice Statement and/or supporting documentation. Controls must be approved by the Issuing Authority or Auditors acting on its behalf.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Issuing Authority keys and CA-key pairs and signing keys shall be generated in a protected environment. CA Key generation shall be multi-person control using random numbers of such length so as to make it computationally infeasible to regenerate it, even with the knowledge of the when and in which equipment they were generated. See Section 6.2.1.

Private Keys used in any Issuing Authority and/or Trust Services process that affects the outcome of Issued Certificates and Certificate Status Information services (such as signing of Certificate Revocation Lists), must be generated under controlled procedures. Participants conducting such key generation shall provide detail of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

Keys used for signing shall only be generated by the Subject or generated under the direct control of the Subject.

Where keys are generated by Registration Authorities, the generation procedure and storage of the Private Key shall prevent it from being exposed outside of the system that created it. Furthermore, it shall be erased from the system immediately after having been transferred to a security environment that is approved by the Issuing Authority and satisfies the requirements of 6.2.1.

6.1.2 Private key delivery to subscriber

If the Private Key is not generated by the Subject, which in any case must only be accomplished, according to 6.1.1, it must be delivered to the Subject by the approved generator of the key and satisfying the requirements of 6.2.1. In this case:

- The security environment containing the Private Key, protected with its initial activation data, shall be distributed to the Subject in a way that prevents it from being found together with the activation data, until it has been delivered to the Subject. This can be achieved by using separate channels of distribution for security environments and their associated activation data, or by clearly separating their distribution in time.

- The security environment issuer may supply the activation data, delivering it directly to the Subject.
- Delivery of a security environment containing a Private Key that is (or will be) associated with a Certificate according to this Certificate Policy, is only allowed to be effected to the Subject in person through a face to face meeting with the Issuing Authority, or other authorised representative of the Issuing Authority. A sufficiently trusted representative of the Issuing Authority for this purpose would normally be the Registration Authority, but must be identified to the Subject at the time of application. To obtain the security environment, the Subject shall present valid identification that at least meets the requirements for initial registration see Section 3.2. The means of identification must be recorded.
- Subjects must acknowledge receipt of the security environment in writing which is retained by the Issuing Authority.
- Controls shall be in place to ensure the Subject shall replace initial activation data for the security environment with personally chosen activation data.

6.1.3 Public key delivery to certificate issuer

Certificate Manufacturer – All Public Keys from Registration Authorities shall be delivered in a secure manner using a standard, recognised protocol; (e.g. PKCS#10 [16]).

Registration Authority - The mechanism by which Subscriber Public Keys are delivered to the Certificate Manufacturer are in accordance with RFC 4210 [23].

6.1.4 CA public key delivery to relying parties

The delivery of Public Keys to the Certificate authority shall use PKCS#10 [16] or other equivalent standards compliant cryptographic mechanism or using a process specifically approved by the Certificate Manufacturer. Specific mechanisms must be approved by the Issuing Authority.

6.1.5 Key sizes

The size of Issuing Authority and any supporting CA-Keys shall be not less than 2048 bit modulus for RSA.

The size of Subjects' Private Keys shall be not less than 1024 bit modulus for RSA.

6.1.6 Public key parameters generation and quality checking

Public Key exponents shall be of values and lengths that make known attacks (e.g. low exponent attacks) infeasible.

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

Certificates Issued under this policy may be used in applications and services as listed in Section 2.2 of the relevant PKI Disclosure Statements [5, 6, 7]. Certificates may be used only for the functions defined in the key usage field of the Certificate.

Use of extensions in the Certificate shall be consistent with Section 7.1.2 of this Certificate Policy.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

CA-Keys shall be protected by high assurance physical and logical security controls. They must be stored in, and operated from inside a specific tamper resistant hardware based security module that complies with FIPS140-2 level 3 [17], its equivalents and successors.

Private Keys used in any Issuing Authority and/or Registration Authority process that affects the outcome of Issued Certificates and Certificate Status Information services (such as signing Certificate Revocation Lists), shall be protected by, maintained in, and restricted to, a hardware cryptographic token designed to meet the level of requirements as specified in FIPS 140-2 level 3 [17], or its equivalents and successors.

CA-Keys shall not be available in unprotected form (complete or unencrypted) except in approved cryptographic modules.

