

nehta

Qualified Certificate Reference

Version 1.1 — 30 June 2009

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

www.nehta.gov.au

Disclaimer

NEHTA makes the information and other material ('Information') in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document Control

This document is maintained in electronic form. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Copyright © 2009, NEHTA.

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

Document Information

Change History

Version	Date	Comments
1.1	2009-06-30	Final

Table of Contents

Document Information	iii
Change History	iii
Table of Contents	iv
Preface	vi
Document Purpose	vi
Scope	vi
Intended Audience.....	vi
Document status	vi
Definitions, Acronyms and Abbreviations.....	vi
References and Related Documents	vi
Conformance	vi
1 Qualified Certificate References	1
1.1 Background	1
1.2 Purpose.....	1
1.3 Structure.....	1
1.4 OCR Elements	1
1.4.1 Type and Value.....	1
1.4.2 http://ns.nehta.gov.au/Qcr/Ref/Direct/PEM/1.0	1
1.4.3 http://ns.nehta.gov.au/Qcr/Ref/Http/1.0	2
1.4.4 http://ns.nehta.gov.au/Qcr/Ref/Ldap/1.0	2
1.4.5 Type Preference.....	2
Definitions	3
Shortened Terms.....	3
Glossary	3
Appendix A: QCR Schema	4
References	5
Normative references.....	5

This page intentionally left blank.

Preface

Document Purpose

The purpose of this document is to describe the NEHTA Qualified Certificate Reference (QCR). A QCR allows clients to obtain an X.509 certificate, which in turn will be used to secure messages, especially for Web services request and response.

Scope

This document only covers identifying parties in NEHTA specifications that use the XML format to represent data. In particular, this includes data in NEHTA Web services specifications.

Intended Audience

This is a technical document.

This document should be read and understood by:

- Solution Architects:
 - To understand how qualified identifiers are represented.
- Developers:
 - To implement qualified certificate references.
- Conformance Testers:
 - To evaluate whether an implementation conforms to qualified certificate references.

The reader is expected to understand URI and URLs.

Document status

This document is a draft and has been released for comment and feedback purposes.

Definitions, Acronyms and Abbreviations

For a lists of abbreviations, acronyms and abbreviations, see the [Definitions section](#) at the end of the document, on page 3.

References and Related Documents

For a list of all referenced documents, see the [References](#) at the end of the document, on page 5.

Conformance

The keywords **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** in this document are to be interpreted as described in [RFC2119].

1 Qualified Certificate References

1.1 Background

Currently, environments exist such that e-health community members may trust several different certification authorities (CAs). Consequently, there is more than one repository containing the X.509 certificates of healthcare providers.

In addition, some healthcare providers may not store their certificates in a public directory. This will be especially true during the various pilots and advance adopters projects with which NEHTA is involved.

1.2 Purpose

The *qualified certificate reference* specification provides a simple means of locating an X.509 certificate from a distributed reference. It also allows for direct retrieval from a PEM value.

1.3 Structure

A qualified certificate reference is a *type/value* tuple. The *type* implies the format of the *value* contents.

See Appendix A: for a listing of the QCR XML Schema.

A qualified certificate reference MUST only refer to a single certificate.

1.4 QCR Elements

1.4.1 Type and Value

Element *type* is a URI. Currently, it may be populated with one of the following constants.

1. `http://ns.nehta.gov.au/Qcr/Direct/Pem/1.0`
2. `http://ns.nehta.gov.au/Qcr/Ref/Http/1.0`
3. `http://ns.nehta.gov.au/Qcr/Ref/Ldap/1.0`

Contents of element *value* depend on what is specified by element *type*. Sections below describe the formats for each allowed type.

1.4.2 `http://ns.nehta.gov.au/Qcr/Ref/Direct/PEM/1.0`

PEM allows direct access to a certificate where the certificate is accessible from a directory. HTTP and LDAP types should be used in preference to PEM. This is partly because a certificate value consumes much more space than a reference. In addition, if a service returns a certificate value, this may give the impression that the service provides a facet of PKI when this is not the intention.

PEM is a textual format for X.509 certificates. A textual format is necessary for transmission in an XML message using Web services. PEM consists of base-64 encoding the distinguished encoding rules (DER) binary format. The resulting text is then delimited by header and footer lines.

