National Authentication Service for Health Public Key Infrastructure Certificates

Software Vendor Implementation Guide

August 2013

<table>
<thead>
<tr>
<th>The Healthcare Identifiers Service</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Author</td>
<td>National Authentication Service for Health (NASH), Australian Government Department of Human Services</td>
</tr>
<tr>
<td>Document Date</td>
<td>AUGUST 2013</td>
</tr>
<tr>
<td>Document Version</td>
<td>V2.0</td>
</tr>
<tr>
<td>Release</td>
<td>August 2013</td>
</tr>
</tbody>
</table>
Notice

This guide is for information only. Implementation of National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificates is the responsibility of software vendors. The Australian Government Department of Human Services (Human Services) doesn’t guarantee that this guide will ensure successful implementation of NASH PKI certificates with your system.

This guide is provided to help software vendors for the purposes specified in section 1.1. Using this guide for any other purpose is unauthorised. It should not be circulated to unrelated entities or persons for an unauthorised purpose.

Intellectual property rights of this document belong to the Australian Government.
# Table of Contents

1  **Introduction** .................................................................................................................................................. 6
   1.1  Document purpose ......................................................................................................................................... 6
   1.2  Intended audience .......................................................................................................................................... 6
   1.3  Feedback ....................................................................................................................................................... 6
   1.4  Scope ........................................................................................................................................................... 7
   1.5  Acronyms and abbreviations .......................................................................................................................... 7
   1.6  Links and References ...................................................................................................................................... 7
   1.7  Legislative, Privacy & Policy Requirements .................................................................................................. 8
   1.8  Assumptions ................................................................................................................................................ 8

2  **NASH releases** ............................................................................................................................................... 9
   2.1  Overview ........................................................................................................................................................ 9
       2.1.1  June 2012 release .................................................................................................................................... 9
       2.1.2  December 2012 release .......................................................................................................................... 9
       2.1.3  February 2013 release ........................................................................................................................... 9
       2.1.4  April 2013 release .................................................................................................................................... 10
       2.1.5  August 2013 release ................................................................................................................................ 10

3  **NASH PKI certificates** .................................................................................................................................. 11
   3.1  **NASH PKI Certificate for Individual Healthcare Providers** .................................................................. 11
       3.1.1  Applying for a NASH PKI Certificate for Individual Healthcare Providers ............................................ 11
       3.1.2  Form Factor .......................................................................................................................................... 11
       3.1.3  Policy .................................................................................................................................................... 12
       3.1.4  Finding the HPI-I number in the certificate ............................................................................................. 12
       3.1.5  Usage ................................................................................................................................................... 13
   3.2  **NASH PKI Certificate for Healthcare Provider Organisations** ................................................................. 13
       3.2.1  Applying for a NASH PKI Certificate for Healthcare Provider Organisations ..................................... 13
       3.2.2  Form factor .......................................................................................................................................... 14
       3.2.3  Policy .................................................................................................................................................... 14
       3.2.4  Finding the HPI-O number in the certificate ............................................................................................. 14
       3.2.5  Usage ................................................................................................................................................... 14
   3.3  **NASH PKI Certificate for Supporting Organisations** ............................................................................. 15
       3.3.1  Availability .......................................................................................................................................... 15
       3.3.2  Form factor .......................................................................................................................................... 15
       3.3.3  Policy .................................................................................................................................................... 15
       3.3.4  Finding the CSP registration number in the certificate .............................................................................. 16
       3.3.5  Usage ................................................................................................................................................... 16

4  **Human Services eHealth record PKI certificates (historical information)** .................................................. 17
   4.1  **Department of Human Services eHealth Record Individual PKI Certificate** ......................................... 17
       4.1.1  Form factor .......................................................................................................................................... 17
       4.1.2  Policy .................................................................................................................................................... 18
       4.1.3  Finding the HPI-I number in the certificate ............................................................................................. 18
       4.1.4  Usage ................................................................................................................................................... 19
   4.2  **Department of Human Services eHealth Record Organisation PKI Certificate** ..................................... 19
       4.2.1  Form factor .......................................................................................................................................... 19
       4.2.2  Policy .................................................................................................................................................... 19
       4.2.3  Finding the HPI-O number in the certificate ............................................................................................. 20
       4.2.4  Usage ................................................................................................................................................... 20

