Australian Government
Australian Digital Health Agency

National Authentication Service for Health (NASH) PKI organisation certificate
Developer Guide

3 July 2020 v1.3
Approved for external use
Document ID: DH-3251:2020

Publication date: 3 July 2020

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000 digitalhealth.gov.au
Telephone 1300 901 001 or email help@digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Version History

Version	Date	Changes
1.0	25/03/2019	• Initial release
1.1	14/05/2019	• Minor fixes
1.2	13/05/2020	• Clarified when the NASH requirements apply to software products • Added Table of Contents
1.3	26/06/2020	• Updated OTS Liaison's name to Developer Support and email address to DevSupport@servicesaustralia.gov.au • Department of Human Service changed to Services Australia

Table of Contents

Intended audience

Software providers whose products connect to the HI Service, the My Health Record system or generate and sign CDA documents that must be signed with a NASH certificate.

Purpose and functionality changes

This document is intended to help software providers:

- transition to using a NASH PKI organisation certificate to connect to both the HI Service and the My Health Record system and to support secure messaging;
- enable software to manage both SHA-1 and SHA-2 NASH PKI organisation certificates; and
- assist healthcare provider organisations manage certificates by implementing alerts prior to the expiry of NASH PKI organisation certificates.

This will involve implementing the following functionality:

- enabling connection to both the HI Service and the My Health Record system with a NASH PKI organisation certificate (NASH-1);
- enabling the use of both NASH SHA-1 and SHA-2 organisation certificates (NASH-2); and
- developing system-generated messages to alert users prior to a certificate's expiry within the software product (NASH-3).

Background

National Authentication Service for Health (NASH) PKI organisation certificate

NASH PKI organisation certificates have been used to connect and upload to the My Health Record system and support secure messaging since 2012.

In September 2018 changes were made to the Healthcare Identifiers (HI) Service to allow NASH PKI organisation certificates to be used to connect to the HI Service. All NASH PKI organisation certificates requested and downloaded via the Health Professional Online Services (HPOS) from the 18th of September 2018 can be used to connect to the Healthcare Identifiers (HI) Service and the My Health Record system. Contracted service providers (CSP)/general supporting organisations (GSO) need to request NASH PKI organisation certificates via a paper form.

Software providers currently using Medicare PKI site certificates to connect the HI Service can update their products or provide patches that will enable the use of a NASH PKI organisation certificate to connect the HI Service.

NOTE: Services Australia has advised Medicare PKI site certificates are scheduled to be deprecated and replaced with PRODA Organisation for authentication. For more information, please contact Developer Support at DevSupport@servicesaustralia.gov.au.

Security

To increase security and compliance with the new GateKeeper Framework 3.1, NASH PKI organisation certificates are migrating from the secure hash algorithm SHA-1 to the more secure SHA-2. Both the My Health Record and HI Service software vendor testing (SVT) environments support the SHA-2 NASH PKI organisation certificates and these certificates are now available for testing.

The HI Service and My Health Record test and production environments can support SHA-2 NASH PKI organisation certificates however, production SHA-2 NASH PKI organisation certificates are not yet being issued.

All software providers will need to update their products or provide patches that will enable healthcare providers to connect to the HI Service using both SHA-1 and SHA-2 NASH PKI organisation certificates to ensure a smooth transition.

NOTE: From the 13th March 2022 Services Australia, including the HI Service, will no longer issue or accept SHA-1 NASH PKI organisation certificates.

Continuity of connection

As NASH PKI organisation certificates reach their expiry date, software products should prompt healthcare organisations to install new certificates to ensure a continuity of connection. A clinical safety risk arises when practices are unable to connect to the My Health Record system and cannot remove or amend incorrect information.

Timeframes

All NASH PKI organisation certificates requested and downloaded via the Health Professional Online Services (HPOS) from the 18th of September 2018 can be used to connect to the Healthcare Identifiers (HI) Service and the My Health Record system. Contracted service providers (CSP)/general supporting organisations (GSO) need to follow the existing process, which is to request NASH PKI organisation certificates via a paper form.

Test NASH PKI organisation certificates are available for connection to the HI Service software vendor testing (SVT) and the My Health Record SVT environments.

SHA-1 NASH PKI organisation certificates will continue to be accepted by Services Australia until March 2022.

By March 2022 a SHA-2 NASH organisation certificate must be used to enable a connection to the HI Service and My Health Record and used to support secure messaging.

How to

NASH-1 - Support NASH PKI organisation certificates

This requirement is applicable to software currently connecting to the HI Service and/or the My Health Record system.

