Document filename:	**NHS PKI Root CA Certificate Policy – APPROVED -v5.0.docx**		
Project / Programme	**Data Security**	Project	**NHS PKI / Certificate Services**
Document Reference			
Project Manager	**Matt Wyatt**	Status	**APPROVED**
Owner	**Clive Star**	Version	**5.0**
Author	**Matt Wyatt**	Version issue date	**01/07/2021**

Certificate Policy for NHS Root Certification Authority

Document Management

Revision History

Version	Date	Summary of Changes
0.1	16th. October 2006	First draft for comment
0.2	17th. November 2006	Second draft for comment.
0.3	27th June 2007	Removal of redundant drafting notes from sections 2.1, 6.4.3, 6.5.2 and 10.2.2
0.4	3rd August 2007	Revised following legal review.
0.5	31 August 2007	Revised following further input from DLA Piper
0.6	24 September 2007	Further revision following discussion between Trustis/DLA Piper
0.7	3rd. October 2007	Further revision by DLA Piper following responses from NHS CFH
0.8	4th. October 2007	Incorporation of changes in V0.7 into NHS CFH document format.
1.0	9th. October, 2007	CP Approved by Dr Mark Ferrar
1.1	8th June, 2009	Updated with new document reference number, ownership information amended, main content not changed.
1.2	28th February, 2011	Updates incorporated for changes to Root Certificate Authority hosting arrangements as required. Updates incorporated from result of 'Document Mapping' exercise approved by the NHS PKI PMA (12/02/10)
1.3	29th March, 2011	Document approved following PMA review
1.4	12th October, 2012	Updated section 6.2.2 to show that a minimum of 3 persons are required for Root CA private key control, other minor typographical amendments made
1.5	12th October, 2012	Document approved by Chair of NHS PKI PMA
1.6	17th April, 2013	Document revised following creation of the Health and Social Care Information Centre (HSCIC)/transferred to HSCIC document template
1.7	22nd April, 2013	Document approved by Chair of NHS PKI PMA
2.0	25th February 2015	Document uplift tor reflect Spine 2 transition
2.1	7th February 2017	Draft in new NHSD document template
2.2	18th April 2018	Document uplift to accommodate Basic Constraints non-compliance in Certificate Profile [7.1.2], updated references and NHS Digital branding
2.3	19th April 2018	PKI Glossary of Terms included within document
2.4	24th April 2018	Uplifted regarding PMA review comments
3.0	4th May 2018	Document approved by Chair of NHS PKI PMA
4.0	29th October 2019	Annual Document Review Minor grammatical changes

		Change to document approvers Removal of references to Contractor Security Policy Removal of version numbers in supporting documentation
4.1	25th June 2021	Amendment to document owner Change to version of DPA (related documents – 19)
5.0	1ST July 2021	Issued version following PMA approval

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
NHS PKI Policy Management Authority members		01/07/2021	5.0

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
Steven Shaw (for and on behalf of the PMA)		Chair of the NHS PKI PMA	4th May 2018	2.4
Matt Wyatt	*Matt Wyatt*	Chair of the NHS PKI PMA	30/10/2019	4.0
Steve Fenwick	*Steve Fenwick*	Specialist Security Services Lead	30/10/2019	4.0
Matt Wyatt	*Matt Wyatt*	Chair of NHS PKI PMA	01/07/2021	5.0

NB. The version of the policy posted on the intranet must be a pdf copy of the signed approved version.

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

Related Documents

These documents will provide additional information.

Current Version numbers are available from the PMA upon request.

Ref no	Doc Reference Number	Title
1	N/A	Online 'Glossary of Terms' – removed, now in Appendix A
2	N/A	PKI 'Glossary of Terms' - removed, now in Appendix A
3	NPFIT-FNT-TO-INFR-0056.01	NHS Level 1 - Issuing Authority Base Certificate Policy
4	N/A	NHS Root Certificate Authority PKI Disclosure Statement

5	NPFIT-FNT-TO-INFR-0053.01	Authentication Certificates PKI Disclosure Statement
6	NPFIT-FNT-TO-INFR-0057.01	Content Commitment Certificates PKI Disclosure Statement
7	NPFIT-FNT-TO-INFR-0059.01	Endpoint Authentication Certificates PKI Disclosure Statement
8	RFC 3647 (http://www.ietf.org/rfc/rfc3647.txt)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
9	RFC 5280 (http://www.ietf.org/rfc/rfc5280.txt)	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
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
~~11~~	~~[as referenced in the S3A, ref. 12]~~	~~Contractor Security Policy~~
12	N/A	tScheme Specification of Service Subject to Assessment (S3A) – Root Certificate Authority for the NHS Public Key Infrastructure
13	RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt)	Key words for use in RFCs to Indicate Requirement Levels
14	https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/nhs-pki-certificate-information/public-key-infrastructure-pki-documentation	NHS PKI Repository
15	NPFIT-FNT-TO-IG-PRJMGT-0093.05	IG Audit and Alerts Gold Standard
16	RFC 2986 http://www.ietf.org/rfc/rfc2986.txt	PKCS #10: Certification Request Syntax Specification

17	http://csrc.nist.gov/groups/STM/cmvp/index.html	FIPS140-2: Security Requirements for Cryptographic Modules
18	N/A	NHS Digital Security Classification Policy
19	https://www.legislation.gov.uk/ukpga/2018/12/contents	UK Data Protection Act (2018)
20	https://www.iso.org/standard/54533.html	ISO 27002: 2013 – Code of Practice for Information Security Management
21	RFC 6818 (http://www.ietf.org/rfc/rfc6818.txt)	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
22	http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf	The EU General Data Protection Regulation (GDPR)
23	[BT Document]	Certification Practice Statement for NHS Root Certification Authority

Contents

0 ABOUT THIS DOCUMENT

0.1 Purpose

The purpose of this document is to describe the procedures and processes by which the NHS Root Certificate Authority (Level 0) generates certificates for the Level 1 Sub-Certificate Authorities operating under this Root within the NHS Public Key Infrastructure.

0.2 Audience

This document has been written for the NHS Digital Policy Management Authority, Data Security Centre, Information Governance Team, Spine Programme and Relying Application Service Providers.