5  **NASH Directory** ............................................................................................................................................ 21
   5.1  Access to the NASH Directory ...................................................................................................................... 21
5.2 Certificate Revocation List and Online Certificate Status Protocol..............22
5.3 LDAP Access Path...........................................................................................................22
5.3.1 Test Environment......................................................................................................22
5.3.2 Production Environment..........................................................................................22
6 NASH PKI test kit..............................................................................................................23
6.1 Certificates in the NASH PKI test kit..........................................................................23
6.2 Applying for a test NASH PKI Certificate for Individual Healthcare Providers........24
6.3 Installing test certificates...............................................................................................24
7 Operational requirements..................................................................................................25
7.1 Operating system compatibility....................................................................................25
7.1.1 Microsoft Windows....................................................................................................25
7.1.2 Mac operating systems.............................................................................................25
7.1.3 Hardware requirements............................................................................................25
7.2 Personal Identification Code (PIC)...............................................................................25
7.2.1 Test certificates.........................................................................................................26
7.2.2 Production certificates...............................................................................................26
7.3 Personal Identification Code Unlock Key (PUK)..........................................................26
7.3.1 Test certificates.........................................................................................................26
7.3.2 Production certificates...............................................................................................26
7.4 Renewing certificates.....................................................................................................26
7.4.1 Test certificates.........................................................................................................26
7.4.2 Production certificates...............................................................................................26
7.5 Revoking certificates.....................................................................................................27
7.5.1 Test certificates.........................................................................................................27
7.5.2 Production certificates...............................................................................................27
8 PKI support and contact information................................................................................28
8.1 Contacts and support for test certificates.................................................................28
9 Systems NASH PKI and eHealth record certificates can be used for......................29
9.1 eHealth record system.................................................................................................29
9.2 Secure messaging.........................................................................................................29
9.3 HI Service......................................................................................................................30
9.4 Claims and payments PKI certificates..........................................................................30
9.4.1 Differences between claims and payments PKI certificates and the NASH and eHealth record PKI certificates...........................................................................................................30
10 Attachment A - NASH, Human Services Claims and Payments PKI Certificate Compatibility Matrix.............................................................................................................31
Document History

This document is a living document and represents the information that is current and known at the time of writing. Over time it will be updated as more information becomes available and National Authentication Service for Health (NASH) functionality is extended for use in eHealth systems.

<table>
<thead>
<tr>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 December 2012</td>
<td>Draft Version of Document for Stakeholder Review</td>
</tr>
<tr>
<td>11 December 2012</td>
<td>Version 0.2 incorporates feedback received from stakeholders</td>
</tr>
<tr>
<td>11 January 2013</td>
<td>Version 0.3 incorporates materials for Supporting Organisation Certificates</td>
</tr>
<tr>
<td>14 February 2013</td>
<td>Version 1.0 final draft for distribution.</td>
</tr>
<tr>
<td>7 May 2013</td>
<td>Version 1.1 updated content to reflect the April Release for Supporting Organisations</td>
</tr>
<tr>
<td>21 June 2013</td>
<td>Version 1.2 updated content to reflect the transition of the DHS eHealth Record Individual PKI Certificate in to NASH PKI Certificate for Individual Healthcare Provider</td>
</tr>
<tr>
<td>2 July 2013</td>
<td>Version 1.3 update after review</td>
</tr>
<tr>
<td>12 August 2013</td>
<td>Update following review by stakeholders</td>
</tr>
</tbody>
</table>
1 Introduction

The National Authentication Service for Health (NASH) allows healthcare providers and supporting organisations to securely communicate and exchange electronic health (eHealth) information.

NASH Public Key Infrastructure (PKI) certificates are used to access the eHealth record system, provide confidence in the integrity of information transmitted and facilitate the secure exchange of eHealth information with other healthcare providers.

1.1 Document purpose

The purpose of this document is to provide information about NASH PKI certificates to software vendors or software development teams that work in healthcare provider organisations.

This document also describes how and when to use NASH PKI certificates, and what to do to get help in order to obtain assistance with any NASH PKI certificate related issues.

It will not explain how certificates are installed onto software vendors’ systems. For more information on installing certificates go to:

- www.microsoft.com for Microsoft Windows operating systems, and
- www.apple.com for Mac OS X operating systems.

This document will be reviewed and updated over time in coordination with software vendor associations, Human Services, Department of Health and Ageing and the National E-Health Transition Authority (NEHTA) to ensure it meets the objective of providing valuable information about NASH PKI certificates.

1.2 Intended audience

The primary audience for this document is the third party software vendors and product managers and planners from healthcare organisations who will have the capability to develop software products that use PKI certificates in eHealth.

The audience includes, but is not limited to:

- software vendors;
- IT managers;
- IT architects and system designers;
- business analysts; and
- system integrators.

1.3 Feedback

Any feedback relating to the content in this document should be emailed to NASH.Business.Team@humanservices.gov.au
1.4 **Scope**

The aim of this document is to inform the audience:

- of changes to NASH and eHealth record PKI certificate policies and usage;
- about the purpose and use of the NASH Directory;
- how to apply for a NASH PKI test kit;
- what is contained in a certificate package and NASH PKI test kit;
- of system requirements for using the NASH PKI test kit; and
- about the related systems using NASH and eHealth record PKI certificates.