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

For any Issuing Authority and supporting CA-Keys and keys that affect the outcome of Issued Certificates and a Certificate Status Information service, at a minimum two-person control is required.

6.2.3 Private key escrow

Subscribers and Subjects shall not provide Private Key escrow services.

Participants providing trust services shall not provide Private Key escrow services.

6.2.4 Private key backup

Permission to back-up private signing keys depends upon the use of the certificate. Typically, keys used for Authentication may be backed-up; keys used for Content Commitment must not be backed up.

See Section 4.12 of this policy and also the relevant PKI Disclosure Statement [5, 6, 7].

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

If Subject Private Keys are not generated in the Entity's cryptographic module, it must be entered into the module via the use of a secure procedure approved by the Issuing Authority. Mechanisms to protect key material and any associated activation data from unauthorised access, modification and use shall be employed.

Participants conducting such key transfer shall provide detail of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf. See Section 6.1.2.

6.2.7 Private key storage on cryptographic module

For any Issuing Authority and supporting CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services and other business processes, prescribed standards are required for the cryptographic protection of Private Keys. See Section 6.2.1.

6.2.8 Method of activating private key

Subjects who are natural persons must be authenticated to their cryptographic module before the activation of the Private Key. This authentication may be in the form of a PIN, pass-phrase password or other activation data. When deactivated, Private Keys must not be exposed in plaintext form.

Where subjects are devices, software or hardware, access controls shall be such that only authorised computer systems or services and/or authorised personnel may activate the Private Key.

Cryptographic modules used by Participants providing Trust Services which are used as components of Certificate lifecycle management shall block themselves after a specified number of consecutive failed attempts to authenticate to the module.

Cryptographic modules used by Participants providing Trust Services and security environments used by Subscribers may contain an unblocking function. Unblocking shall require the authorised personnel to use a mechanism to authenticate to the module.

Participants conducting unblocking must provide detail of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

6.2.9 Method of deactivating private key

When private Keys are deactivated, they must be cleared from memory before the memory is unassigned. Any memory space where keys have been stored must be over-written before this space is released to the operating system.

The applicability of and, where relevant the value of, the inactivity time-out period are specified in the relevant PKI Disclosure statement [5, 6, 7].

6.2.10 Method of destroying private key

Strict controls over destruction of Issuing Authority, supporting CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services, must be exercised.

Whether active, expired or archived, the Issuing Authority must approve the destruction of Issuing Authority and supporting CA-Keys.

6.2.11 Cryptographic Module Rating

See Section 7.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys shall be archived in accordance with Section 5.5 of this Certificate Policy.

6.3.2 Certificate operational periods and key pair usage periods

Usage periods for key pairs shall be governed by validity periods set in Issued Certificates. These shall have the following maximum values:

- Subjects (Authentication and Content Commitment)– up to two (2) years.
- Entrust Security Officer – two (2) years
- CA interacting applications (i.e. CMS/COWS) – two (2) years
- Devices – up to three (3) years.
- On-line intermediate Issuing Authorities – ten (10) years.
- Off-line primary Issuing Authorities – twenty (20) years.

Certified Private Keys shall not be extended beyond the initial lifetime of the Certificate Issued to authenticate them. This means that a renewal which would result in Certificate expiry after the expiry date for the original Certificate issued for that Key Pair is not permitted.

6.4 Activation data

6.4.1 Activation data generation and installation

All Issuing Authority supporting CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services shall have activation data that is 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. Where PINs, passwords or pass-phrases are used, an entity must have the capability to change these at any time.

The unlocking of a smartcard is performed as detailed in the current version of the document “Registration Authorities Operational Process & Guidance" [21]. Delivery of the unblocking code requires strong identification of the holder. See Section 6.2.8.

6.4.2 Activation data protection

All Issuing Authority, supporting CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services shall have mechanisms for the protection of activation data which is appropriate to the Keys being protected.

Details of protection shall be provided in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Participants providing Trust Services shall implement security measures that have been identified through a risk assessment exercise and must cover the following functionality where appropriate:

- Access control to trust services and PKI roles.
- Enforced separation of duties for PKI roles.
- Identification and authentication of PKI roles and associated identities.
- Use of cryptography for session communication and database security.
- Archival of Participant history and audit data.
- Audit of security related events.
- Trusted path for identification of PKI roles and associated identities.
- Recovery mechanisms for keys of PKI Participants providing trust services.

