NHS Connecting for Health	**NHS PKI – Subscriber Agreement for the NHS 111 Number Programme**			
	Programme	NHS Informatics	**Document Record ID Key**	
	Sub-Prog / Project	Architecture		
	Prog. Director	Shaun Fletcher	Status	APPROVED
	Owner	James Wood	Version	1.0
	Author	Mark Penny	Version Date	10th December, 2012

NHS PKI – Subscriber Agreement for the NHS 111 Number Programme

Amendment History:

Version	Date	Amendment History
0.1		First draft for comment
0.2	21st November, 2012	DLA Piper amended version
0.3	23rd November, 2012	Amended to focus specifically on NHS 111 Number Programme Subscribers
0.4	25th November, 2012	DLA Piper amended version
0.5	27th November, 2012	Version for approval
1.0	10th 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
NHS PKI Policy Management Authority				0.5

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/Chair of NHS PKI Policy Management Authority		1.0
Alistair Donaldson (for and on behalf of the PMA)		Digital Information and Health Policy Directorate		1.0

Distribution:

All NHS 111 Number Programme Subscribers to the NHS PKI

The document will be made available at the NHS PKI Repository locations listed below.

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	NPFIT-FNT-TO-INFR-0056.01	NHS Level 1 Issuing Authority Base Certificate Policy	2.0
4	NPFIT-FNT-TO-INFR-0059.01	Endpoint Authentication PKI Disclosure Statement	3.0
5	http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/$file/authentication.htm	Registration and Authentication - e-Government Strategy Framework Policy and Guidelines	3.0 (September 2002)
6	TBD	NHS PKI – Relying Party Agreement for the NHS 111 Number Programme	1.0
7	TBD	NHS 111 Number Programme Certificate Request Form	TBD

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 document is to provide NHS 111 Number Programme Subscribers with the terms and conditions under which they can use Certificates issued from the NHS Public Key Infrastructure ('**NHS PKI**') provided as part of the National System.

Note that this document does not substitute or replace the Certificate Policy [3] under which Certificates from the NHS PKI are issued. Therefore, Subscribers must read the Certificate Policy [3] **before** applying for any Certificate from the NHS PKI.

1.2 Audience

This document has been written for NHS 111 Number Programme Subscribers to the NHS PKI.

The parties to this Agreement are the Issuing Authority and the Subscriber as identified by the NHS 111 Number Programme Certificate Request Form [7]

1.3 Content

The Related Documents set out on page 3 are expressly incorporated into this Agreement.

In the event of any ambiguity, inconsistent or incompatible provisions, the Certificate Policy [3] shall take precedence, followed by the provisions of the Endpoint Authentication PKI Disclosure Statement [4] then this NHS 111 Number Programme Subscriber Agreement, then the NHS 111 Number Programme Relying Party Agreement [6].

1.4 Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NHS Connecting for Health. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

Any party relying on or using any information contained in this document and/or relying on or using any system implemented based upon information contained in this document should do so only after performing a risk assessment. It is important to note that a risk assessment is a prerequisite for the design of effective security countermeasures. A correctly completed risk assessment enables an NHS organisation to demonstrate that a methodical process has been undertaken which can adequately describe the rationale behind any decisions made. Risk assessments should include the potential impact to live services of implementing changes.

This means that changes implemented following this guidance are done so at the implementers' risk. Misuse or inappropriate use of this information can only be the responsibility of the implementer.

2 Term of Agreement

This Subscriber Agreement is in force from the date of publication and at the point where a Subscriber accepts the terms of the Subscriber Agreement, both for itself and on behalf of Subjects for whom it is responsible, by undertaking one or more of the following actions:

- Signing the NHS PKI Subscriber Agreement (either physically or electronically)
- Downloading Certificates issued to the Subscriber which have been signed by one of the NHS PKI Certificate Authorities
- Making use of the Private Key associated with a Certificate issued by the NHS PKI for any purposes as defined in the Certificate Policy [3].

This Subscriber Agreement may change from time to time. Any amendments will be published to the NHS PKI Repository[1] and a 'notice of amendment' published to the same location. It is the responsibility of Subscribers to ensure that they are aware of any changes or amendments to this Subscriber Agreement by checking the NHS PKI Repository on a regular basis. Continued use of the NHS PKI or a Certificate by the Subscriber, or any Subject on whose behalf it has subscribed for a Certificate, after that date will be deemed to be acceptance of that change.

