NHS Connecting for Health	**Authentication Certificates PKI Disclosure Statement**			
	Programme	NPFIT	**Document Record ID Key**	
	Sub-Prog / Project	Infrastructure	NPFIT-FNT-TO-INFR-0053.01	
	Prog. Director	Chris Wilber	Version	2.0
	Owner	James Wood	Status	APPROVED
	Author	Trustis Limited/Mark Penny	Version Date	10th November, 2011

Authentication Certificates PKI Disclosure Statement

Amendment History:

Version	Date	Amendment History
0.1	23rd October 2006	First draft for comment
0.2	23rd November 2006	Inclusion of a section (2.17) on Certificate Manufacturers
0.3	4th. January 2007	Comments from Malcolm McKeating and clarification of organisations as Subscribers
0.4	20th February 2007	Refine description of authentication certificates for individuals only and inclusion of PMA mailbox address and limitations on use of contact mailboxes
0.5	3rd August 2007	Some revisions to formatting and updating of some content as a result of feedback. Also revisions as a result of legal review.
0.6	31st. August 2007	Revised following further input from DLA Piper
0.7	19th.November 2007	Changes to section 2.18 – validity periods for Certificate Status Information.
0.8	16th. January 2008	Remove reference to Content Commitment CP in section 1.1. Section 2.2 add wording to the effect that registration documents are available on NHS internal network only
0.9	25th July 2008	Owner change
1.0	3rd November 2008	Confirm contact details (internet) and minor revisions
1.1	24th November 2008	Minor corrections
1.2	27th November 2008	Minor corrections
1.3	28th November 2008	Finalise corrections
1.4	5th June, 2009	Updated with new document reference number
1.5	November, 2009	Further updates by Trustis in light of Certificate Manufacturer review
1.6	6th May, 2011	Annual review and update
1.7	1st June, 2011	Update following Certificate Manufacturer and NHS PKI Policy Management Authority review
1.8	23rd September, 2011	Further update following management decision to progress with CA Key Changeover option for extending the NHS PKI Service
2.0	10th November, 2011	Document approved by PMA

Forecast Changes:

Anticipated Change	When
Annual Review	November, 2012

Reviewers:

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
PMA Members				

Approvals:

This document must be approved by the following:

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

Distribution:

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

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

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

WWW: TBD

Document Status:

This is a controlled document.

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

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number/URL	Title	Version
1	http://intranet.connectingforhealth.nhs.uk/departments/npo/glossary/glossary (internal) http://www.connectingforhealth.nhs.uk/factsandfiction/acronyms (external)	Online 'Glossary of Terms'.	N/A
2	http://nww.connectingforhealth.nhs.uk/infrasec/nhspki/glossary (N3 connection required)	PKI 'Glossary of Terms'	N/A
3	http://nww.connectingforhealth.nhs.uk/iim/documents/ra01partb.doc	RA User Registration form	
4	http://nww.connectingforhealth.nhs.uk/iim/documents/ra01parta.doc	RA User Registration Terms & Conditions	
5	http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/links/IGASv1.doc	IG Statement of Compliance	1.0
6	NPFIT-FNT-TO-INFR-0056.01	NHS Level 1 Issuing Authority Base Certificate Policy	1.6
7	http://nww.connectingforhealth.nhs.uk/infrasec/nhspki/docs	NHS PKI Repository	N/A
8	http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550	NHS Confidentiality Code of Practice	N/A
9	http://www.legislation.gov.uk/ukpga/1998/29/contents	UK Data Protection Act (1998)	N/A

Glossary of Terms:

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

Term	Acronym	Definition

Contents

1 About this Document

1.1 Purpose

The purpose of this Public Key Infrastructure (PKI) Disclosure Statement (PDS) document is to support the NHS Level 1 - Issuing Authority Base Certificate Policy [6], by describing the elements of this policy that are of relevance to Authentication Certificates issued to individuals in a manner that is straightforward to follow for the community of users issued with these certificates.

1.2 Audience

This document has been written for all subscribers of Authentication digital certificates issued to provide an Authentication mechanism for constructing access rights to CRS and other CRS enabled applications.

This document is also of relevance to the Certificate Manufacturers listed in section 2.17 of this document.

1.3 Content

This document comprises the following sections.

- Section 1 – About this Document.
- Section 2 – PKI Disclosure Statement (PDS).

Section 2 contains the full list of provisions contained in this PDS. The full contents are given in the contents list.

2 NHS Authentication Certificate Policy PKI Disclosure Statement

Important Notice:

This document (PKI Disclosure Statement) does not by itself constitute the Certificate Policy under which Certificates governed by this Certificate Policy are issued. You must read the Certificate Policy before you apply for or rely on a Certificate issued by the NHS Issuing Authority.