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

Participants providing Trust Services shall document procedures in the Certification Practice Statement and/or supporting documentation. Procedures shall at a minimum include logging and audit requirements for processes related to initialisation, resetting, shutdown or reconfiguration of Certificate Authorities and any services that affect the outcome of Issued Certificates and Certificate Status Information.

6.5.2 Computer security rating

Participants providing Trust Services may use system components that do not possess a formal computer security rating provided that all requirements of this Certificate Policy are satisfied.

Any hardware security module or device holding CA Keys must comply with the requirements of 6.2.1 of this Certificate Policy.

Where specific additional requirements prescribe systems or security environments that fulfil specific security ratings, these must be detailed in the Certification Practice Statement and/or supporting documentation.

6.6 Life cycle technical controls

6.6.1 System development controls

The development of software, that implements Trust Service functionality shall as a minimum be performed in a controlled environment that, together with at least one of the following approaches, shall protect against the insertion of malicious logic.

- The system developer shall have a quality system compliant with international standards; or
- The system developer shall have a quality system available for inspection and approval by the Issuing Authority.

6.6.2 Security management controls

The configuration of systems operated by Participants providing Trust Services as well as any modifications, upgrades and enhancements must be documented and controlled. There must be a method of detecting unauthorised modification or configuration of the software supporting Trust Services. Participants providing Trust Services shall ensure that it has a configuration management process in place to support the evolution of the systems under its control.

Details of security management systems shall be provided in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or Auditors acting on its behalf.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Trust Service Provider systems must be protected from attack through any open or general-purpose network with which they are connected. Such protection must be provided and configured to allow only the minimal set of functions, protocols and commands required for the operation of the Trust Service.

Participants providing Trust Services shall detail the standards, procedures and controls for network security in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or Auditors acting on its behalf.

6.8 Time-stamping

Time recording shall be implemented for all Certificate and other related activities that require recorded time. A synchronised and controlled time source shall be used.

Participants providing Trust Services shall detail the time source used and mechanisms for its control in supporting documentation which must be approved by the NHS Issuing Authority.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificate Profiles are under the direct control of the Policy Management Authority.

Procedures for development of Certificate Profiles shall incorporate approval by the Policy Management Authority prior to implementation.

7.1.1 Version number(s)

Only Certificates conformant to X.509 Version 3 and IETF RFC 3280 [9] may be issued.

7.1.2 Certificate extensions

All Entity PKI software must correctly process the extensions identified in 4.2.1 and 4.2.2 of the IETF PKIX Certificate profile (RFC 3280 [9]). The following are common Certificate extensions:

- The Basic Constraints extension is set to TRUE for CA certificates only; its use is critical in specifying that it is a CA certificate. Subscriber and End Entity Certificates have the value set to FALSE.
- The Certificate Policies extension is mandatory and shall contain the appropriate OID for Certificates to indicate the use of this policy (according to 7.1.6). The Certificate Policy Qualifier Info extension shall be used to direct End-Entities to where this policy and other relevant information may be found.
- Where CRLs are used to produce Certificate Status information, the CRL Distribution Point extension is mandatory, and shall identify a location where the latest CRL Issued by the Issuing Authority can be obtained.

7.1.3 Algorithm object identifiers

RSA 1024, RSA 2048 in accordance with RSA PKCS#1 [24].

7.1.4 Name forms

The use of all name forms shall be consistent with section 3.1 of this Policy. Name forms shall be approved by the Issuing Authority.

7.1.5 Name constraints

Subject and issuer Distinguished Names must be present in all Certificates issued.

7.1.6 Certificate policy object identifier

This Certificate Policy has been assigned an OID as defined in section 2.12 of PKI Disclosure Statements [5, 6, 7]. This shall be included in the Certificate Policies extension of all Certificates Issued under this Certificate Policy.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

Only Certificate Revocation Lists conforming to X.509 version 2 and IETF RFC 3280 [9] may be issued.

An alternative to CRLs is permitted. The Issuing Authority may allow for provision of an on-line Certificate Status checking service, which meets the requirements of this policy.