3 Definitions

A definition of the terms used in this Subscriber Agreement can be found in the online 'Glossary of Terms' [1] and the online 'PKI Glossary of Terms' [2]

4 Certificates

- From the perspective of NHS 111 Number Programme Subscribers, the NHS PKI only provides NHS PKI End Entity certificates for system authentication and secure messaging. These certificates are only issued to systems via registered system administrators who are positively identified as working for their particular organisation. Registration of a messaging system involves approval of registration and checking of ownership of DNS registration prior to issuance of a digital certificate via a self-service portal. This provides functionality and security features which correspond to a specific level of trust within the NHS PKI.

[1] See 'Distribution' section, page 2.

5 Your Obligations

The following obligations apply to Subscribers to the NHS PKI:

- The Subscriber must read the Subscriber Agreement (and any associated documents, see Section 18 of this document) prior to applying for, accepting or using any Certificate issued from the NHS PKI. If a Subscriber does not wish to be bound by the terms of this Subscriber Agreement (and other associated documentation, see Section 18), they must **not** apply for, accept or make use of any Certificate issued from the NHS PKI.
- The Subscriber must, on its own behalf and on behalf of any Subjects for whom it is responsible, accept the terms of this Subscriber Agreement, together with the terms and conditions stipulated in the Certificate Policy [3] and the associated NHS 111 Number Programme Certificate Request Form [7], or the 'online' version of the same, and the Endpoint Authentication PKI Disclosure Statement [4] prior to using any Certificate issued from the NHS PKI.
- The Subscriber warrants, represents and undertakes that it has obtained the sponsorship of a suitable Sponsor if sponsorship is required for obtaining a Certificate from the NHS PKI.
- The Subscriber consents, and warrants, represents and undertakes that it has obtained the consent of all the Subjects for whom it is subscribing, to the collection and processing of any ‘personal data’ (as defined by the Data Protection Act 1998) required for the issue and use of a Certificate. Personal data may be used for the purpose of operating the NHS PKI and may be disclosed to other Subjects, Subscribers, Relying Parties, End-Points, service providers, contractors and agents of the Issuing Authority, as well as any other users of and participants to the NHS PKI. The Issuing Authority's privacy policy is set out in section 2.8 of the Endpoint Authentication PKI Disclosure Statement [4].
- The Subscriber consents to supply information to the Registration Authority and/or Issuing Authority which is both true and accurate. The Subscriber will notify the Registration Authority and/or Issuing Authority immediately should there be any changes to such information.
- The Subscriber warrants, represents and undertakes that it holds the rights to any and all trademarks which may be submitted as part of any application for Certificates from the NHS PKI.
- The Subscriber warrants, represents and undertakes that it will only use, and will only permit Subjects for whom it is responsible to use, Certificates issued from the NHS PKI for the purposes listed in the Certificate Policy [3] and the Endpoint Authentication PKI Disclosure Statement [4].
- Before using any Certificate issued from the NHS PKI, the Subscriber must ensure, and shall procure that Subjects for whom it is responsible do likewise, that they have checked the accuracy of the Certificates contents and if there are any inaccuracies or errors, to report them immediately to the Registration Authority and/or Issuing Authority.
- The Subscriber will protect all Private Keys, PINS, passwords and other confidential information associated with their Certificate(s) which have been

issued from the NHS PKI and will protect them in a manner commensurate with the terms of the relevant Certificate Policy [3] and shall procure that Subjects for whom they are responsible do likewise.

- The Subscriber will inform the Registration Authority and/or Issuing Authority immediately if it suspects or knows that the private key or any other confidential information relating to a Certificate or Certificates issued from the NHS PKI that it holds has been compromised by any 3rd party, and shall procure that Subjects for whom they are responsible do likewise. On receipt of such information, the Issuing Authority will revoke the compromised or suspected compromised Certificate(s).
- The Subscriber shall check the Certificate Status Information published in accordance with Section 2.18 of the Endpoint Authentication PKI Disclosure Statement [4] before using a Certificate, and shall procure that Subjects for whom it is responsible do likewise.
- The Subscriber will cease to use the Private Key of any Certificate issued from the NHS PKI where that Certificate has been revoked or has expired.

6 Limitations on Use

Certificates issued by the NHS PKI should only be used by Subscribers for one of the purposes described in Section 2.2 of the Endpoint Authentication PKI Disclosure Statement [4], and shall procure that Subjects for whom it is responsible do likewise.

The NHS PKI Issuing Authority is not responsible for:

- assessing the appropriateness of usage of a Certificate; or
- any use of a Certificate for a purpose that is not set out in the Endpoint Authentication PKI Disclosure Statement [4].

Subscribers should also note Section 1.4.2 (Prohibitions to Certificate Uses) of the Certificate Policy [3].

