

	End-Point Authentication Certificates PKI Disclosure Statement			
	Programme	NHS Informatics	Document Record ID Key	
	Sub-Prog / Project	Architecture	NPFIT-FNT-TO-INFR-0059.01	
	Prog. Director	Shaun Fletcher	Version	2.2
	Owner	James Wood	Status	APPROVED
	Author	Trustis Limited/Mark Penny	Version Date	10 th December, 2012

End-Point Authentication Certificates PKI Disclosure Statement

Amendment History:

Version	Date	Amendment History
0.1		First draft for comment
0.2		Updated following legal review
0.3	31 st . August 2007	Revised following further input from DLA Piper
0.4	1st September 2008	Change owner
0.5	19 th June, 2009	Further updates to layout, reference number and minor corrections to bring into line with other PDS documents
0.6	26 th June 2009	Further minor updates to content
0.7	26 th June 2009	Document reference updated
1.0	29 th June, 2009	Document Approved
1.1	9 th May, 2011	Annual review and update
1.2	1 st June, 2011	Update following Certificate Manufacturer and NHS PKI Policy Management Authority review
1.3	23 rd September, 2011	Further update following management decision to progress with CA Key Changeover option for extending the NHS PKI Service
2.0	10 th November, 2011	Document approved by PMA
2.1	13 th August, 2012	Document updated to reflect requirements for usage of NHS PKI End Entity certificates by the NHS 111 Number Programme and its suppliers
2.2	10 th December, 2012	Document approved

Forecast Changes:

Anticipated Change	When
Annual Review	November, 2013

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		2.2
Alistair Donaldson (for and on behalf of the PMA)		Digital Information and Health Policy Directorate		2.2

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	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/implementation/documents/RA01_Short_part_A.doc	RA User Registration form	
4	http://nww.connectingforhealth.nhs.uk/implementation/documents/RA01_Short_part_B.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
10	https://esw.national.ncrs.nhs.uk/cda-docs/help/Guidelines-for-use-of-the-NCRS-Spine-ESW-interface.pdf	Guidelines for use of the NCRS SPINE ESW Interface	Issue 1, Draft B
11	http://nww.connectingforhealth.nhs.uk/deployment/dir/dir-documents/epr-training.zip	Strategic EPR Training Package	N/A
12	TBD	NHS PKI – Subscriber Agreement for the NHS 111 Number Programme	1.0

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	7
1.1	Purpose	7
1.2	Audience	7
1.3	Content.....	7
2	NHS Authentication Certificate Policy PKI Disclosure Statement.....	8
2.1	Policy Management Authority and NHS Issuing Authority Contact Information 9	
2.2	Certificate Type, validation procedures and usage.....	9
2.3	Reliance Limits	10
2.4	Obligations of Subscribers.....	10
2.5	Certificate Status checking Obligations of Relying Parties	11
2.6	Limited Warranty and Disclaimer/Limitation of Liability.....	11
2.7	Applicable Agreements, Certification Practice Statement, Certificate Policy	12
2.8	Privacy Policy	12
2.9	Refund Policy	13
2.10	Applicable Law and Dispute Resolution	13
2.11	CA & Repository Licences Trust Marks and Audit.....	13
2.12	Identification of this Certificate Policy.....	13
2.13	Approved Registration Authorities	14
2.14	Approved Repositories	14
2.15	Eligible Subscribers and Subjects	14
2.16	Eligible Relying Parties.....	14
2.17	Certificate Manufacturers	15
2.18	Certificate Status Information	15

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 Endpoint (computer applications and devices) Authentication Certificates issued for use with NHS CFH approved systems for the NHS Care Records Service. The description of the elements within this Certificate Policy is provided in a manner that is straightforward to follow for the Service Provider community and the technical staff at NHS organisations issued with these certificates.

1.2 Audience

This document has been written for all Subscribers of Endpoint Authentication digital certificates issued to Service Providers for NHS CFH approved computer applications and devices for the NHS Care Records Service.

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. The applicable Certificate Policy must be read in conjunction with this PDS before any systems or processes rely on a Certificate issued by the NHS Issuing Authority.

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

- Endpoint 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 Endpoint 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 Endpoint 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.

Endpoint Authentication Certificates may only be used for:

- Authenticating NHS CFH approved¹ computer applications and devices for connectivity to the NHS National Systems (including LDAP and messaging interfaces) from Service Provider organisations.
- Authenticating and securing components of the NHS National Systems.

These Certificates shall not be used for any other purpose than those specified above. Applicants for Certificates are either required to submit the NHS site details

¹ Approved in this case means any solution, system or software which has been assured and approved through NHS CFH assurance processes and has received formal approval for deployment.

as described in the current version of the "Guidelines for use of the NCRS SPINE ESW Interface" document [10] or use the defined process which is in place for requesting Certificates via their Programme contact.

For those accessing ESW directly, information is additionally available in the EPR Training Guide [11] which is also available on CD from the Certificate Manufacturer at the following address:

Spine Programme Management Office
BT
1 Sovereign Street
Leeds
LS1 4BT

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

Subscribers must ensure compliance with all obligations described in the NHS CFH document "Information Governance Statement of Compliance" (IGSoC) [5].

It is the responsibility of the Subscriber and their Subjects to:

- Ensure all information submitted in support of a certificate application is true, accurate and they hold such rights as necessary to any trademarks 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 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.
- Immediately notify the Issuing Authority of a suspected or known key compromise in accordance with the procedures laid down in the NHS Issuing Authority Base Certificate Policy.

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

WARNING

If a Subscriber's Private Key is compromised, the communication channel of the Endpoint device or application and the information held on that system is at risk.

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 express 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 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 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 locations as relevant to the particular Certificate usage:

- Registration Authority User Enrolment form (RA01) [3]
- 111 Number Programme Subscriber Agreement [12]

2.9 Refund Policy

Not specified. This is subject to individual agreement or contract with the NHS Issuing Authority.

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.
- A UKAS approved tScheme audit body.

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 for issuing Endpoint Authentication Certificates:

- NHS Issuing Authority
- British 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 Subscribers and Subjects are eligible to be issued with Certificates under this Certificate Policy:

- Subscriber (organisation) – a Service Provider organisation that has not been issued with Certificates but has Subjects (NHS organisations) under its contractual control who have been issued with Certificates for authentication of an NHS CRS connection.
- Subject (organisation) – the NHS organisation that is identified by the Fully Qualified Distinguished Name (FQDN) in the 'Subject' name field of the Endpoint Authentication Certificate.
- Endpoint Devices: the holder of the device Certificate shall be the Service Provider organisation applying for the Certificate.

2.16 Eligible Relying Parties

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

- British Telecommunications PLC
- 111 Number Programme contracted suppliers

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 to Relying Parties via Certificate Revocation Lists (CRLs) and shall be scheduled for publication at a maximum of every 12 hours. The CRL has a validity period of 24 hours maximum and a publication period of 12 hours.

Other mechanisms for determining a Certificates Status may be made available from time to time and will be agreed between the Programme contact and the contractual suppliers of the appropriate service or services.