7.2.2 CRL and CRL entry extensions

All Certificate holder software that is Certificate-aware must correctly process all CRL extensions as defined in RFC 3280 [9].

7.3 OCSP profile

7.3.1 Version number(s)

OCSP and other forms of Certificate Status Information provision are permitted.

Repositories shall detail the mechanisms for on line Certificate Status Information provision in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or Auditors acting on its behalf.

Mechanisms for on line Certificate Status discovery shall be specified in Section 2.18 of the PKI Disclosure Statements [5, 6, 7].

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The details for assessment are specified in contractual arrangements between the Issuing Authority and the Participants providing Trust Services.

For all Participants providing Trust Services, audit must be sufficient to demonstrate to both the Issuing Authority and Policy Management Authority that the services comply with this Certificate Policy and any supporting policy documents applicable to their services.

For Certificate Manufacturers, assessment shall be against the existing contractual arrangements, plus any other prescribed criteria defined by the Policy Management Authority and agreed with the Certificate Manufacturer.

For Certificate Manufacturers, audit shall be conducted against the requirements defined in the existing contract and any other agreed arrangements, by an approved third party auditor and conducted not less than annually.

The Issuing Authority may exercise right to audit any Participants providing Trust Services at any time.

8.2 Identity/qualifications of assessor

The suitability of assessors to perform assessment of the Issuing Authority and its associated Registration Authorities is decided by the Policy Management Authority.

Approved Auditors are as defined in section 2.11 of PKI Disclosure Statements [5, 6, 7] and may include internal auditing resources of Participants, subject to the approval of the Policy Management Authority.

For Certificate Manufacturers, audit shall be conducted by an approved third party auditor.

8.3 Assessor's relationship to assessed entity

The acceptability of auditors is decided by the Policy Management Authority.

8.4 Topics covered by assessment

Audit is required to ensure a Participant providing Trust Services is operating in accordance with its Certification Practice Statement or any supporting documentation, this Certificate Policy and any declared assurance or approval schemes under which Trust Services are operated.

Where the Participants providing Trust Services use any designated authorised agents in order to provide service, the audit shall include the operations of such designated authorised agents.

Audit will address all aspects of Trust Service operations (whether they directly or indirectly influence compliance with the Certification Practice Statement or any supporting documentation) to ensure overall standards of operation are commensurate with this Certificate Policy.

8.5 Actions taken as a result of deficiency

For compliance audits of Participants providing Trust Services, where significant exceptions or deficiencies are identified, the Issuing Authority will inform the Policy Management Authority and determine action to be taken. A remedial action plan will be developed with input from the auditor. The Policy Management Authority has overall responsibility to ensure implementation of the action plan. If an immediate threat to the security or integrity of the PKI services is identified, a corrective action plan which may include suspension or termination of non complaint services will be developed, approved by the Policy Management Authority and implemented by the Issuing Authority. For lesser exceptions or deficiencies, the Issuing Authority will determine the course of action to be taken.

8.6 Communication of results

Where compliance with third party assurance or approval schemes under which Trust Services are operated has been audited, approval status shall be made publicly available by the Participants providing Trust Services.

In the event of identification of material non-compliance with this Certificate Policy, the Issuing Authority shall make available to Subscribers, Subjects and Relying Parties details of the deficiency or deficiencies and any remedial action or actions required to be undertaken.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The Issuing Authority shall establish any fees for the Issuance of Certificates. Where fees are charged, the fee schedule shall be published and available to Subscribers at the time of application for a Certificate.

9.1.2 Certificate access fees

The Issuing Authority shall establish any fees for access to Certificate and Certificate Status Information. Where fees are charged, the fee schedule shall be made available to End Entities and Relying Parties.

9.1.3 Revocation or status information access fees

The Issuing Authority shall establish any fees for access to Certificate and Certificate Status Information. Where fees are charged, the fee schedule shall be made available to End Entities and Relying Parties.

9.1.4 Fees for other services

The Repository shall not impose any fees on the availability or distribution of this Certificate Policy, or any document incorporated by reference in any Certificate Issued under this Certificate Policy.

Fees for services such as access to archived information are permitted subject to approval by the Issuing Authority. If such fees are charged, the fee schedule shall be published and available to all affected parties.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

The Issuing Authority maintains adequate insurance coverage or alternative mechanisms to fulfil its obligation in relation to the Issuance of Certificates.