0.3 Content

This document comprises these following sections / topics:

- Section 1 – Introduction to the Document
- Sections 2 - 9 inclusive, describes the processes and procedures for the operation of the NHS Root Certificate Authority. These sections follow the format and scope of by the Internet Engineering Task Force standard RFC 3647 [8], Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Details of these sections are given in the document contents list.

1 INTRODUCTION

1.1 Overview

This Certificate Policy (CP) is a named set of rules that indicates the applicability of Certificates created specifically for the purpose of signing CA certificates for level 1 Certificate Authority services supporting the various Programmes which comprise the 'Health and Social Care' system. The responsibility for this Certificate Policy lies with NHS Digital's Policy Management Authority (PMA), and any queries regarding the content of this Certificate Policy should be directed to the Policy Management Authority.

Explanations of the various terms used throughout this document can be found in Appendix A.

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 Issues Root Certificates in accordance with this Certificate Policy has made its own stipulations regarding Participants, further restrictions on usage of Certificates, additional liability provisions, etc. These stipulations are contained in this CP.

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.

As this Certificate Policy (CP) is concerned only with the production of certificates for use by Level 1 Certificate Authority operations, the audience for this CP is limited to the PMA, NHS Issuing Authority, and members and representatives of service providers to the NHS where appropriate. There is a requirement for Spine Service Provider(s) to produce a Certification Practice Statement (CPS) that supports this CP. Additionally, the provision of secure processing facilities is a contractual requirement of service providers and described in the contract(s) between NHS Digital and the Certificate Manufacturer, the associated Specification of Service Subject to Assessment (S3A) and section 5 of this Certificate Policy.

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 [13].

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 Certificate Policy based on this document has also been assigned an OID as defined in Section 2.12 of the related PKI Disclosure Statement [4].

1.3 PKI participants

The NHS Issuing Authority has an obligation to operate a PKI in accordance with the Certificate Policies it defines and publishes. The NHS 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. The roles for the NHS Root Certification service Participants are defined in the PKI Disclosure Statement.

- Policy Management Authority
- Trust Service Providers,
  - NHS Issuing Authority,
  - Certificate Manufacturer; see section 2.17 of the PKI Disclosure Statement [4].
  - Registration Authority; see section 2.13 of the PKI Disclosure Statement [4].
  - Repository; see section 2.14 of the PKI Disclosure Statement [4].
- End Entities,
  - Subscribers; see section 2.15 of the PKI Disclosure Statement [4].
  - Relying Parties; see section 2.16 of the PKI Disclosure Statement [4].

Under this scheme the End-Entity is any Level 1 CA operating as a Spine Service Provider which has a business relationship with the NHS Issuing Authority and in all matters the End-Entity relationship is with the NHS Issuing Authority.

Subjects (Level 1 CAs) hold Certificates on behalf of Subscribers and their representatives act on their behalf. In all cases however, the business relationship with the NHS Issuing Authority is held by the Subscriber.

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

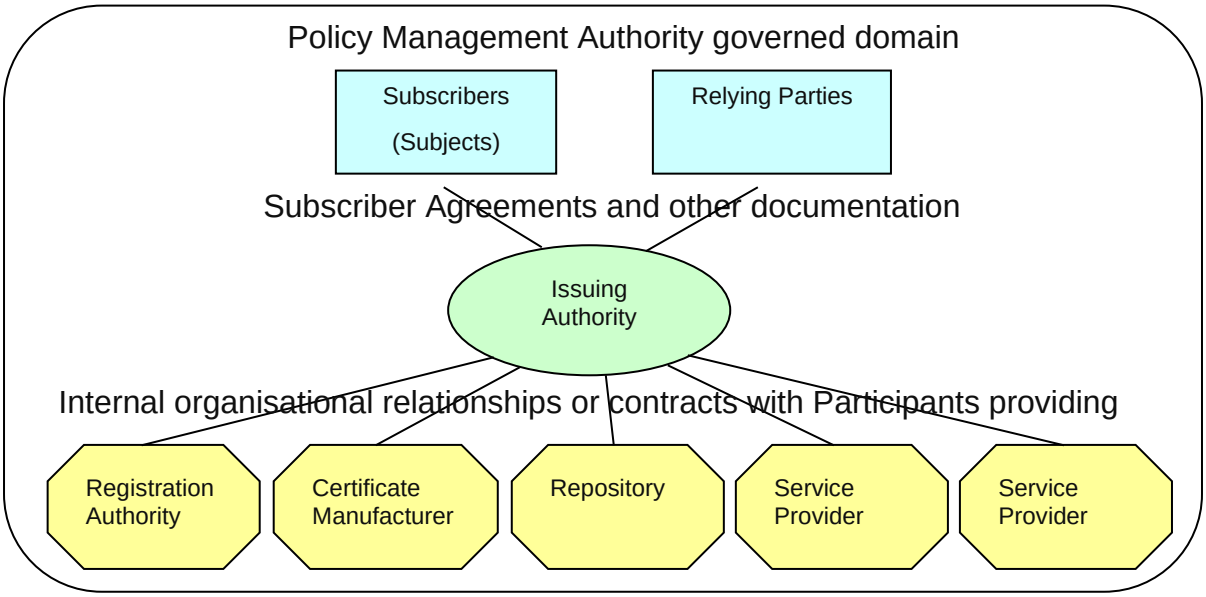

Figure 1. Roles & Business Relationships

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 NHS 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. The NHS Issuing Authority is responsible for ensuring the provision of a Certification Practice Statement that supports this Certificate Policy.

The NHS Issuing Authority publishes a summary of important provisions that form a part of this Certificate Policy, together with any further provisions in a document known as a 'PKI Disclosure Statement'. These provisions typically include, but are not limited to the following:

- Policy Management Authority & NHS 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, Certification Practice Statement, 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

1.3.1.2 Certificate Manufacturer

The Certificate Manufacturer is contracted by the NHS Issuing Authority to provide Certificate management operational services for the NHS Root Certification Authority as part of the contracted SPINE Services.

The Certificate Manufacturer is approved by the NHS Issuing Authority to manage Certificates on its behalf or for 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 NHS Issuing Authority.

The Certificate Manufacturer must demonstrate compliance with this Certificate Policy. Compliance is demonstrated via a Certification Practice Statement. This does not override the requirement for Participants providing trust services to adhere to any and all contractual clauses. Where the Certification Practice Statement 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 Statement [4].