This document does not detail the technical aspects of how to use NASH or eHealth record PKI certificates in health related systems or solutions.

1.5 **Acronyms and abbreviations**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEST</td>
<td>Australian Eastern Standard Time</td>
</tr>
<tr>
<td>AHPRA</td>
<td>Australian Health Practitioner Regulation Agency</td>
</tr>
<tr>
<td>CCA</td>
<td>Compliance Conformance and Accreditation</td>
</tr>
<tr>
<td>CDA</td>
<td>Clinical Document Architecture</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>Human Services</td>
<td>Australian Government Department of Human Services</td>
</tr>
<tr>
<td>HPI-I</td>
<td>Healthcare Provider Identifier – Individual</td>
</tr>
<tr>
<td>HPI-O</td>
<td>Healthcare Provider Identifier – Organisation</td>
</tr>
<tr>
<td>HI</td>
<td>Healthcare Identifiers</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>NASH</td>
<td>National Authentication Service for Health</td>
</tr>
<tr>
<td>NEHTA</td>
<td>National E-Health Transition Authority</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>OTS</td>
<td>Online Technical Support</td>
</tr>
<tr>
<td>PIC</td>
<td>Personal Identification Code</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PUK</td>
<td>Personal Identification Code Unlock Key</td>
</tr>
<tr>
<td>SASL</td>
<td>Simple Authentication and Security Layer</td>
</tr>
</tbody>
</table>
1.6 Links and References

Further information regarding:

- NASH PKI certificates can be found at humanservices.gov.au/nash;
- secure messaging, including links to the Standards Australia Standards, can be found at nehta.gov.au/connecting-australia/secure-messaging;
- Healthcare Identifiers (HI) Service (and use of healthcare identifiers) can be found at humanservices.gov.au/hiservice;
- healthcare identifiers can be found at health.gov.au/ehealth;
- the NASH Directory can be found at certificates-australia.com.au;
- information on the National e-Authentication Framework can be found at finance.gov.au/e-government/security-and-authentication/authentication-framework.html; and
- healthcare identifiers and eHealth record legislation can be found at comlaw.gov.au.

1.7 Legislative, Privacy & Policy Requirements

The NASH PKI certificates contain embedded healthcare identifiers. The use and disclosure of healthcare identifiers is regulated by the Healthcare Identifiers Act 2010. It is important that your organisation ensures that certificates are always used for the purpose related to the provision of healthcare.

Information on the contents of specific certificate policies can be obtained at humanservices.gov.au/pki > PKI Policy documents

1.8 Assumptions

It is assumed that software vendors have the technical capability to install certificates onto their systems. A detailed step by step guide on the installation of certificates is therefore not provided in this document.

Further information on the installation of certificates can be found at:

- www.microsoft.com for Microsoft Windows operating systems; and
- www.apple.com for Mac OS X operating systems.
2 NASH releases

2.1 Overview

Human Services have and will continue to implement NASH services for the health sector. NASH releases implemented to date are described below:

2.1.1 June 2012 release

In June 2012, Department of Human Services eHealth Record Individual and Organisation PKI Certificates were released to support the launch of the eHealth record system. Test certificates were available to vendors in June, and production certificates were available from 1 July 2012.

The eHealth record PKI certificates are modified Human Services PKI certificates leveraged from the existing Human Services issued PKI solution which is Gatekeeper Accredited. The subject fields on these certificates are based on the NASH certificate profiles to minimise impacts to eHealth record software vendors.

2.1.2 December 2012 release

In December 2012, changes were made to the Department of Human Services eHealth Record Organisation PKI certificate policy. The policy changed to allow NASH PKI certificates to be used for secure messaging, and the certificate name also changed to NASH PKI Certificate for Healthcare Provider Organisations.

The policy changes came into effect from 17 December 2012 and applied to all existing Department of Human Services eHealth Record Organisation PKI Certificates that were already issued to healthcare provider organisations.

Healthcare provider organisations with existing Department of Human Services eHealth Record Organisation PKI Certificates were notified of these changes in writing.

In December the secure NASH Directory was also created. The NASH Directory is hosted by Verizon and lists healthcare provider organisations and supporting organisations that have an active NASH PKI certificate, and helps healthcare providers communicate securely.

Healthcare providers’ access to the secure NASH Directory is authenticated by using:

- a Department of Human Services eHealth Record Individual PKI Certificate (from August 2013 this will be called a NASH PKI Certificate for Individual Healthcare Providers)
- a Department of Human Services eHealth Record Organisation PKI Certificate, or
- a NASH PKI Certificate for Healthcare Provider Organisations.