Insurance requirements for Participants providing Trust Services are specified in contractual arrangements between the Issuing Authority and Participants.

9.2.2 Other assets

In some cases the Issuing Authority facilitates mechanisms other than insurance to bear the liability to End Entities. Where this is the case, arrangements to fulfil liability commitments are specified in Section 2.6 of the PKI Disclosure Statements [5. 6. 7].

9.2.3 Insurance or warranty coverage for end-entities

The Issuing Authority does not provide warranty coverage to End Entities.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The Issuing Authority and all Participants providing Trust Services shall classify personal, privacy related or corporate information as Confidential. Such information shall not be released without the prior consent of the Subscriber, unless required otherwise by law.

All private and secret keys and associated activation data, used or otherwise handled by a Participant operating under this Certificate Policy shall be kept confidential unless required otherwise by law.

Audit logs and records shall not be made available as a whole, except:

- As required by law.
- As part of an audit, (in which case only to an approved auditor).
- For verification of audit logs (see section 5.4.7.).Only records of individual transactions may be released.

This information will only be disclosed by the Certificate Manufacturer in accordance with the governing Certificate Policy or as required by law.

9.3.2 Information not within the scope of confidential information

Certificates and Certificate Status Information are not classified as Confidential or as private. Identification information or other personal or corporate information appearing on Certificates is not considered Confidential.

9.3.3 Responsibility to protect confidential information

The Issuing Authority carries overall responsibility to protect Confidential information. Responsibly to maintain the confidentiality of information is devolved to all Participants via this Certificate Policy and applicable supporting documentation.

9.4 Privacy of personal information

Participants and all others using or accessing any personal data in connection with matters dealt with by this Certificate Policy shall comply with the Data Protection Act 1998 [19], and any other relevant legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction. Unless specified by special agreement, in the course of accepting a Certificate, all Subscribers (Subjects) have agreed to allow their personal data submitted in the course of Registration to be processed by and on behalf of the Issuing Authority and used as explained in the registration process, and have been given an opportunity to opt out of having their personal data used for particular purposes. They have also agreed to let certain personal data appear in publicly accessible directories and be communicated to others.

9.4.1 Privacy plan

All Participants shall comply with Data Protection and privacy legislation applicable within the European Economic Area and the privacy requirements of this Certificate Policy and applicable supporting documentation. The Privacy Policy applicable to this governing Certificate Policy together with any specific obligations and requirements are defined in Section 2.8 of the PKI Disclosure Statements [5, 6, 7].

Privacy information shall be classified and treated as Confidential. Where applicable, privacy information shall have such additional controls applied as required to comply with data protection and privacy legislation applicable in the European Economic Area.

9.4.2 Information treated as private

See section 9.3.1.

9.4.3 Information not deemed private

See section 9.3.2.

9.4.4 Responsibility to protect private information

The Issuing Authority carries overall responsibility to protect private information. It is also the responsibility of all Participants to protect private information as specified via this Certificate Policy and applicable supporting documentation.

Participants also carry a responsibility to protect private information so as to comply with Data protection and privacy legislation for the jurisdiction in which they operate.

9.4.5 Notice and consent to use private information

Where personal data is being processed, notification to the data subject and other notifications and declaration on use must be given as required to comply with data

protection and privacy legislation for the jurisdiction in which it is being processed. See section 9.4.

9.4.6 Disclosure pursuant to judicial or administrative process

Information shall only be disclosed where so required by due process of law and subject to any duty of confidence to provide such information and/or data as is demanded in any legal enquiries or proceedings.

9.4.7 Other information disclosure circumstances

Information held by the Certificate Manufacturer may also be disclosed:

- At the owner's request - to facilitate such disclosure an authenticated request from the information owner must be provided prior to the release of the information.
- At the specific request of the Policy Management Authority - In the case of confidential or privacy related information, the approval of the data subject shall be obtained prior to release.

9.5 Intellectual property rights

Each Participant acknowledges and accepts that it is responsible for the content of any information it incorporates, or which is incorporated at its request, in a certificate. Consequently, it shall take all reasonable precautions to ensure that this information does not breach the intellectual property rights of any third party or would otherwise cause any person unnecessary offence, damage or distress and shall on reasonable demand hold blameless and indemnify any other Participant as reasonably necessary.