1.3.2 Registration Authorities

The Registration Authority of the Certificate Manufacturer is responsible for validating the identity of eligible applicants notified by the NHS Issuing Authority to be Issued with CA Certificates for Level 1 CAs together with ensuring the accuracy and integrity of required information presented by applicant CAs. The Registration Authority is an integral function of the Certificate Manufacturer whose 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 a single Registration Authority operated by the Certificate Manufacturer is required. This Registration Authority must demonstrate compliance with this Certificate Policy. Compliance is documented and controlled via adherence to the CPS and supporting Registration Policy and Procedures.

The NHS Issuing Authority has approved the Registration Authorities specified in section 2.13 of PKI Disclosure Statement [4] with respect to Certificates governed by this Certificate Policy.

1.3.3 Subscribers

A Subscriber is the individual (End-Entity) authorised to represent the Spine Service Provider organisation that has applied for and received a Certificate. It is the Subscriber that contracts with the NHS Issuing Authority for the Issuance of Certificates on behalf of the organisation. The Subscriber bears responsibility for the use of the Private Key associated with the Certificate.

1.3.4 Subjects

The Subject is the entity that is identified in a 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.

Eligible Subjects are limited to Certificate Authorities.

1.3.5 Relying Parties

Relying Parties are Subscribers to this Certificate Policy.

Relying Parties are specified in section 2.16 of the PKI Disclosure Statement [4].

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 is the governing body 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 PKI Disclosure Statement [4].

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 Subscribers and Relying Parties can obtain Certificates and validate status information on Certificates Issued under this Certificate Policy.

The NHS Issuing Authority has approved the Repositories identified in section 2.14 of PKI Disclosure Statement [4] to provide these services.

1.4 Certificate usage

Certificate usage is defined by the Certificate Profile. Certificate Profiles must be approved by the PMA.

1.4.1 Appropriate certificate uses

The purposes for which Certificates Issued under this policy may be used are specified in section 2.2 of the PKI Disclosure Statement [4].

1.4.2 Prohibited certificate uses

All other application use and any other usage categories for Certificates Issued under this Certificate Policy are prohibited as described in section 2.2 of the PKI Disclosure Statement [4].

1.5 Policy administration

1.5.1 Organisation 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 specified in section 2.1 of the PKI Disclosure Statement [4].

The Policy Management Authority is responsible for administering this Certificate Policy.

1.5.2 Contact person

In the first instance the NHS Issuing Authority should be contacted regarding the contents of this Certificate Policy.

Contact details are provided in section 2.1 of the PKI Disclosure Statement [4].

1.6 Person determining CPS suitability for the policy

The Policy Management Authority will determine the level of suitability of the Certification Practice Statement required for this Certificate Policy.

In the first instance, the NHS Issuing Authority should be contacted regarding the inclusion of additional Certification Authorities to operate within or interoperating with the trust infrastructure controlled by the NHS Root CA operated under this Certificate Policy.

Contact details are provided in section 2.1 of the PKI Disclosure Statement [4].

1.6.1 CPS approval procedures

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

1.7 Definitions and acronyms

Explanations of the various terms used throughout this document can be found in Appendix A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

An information Repository shall be made available under the terms of this Certificate Policy. The NHS 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 NHS Issuing Authority shall ensure the following items relating to this policy are published for all Participants of this PKI via the Repository:

- The Authority Revocation List.
- The NHS Root Authority's public signature verification key.

No copies of documentation will be made available in hard copy format.

2.3 Time or frequency of publication

Information as listed in 2.2 shall be published promptly following its creation.

The Authority Revocation List (ARL) is to be updated and issued at least annually.

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 the authorised 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 Name field of Certificates Issued under this Certificate Policy and in accordance with IETF PKIX RFC 5280 [9]. Each Entity may in addition, use an alternative name via the 'SubjectAlternative' Name field, which must also be in accordance with IETF PKIX RFC 5280 [9].

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 subscribers

The anonymity or pseudonymity of Subscribers is not permitted under this Certificate Policy, unless this is explicitly requested by the NHS 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 Subscriber 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 an organisational entity is as follows:

Element	Description
Common Name	Where the Subject is an organisation, 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 registered business address of the entity or the physical location where the entity conducts business or the delivery address for the entity's 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 5280 [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 the NHS 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 NHS Issuing Authority is liable for the inclusion of trademarks, trade names or other information under restricted use. Contractual arrangements shall require Subscribers to warrant legitimacy of their registration details provided to the NHS 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.

3.2.2 Authentication of organization identity

The organisational identity of the service provider operating NHS Level 1 Sub-Certificate Authorities must be established via a formal contractual relationship with NHS Digital.

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

3.2.3 Authentication of individual identity

The authentication of CA devices shall be in accordance with section 2.2 of the PKI Disclosure Statement . The Spine Service Provider as the Subscriber is contractually liable for ensuring the accuracy of the evidentiary information for CAs in accordance with the requirements of the Contract and PKI documentation suite as a minimum and shall document the mechanisms used to support the level of authentication assurance.

The PMA may specify additional requirements for any Subscriber.

3.2.4 Non-verified subscriber information

Use of non-verified information is not permitted in Certificates governed by this Certificate Policy.

3.2.5 Validation of authority

Validation of authority (i.e. the determination of whether a Subscriber 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 NHS Issuing Authority.

3.2.6 Criteria for interoperation

The criteria for CA interoperability will be defined by the Policy Management Authority. The Policy Management Authority will also determine whether any specific Certification Authority is approved for interoperation. Such a requirement for interoperability may occur when another Certification Authority wishes to operate within or interoperate with the PKI governed by this Certificate Policy.

The Policy Management Authority operates a formal mechanism 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 NHS Issuing Authority, whose contact details are given in Section 2.1 of the PKI Disclosure Statement [4].

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 time expiry is permitted.

Re-key requests from Subscribers and any participant shall at minimum, incorporate the mechanisms described in sections 3.2.3 and 3.3.3 for Authentication that fulfils initial authentication requirements. Proof of possession of a valid Certificate as Authentication is permitted.

3.3.2 Identification and authentication for re-key after revocation

Re-Key after Revocation requests to the NHS Issuing Authority is not permitted.