7 Compromise of NHS PKI Security

A Subscriber must not attempt to monitor, reverse engineer or otherwise interfere with the technical implementation of the NHS PKI nor otherwise intentionally compromise the security of the NHS PKI (unless the Subscriber cannot be prohibited from doing so under applicable law), except by prior approval of the Issuing Authority.

It reserves the right to revoke the Certificate(s) of any Subscriber who it knows has or suspects has allowed their Private Key to be discovered by a 3rd party or who has used their Private Key in any way not in accordance with the Certificate Policy [3] or the Endpoint Authentication PKI Disclosure Statement [4].

8 NHS PKI Warranties

The Issuing Authority warrants that:

- It shall take all reasonable skill and care during the processing and issue of Certificates to ensure that material defects or errors are not introduced into any relevant Certificate; and

- It shall take all reasonable skill and care in 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 the Certificate Policy [3].

9 Disclaimer of Warranties

Except for the express limited warranties contained in Section 8, Participants acknowledge and agree this Subscriber Agreement 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 Subscriber Agreement or not) relating to the subject matter of this Subscriber Agreement, other than as expressly set out in this Subscriber Agreement.

10 Indemnity

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

- Use of Certificates and/or Public/Private Key pairs Issued under the Certificate Policy [3] in a manner that is not in accordance with the Certificate Policy [3]; and
- Subscribers' negligence, default or breach of the Certificate Policy [3] in any other manner.

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

- As soon as reasonably practicable give written notice of that matter to the Issuing Authority specifying in reasonable detail the nature of the relevant claim. (See Section 17 for contact details.)
- Not make any admission of liability, agreement or compromise in relation to the relevant claim without the prior written consent of the Issuing Authority (such consent not to be unreasonably conditioned, withheld or delayed); and
- Give the Issuing Authority and its professional advisers reasonable access to the premises and personnel of the Subscriber(s) and to any relevant assets, accounts, documents and records within the power or control of the Subscriber(s) so as to enable the Issuing Authority and its professional advisers to examine such premises, assets, accounts, documents and records, and to take copies at their own expense for the purpose of assessing the merits of the relevant claim.

The terms of Section 10 will survive any termination of this Agreement.

11 Limitations of Liability

By signing a Certificate containing a policy identifier which indicates issuance under the terms of the Certificate Policy [3], an Issuing Authority certifies to all who reasonably rely on the information contained in the Certificate in accordance with the Certificate Policy [3], that the information in the Certificate has been checked according to the procedures laid down in the referenced Certificate Policy [3].

The Issuing Authority assumes no liability whatsoever in relation to the use of Certificates or associated Public/Private Key pairs Issued under the referenced Certificate Policy [3] for any use other than in accordance with the referenced Certificate Policy [3] and the Endpoint Authentication PKI Disclosure Statement [4].

The Subscriber acknowledges that the Certificate is issued without charge and that it has not entered into this Subscriber agreement for commercial reasons. Accordingly, the Subscriber acknowledges and agrees that the Issuing Authority shall not be liable for any consequential, indirect or incidental damages, nor for any loss of business, loss of profit or loss of management time, whether foreseeable or unforeseeable, arising out of breach of any express or implied warranty, breach of contract, tort, misrepresentation, negligence, strict liability however arising, or in any other way arising from or in relation to the use of or reliance on, any Certificate except only in the case of the Issuing Authority's negligence, wilful misconduct, or where otherwise required by applicable law.

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

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

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

12 Force Majeure

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

13 Severability

Each provision of this Subscriber Agreement operates separately. If any part is held by a court to be unreasonable, invalid, illegal, or unenforceable at law, then that impediment shall not affect any other provision as if that provision or provisions had never been contained herein and, insofar as possible, the remainder of this agreement shall be construed to maintain the original intent of the Subscriber Agreement.

14 Governing Law

This Subscriber Agreement 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 Subscriber Agreement, then such matter shall be settled by mediation between the parties according to Section 15.

15 Dispute Resolution

All disputes shall be referred in writing to the Issuing Authority. The Issuing Authority shall deal with such disputes in accordance with its dispute resolution process specified in section 2.10 of the Endpoint Authentication PKI Disclosure Statement [4].

16 Non-Assignment

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

17 Notices

All notices, requests or demands in relation to this Subscriber Agreement should be made by e-mail to the NHS PKI Policy Management Authority at: pma@nhs.net

18 Entire Agreement

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

- Certificate Policy [3]
- Endpoint Authentication PKI Disclosure Statement [4]
- Relying Party Agreement [6]
- Glossary of Terms [1, 2]

- NHS 111 Number Programme Certificate Request Form [7]

The parties acknowledge and agree that they have not relied on any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement, provided that nothing in this Section 18 shall operate to exclude liability for fraud.