9.6 Representations and warranties

The Issuing Authority warrants that:

- It shall take all reasonable skill and care during the processing and issue of Certificates to ensure that material defects or errors are not introduced into any relevant Certificate; and
- The issuance and management of Certificates including processing of applications and revocation requests and publication of Certificate Status Information are conducted in compliance with all material requirements of this Certificate Policy.

9.7 Disclaimers of warranties

The Participants acknowledge and agree this Certificate Policy does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this Certificate Policy or not) relating to the subject matter of this Certificate Policy, other

than as expressly set out in this Certificate Policy or incorporated between the Certificate Manufacturer and the Issuing Authority.

9.8 Limitations of liability

By signing a Certificate containing a policy identifier which indicates the use of this Certificate Policy, an Issuing Authority certifies to all who reasonably rely on the information contained in the Certificate, that the information in the Certificate has been checked according to the procedures laid down in this Certificate Policy.

The Issuing Authority assumes no liability whatsoever in relation to the use of Certificates or associated Public/Private Key pairs Issued under this Certificate Policy for any use other than in accordance with this Certificate Policy and any other agreements.

The Issuing Authority shall not be liable for any consequential, indirect or incidental damages, nor for any loss of business, loss of profit or loss of management time, whether foreseeable or unforeseeable, arising out of breach of any express or implied warranty, breach of contract, tort, misrepresentation, negligence, strict liability however arising, or in any other way arising from or in relation to the use of or reliance on, any Digital Certificate except only in the case of the Issuing Authority's negligence, wilful misconduct, or where otherwise required by applicable law.

Nothing in this Certificate Policy excludes or restricts liability for death or personal injury resulting from negligence or the negligence of its employees, agents or contractors or liability arising from fraudulent misrepresentation,

The Issuing Authority excludes all liability of any kind in respect of any transaction into which an End-Entity may enter with any third party.

The Issuing Authority is not liable to End Entities either in contract, tort (including negligence) or otherwise for the acts or omissions of other providers of telecommunications or Internet services (including domain name registration authorities) or for faults in or failures of their equipment.

Each provision of this Policy, excluding or limiting liability, operates separately. If any part is held by a court to be unreasonable or inapplicable, the other parts shall continue to apply.

The Issuing Authority limits any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the Issuance, use of, or reliance upon Certificates or associated Public/Private key pairs Issued under this policy, in excess of that specified in Section 2.6 of the PKI Disclosure Statements [5, 6, 7].

Those utilising this PKI to protect their services or transactions may establish their own liability limits for prescribed transaction types under their control. Where this is done, the revised limits shall be published and available to all affected parties.

9.9 Indemnities

Subscribers will immediately indemnify and keep indemnified the Issuing Authority from and against all costs, claims, demands, liabilities, expenses, damages or losses (including without limitation any direct or indirect consequential losses, loss of profit and loss of reputation, and all interest, penalties and legal and other professional costs and expenses) arising out of or in connection with:

- Use of Certificates and/or Public/Private Key pairs Issued under this policy in a manner that is not in accordance with this Certificate Policy; and
- Subscribers' negligence, default or breach of this Certificate Policy in any other manner.

If the Subscriber(s) becomes aware that a third party may make a claim against, or notifies an intention to make a claim against, the Issuing Authority which may reasonably be considered as likely to give rise to a liability, the Subscriber(s) shall:

- As soon as reasonably practicable give written notice of that matter to the Issuing Authority specifying in reasonable detail the nature of the relevant claim.
- Not make any admission of liability, agreement or compromise in relation to the relevant claim without the prior written consent of the Issuing Authority (such consent not to be unreasonably conditioned, withheld or delayed); and
- Give the Issuing Authority and its professional advisers reasonable access to the premises and personnel of the Subscriber(s) and to any relevant assets, accounts, documents and records within the power or control of the Subscriber(s) so as to enable the Issuing Authority and its professional advisers to examine such premises, assets, accounts, documents and records, and to take copies at their own expense for the purpose of assessing the merits of the relevant claim.

9.10 Term and termination

9.10.1 Term

This Certificate Policy is extant from the date of publication and shall remain in force until otherwise terminated in accordance with Section 9.10.2, replaced or withdrawn by notice provided by the Issuing Authority, or is explicitly identified to be terminated.