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 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 NHS Issuing Authority or Registration Authority acting on its behalf, is authorised to conduct Revocation. In such cases the NHS 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:

- A Subscriber.
- A Representative of the NHS Issuing Authority.

Certificate applicants must comply with the procedures described in this document. Eligible Subscribers are specified in Section 2.15 of the PKI Disclosure Statement [4].

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

4.1.2 Enrolment responsibilities

Enrolment responsibilities are described in section 2.4 of the PKI Disclosure Statement [4].

4.1.2.1 Registration Authorities and their Representatives

The NHS Issuing Authority directly controls enrolment. Participants approved to act as Registration Authorities are specified in section 2.13 of the PKI Disclosure Statement [4].

Issuance of Certificates to CA Service Operators shall be conducted by the Certificate Manufacturer in accordance with this policy and the contractual requirements for Spine Services provision.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Certificate Manufacturer, through a suitably designated representative is permitted to conduct authentication of Subscribers and Subjects in accordance with NHS Digital contractual requirements.

4.2.2 Approval or rejection of certificate applications

The Policy Management Authority will either approve or reject a Certificate application.

Where approved, the Certificate application will be processed by the Certificate Manufacturer.

Where a Certificate application is rejected, the reasons for rejection will be given to the applicant by the Policy Management Authority.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificates shall be Issued by the Certificate Manufacturer (i.e. Certificate Authority) only in response to a properly constructed, signed and validated Certificate request from the Issuing Registration Authority. Only the NHS Issuing Authority can communicate with the 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) may communicate with the Subscriber (Subject) as part of the secure Certificate Issuance process, if instructed to do so by the NHS Issuing Authority.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

A Subscriber shall explicitly indicate acceptance of a Certificate to the NHS Issuing Authority via a procedural process.

Receipt of a Certificate via authentication by the Subscribers representative constitutes acceptance of the Certificate.

Acceptance of tokens, smart cards, hardware security modules 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 NHS Issuing Authority shall ensure that the authorised representative of the Subscriber, during application for or delivery of a Certificate, is provided with the details of terms and conditions stipulated in this governing Certificate Policy and any other applicable contractual commitments.

The Subscriber or the Subscriber's authorised representative must acknowledge that it agrees to the terms and conditions stipulated in the Certificate Policy and other applicable contractual commitments prior to first use of the Certificate.

The NHS Issuing Authority shall undertake to clearly inform the Subscriber that by accepting a Certificate Issued under this Certificate Policy, a Subscriber 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 Subscriber's Private Key.
- All information given by the Subscriber to the NHS Issuing Authority is true and accurate.

4.4.2 Publication of the certificate by the CA

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

Further "publication" of the Certificate may be permitted by the NHS Issuing Authority. Details of approved Repositories are provided in section 2.14 of the PKI Disclosure Statement [4]. An information Repository is additionally located at [14].

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

The Subscriber 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 notified to the Subscriber by the NHS Issuing Authority.

4.5.2 Relying party public key and certificate usage

A Relying Party may only rely on a Subscriber's Public Key and Certificate for the specific functions stipulated and published by the NHS Issuing Authority, or where PKIs interoperate, 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 Statement [4].

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificates may, subject to approval by the NHS Issuing Authority be Renewed at any time during their Operational Period. Renewal of Expired, Revoked or Suspended Certificates is not permitted.

Renewal requests shall at minimum, include the authentication of representatives of both the NHS Issuing Authority and Service Provider through proof of possession of a valid Certificate or other mechanisms as agreed by the NHS PKI PMA.

Unless specifically and expressly approved by the NHS Issuing Authority, renewal shall incorporate Re-Key of the Certificate.

4.6.2 Who may request renewal

Renewal applications may be made by:

- Existing Subscribers.
- The NHS Issuing Authority.

.

4.6.3 Processing certificate renewal requests

The NHS Issuing Authority 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 Subject.

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:

- Existing Subscribers.
- The NHS Issuing Authority.

4.7.3 Processing certificate re-keying requests

The NHS Issuing Authority will either approve or reject an application for Re-Key of a Certificate.

Certificate Re-Key requests are processed by the Certificate Manufacturer (i.e. Certificate Authority) in response to a properly constructed and signed Certificate request from the NHS Issuing 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 by one of the other 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 Certificates; at least until their assigned validity period expires.

Upon Revocation of a Subscriber's Certificate, the NHS Issuing Authority shall undertake to inform the Subscriber.

Suspension of Subscriber Certificates is not permitted under this policy.

4.9.1 Circumstances for revocation

The circumstances under which Certificate Revocation may be requested (and carried out) is defined and implemented by the NHS Issuing Authority and published as appropriate.

The NHS Issuing Authority or Policy Management Authority must conduct verification of Revocation 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 Subscriber (Subject) withdraws from or is no longer eligible to participate in the Public Key Infrastructure governed by this Certificate Policy.

The NHS Issuing Authority may Revoke a Certificate when a Subscriber fails to comply with 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 an entity of the NHS Issuing Authority or; the Policy Management Authority or the Certificate Manufacturer.

The Revocation request must present a valid circumstance for Revocation according to 4.9.1.

Approval of a Revocation request may only be granted by:

- The Policy Management Authority.
- The NHS Issuing Authority.

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:

- By formal written representation to the NHS Issuing Authority or Policy Management Authority.

- By personal representation to the NHS Issuing Authority or Policy Management Authority.

Certificate Revocation requests will be received by the NHS Issuing Authority or the Policy Management 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 CA Certificate to be Revoked must be recognised. Where reliable authentication of the Revocation request is not possible or even omitted, the Policy Management Authority or NHS Issuing Authority is authorised to conduct Revocation. In such cases the NHS Issuing Authority or Policy Management 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 NHS Issuing Authority or its representative to achieve a satisfactory level of assurance of the validity of the request.

Certificate Revocations are processed by the Certificate Manufacturer (or Certificate Authority) in response to a properly constructed and signed Revocation request from the NHS Issuing Authority or Policy Management Authority.

4.9.4 Revocation request grace period

None.

If the Revocation request is approved, it must be enacted as soon as practicable. Updated Revocation Status Information must be issued and published immediately.

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 NHS Issuing Authority or Policy Management Authority is not constrained. The NHS Issuing Authority or Policy Management 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 authorised Revocation requests. The maximum time taken for this element is determined by the NHS Issuing Authority in its contract with the Certificate Manufacturer.