1.4.2.1 Example

```
-----BEGIN CERTIFICATE-----
MIIDVTCCAr6gAwIBAgIBCjANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQGEwJBVTEEM
MAoGA1UECBMDUWxkMQ4wDAYDVQQKEwVOZUhuUQTEZMBcGA1UECXMQU2VjdXJlIE1l
c3NhZ2Z1uZzEPMA0GA1UEAxMQU01JIEENBMB4XDTA5MDQyMjIzMDQyMDQy
-----
```

```
MTIzMjQ0NVowXjELMAkGA1UEBhMCQVUxDDAKBgNVBAGTA1FsZDEOMAwGA1UEChMF
TkVIVEExGTAXBgNVBAsTEFNlY3VyZSBZNzXNzYwdpbmcxFjAUBgNVBAMTDTE5Mi4x
NjguNDANjIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDECaomq5Mk
ujd4yPARNvbiJXwiVni9KlSQSRlTOJIXIamkzA3DndPP+hOXs4fRWNeqXp/mA5F8
Ra/4bvbqnbGdv3fRgQmnJfImfPIMMIM8KtoYu0T0Q/WuwK4FzuUT91bCgV+hUc5z
yaMhr/oBSSLm+ry9UbrUESDNi2hgh8MyLQ+YkAU2nhRGZ6CyeWWuXJMZkGum8iMn
B0Bbueyp+jQeC8zQE9bG163PJ8jY6FaI+PpD0o5jhPlVAc6wgCFtctpQeY9geXHo
aUz+uulPt7nPzAz9RJE18J51FXvb2Bqe9u8Mscod9Yy9wi0JEs2+orscRFgMYoOM
YxqVksZuaK0RAGMBAAGjgaUwgaIwCQYDVR0TBAlwADALBgNVHQ8EBAMCBLawJwYD
VR0lBCAwHgYIKwYBBQUHAWEGCCsGAQUFBwMCCBggrBgEFBQcDADAPBgNVHREECDAg
hwTAQcG+MB0GA1UdDgQWBBTqpwOicOmdDFXW/YOYVj8/MiED5DAFbgNVHSMEGDAW
gBSvkkKdVY78o6oEYSK9MlWV7JwFDAOBgNVHSAEBzAFMAMGAQAwDQYJKoZIhvcN
AQEFBQADgYEAS+nQ9usbG2QEgPWOWCPRY/PQ/g83Wgeobb0C5LIPCecEbNcWiiUH
+e0J1QdeoUnE3bg9jrvce585pPh3wubOdJXUqROfnik2qsgTdOBstbo+tZdrUdVQ
VF4aX5Dwn4CkkPDc0/ABOwonprfRH9wo3ogFNSPAHXJbCd80rZBm0Bo=
-----END CERTIFICATE-----
```

1.4.3 <http://ns.nehta.gov.au/Qcr/Ref/Http/1.0>

Values of this type MUST conform to the HTTP conventions specified in [RFC2585]. A QR of this type should be in used in preference to the other types.

1.4.3.1 Example

<http://www.healthcare.com.au/pki/clinic234.cer>

1.4.4 <http://ns.nehta.gov.au/Qcr/Ref/Ldap/1.0>

Values of this type MUST conform to [RFC4516]. A QR of this type should be in preference to the *PEM* type.

1.4.4.1 Example

```
ldap://ldap.healthcare.com.au:6666/cn=RP%20gp2%20org%20
:2330726155,ou=
RP%20gp2%20org,o=RP%20gp2%20org,l=TUGGERANONG,st=ACT,c=AU
```

1.4.5 Type Preference

If multiple lookup methods are possible, preference should be given to HTTP based URLs as the HTTP protocol has ubiquitous support in software toolkits, has less network round trips than LDAP, and is better able to operate through firewalls and existing infrastructure.

Order of type preference is:

1. HTTP
2. LDAP
3. PEM

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
CA	Certification Authority
CRL	Certificate Revocation List
HTTP	Hypertext Transport Protocol
LDAP	Lightweight Directory Access Protocol
NASH	National Authentication Service for Health
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
QCR	Qualified Certificate Reference
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name

Glossary

This table lists specialised terminology in alphabetical order.

Term	Description
Identifier	A value used to refer to an entity. The identifier only has meaning within the scope of the type of identifier that was issued.
Qualified Certificate Reference	A tuple consisting of <i>type</i> , a qualified identifier, and <i>value</i> , the contents of which depend on <i>type</i> .
Qualified Identifier	A globally unique identifier that is made up of a qualifier and an identifier.

Appendix A: QCR Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:tns=
    "http://ns.nehta.gov.au/CoreConnectivity/Xsd/QualifiedCertRef/1.1"
  targetNamespace=
    "http://ns.nehta.gov.au/CoreConnectivity/Xsd/QualifiedCertRef/1.1"
  elementFormDefault="qualified">
  <xsd:element name="qualifiedCertRef" type="tns:QualifiedCertRef"/>
  <xsd:complexType name="QualifiedCertRef">
    <xsd:sequence>
      <xsd:element name="type"
        type="xsd:anyURI" minOccurs="1" maxOccurs="1"/>
      <xsd:element name="value"
        type="xsd:string" minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

References

Normative references

The following referenced documents are required for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- [RFC2119] IETF, *RFC 2119: Keywords for use in RFCs to Indicate Requirement Levels*, S. Bradner, March 1997, <http://ietf.org/rfc/rfc2119.txt>
- [RFC2396] IETF, *RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax*, T. Berners-Lee, R. Fielding, U. C. Irvine, L. Masinter, August 1998, <http://ietf.org/rfc/rfc2396.txt>
- [RFC4516] Smith, M et al, *Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator*, RFC 4516, June 2006 <http://www.ietf.org/rfc/rfc4516.txt>
- [RFC2585] Housley, R et al, *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*, RFC 2585, May 1999 <http://www.ietf.org/rfc/rfc2585.txt>