9.10.2 Termination

Without prejudice to any other rights to which it may be entitled, the Issuing Authority may give notice in writing to the Subscriber(s) terminating their agreement with immediate effect if:

- The Subscriber(s) commits a material breach of any of the terms of this Policy and (if such a breach is remediable) fails to remedy that breach within 30 days of being notified in writing of the breach.
- An order is made or a resolution is passed for the winding up of the Subscriber(s) or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order of the Subscriber(s).
- An order is made for the appointment of an administrator to manage the affairs, business and property of the Subscriber(s) or documents are filed with a court of competent jurisdiction for the appointment of an administrator of the Subscriber(s) or notice of intention to appoint an administrator is given by the Subscriber(s) or its directors or by a qualifying floating charge holder (as defined in paragraph 14 of Schedule B1 to the Insolvency Act 1986 [25]).
- A receiver is appointed of any of the Subscriber(s) assets or undertaking or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of the Subscriber(s) or if any other person takes possession of or sells the other party's assets.
- The Subscriber makes any arrangement or composition with its creditors or makes an application to a court of competent jurisdiction for the protection of its creditors in any way.
- The Subscriber(s) ceases to trade or threatens to cease trade.
- There is a change of control of the Subscriber(s).
- The Subscriber(s) takes or suffers any similar or analogous action in any jurisdiction in consequence of debt.

Should this Certificate Policy be terminated prior to all Certificate Authorities operating under its governance, Issued Certificates shall be Revoked as part of the termination actions. See Section 5.8.

9.10.3 Effect of termination and survival

Any Certificate issued prior to termination of this Certificate Policy which shall survive its termination and shall endure, subject to the termination or revocation of the Certificate, until expiry of its stated validity period. Without prejudice to the generality of this clause 9.10.2, the terms of this Certificate Policy shall continue to apply in respect of any such Certificate.

9.11 Individual notices and communications with participants

9.11.1 Subscribers

Whenever any Subscriber hereto desires or is required to give any notice, demand, or request with respect to this Certificate Policy, such communication shall be made either by using digitally signed messages consistent with the requirements of this Certificate Policy, or by paper-based communications. Electronic communications

shall be effective upon the sender receiving a valid, digitally signed acknowledgment of receipt from recipient. Such acknowledgement must be received within five working (5) days, or else notice must then be given by paper-based communications. Such paper-based communications must be delivered by a service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed to the Issuing Authority as detailed in Section 2.1 of the PKI Disclosure Statements [5, 6, 7] issued under this Certificate Policy. All such communications shall be effective upon receipt.

A Subscriber requiring receipt of notice under this Certificate Policy is required to provide notice of:

- Changes in address including postal and e-mail addresses.
- Changes in financial or other status, which would change the basis upon which the Certificate has been granted.
- Any other notice pertinent to the maintenance of the provisions of this Certificate Policy.

9.11.2 Issuing Authority

All notices by the Issuing Authority shall be provided by digitally signed or unsigned messages, or by making such notice accessible online in a similar manner as that used for the publication of this Certificate Policy.

Notice requirements with regard to termination of Issuing Authority operations are specified in Section 5.8.

Notice requirements with regard to changes in this Certificate Policy are specified in Section 9.12.2.

9.11.3 Notification

Any notices given in 9.11.2 shall be deemed served effective upon dispatch.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this Certificate Policy fall into three categories:

- Editorial or typographical corrections, or changes to the contact details which may be made without notification or are awaiting comments.
- Changes which, in the judgement of the Policy Management Authority, will not materially impact a substantial majority of the Subscribers or Relying Parties using this Certificate Policy.
- Changes which, in the judgement of the Policy Management Authority, are likely to have a material impact upon a significant number of users of this Certificate Policy.

Where the amendments are likely to have a major impact on the majority of users of this Certificate Policy then it may be replaced by a new document (ref. Section 9.12.3).

9.12.2 Notification mechanism and period

All proposed changes that may materially impact users of this Certificate Policy will be notified in accordance with Section 10.11 of this Certificate Policy by the Issuing Authority registered with the Policy Management Authority, and will be prominently posted on the World Wide Web site of the Issuing Authority who shall ensure that notice of such proposed changes is posted in their Repositories and shall make commercially reasonable efforts to advise End Entities of such proposed changes.