4.9.6 Revocation checking requirement for relying parties

The Certificate status checking obligations of Relying Parties are specified in section 2.5 of the applicable PKI Disclosure Statement [4]. Where a Relying Party chooses to check the Certificate Status Information of a Certificate upon which they wish to rely, this must be performed via an Authority Revocation List (ARL) or equivalent on-line protocol that permits authenticity and integrity of the Status Information to be verified.

4.9.7 CRL issuance frequency (if applicable)

The frequency for ARL issuance is defined in section 2.18 of the PKI Disclosure Statement [4].

4.9.8 Maximum latency for CRLs (if applicable)

Where ARLs are published, the ARL validity period shall be at a maximum of one calendar year unless an alternative validity period is agreed by the NHS PKI PMA on a case-by-case basis.

4.9.9 On-line revocation/status checking availability

Where applicable, the availability of on-line Certificate Status checking is published by the NHS Issuing Authority. The frequency of publication of new status information should be no less than the frequency specified in section 2.18 of the PKI Disclosure Statement [4].

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 Statement [4].

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements re key compromise

In the event of the compromise, or suspected compromise, of any Subject's Private Key, the Subscriber must notify the NHS Issuing Authority or Policy Management Authority immediately and must indicate the nature and circumstances of the compromise, to the fullest extent known.

4.9.13 Circumstances for suspension

This Certificate Policy does not support Suspension of Subscriber Certificates.

4.9.14 Who can request suspension

See Section 4.9.13.

4.9.15 Procedure for suspension request

See Section 4.9.13.

4.9.16 Limits on suspension period

See Section 4.9.13.

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 Statement [4].

4.10.2 Service availability

The availability of any Certificate Status checking services to Relying Parties is defined by the NHS Digital, Digital Delivery Centre (DDC) in accordance with its role as the NHS Spine Service Provider.

4.10.3 Optional features

No stipulations.

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 NHS Issuing Authority and communicated directly to the Subscriber 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 NHS 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 CA Keys. Such mechanisms must comply with all provisions of this Certificate Policy.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

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 not stipulated, specific details on controls operated for components of the PKI infrastructure must be detailed in a Subscriber’s CPS or supporting documentation.

Controls must be approved by the Policy Management Authority.

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 requirements for a Security Zone.
- 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.

The processes under which the Certificate Manufacturer operates must be tScheme approved and audited annually.

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 files. Controls must be detailed in the Certification Practice Statement or other 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 files is to be sanitised or destroyed before being released for disposal.

All documentation classified as 'Official - Sensitive' or equivalent shall be subject to a defined secure disposal procedure. This procedure shall be detailed in the Certification Practice Statement or supporting documentation

5.1.8 Off-site backup

Offsite 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 will be employed to reflect the requirements of those roles and responsibilities. Controls shall be detailed in the Certification Practice Statement or supporting documentation.

The Certificate Manufacturer must ensure that all personnel are adequately trained and understand their responsibility for Certificate management tasks. Where trusted roles are required for the Certificate Manufacturer, these will be shall be detailed in a CPS or supporting documentation and at a minimum comply with any and all contractual clauses. Any such arrangements must be approved by the NHS Issuing Authority or auditors acting on its behalf.

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, the verification process 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 access to 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 as prescribed in section 6.2.2 of this Certificate Policy. 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.

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.

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. Any such additional requirements shall be detailed in a Certification Practice Statement 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 local procedures and any and all contractual clauses related to the operation of this PKI. Individuals not security cleared must be under supervision by approved and security cleared 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 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

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. Archiving of records must at a minimum be conducted in accordance with ISO 27002:2013 [20] and any subsequent revisions, or any standard that supersedes it.

As a minimum the following data must be recorded:

- Trust Service Provider key creation ceremony records.
- Trust Service Provider's policies and procedures.
- Contractual obligations – Certificate Manufacturer.
- System equipment and configuration.
- Subscriber identity authentication and supporting evidence records.
- Documentation of receipt and acceptance of Certificates.
- Documentation of receipt of tokens.
- All Certificates issued or published.
- Messages received from authorised sources requesting an action on the part of the NHS Issuing Authority.
- 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 ARLs and 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 Root CA signing key.
- All personnel/role changes for trusted roles.
- All messages to the CA requesting an action of the CA and the subsequent action taken by the CA.

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 supporting documentation. Procedures must be approved by the NHS 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 document “IG Audit and Alert 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)

5.4.4 Protection of audit log

The electronic audit log system is securely managed in accordance with ISO 27002:2013 [20] and any subsequent revisions or any standards that supersede it as a minimum requirement 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
- System equipment and configuration Certificate requests.
- Revocation requests.
- Certificate Holder identity authentication and supporting evidence records.
- Documentation of receipt and acceptance of Certificates.
- All Certificates issued or published.
- All ARLs and CRLs issued and or published.

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

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 are archived and held in a number of secure locations.

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 NHS Issuing Authority are to be interrupted, suspended or terminated, the NHS Issuing Authority shall ensure the continued availability of the archive. All requests for access to such archived information shall be sent to the NHS Issuing Authority or to the entity identified by the NHS Issuing Authority prior to terminating its service.

5.6 Key changeover

Subscriber - a Subscriber 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 Subscriber.
- The Policy Management Authority.
- The NHS Issuing Authority.

Subscribers must be re-authenticated in the same manner as for an initial registration.

Where a Subscriber's Certificate has been Revoked as a result of suspected or actual non-compliance, the NHS Issuing Authority must verify that the reasons for non-compliance have been satisfactorily addressed and resolved prior to Certificate Re-issuance.

All CA signing keys shall be generated and a new CA Certificate corresponding to these keys shall be Issued at minimum three months prior to the expiration of the old CA Certificate.

After generation of the new NHS Issuing Authority (CA) signing keys, the NHS 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 NHS 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 NHS 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 (see [14])

All copies of old NHS 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.

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 NHS Issuing Authority services. Business continuity plans for Participants providing Trust Services shall be detailed in the CPS or supporting documentation. Plans must be approved by the NHS 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 comprise of a CA or CA Keys, the NHS 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 4.9.6 of this Certificate Policy.
- Cease any further Certificate Issuance from the affected CA.

The Policy Management Authority shall make any determination relating to the Revocation of the Root CA Certificate.