2.1.3 February 2013 release

In February 2013, NASH PKI Certificates for Supporting Organisations were made available to supporting organisations which are defined as supporting the delivery of healthcare, but are not themselves healthcare provider organisations. At present these are organisations that function as secure messaging intermediaries who need to assert their identity when forwarding secure messages.
In order to become a secure messaging intermediary you will need to register as a contracted service provider (CSP) in the HI Service, receive a CSP identifier and be linked to at least one healthcare provider organisation.

Test certificates were made available for vendors in December 2013 and production certificates were made available in February 2013.

### 2.1.4 April 2013 release

In April 2013, the supporting organisation policy was updated to include general supporting organisations (GSOs) in the definition of supporting organisations. For a complete definition refer to the NASH PKI Certificate for Supporting Organisations certificate policy.

### 2.1.5 August 2013 release

In August 2013, changes were made to the Department of Human Services eHealth Record Individual PKI certificate policy. The certificate name changed to *NASH PKI Certificate for Individual Healthcare Providers* and these certificates expire two years from their issuance date.
3 NASH PKI certificates

3.1 NASH PKI Certificate for Individual Healthcare Providers

The Department of Human Services eHealth Record Individual PKI Certificate was no longer issued from August 2013. Individual certificates issued after August 2013 are known as the NASH PKI Certificate for Individual Healthcare Providers.

3.1.1 Applying for a NASH PKI Certificate for Individual Healthcare Providers

The NASH PKI Certificate for Individual Healthcare Providers is available to all active individual healthcare providers registered with the HI Service. When an individual healthcare provider registers with the HI Service, they are allocated a Healthcare Provider Identifier – Individual (HPI–I) number. Healthcare providers can apply for a NASH PKI certificate by completing the Application to Request a National Authentication Service for Health PKI Certificate for Individual Healthcare Providers. The form is available on the Human Services website. Providers need to fax the form to the number on the form.

If a healthcare provider doesn’t know their HPI–I number, they can call the Australian Health Practitioner Regulation Agency (AHPRA), or Human Services on 1300 361 457.

3.1.2 Form Factor

The NASH PKI Certificate for Individual Healthcare Providers is sent on a smartcard, with a smartcard reader, or a USB token.
The USB token has a key tag labelled ‘NASH PKI Record’ (not shown below).

3.1.3 Policy


Minor changes have been made to the policy since it was introduced on 1 July 2012. This certificate is valid for two years from the date it’s issued.

For the complete certificate policy go to humanservices.gov.au/nash

3.1.4 Finding the HPI-I number in the certificate

You can find the HPI–I number in the subject field in the:

- Domain Component (DC) subfield, or
- Common Name (CN) subfield.
3.1.5 Usage

The *NASH PKI Certificate for Individual Healthcare Provider* can be used to access the:

- eHealth record system through the eHealth Record Provider Portal; and
- NASH Directory.

3.2 NASH PKI Certificate for Healthcare Provider Organisations

The *Department of Human Services eHealth Record Organisation PKI Certificate* was no longer issued from 17 December 2012. Organisation certificates issued after 17 December 2012 are called the *NASH PKI Certificate for Healthcare Provider Organisations*.

3.2.1 Applying for a NASH PKI Certificate for Healthcare Provider Organisations

The *NASH PKI Certificate for Healthcare Provider Organisations* is available to all active healthcare provider organisations registered with the HI Service. When a healthcare provider organisation registers with the HI Service, they are allocated a Healthcare Provider Identifier – Organisation (HPI–O) number.

Healthcare organisations can apply for a certificate by completing the *Application to Request a National Authentication Service for Health Public Key Infrastructure Certificate for Healthcare Provider Organisations*. The form is available on the Human Services website. The form needs to be faxed to the number on the form.

If organisations don’t know their HPI–O number, they can call Human Services on 1300 361 457.
3.2.2 Form factor

The NASH PKI Certificate for Healthcare Provider Organisations is sent on a CD and has the title ‘NASH’ on the front.

![CD Image]

3.2.3 Policy


This certificate is valid for two years from the date it’s issued.

For the complete certificate policy go to humanservices.gov.au/nash

3.2.4 Finding the HPI-O number in the certificate

You can find the HPI–O number in the subject field in the:

- Common Name (CN) subfield; or
- Domain Component (DC) subfield.

Note: The Subject Alternative Name field shouldn’t be used because this field won’t be included on future certificates.

