Document filename:	**NHS PKI - Root CA PKI Disclosure Statement - APPROVED - v4.0**		
Project / Programme	**Data Security Centre**	Project	**NHS PKI / Certificate Services**
Document Reference	DOC-00025868		
Project Manager	**Matt Wyatt**	Status	**Published**
Owner	**Neil Bennett**	Version	**4.0**
Author	**Matt Wyatt**	Version issue date	**01/07/2021**

NHS Root Certificate Authority PKI Disclosure Statement

Document management

Revision History

Version	Date	Summary of Changes
0.1	-	First draft for comment
0.2	27th. June 2007	Alignment with NHS Root CP following drafting note clarifications
0.3	3rd August 2007	Updates following legal review.
0.4	31st. August 2007	Revised following further input from DLA Piper
0.4a	18th September 2007	Final Draft for auditors – prior to PMA approval
0.5	12th March, 2009	Updated Owner information, headers etc – main document content has not been updated
0.6	30th April, 2009	Updated 'Privacy Policy' wording
1.0	30th April, 2009	Document approved for publication
1.1	5th June, 2009	Updated with new document reference number
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	17th April, 2013	Document revised following creation of the Health and Social Care Information Centre (HSCIC)/transferred to HSCIC document template
1.5	22nd April, 2013	Document approved by Chair of NHS PKI PMA.
2.0	26th February 2015	Document uplift tor reflect Spine 2 transition
2.1	6th August 2019	Annual document review Minor grammatical changes References to HSCIC and CFH replaced with NHS Digital Change to approvers Change to contact email addresses Web URLs amended Removal of references to IGSoC Removal of version numbers in associated documents Included Appendix A – Glossary of Terns

3.0	6th November 2019	Publication of version 3.0 after approval of version 2.1
3.1	25th June 2021	Changes to reflect audit findings Changes to owner Section 2.18 updated
4.0	1st July 2021	Published after PMA Approval

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
NHS PKI Policy Management Authority		01/07/2021	3.1

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
James Wood (for and on behalf of the PMA)				2.0
Matt Wyatt	*Matt Wyatt*	Chair of NHS PKI PMA		2.1
Steve Fenwick	*Steve Fenwick*	Specialist Security Services Lead		2.1
Matt Wyatt	*Matt Wyatt*	Chair of NHS PKI PMA		4.0

Glossary of Terms

Term / Abbreviation	What it stands for

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Related Documents

These documents will provide additional information:

Ref no	Doc Reference Number	Title
1	Appendix A	Online 'Glossary of Terms'.
2	Appendix A	PKI 'Glossary of Terms'
3	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	Certificate Policy for NHS Root Certification Authority
4	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 Root Certificate Authority PKI Disclosure Statement
5	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	Authentication PKI Disclosure Statement
6	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	Content Commitment PKI Disclosure Statement
7	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	Endpoint Authentication PKI Disclosure Statement

Ref no	Doc Reference Number	Title
8	RFC 3647 (http://www.ietf.org/rfc/rfc3647.txt)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
9	RFC 3280 (http://www.ietf.org/rfc/rfc3280.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~~	~~TBD~~	~~Contractor Security Policy~~ This document has been retired
~~12~~	~~http://systems.hscic.gov.uk/infogov/igsoc~~	~~Information Governance Statement of Compliance (IGSoC)~~ This process has been retired
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	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	https://webarchive.nationalarchives.gov.uk/20160729133521/http://systems.hscic.gov.uk/infogov/security/risk	Guidance for the Classification Marking of NHS Information
19	http://www.legislation.gov.uk/ukpga/1998/29/contents	UK Data Protection Act (1998)
20	http://www.iso.org/iso/catalogue_detail?csnumber=50297	ISO 27002: 2005 – Code of Practice for Information Security Management

Contents

1. Introduction

1.1. Purpose of Document

The purpose of this PKI Disclosure Statement (PDS) document is to support the NHS Root Certificate Authority Certificate Policy [3], by describing the elements of this policy that are of relevance to Certificates issued by the NHS Root Certificate Authority in a manner that summarises the salient points for the community of users. The NHS Root Certificate Authority is managed by the NHS Issuing Authority, under the overall control of the Policy Management Authority.

1.2. Audience

This document has been written for all parties that will use certificates issued by the NHS Root Certification Authority and NHS Service Providers.

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 Root Certificate Authority 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 Root Certificate Authority and this can be obtained by contacting the Policy Management Authority by the method detailed in section 2.1 of this document or by locating the relevant Certificate Policy in the Repository available at [14].

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

- PKI Disclosure Statement (this document).
- NHS Certificate Policy for the Root Certification Authority (CA) [3].