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 CPS or supporting documentation. Plans must be approved by the NHS 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 Manufacturer 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, 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.

5.8 CA or RA termination

Termination of a CA is regarded as the situation where all service associated with the NHS 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.

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

- Inform both the NHS 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 NHS 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 in accordance with the NHS Digital Records Management Policy but in any event not less than 7 years.

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 must be detailed in supporting documentation. Controls must be approved by the NHS Issuing Authority.

6.1 Key pair generation and installation

6.1.1 Key pair generation

NHS 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 NHS 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 supporting documentation. Procedures must be approved by the NHS Issuing Authority or Auditors acting on its behalf.

Subscribers’ (Subjects’) Key Pairs may be generated by the Subscriber (Subject). Procedures must be approved by the NHS Issuing Authority or Auditors acting on its behalf.

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

6.1.2 Private key delivery to subscriber

Not Applicable.

6.1.3 Public key delivery to certificate issuer

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

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 NHS Issuing Authority.

6.1.5 Key sizes

The size of Certificate Manufacturer (i.e. Certificate Authority) and any supporting CA-Keys shall be not less than 2048 bit modulus for RSA.

The size of Subscribers' Private Keys shall be not less than 2048 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 Certificate Policy may be used only for those purposes defined in section 2.2 of the PKI Disclosure Statement [4].

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 that affect 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 at level 3.

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 NHS Issuing Authority and supporting CA Keys, and keys that affect the outcome of Issued Certificates and Certificate Status Information services, at a minimum, three-person control is required.

6.2.3 Private key escrow

Subscribers shall not provide Private Key escrow services.

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

6.2.4 Private key backup

Participants providing Trust Services may backup and archive Private Keys, including CA- keys.

Subscribers (Subjects) may backup their own keys.

In all cases key backups shall at a minimum be protected to the standards commensurate with that stipulated for the primary version of the key.

In the case of aggregated backups of keys, (for example, many keys backed-up inside and protected by a single security environment), the backed-up keys must be protected at a level commensurate with that stipulated for the NHS Issuing Authority's private signing key.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

If Subscriber 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 or Subscribers conducting such key transfer shall provide detail of the procedure in 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 NHS 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

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 shall provide detail of the procedure in supporting documentation. Procedures must be approved by the NHS Issuing Authority or Auditors acting on its behalf.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

Strict controls over destruction of the Root CA Key, and keys that affect the outcome of Issued Certificates and Certificate Status Information services must be exercised.

Whether active, expired or archived, the NHS Issuing Authority must approve the destruction of the Root CA Key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

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:

- Trust Service Provider trusted roles – five (5) 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 NHS 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.

If applicable, unblocking code for a cryptographic module (if available) shall only be delivered to the legitimate holder of the module after an express request from the holder. Delivery of the unblocking code requires strong identification of the holder. See Section 6.2.8.

6.4.2 Activation data protection

All NHS 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 supporting documentation. Procedures must be approved by the NHS 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 threat 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 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 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 NHS 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 supporting documentation (such as the CPS) which must be approved by the NHS 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 supporting documentation which must be approved by the NHS Issuing Authority.

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 5280 [9] may be Issued.

7.1.2 Certificate extensions

All Entity PKI software must correctly process the extensions identified in 3.2.1 and 3.2.2 of the IETF PKIX Certificate profile. The following are required Certificate extensions:

- The Basic Constraints extension is set to TRUE for CA-certificates only; its use is critical specifying that it is a CA Certificate. This extension is marked as CRITICAL in subordinate CA certificates, but not in the Root CA certificate. This is a known non-conformance with x.509 RFC5280 standard and is accepted by the NHS Issuing Authority.
- Where CRLs (ARLs) are used to produce Certificate Status information, the CRL (ARL) Distribution Point extension is mandatory and shall identify a location where the latest CRL Issued by the NHS Issuing Authority can be obtained.

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

The use of all name forms shall be consistent with section 2.1 of this Policy. Name forms shall be approved by the NHS 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 the PKI Disclosure Statement [4]. This may 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 5280 [9] may be issued.

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

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)

No stipulations.

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 NHS Issuing Authority and the Participants providing Trust Services.

For all Participants providing Trust Services audit must be sufficient to demonstrate to both the NHS 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 prescribed criteria defined by the Policy Management Authority.

For Certificate Manufacturers audit shall be conducted by an approved third-party auditor and conducted not less than annually.

The NHS 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 NHS Issuing Authority is decided by the Policy Management Authority. Approved auditors are defined in section 2.11 of the PKI Disclosure Statement [4] 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 this Certificate Policy, any supporting documentation and any declared assurance or approval schemes under which Trust Services are operated.

Where the Participants providing Trust Services uses 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 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 NHS 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-compliant services will be developed, approved by the Policy Management Authority and implemented by the NHS Issuing Authority. For lesser exceptions or deficiencies, the NHS 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 NHS Issuing Authority shall make available to Subscribers details of the deficiency and any remedial action required to be taken.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

The NHS 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.

9.1.3 Revocation or status information access fees

The NHS 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.

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 NHS Issuing Authority. If such fees are charged, the fee schedule shall be published and made available to all affected parties.

9.1.5 Refund policy

Refunds are specified in the commercial arrangements between the NHS Issuing Authority and Subscribers.

9.2 Financial responsibility

9.2.1 Insurance coverage

The NHS 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 NHS 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 Statement [4].

9.2.3 Insurance or warranty coverage for end-entities

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The NHS Issuing Authority and all Participants providing Trust Services shall classify personal, privacy related or corporate information as 'Official - Sensitive' [18]. Such information shall not be released without the prior consent of the Subscriber, unless required otherwise by law.

All private and secret keys and associate activation data, used or otherwise handled by Participants 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.
- Or as part of 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 'Official - Sensitive' [18] or as private. Identification information or other personal or corporate information appearing on Certificates is not considered 'Official - Sensitive' [18].

9.3.3 Responsibility to protect confidential information

The NHS Issuing Authority carries overall responsibility to protect all information classified as Official - Sensitive [18] that it holds. Responsibility to maintain the confidentiality of information for information that they hold 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], the EU General Data Protection Regulation (GDPR) [22], 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 NHS 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 Statement [4].