3.2.5 Usage

The NASH PKI Certificate for Healthcare Provider Organisations is used to:

- access patient eHealth records in the eHealth record system;
- sign and encrypt electronic communications between healthcare provider organisations, or between healthcare provider organisations and supporting organisations; and
- access the NASH Directory.
3.3 NASH PKI Certificate for Supporting Organisations

3.3.1 Availability

Supporting Organisations help healthcare providers to access, send and receive health information. The NASH PKI Certificate for Supporting Organisations can be issued to organisations that are registered in the HI Service as either a CSP or a GSO. For a complete definition of a CSP and GSO refer to the NASH PKI Certificate for Supporting Organisations certificate policy.

Information about how to apply for a NASH PKI Certificate for Supporting Organisations is available on the Human Services website.

Supporting organisations will also be required to abide by a Relying Party Agreement.

3.3.2 Form factor

The NASH PKI Certificate for Supporting Organisations is sent on a CD and has the title ‘NASH’ on the front.

3.3.3 Policy

The current certificate policy for the NASH PKI Certificate for Supporting Organisations is the Commonwealth Department of Human Services Community of Interest Certificate Policy for the National Authentication Service for Health PKI Certificate for Supporting Organisations.
Further information on the *NASH PKI Certificate for Supporting Organisations* can be found at humanservices.gov.au/nash

### 3.3.4 Finding the CSP registration number in the certificate

You can find the registration number in the subject field in the:

- Common Name (CN) subfield; or
- Domain Component (DC) subfield.

### 3.3.5 Usage

The *NASH PKI Certificate for Supporting Organisations* is used to:

- sign and encrypt electronic communications between supporting organisations, or between healthcare organisations and supporting organisations; and
- access the NASH Directory.
4 Human Services eHealth record PKI certificates (historical information)

The Department of Human Services eHealth Record Organisation PKI Certificate was no longer issued from 17 December 2012.

The Department of Human Services eHealth Record Individual PKI Certificate was no longer issued from August 2013.

All new certificates issued to healthcare providers are called NASH PKI certificates. Although these certificates are no longer issued, the certificates were valid for one year from the date of issue. Existing Human Services eHealth record PKI certificates will be replaced by a NASH PKI certificate upon renewal.

4.1 Department of Human Services eHealth Record Individual PKI Certificate

4.1.1 Form factor

The Department of Human Services eHealth Record Individual PKI Certificate was sent on a smartcard, with a smartcard reader, or a USB token.
The USB token has a key tag labelled ‘eHealth record’ (not shown below).

4.1.2 Policy

The policy for the Department of Human Services eHealth Record Individual PKI Certificate was the Commonwealth Department of Human Services Community of Interest Certificate Policy for eHealth Record Individual PKI Certificates.

This certificate was valid for one year from the date it was issued.

For the complete certificate policy go to humanservices.gov.au/pki>PKI Policy documents

4.1.3 Finding the HPI-I number in the certificate

The identifier can be obtained from either of the following locations in the Subject field:

- Common Name (CN) subfield; or
- Domain Component (DC) subfield.
4.1.4 Usage

The Department of Human Services eHealth Record Individual PKI Certificate can be used to access the:

- eHealth record system via the eHealth Record Provider Portal; and
- NASH Directory.

4.2 Department of Human Services eHealth Record Organisation PKI Certificate

4.2.1 Form factor

The Department of Human Services eHealth Record Organisation PKI Certificate was sent on a CD and has the title ‘eHealth record’ on the front.

4.2.2 Policy

The policy for the Department of Human Services eHealth Record Organisation PKI Certificate was the Commonwealth Department of Human Services Community of Interest Certificate Policy for eHealth Record Organisation PKI Certificates.

This certificate was valid for one year from the date it was issued.
For the complete certificate policy go to humanservices.gov.au/pki > PKI Policy

4.2.3 Finding the HPI-O number in the certificate

You can find the HPI–O number in the subject field in the:

- Common Name (CN) subfield; or
- Domain Component (DC) subfield.

**Note:** The Subject Alternative Name field shouldn’t be used because this field won’t be included on future certificates.

4.2.4 Usage

The *Department of Human Services eHealth Record Organisation PKI Certificate* is used to:

- access patient eHealth records in the eHealth record system;
- sign and encrypt electronic communications between healthcare provider organisations, or between healthcare provider organisations and supporting organisations; and
- access the NASH Directory.
5 NASH Directory

The NASH Directory is a secure directory which lists active NASH PKI certificates for healthcare provider organisations and supporting organisations. The NASH Directory can be searched on key words to find an entity's Public Key Certificate.

The following picture shows the Verizon business web site that hosts the NASH Directory.

![Verizon Business Website](image)

5.1 Access to the NASH Directory

The NASH Directory is a secure directory that implements client authentication using a NASH PKI certificate.


It is recommended to connect to LDAP then use START TLS sub-command to perform mutual authentication using Simple Authentication and Security Layer (SASL) rather than LDAP Secure (LDAPS).