The Certificate Policy under which Certificates are issued is defined by two documents:

- Authentication Certificates PKI Disclosure Statement (this document).
- NHS Level 1 - Issuing Authority Base Certificate Policy [6]

The purpose of this document is to:

- Summarise the key points of the NHS Level 1 - Issuing Authority Base Certificate Policy [6] for the benefit of Subscribers, Subjects and Relying Parties.
- Provide additional detail and further provisions that apply to the NHS Level 1 - Issuing Authority Base Certificate Policy [6] and which are incorporated by reference.

Certificates issued by the Issuing Authority reference this document, and consequently the NHS Level 1 - Issuing Authority Base Certificate Policy [6].

Terms used in the document are defined in the online version of the NHS CFH ‘Glossary of Terms’ document [1] and the PKI ‘Glossary of Terms’ [2]

2.1 Policy Management Authority and NHS Issuing Authority Contact Information

The points of contact for Information Security and Risk Management policy issues only are as follows:

Policy Management Authority:

pma@nhs.net

NHS Issuing Authority:

cfh.infosecteam@nhs.net

2.2 Certificate Type, validation procedures and usage

The Authentication Certification Services provided by the NHS Issuing Authority implement a closed public key infrastructure (PKI) in the sense that access and participation is only open to those who both satisfy eligibility criteria and are approved by the NHS Issuing Authority. Participants providing trust services and End-Entities authorised and approved to issue, obtain, use, and/or rely upon Certificates that reference this Certificate Policy are clearly defined. Participation is conditional upon agreeing to be bound by the terms of this Certificate Policy.

The Authentication Certification Services are provided by the NHS Issuing Authority to support secure operations and interactions with the general public, agent organisations, partners, customers and external contractors, in the direct pursuit of NHS related business or in the authorised usage of services provided by the NHS Issuing Authority. Certificates provided by this service are supported by strong cryptography and highly robust registration mechanisms to a defined and assured level of trust and security.

Authentication Certificates may only be used for:

- Authenticating access to electronic systems containing patient, health care or social care information which are provided as part of the NHS National Systems.

These Certificates shall not be used for any other purpose than those specified above. Applicants for Certificates are required to submit to the validation of identity credentials and their eligibility to hold such a certificate as detailed in:

- Registration Authority User Enrolment form (RA01) [3] and
- Registration Authority User Enrolment Terms & Conditions [4].

Both these forms are available on the N3 network only.

2.3 Reliance Limits

The NHS Issuing Authority does not set reliance limits for Certificates it issues. Reliance limits may be set by applicable law or by agreement. See limitation of Liability below.

2.4 Obligations of Subscribers and Subjects

Subscribers (organisation) and Subjects who are the agents of the Subscriber must comply with the requirements as defined in the CFH document **RA01 Form – Registration for use of National Programme systems [3].**

Subscribers must ensure compliance with all obligations described in the NHS CFH document “Statement of Compliance” (SoC) [5]. It is the responsibility of the Subject to:

- Ensure all information submitted in support of a certificate application is true, accurate and they hold such rights as necessary to any trade marks or other such information submitted during the application for a certificate.
- Review the issued Certificate to confirm the accuracy of the information contained within it before installation and first use.
- Use a trustworthy system for generating or obtaining a key pair and to prevent any loss, disclosure, or unauthorised use of the private key.
- Keep private keys confidential.
- Keep confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to Certificates and PKI facilities.
- Make only true and accurate representations to the Registration Authority and/or Issuing Authority as to the information required to determine eligibility for a certificate and or information contained within the Certificate.
- In accordance with the ”NHS Level 1 Issuing Authority Base Certificate Policy” [6], exclusively use the Certificate for legal purposes and restricted to those authorised purposes detailed by this Certificate Policy. Usage of a Certificate for any purpose outside of those purposes detailed in this Certificate Policy is made at the Subjects own risk and the Issuing Authority/Policy Management Authority accepts no liability for such usage.
- Immediately notify the Registration Authority and/or Issuing Authority of a suspected or known key compromise in accordance with the procedures laid down in the NHS Issuing Authority Certificate Policy.

For a device or application, the individual responsible for the device or application must accept these responsibilities.

Warning: If a Subjects Private Key is compromised, unauthorised persons may be able to commit the Subscriber to unauthorised obligations.

2.5 Certificate Status checking Obligations of Relying Parties

Relying Parties must comply with the requirements as defined in the Relying Party Agreement, or existing contractual agreements and this PKI Disclosure Statement.