Impacted Participants may file comments through the relevant Issuing Authority or directly with the Policy Management Authority. The period for comment will be as follows:

- For changes which, in the judgement of the Policy Management Authority, will not materially impact a substantial majority of users of this Certificate Policy comments shall be received within 15 days of original notice.
- Changes which, in the judgement of the Policy Management Authority, are likely to have a material impact upon a significant number of users of this Certificate Policy comments shall be received within 15 days of original notice.
- Any action taken as a result of comments filed in accordance with the above is wholly at the discretion of the Policy Management Authority.
- If the proposed change is modified as a result of comments received notice of the modified proposed change shall be given at least 15 days prior to the change taking effect.
- Approval for incorporation of any changes to this Certificate Policy is wholly at the discretion of the Policy Management Authority.

9.12.3 Circumstances under which OID must be changed

If amendments to this Certificate Policy are determined by the Policy Management Authority to be sufficiently significant, the Policy Management Authority reserves the right to assign a new Object Identifier (OID) to the modified Certificate Policy.

9.13 Dispute resolution provisions

All disputes shall be referred in writing to the Issuing Authority. The Issuing Authority shall deal with such disputes in accordance with its dispute resolution process specified in section 2.10 of the PKI Disclosure Statements [5, 6, 7].

9.14 Governing law

This Certificate Policy shall be governed by the law of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales. In the event of any dispute (other than one relating to the infringement of intellectual property rights, for which an injunction would be the appropriate remedy) arising from or concerning this Certificate Policy, then such matter shall be settled by mediation between the parties according to Section 9.13.

9.15 Compliance with applicable law

All Participants within the PKI will comply with all applicable law and regulations, for example those relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The parties acknowledge that, except for documents expressly referred to or incorporated by reference herein, this Policy constitutes the entire agreement and understanding of the parties and supersedes any previous agreement between the parties relating to the subject matter of this Policy. For the purposes of this clause, such documents shall be:

- PKI Disclosure Statements.
- Relying Party Agreement.
- Subscriber Agreement.
- Glossary of Terms.

In the event of any ambiguity, inconsistent or incompatible provisions, this Policy shall take precedence, followed by the provisions of the PKI Disclosure Statements then Subscriber Agreement, then Relying Party Agreement.

9.16.2 Assignment

This Certificate Policy shall be binding upon, and inure to the benefit of all parties hereto. The rights and obligations detailed in this Certificate Policy are not assignable by the parties and any shall not be assigned without the prior written consent of the NHS Issuing Authority.

9.16.3 Severability

In the event that any one or more of the provisions of this Certificate Policy shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but this Certificate Policy shall then be construed as if such unenforceable provision or provisions had never been

contained herein, and insofar as possible, construed to maintain the original intent of the Certificate Policy.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No delay, neglect or forbearance on the part of one party in enforcing against any other party any term or condition of this Certificate Policy shall either be or be deemed to be a waiver or in any way prejudice any right of that party under this Certificate Policy. No right, power or remedy in this Certificate Policy conferred upon or reserved for a party is exclusive of any other right, power or remedy available to that party. Each party shall bear its own legal costs and other costs and expenses arising out of or in connection with this Certificate Policy.

9.16.5 Force Majeure

The Issuing Authority shall have no liability to the Participants under this Policy if it is prevented from or delayed in performing its obligations under this Policy, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of the Issuing Authority or any other party), failure of a utility service or transport network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors.

If any such events, affecting the availability of, or access by a Relying Party to, Certificate Status Information as described in the preceding paragraph, continue for a continuous period of more than 72 hours, [the Issuing Authority] may terminate this Policy by written notice to the other parties.

9.17 Other provisions

9.17.1 Certificate Policy Content

Section and paragraph headings shall not affect the interpretation of this Policy and the content of Section 0.3 is descriptive only for reference purposes and such section shall be interpreted accordingly.

9.17.2 Third party rights

Subject to clause 9.3 (Confidentiality of business information), a person who is not a party to this Certificate Policy has no right under the Contracts (Rights of Third Parties) Act 1999 [26] to enforce any of its terms, but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

Any rights created above may be altered or extinguished by the parties without the consent of the third party beneficiaries.