The following root certificates and Certificate Revocation Lists (CRLs) can be found on the side bar under Medicare Australia PKI as shown in the figure above:

- Medicare Australia Root Certification Authority (CA) certificate;
- Medicare Australia Root CA CRL;
- Medicare Australia Organisation Certification Authority (OCA) certificate; and
- Medicare Australia OCA CRL.
There are two MA OCA certificates in operation. Software vendors would require both OCA certificates.

5.2 Certificate Revocation List and Online Certificate Status Protocol

The Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP) are mechanisms in the NASH Directory that are available to check the status of a certificate. The CRL is publicly available and does not require a certificate to access it.

The CRL is refreshed every 50 minutes and is valid for two hours. The OCSP is available in the production and test environments.

5.3 LDAP Access Path

5.3.1 Test Environment

The access details for the Test environment are:

- NASH Directory (Test)
  Domain Name: nashtest.certificates-australia.com.au
  Port: 389 for TLS and 636 for LDAPS

- Healthcare Public Directory (Test)
  IP Address: 203.2.208.10
  Port: 389

The test Medicare Australia Organisation Certification Authority certificate and CRL can be found using the Distinguished Name:
DN: cn=Test Medicare Australia Organisation Certification Authority, ou=Medicare Australia, o=GOV

5.3.2 Production Environment

The access details for the production environment are:

- NASH Directory (Production)
  Domain Name: nash-directory.certificates-australia.com.au
  Port: 389 for TLS and 636 for LDAPS

- Healthcare Public Directory (Production)
  IP Address: 203.2.208.36 or 152.91.29.18
  Port: 389

The Medicare Australia Organisation Certification Authority certificate and CRL can be found using the Distinguished Name:
DN: cn=Medicare Australia Organisation Certification Authority, ou=Medicare Australia, o=GOV
6  NASH PKI test kit

Test certificates allow software vendors to authenticate to the test environment for the eHealth record system, and test sending and receiving secure messages.

Test certificates can’t be used in production and cannot be used for the HI Service or any other online program.

When software vendors apply for a test kit, they agree to the terms and conditions of licence. You’re bound by these terms and conditions when using the test kit.

The NASH PKI test kit includes:

- NASH PKI Certificate for Healthcare Provider Organisations;
- NASH PKI Certificate for Individual Healthcare Providers; and/or
- NASH PKI Certificate for Supporting Organisations (on request).

You can get a test kit by contacting the Human Services Online Technical Support (OTS) Liaison Team email at otsliaison@humanservices.gov.au

The following steps detail the application process for a NASH PKI test kit:

1. Request a NASH PKI test kit by emailing OTS Liaison Team with the reason why you need the test kit.
2. The OTS Liaison Team sends through a Licence Agreement, including the Terms and Conditions of Use which need to be signed and send back to the OTS Liaison Team.
3. When the OTS Liaison Team receives the completed and signed Licence Agreement, and Terms and Conditions, they will send the test kit to the requesting software vendor.

Attachment A – NASH, and Human Services Claims and Payments PKI Certificate Compatibility Matrix details systems that can be accessed using the different types of certificates.

6.1  Certificates in the NASH PKI test kit

When you get the NASH PKI test kit, check that it has the following certificates:

- an active test NASH PKI Certificate for Healthcare Provider Organisations for a test organisation;
- an active test NASH PKI Certificate for Healthcare Provider Organisations for a different test organisation;
- a revoked test NASH PKI Certificate for Healthcare Provider Organisations for a test organisation; and
- an active test NASH PKI Certificate for Supporting Organisations for a test organisation (if requested).

Note: Test organisation names will vary from test kit to test kit. Any healthcare identifiers embedded in the certificates are test healthcare identifiers.

Both active test NASH PKI Certificates for Healthcare Provider Organisations can be used to ensure that access is available to the NASH Directory and that secure messaging is operating correctly.
You should use the revoked test NASH PKI Certificate for Healthcare Provider Organisations with the test NASH PKI Certificate for Healthcare Provider Organisations to check that secure messaging can't occur between two organisations when one of the organisations has a revoked certificate.

The revoked test certificate can also be used to confirm that an organisation can't access the NASH Directory when they use a revoked certificate.

The test NASH PKI Certificate for Supporting Organisations can be used to check that secure messaging is operational between intermediary organisations.

It can also be used to check that the NASH Directory can be accessed with a supporting organisation NASH PKI certificate.

Test certificates are valid for two years.

6.2 Applying for a test NASH PKI Certificate for Individual Healthcare Providers

To get a test NASH PKI Certificate for Individual Healthcare Providers, email the Human Services OTS Liaison Team at otsliaison@humanservices.gov.au.