A Relying Party may justifiably rely upon a Certificate only after:

- Ensuring that reliance on Certificates issued under this Certificate Policy is restricted to appropriate uses (see “Certificate Type, validation procedures and usage” above for a summary of approved usages).

- Ensuring that the Certificate remains valid and has not been Revoked or Suspended by accessing any and all relevant Certificate Status Information
- Determining that such a Certificate provides adequate assurances for its intended use.
- Take any other precautions prescribed in this Certificate Policy.

2.6 Limited Warranty and Disclaimer/Limitation of Liability

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 other use than in accordance with this Certificate Policy and other agreements. Subscribers will immediately indemnify the NHS Issuing Authority from and against any such liability and costs and claims arising therefrom.

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 excess or implied warranty, breach of contract, tort, misrepresentation, negligence, strict liability however arising from or in relation to the use of or in relation to the use of or reliance on any Certificate except only in the case of the NHS Issuing Authority's negligence, wilful misconduct, or otherwise required by 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.

The NHS Issuing Authority excludes all liability of any kind in respect of any transaction into which an End Entity (Certificate Holder or Relying Party) may enter with any third party.

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

Each provision of this Certificate 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.

2.7 Applicable Agreements, Certification Practice Statement, Certificate Policy

The full Certificate Policy, Subscriber Agreement and Relying Party Agreement are published by the Issuing Authority and available at the locations [7] referenced in this PKI Disclosure Statement.

Such information is also made available subject to approval of a formal application in writing to the Issuing Authority at one of the e-mail addresses given in Section 2.1 above.

2.8 Privacy Policy

The NHS Issuing Authority strongly believes in an individual's rights to privacy, and operates this Certification Service according to the "NHS Confidentiality Code of Practice" [8] and the RA01 Terms and Conditions [4], including compliance to the Data Protection Act 1998 [9]. Details can be obtained from the following location:

- Registration Authority User Enrolment form (RA01) [3].

2.9 Refund Policy

Not applicable.

2.10 Applicable Law and Dispute Resolution

Disputes shall be handled in accordance with the NHS Issuing Authority's documentation, which can be obtained by applying to the NHS Issuing Authority. Contacts details are provided in section 2.1 of this document.

2.11 CA & Repository Licences Trust Marks and Audit

Certificates are manufactured under this Certificate Policy through the use of a NHS Connecting for Health service which is operated in conformance with ISO 27001.

Audit shall be carried out on a periodic basis required to maintain security and trust accreditations. The following Auditors have been approved under this policy:

- Audit resources of contracted Participants providing trust services.
- A certified public accountant with demonstrated expertise in computer security or an accredited computer security professional.

2.12 Identification of this Certificate Policy

This Certificate Policy has been assigned an Object Identifier (OID) of:

- 1.2.826.0.1275.101.0.3.2.0

2.13 Approved Registration Authorities

The Registration Authorities at the following levels have been approved by the NHS Issuing Authority:

- NHS Connecting for Health (authorised to Register additional RAs).
- NHS Strategic Health Authorities (authorised to Register additional RAs).
- NHS Trusts.
- BT Telecommunications PLC

2.14 Approved Repositories

The following Repositories have been approved by the NHS Issuing Authority under this Certificate Policy:

- NHS Connecting for Health
- British Telecommunications PLC

2.15 Eligible Subscribers and Subjects

The following types of Subjects and Subscribers are eligible to be issued with Certificates under this Certificate Policy:

- Subjects - agents of an organisation (Subscriber) that has not been issued with Certificates but has Subjects (End-Entities) under its control who have been issued with Certificates to perform and fulfil the business requirements of the organisation.
- Regulated health professionals.
- Non-regulated health professionals.
- Persons who have a requirement and approval for access to the NHS National Systems.
- Organisational support staff not already registered as regulated or non-regulated health professionals.
- Subscriber - Organisations contracted and approved to use the NHS NPfIT Spine infrastructure.

Details of the Subscriber Agreement are incorporated into the **RA01 Form – Registration for use of National Programme systems** and can be found at:

- Registration Authority User Enrolment Terms & Conditions [4].

.

2.16 Eligible Relying Parties

The following types of Relying Parties are eligible to rely on Certificates issued under this Certificate Policy:

- NHS CFH.
- British Telecommunications PLC.

2.17 Certificate Manufacturers

The following Certificate Manufacturers have been approved by the NHS Issuing Authority under this Certificate Policy:

- British Telecommunications PLC.

2.18 Certificate Status Information

Certificate Status Information is made available via Certificate Revocation Lists, (CRLs) and shall be scheduled for publication at a maximum interval of 12 hours. The CRL shall have a maximum validity period of 24 hours.

CRLs are published for access by Relying Parties.