nehta

Qualified Certificate Reference

Version 1.2 — 5 March 2010

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.

Document Information

Change History

Version	Date	Comments
1.1	2009-06-30	Release
1.2	2010-03-05	Revised with new namespaces

Table of Contents

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.
- Testers:
  - To evaluate whether an implementation conforms to qualified certificate references.

The reader is expected to understand URI and URLs.

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 IETF's RFC 2119 [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

1.3.1 Schema

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.

1.3.2 Type element

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

- `http://ns.electronichealth.net.au/qcr/type/pem/2010`
- `http://ns.electronichealth.net.au/qcr/type/http/2010`
- `http://ns.electronichealth.net.au/qcr/type/ldap/2010`

1.3.3 Value element

Contents of element *value* depend on what is specified by element *type*. The section below describes the formats for each allowed type.

1.4 Values

1.4.1 http://ns.electronichealth.net.au/qcr/type/pem/2010

PEM allows for direct access to a certificate for cases where the certificate is not stored in a directory or the directory information is not known. Because the certificate value consumes more space than a reference, *HTTP* and *LDAP* types should be used in preference to *PEM*.

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.

1.4.1.1 Example

```
-----BEGIN CERTIFICATE-----
MIIDVTCCAr6gAwIBAgIBCjANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQGEwJBVTEM
MAoGA1UECBMDUWxkMQ4wDAYDVQQKEwVOZUhUQTEZMBcGA1UECxMQU2VjdXJlIE1l
c3NhZ2luZzEPMA0GA1UEAxMGU01JIENBMB4XDTA5MDQyMjIzMjQ0NVoXDTEyMDQy
MTIzMjQ0NVowXjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA1FsZDEOMAwGA1UEChMF
TkVIVEExGTAXBgNVBAsTEFNlY3VyZSBNZXNzYWdpbmcxFjAUBgNVBAMTDTE5Mi4x
NjguNDAuNjIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDECaomq5Mk
ujd4yPARNvbiJXwiVni9KlSQSRlTOJIXIamkzA3DndPP+hOXs4fRWNeqXp/mA5F8
Ra/4bvbqnBGdv3fRgQmnJfImfPIMMIM8KtoYu0T0Q/WuwK4FzuUT91bCgV+hUc5z
yaMHr/oBSSLM+ry9UbRUEsDNi2hgh8MyLQ+YkAU2nhRGZ6CyeWWuXJMZkGum8iMn
B0Bbueyp+jQeC8zQE9bG163PJ8jY6FaI+PpD0o5jhPlVAc6wgCFtctpQeY9geXHo
aUz+uulPt7nPzAz9RJEl8J51FXvb2Bqe9u8Mscod9Yy9wi0JEs2+orscRFgMYoOM
YxqVksZuaK0RAgMBAAGjgaUwgaIwCQYDVR0TBAIwADALBgNVHQ8EBAMCBLAwJwYD
VR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMCBggrBgEFBQcDADAPBgNVHREECDAG
hwTAqCg+MB0GA1UdDgQWBBTqpWOiCOmddFXW/YOYVj8/MiED5DAfBgNVHSMEGDAW
gBSvvkKkdVy78o6oEYSK9MlWV7JwFDAOBgNVHSAEBzAFMAMGAQAwDQYJKoZIhvcN
AQEFBQADgYEAS+nQ9usbG2QEgPWOWCPRY/PQ/g83Wgeobb0C5LIPCecEbNcWiiUH
+e0J1QdeoUnE3bg9jrvce585pPh3wubOdJXUqROfnik2qsgTdOBstbO+tZdrUdVQ
VF4aX5Dwn4CkkPDc0/ABOwonprfRH9wo3ogFNSPAHXJbCd80rZBm0Bo=
-----END CERTIFICATE-----
```

1.4.2 http://ns.electronichealth.net.au/qcr/type/http/2010

Values of this type should conform to the appropriate rules defined by [NCRS2009], i.e. the HTTP conventions of RFC 2585.

QCRs of this type should be used in preference to the PEM and the LDAP type.

1.4.2.1 Example

```
http://www.example.com/pki/clinic234.cer
```

1.4.3 http://ns.electronichealth.net.au/qcr/type/ldap/2010

Values of this type should conform to the appropriate rules defined by [NCRS2009], i.e. RFC 2416.

QCRs of this type should be in preference to the *PEM* type.

1.4.3.1 Example

```
ldap://ldap.example.com:6666/
cn=ExampleOrg :2330726155,ou=ExampleUnit,o=ExampleOrg,c=AU
```

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

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

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 identifier	A globally unique identifier that is made up of a qualifier and an identifier.
Qualified Certificate Reference	A tuple consisting of *type*, a qualified identifier, and *value*. The contents of the *value* depends on the *type*.

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.electronichealth.net.au/qcr/xsd/QualifiedCertRef/2010"
 targetNamespace=
  "http://ns.electronichealth.net.au/qcr/xsd/QualifiedCertRef/2010"
 elementFormDefault="qualified">

  <xsd:element name="qualifiedCertRef" type="tns:QualifiedCertRefType"/>

  <xsd:complexType name="QualifiedCertRefType">
    <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 indispensable 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

[NCRS2009] NEHTA, *NASH Certificate Reference Specification v1.0*, 30 April, 2009.