Privacy information shall be classified and treated as ‘Official - Sensitive’. 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 NHS Issuing Authority carries overall responsibility to protect privacy information. Responsibility to protect privacy information is devolved to all Participants via this Certificate Policy and applicable supporting documentation.

Participants also carry responsibility to protect privacy information 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:

- On 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 information 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 it incorporates, or which is incorporated at its request within a Certificate. Consequently, it shall take all reasonable precautions to ensure that this information does not infringe the intellectual property rights of any third party or would otherwise cause any person any unnecessary offence, damage or distress, and it shall, on reasonable demand, hold blameless and indemnify any other Participant as reasonably necessary.

9.6 Representations and warranties

The NHS 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.
- 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 NHS Issuing Authority.

9.8 Limitations of liability

By signing a Certificate under this Certificate Policy, the NHS 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 NHS 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 NHS 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 NHS 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 NHS 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 NHS 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 NHS 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 Statement [4].

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 NHS 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 NHS 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 NHS 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 NHS Issuing Authority (such consent not to be unreasonably conditioned, withheld or delayed); and
- Give the NHS 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 NHS 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 NHS 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 (whether in respect of this Certificate Policy, any written agreement between the parties or otherwise), the NHS Issuing Authority may revoke the Subscriber's license to issue and/or manage Certificates 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 of the Insolvency Act 1986). of the
- 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. In accordance with the termination actions set out in paragraph 5.8 the NHS Issuing Authority may terminate any Issued Certificate if this Certificate Policy is revoked, withdrawn or otherwise terminated without replacement prior to the termination or expiry of any licenses granted to the Certificate Authorities to operate under its governance.

9.10.3 Effect of termination and survival

Any Certificate issued prior to termination shall survive that termination of the Certificate Policy and shall endure, subject to any termination or revocation of the relevant Certificate, until expiry of its state validity period. Without prejudice to the generality of this clause 9.10.3, 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 Service of Notices

Whenever a party to this Certificate Policy desires or is required to give any notice, demand, or request, such communication shall be made either by using digitally signed messages consistent with the requirements of this Certificate Policy, or by sending it by pre-paid first class post, recorded delivery or registered post, by fax or by personal delivery.

A notice shall be deemed to have been received on the occurrence of the earlier of:

- Upon the sender receiving a valid, digitally signed acknowledgement of receipt from recipient;
- If delivered personally, at the time of delivery;
- In the case of pre-paid first class post, two days from the date of posting;
- In the case of recorded delivery or registered post, on the day recorded by the courier as having been delivered if received before 16:00 hours and otherwise at 09:00 of the next day; and
- In the case of fax, on the day of transmission if sent before 16:00 hours of any day and otherwise at 09:00 hours on the next day, provided that, at the time of transmission of a fax, an error-free transmission report has been received by the sender.

Electronic communications shall be effective provided that an acknowledgement is received within two days. If acknowledgement is not received then the sender must give notice by paper-based communications.

Any notices given under or in relation to this Certificate Policy shall be in writing, signed by or on behalf of the party giving it and shall be served by delivering it personally or to the address and for

the attention of the relevant party notified for such purpose or to such other address as that party may have stipulated.

9.11.2 Subscribers

Subscribers shall address notices to the NHS Issuing Authority as detailed in Section 2.1 of the PKI Disclosure Statement [4] of this Policy.

A Subscriber 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.

9.11.3 Issuing Authority

All notices by the NHS 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 NHS 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.

9.11.4 Notification

Any notices given in 9.11.3 shall be deemed served effective upon dispatch.

9.12 Amendments

9.12.1 Procedure for amendment

Approved 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 must 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 9.11 of this Certificate Policy by the NHS Issuing Authority registered with the Policy Management Authority, and will be prominently posted on a Web site (either internal or external or both). The NHS Issuing Authority 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 users may file comments through the NHS 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 5 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 at the sole 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 30 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 NHS Issuing Authority. The NHS Issuing Authority shall deal with such disputes in accordance with its dispute resolution process specified in Section 2.10 of the PKI Disclosure Statement [4].

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:-

- Glossary of Terms [1], [2]
- PKI Disclosure Statement [4]
- Documents as listed in the 'Related Documents' section of this Policy

In the event of any ambiguity, inconsistent or incompatible provisions, this Policy shall take precedence, followed by the provisions of the PKI Disclosure Statement.

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 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 NHS 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 NHS 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 NHS 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 1.3 is descriptive only for reference purposes and such sections 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 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 beneficiaries.

Appendix A - PKI Glossary of Terms

Asymmetric Cryptography

In this type of cryptography, a key pair - Private and Public Key is used. The Private Key is kept secret and the Public Key is widely distributed. Each key is used to validate operations performed by the other key.

Authentication

The presentation of a credential by a user to a system in order that the users identity may be established so as to determine whether the user is able to access the system.

Authorisation

The action of determining once a user has authenticated to a system what aspects or parts of the system the user is actually allowed to use.

Certificate

See ‘Digital Certificate’

Certification Authority (CA)

A ‘Certification Authority’ is a trusted party that issues, signs and validates digital certificates and is responsible for the full lifecycle management of such certificates

Certificate Manufacturer

The ‘Certificate Manufacturer’ is the organisation which has responsibility for producing certificates and managing the PKI service in line with the applicable Certificate Policy(s) and PKI Disclosure Statement(s). The ‘Certificate Manufacturer’ is responsible for producing the ‘Certificate Practice Statement’ which shows how they conform to the applicable Certificate Policy(s) and PKI Disclosure Statement(s).

Common Name (CN)

The ‘Common Name’ is the name of the Subscriber/End-Entity e.g. John Smith. If the Subscriber/End-Entity is a Web server, the CN is the Fully Qualified Domain Name (FQDN) of the Web server.

Certificate Policy (CP)

A ‘Certificate Policy’ is a set of rules and statements governing the use of, management of and issuance of digital certificates from a Certification Authority.

Certificate Practice Statement (CPS)

The ‘Certificate Practice Statement’ (CPS) contains a list of elaborated processes and procedures which support the applicable Certificate Policy(s) and PKI Disclosure Statement(s) and show how the PKI is managed and supported from an operational perspective.

Certificate Revocation List (CRL)

A ‘Certificate Revocation List’ (CRL) provides a list of revoked certificates within a given PKI. A CRL is issued and signed by the Certificate Authority (CA) which issued the certificate or certificates which are to be suspended or revoked. An updated CRL is issued by the CA at regular, pre-defined intervals.