This test certificate is valid for two years.

6.3 Installing test certificates

When the software vendor has received the certificate it can be installed into the software vendor's own development environment. It is assumed that software vendors have the technical capability to install certificates onto their systems.

For any questions, or if you need technical support to install the certificates, call the OTS Liaison Helpdesk on 1300 550 115 (call charges apply. Calls from mobile phones may be charged at a higher rate) Monday to Friday, between 8.30 am and 5.00 pm, Australian Eastern Standard Time (AEST).
7 Operational requirements

7.1 Operating system compatibility

NASH PKI certificates are compatible on machines running the following operating systems:

- Microsoft Windows, and
- Mac OS X operating systems.

Please contact the OTS Helpdesk on 1300 550 115 for information about installing certificates on other operating systems.

7.1.1 Microsoft Windows

The following Microsoft Windows operating system versions are supported for all NASH PKI certificates:

- XP Pro
- Vista 32bit
- Vista 64bit
- Win 7 32bit, and
- Win 7 64bit.

7.1.2 Mac operating systems

The following Mac operating system versions are supported for all NASH PKI certificates:

- OS X 10.4
- OS X 10.5
- OS X 10.6
- OS X 10.7, and
- OS X 10.8.

7.1.3 Hardware requirements

To install a certificate from a smartcard reader or USB token, you need a USB 2.0 port.

To install a certificate from a CD, you need a CD-ROM.

Note: This document doesn’t detail the minimum hardware requirements needed to run vendor software.

7.2 Personal Identification Code (PIC)

A PIC is the secure code needed to access the certificate. The certificate will be locked if the PIC has been incorrectly entered three times.
7.2.1 Test certificates

The test kit will include a PIC for each certificate, and is needed to install the test certificate. If you lose your PIC, you need to contact the OTS Helpdesk on 1300 550 115.

7.2.2 Production certificates

The PIC will be mailed in a separate envelope for all production certificates.

**Important:** When installing organisation certificates, the original CD must be kept in a secure place to help with future installations.

7.3 Personal Identification Code Unlock Key (PUK)

A PUK is needed to unlock your certificate if the PIC has been entered incorrectly three times. The PUK is only used for the NASH PKI Certificate for Individual Healthcare Providers and the Department of Human Services eHealth Record Individual PKI Certificate.

If the PUK is entered incorrectly three times the certificate becomes unusable and you will need to request a replacement certificate.

7.3.1 Test certificates

The test certificate PUK can be provided over the phone to software vendors if they call the OTS Helpdesk on 1300 550 115.

7.3.2 Production certificates

Healthcare providers can get their certificate's PUK over the phone by calling the eBusiness Service Centre on 1800 700 199. Operating Hours: Monday to Friday (excluding public holidays) 8.30 am to 5.00 pm AEST.

7.4 Renewing certificates

NASH PKI certificates have a lifespan of two years from the date they were issued and need to be renewed before this timeframe has lapsed.

7.4.1 Test certificates

Software vendors can renew their test certificates by calling the OTS Helpdesk on 1300 550 115. There is no requirement to complete another form.

7.4.2 Production certificates

The certificate user will be sent a letter close to the certificate expiry date asking them to renew their certificate.

The current process for certificate renewals will apply to renewing NASH PKI certificates.
7.5 Revoking certificates

Certificates that have been lost, compromised or are no longer required can be revoked. Lost certificates can be revoked and then replaced if they are still needed.

7.5.1 Test certificates

Support for revoked certificates is available by calling the OTS Helpdesk on 1300 550 115, Monday to Friday (excluding public holidays) 8.30 am to 5.00 pm AEST.

7.5.2 Production certificates

The Request to Revoke or Reissue a Public Key Infrastructure Certificate form is available at humanservices.gov.au/pki

Revocations are processed during normal business hours from Monday to Friday between 8.30 am and 5.00 pm AEST (excluding public holidays).

For more information about revoked certificates call the eBusiness Service Centre on 1800 700 199, Monday to Friday (excluding public holidays) 8.30 am to 5.00 pm AEST.
8 PKI support and contact information

8.1 Contacts and support for test certificates

Software vendors who need support for test certificates can call the:

- **OTS Liaison team** supports software vendors through answering enquiries, and are responsible for customer relationship management and liaising, administering the NASH PKI test kit for software vendors.
  Call: 1300 550 115 or
  Email: otsliaison@humanservices.gov.au

- **OTS Helpdesk** supports software vendors with diagnosing and resolving technical issues during the development and production stages.
  Call: 1300 550 115 or
  Email: pki@humanservices.gov.au

International callers will need to call direct to +61 2 6124 7386

8.2 Contacts and support for NASH PKI production certificates

NASH PKI production certificate subscribers can contact the eBusiness Service Centre on 1800 700 199 or email pki@humanservices.gov.au.