The purpose of this document is to:

- Summarise the key points of the NHS Certificate Policy for the Root CA [3].
- Provide additional detail and further provisions that apply to the NHS Certificate Policy for the Root CA [3] and which are incorporated by reference.

Certificates issued by the NHS Issuing Authority for use by level 1 CAs in the NHS Public Key Infrastructure (PKI) may reference this document and consequently the NHS Issuing Authority Root CA Certificate Policy.

Explanations of the various terms used throughout this document can be found at the Appendix A ([1], [2]).

2.1. Policy Management Authority and NHS Issuing Authority Contact Information

The points of contact are as follows:

- Policy Management Authority: **pma@nhs.net**
- NHS Issuing Authority: **pma@nhs.net**

Note: If the mailboxes identified above are used for any other purpose than those specified, such messages may be deleted without any action being taken.

2.2. Certificate type, validation procedures and usage

The Root CA Certification Service provided by the NHS Issuing Authority is a closed 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. Only 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 Registration Authority shall verify against the requirements of the PMA, 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.

The Root CA Services are provided by the NHS Issuing Authority in the direct pursuit of NHS Digital 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.

Certificates many only be issued to Certificate Authorities.

Certificates may only be used for:

- Certificate Signature
- CRL Signature
- Signing of on-line status information.

These Certificates shall not be used for any other purpose than those specified above.

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 section 2.6 for the limitation of Liability.

2.4. Obligations of Subscribers

Subscribers are restricted to Certificate Authorities operating as Level 1 CAs in the NHS PKI. All Subscribers are bound by the terms and conditions of the contractual arrangements between them and the NHS Issuing Authority.

It is the responsibility of the Subscriber 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.
- In accordance with the NHS Root Authority Certificate Policy [3], exclusively use the Certificate for legal purposes and restricted to those authorised purposes detailed by the NHS Root Authority Certificate Policy [3].
- Immediately notify the NHS Issuing Authority or Policy Management Authority of a suspected or known key compromise in accordance with the procedures laid down in the NHS Root Authority Certificate Policy [3].

- Define their Subscribers and Relying Parties in the Certificate Policy of the Subjects (Certificate Authorities) that operate under this Certificate Policy.

2.5. Certificate Status Checking Obligations of Relying Parties

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 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 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.

2.7. Applicable Agreements, Certification Practice Statement, Certificate Policy

The full Certificate Policy is published by the NHS Issuing Authority and available from the contact points given in section 2 of this document. It is also available from the NHS PKI Repository [14].

Such information may also be disclosed to other interested parties at the discretion of the Policy Management Authority.

2.8. Privacy Policy

The NHS Root Certificate Authority does not process personal information.

Information about organisations may be held by the Health and Social Care Information Centre (HSCIC – trading as NHS Digital) in connection with operation of the NHS Root Certificate Authority and associated procedures.

If you have any queries about the information held in connection with the NHS Root Certificate Authority, you can contact the NHS Issuing Authority at the e-mail address listed in Section 2.1 (“Policy Management Authority and NHS Issuing Authority Contact Information”)

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.

The provision of the NHS Issuing Authority Certification Services shall be governed by English law and all parties shall submit to the exclusive jurisdiction of the courts of England and Wales

2.11. CA and Repository Licenses, Trust Marks and Audit

Certificates are manufactured under this Certificate Policy through the use of the NHS Digital service which is operated in conformance with ISO27002:2005 [20] or any other standard that replaces or supersedes it.

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 **1.2.826.0.1275.100.0.3.1.0** and this OID may be included in certificates issued under this Certificate Policy and remains the property of the NHS at all times.

2.13. Approved Registration Authorities

The NHS Issuing Authority has approved the following Registration Authority to operate with respect to Certificates governed by this Certificate Policy.

- Health and Social Care Information Centre (trading as NHS Digital)

2.14. Approved Repositories

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

- NHS Digital (online Repository at [14])
- British Telecommunications PLC.

2.15. Eligible Subscribers

Eligible Subscribers are limited to operators of NHS Level 1 CAs or, operators of CAs who have been accepted by the PMA as having demonstrated both compliance with this Certificate Policy and the requirements for NHS Level 1 CAs. Subscribers must also have been accepted by the PMA to participate as part of the trust infrastructure controlled by the NHS Root CA. These are:

- The Health and Social Care Information Centre (HSCIC – trading as NHS Digital)

2.16. Eligible Relying Parties

Relying Parties eligible to rely on Certificates issued under this Certificate Policy are Subscribers only. These are:

- The Health and Social Care Information Centre (HSCIC – trading as NHS Digital)

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 an Authority Revocation List (ARL) and shall be scheduled for publication at least once every calendar year.

Publication of up to date ARLs shall be conducted as soon as practical if any CA Certificate is revoked for whatever reason following review and approval by the PMA at an emergency meeting.

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.