Certificate Status Information

‘Certificate Status Information’ indicates whether a certificate has been revoked or suspended. Such information is often supplied in bulk (via Certificate Revocation Lists) or can be requested for individual certificates via services such as Online Certificate Status Protocol (OCSP).

Credential

The representation in some form (e.g. paper based, electronic etc.) of proof of identity or knowledge. For example, a digital certificate issued from a trusted PKI to a Subscriber attests to the identity of the holder since only the Subscriber has access to and can use the Private Key.

Digital Certificate

A digital certificate is a secure electronic identity that certifies the identity of the holder. Issued by a Certification Authority, it typically contains a user's name, public key, allowed uses for the certificate and other related information. A digital certificate is tamper-proof and cannot be forged, and is signed by the private key of the Certification Authority which issued it.

Digital Signature

A Digital Signature is created by signing the Message Digest (Message Hash) of the original data or message using a certificate’s Private Key. A digital signature assures the identity of the sender and the integrity of the data and can be checked by the recipient using the senders Public Key.

End-Entity

An ‘End-Entity’ is an entity that participates in the PKI. An ‘End-Entity’ could be a server, service or a person. An ‘End-Entity’ is also known as a ‘Subscriber’.

Hash Function

A Hash Function is a transformation that takes an input and returns a fixed-size string, which is called the hash value (sometimes termed a message digest, a digital fingerprint, a digest or a checksum). The ideal hash function has three main properties - it is extremely easy to calculate a hash for any given data, it is extremely difficult or almost impossible in a practical sense to calculate a text that has a given hash, and it is extremely unlikely that two different messages, however close, will have the same hash.

Issuing Authority

The Issuing Authority is responsible for determining who can be issued with a certificate bearing the Issuing Authority’s name. The Issuing Authority is named within all certificates which are issued.

Message Authentication Code (MAC)

Similar to a Message Digest (Hash/Fingerprint), except the Shared Secret Key is used in the process of calculating the Hash. Since a shared secret key is used, an attacker cannot change the Message Digest. However the shared secret key has to be first communicated to the participating entities, unlike Digital Signature where the Message Digest is signed using the Private Key.

Message Integrity

‘Message Integrity’ is the property of ensuring that a message sent from one person or system to another has not been altered in transit either maliciously or accidently.

Non-repudiation

‘Non-repudiation’ is the property of being unable to deny being the author and/or sender of a message due to the use of message hashing/digital signing which proves beyond doubt that the messages integrity/source have not been compromised.

Online Certificate Status Protocol (OCSP)

A service which can be used to ascertain the status of a single certificate. Its main benefit is speed of response to the system requesting the status. OCSP provides one of three responses to the requestor for the status of each certificate requested: “Good”, “Revoked” or “Unknown”.

Private Key

The Private Key is the Key in Asymmetric Cryptography that is kept secret by the owner (End-Entity/Subscriber). The ‘private key’ can be used for authentication and digital signing purposes.

Public Key

The Public Key is the Key in Asymmetric Cryptography that is widely distributed. It can be used as the key for encryption of data or as the key which checks the validity of a digital signature.

Personal Identification Number (PIN)

A sequence of digits used to verify the identity of the holder of a token. It is a type of password.

Policy Management Authority (PMA)

The PMA is responsible for setting the strategic direction and over-arching policy for management and control of the NHS PKI. The PMA brings together key stakeholders in order to make such decisions. In the context of the NHS PKI, the PMA is additionally responsible for directing the work of the PKI Technical Group (PTG).

PKI Disclosure Statement

A PKI Disclosure Statement summarises the main points of the Certificate Policy for the benefit of Subscribers and Relying Parties. In addition, it provides further elaboration of some aspects of the Certificate Policy where additional detail is required.

PKI Technical Group (PTG)

The PTG is responsible under the Policy Management Authority’s (PMA) direction for investigating and researching PKI technical issues and reporting back on potential solutions. A secondary responsibility is to make technical recommendations on improving operating procedures.

Registration Authority (RA)

A person, group or organisation responsible for the identification and authentication of an applicant (or Subscriber) for a digital certificate. Such responsibilities are conferred on the RA by the Issuing Authority. An RA does not issue or sign certificates.

Relying Party

A ‘Relying Party’ is an individual, group, organisation, system, service or other entity which relies on the information presented in a digital certificate or information which has been signed or encrypted using a digital certificate. A ‘Relying Party’ is not necessarily a ‘Subscriber’ to a PKI (i.e. a ‘Relying Party’ does not necessarily have digital certificates issued to it from the PKI whose certificates it is ‘relying’ on.)

Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is a security protocol that provides authentication (Digital Certificate), confidentiality (encryption), and data integrity (Message Digest - MD5, SHA etc).

SHA Hash Functions

The SHA hash functions are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing

Standard. SHA stands for Secure Hash Algorithm, SHA-1 is a 160-bit one-way hash function. SHA-224, SHA-256, SHA-384 and SHA-512 are usually referred to as SHA-2 implementations with the number relating to the bit length.

Shared Secret

See ‘Symmetric Cryptography’

Subscriber

A ‘Subscriber’ can be an individual, group, organisation, system, service or other entity which uses of a certificate or certificates issued from a PKI in order to make identity claims, sign documents/messages, encrypt data and so forth. A ‘Subscriber’ is holder of the Private Key of any certificate issued to them and the only entity which can make use of that Private Key.

Symmetric Cryptography

In ‘Symmetric Cryptography’, the message or data is encrypted and decrypted by using the same key. Use of the same key for encryption/decryption is sometimes known as ‘shared secret’ cryptography in that the key should only be known (or ‘shared’) between the parties involved in the transaction.

tScheme

tScheme provides independent, self-regulating and industry led assurance activities against a strict set of assessment criteria under which trust services (such as the NHS PKI) can be approved.

Additional information about tScheme can be found at the following web page:
http://www.tscheme.org/about/index.html

Validity Period

The length of time which the certificate is valid for use by the Subscriber/End-Entity for the designated reasons (e.g. digital signing, authentication etc.) Once a certificate’s Validity Period has ended, the certificate is considered ‘expired’ and should no longer be used or trusted.