More information is available at humanservices.gov.au/pki
9 Systems NASH PKI and eHealth record certificates can be used for

The NASH PKI and eHealth record certificates are used for the eHealth record system and for secure messaging.

Access to these systems is governed by the relevant certificate policy. If a certificate is used for a reason that’s not specified in the policy it’s a breach of the conditions of use for that certificate.

9.1 eHealth record system

The eHealth record system is a secure, voluntary, electronic record accessible by the patient, the patient’s authorised representatives, nominated representatives and treating healthcare providers.

It gives healthcare providers access to a patient’s health information, making continuity of care easier and contributing to improved treatment decisions.

Organisations and healthcare providers must be registered in the HI Service before they can participate in the eHealth record system.

Individual healthcare providers can access the eHealth record system through the Provider Portal using the NASH PKI Certificate for Individual Healthcare Providers or Department of Human Services eHealth Record Individual PKI Certificate.

Healthcare organisations can access the eHealth record system if their software is compatible with the eHealth record system by using the NASH PKI Certificate for Healthcare Provider Organisations or Department of Human Services eHealth Record Organisation PKI Certificate.

Software vendors should provide advice on how healthcare providers install the NASH PKI Certificate for Healthcare Provider Organisations and Department of Human Services eHealth Record Organisation PKI Certificate on their systems.

Healthcare providers have an obligation to keep the private key safe. The software vendor needs to make sure their software product doesn’t expose the private key to unauthorised access.

The HPI–O is embedded in the NASH PKI Certificate for Healthcare Provider Organisations and the Department of Human Services eHealth Record Organisation PKI Certificate. It authenticates subscribers in the eHealth record system. Storage, usage and disclosure of healthcare identifiers are governed by the Healthcare Identifier Act 2010.

All documents submitted to the eHealth record system must be sealed using an organisational certificate in accordance with the NEHTA CDA Package Specification v1.0 (vendors.nehta.gov.au/public/fileServer.cfm?activityContentId=129). The certificate may be a NASH PKI Certificate for Healthcare Provider Organisations.

9.2 Secure messaging

To send secure messages, healthcare providers and organisations need a NASH or eHealth record PKI certificate to digitally sign and encrypt messages. These certificates are used in secure messaging for four different purposes:

- digitally signing the payload;
- encrypting the payload;
- TLS client authentication; and
- TLS server authentication and session establishment.

A commercial SSL certificate is to be used for this purpose.

Secure messaging has a range of different requirements for the certificates it uses. The NASH PKI Certificates for Healthcare Provider Organisations will meet the identifying information (HPI-O) requirements from secure messaging.

For more information about standards for secure messaging go to the NEHTA website at nehta.gov.au/connecting-australia/secure-messaging

9.3 HI Service

NASH PKI Certificates cannot be used to access the HI Service through either HPOS or via B2B services

9.4 Claims and payments PKI certificates

9.4.1 Differences between claims and payments PKI certificates and the NASH and eHealth record PKI certificates

NASH PKI certificates currently look the same as existing Human Services claims and payments PKI certificates, apart from the label on the certificate.

Key differences between the two certificates are:

- NASH PKI certificates have a different policy which allows them to be used exclusively for the eHealth record system and secure messaging;
- the subject name of the NASH PKI certificate uses a NASH format that includes the healthcare identifier; and
- NASH PKI Certificate for Individual Healthcare Providers has ‘Utility’ and ‘Content Commitment’ profiles. Utility certificates support both signing and encryption.

NASH PKI certificates share the same software drivers, middleware and utilities with existing Human Services claims and payments PKI certificates and the HI Service. The need to distinguish between different PKI tools will depend on the vendor implementation.
## 10 Attachment A - NASH, Human Services Claims and Payments PKI Certificate Compatibility Matrix

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>eHealth Record System</th>
<th>NASH</th>
<th>HI Service</th>
<th>Secure Messaging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Human Services Individual PKI Certificate</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Department of Human Services Site PKI Certificate</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Department of Human Services PBS Certificate (For Pharmacy)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Department of Human Services HI Individual PKI Certificate (For AHPRA registered HPI-I)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Department of Human Services HI OMO PKI Certificate</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Department of Human Services HI Network Organisation PKI Certificate</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NASH PKI Certificate for Individual Healthcare Provider*</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>NASH PKI Certificate for Healthcare Provider Organisations*</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>NASH PKI Certificate for Supporting Organisations</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
</tbody>
</table>

* Usage also applies to Department of Human Services eHealth Record Organisation PKI Certificate
* Usage also applies for Department of Human Services eHealth Record Individual PKI Certificate