- Update your software so that the NASH PKI organisation certificates may be used to connect to the HI Service (currently software selects the Medicare PKI site certificate for authentication when connecting to the HI Service).
- Continue to allow Medicare PKI site certificates to be used by healthcare organisations to connect to the HI Service until they are phased out.
- Test to ensure your software connects to the HI Service and the My Health Record system with the use of a NASH PKI organisation certificate.

NASH-2 - Support SHA-2 NASH PKI organisation certificates

This requirement is applicable to software currently connecting to the HI Service and/or the My Health Record system, as well as software that generates CDA documents (must be signed using a NASH certificate).

- When the SHA-2 Root Certificate Authority (CA) and Organisation Certificate Authority (OCA) Certificates are available, update your software installation process to ensure you are installing both the SHA-1 and SHA-2 Root CA and OCA Certificates as Trusted Root Certificate Authorities.

- Obtain a copy of the test SHA-2 NASH PKI organisation certificates to ensure any rules around the import or use of certificates work as expected. For example, if your software:
    - Validates Certificate Policy IDs; or
    - Extracts the HPI-O number out of the certificate Subject Name - do not use Subject Alternative Name
- Test and futureproof your software to use the both SHA-1 and SHA-2 NASH PKI organisation certificates for both HI Service and My Health Record interactions.

NASH-3 - Ensure users of the software update NASH PKI organisation certificates prior to their expiry date

(not applicable for contracted service providers (CSP) or general supporting organisations (GSO) – see note below)

This requirement is applicable to software currently connecting to the HI Service and/or the My Health Record system, as well as software that generates CDA documents (must be signed using a NASH certificate).

- Develop system-generated messages to alert the users prior to a certificate's expiry within the software product.
- Regular alerts (such as daily) are required from two (2) months until the certificate has been renewed.
- See below for a suggested warning message. Keep in mind this may differ depending on whether certificates are installed by users or the software vendor. You may also want to reference manuals and other help support.

> *'Your NASH PKI organisation certificate will expire in ### days. Please contact your Organisation Maintenance Officer (OMO) or system administrator to download and install a new NASH PKI organisation certificate from the Health Professional Online Services (HPOS) portal.*
>
> *NASH PKI organisation certificates can be downloaded from under the "certificates" tab from within the HPOS portal.'*

NOTE for CSP/GSO: certificate expiry needs to be managed by the CSP organisation to ensure continuity of connection to the HI Service and My Health Record for your clients.

Testing

SHA-1 and SHA-2 NASH PKI organisation certificates

HI Service Notice of Connection (NOC) or Compliance, HI Conformance and Accreditation (CCA) is not required when making the above changes for conformant software providers who already connect to the HI Service. Existing testing requirements may apply for other functionality changes.

A successful HI Service and My Health Record connection request and response is sufficient for connection testing. For secure messaging transactions, software providers should verify successful transactions. For any errors/failures, requests for assistance can be made to hi.ots.helpdesk@servicesaustralia.gov.au.

Managing expiring certificates

Software providers can implement a configuration option to change the certificate expiry period (in days) to test the certificate expiry alert messages. This allows the value to be changed to test activation of the alert messages.

The following code can be used:

```
// Load Certificate
            X509Certificate2 certificate = X509CertificateUtil.GetCertificate(
                "Thumbprint",
                X509FindType.FindByThumbprint,
                StoreName.My,
                StoreLocation.CurrentUser,
                true
                );

            // Test Certificate loaded and if so, check expiry date
            int alertUserIfDaysTillCertificateExpiresIsLessThan = 60;
            if (certificate != null)
            {
                double daysTillExpire = (DateTime.Now -
certificate.NotAfter).TotalDays;
                if (daysTillExpire < alertUserIfDaysTillCertificateExpiresIsLessThan)
                {
                    // Certificate less than 60 days till expires
                    // Raise a warning to the user

                }
            }
            else
            {
                // Warn user no certificate found
            }
```

Connecting to the test environments and obtaining test certificates

Please contact Services Australia, Developer Support at DevSupport@servicesaustralia.gov.au for assistance in connecting your software product with the HI Service vendor environment and the My Health Record software vendor testing (SVT) environment.

To obtain your test certificates please download the NASH test kit and NASH test certificates ordering forms from the site below and return to DevSupport@servicesaustralia.gov.au.

- NASH Test Kit form – https://developer.digitalhealth.gov.au/sites/default/files/application-request-nash-pki-test-certificate.pdf

- NASH Test Certificates order form - https://developer.digitalhealth.gov.au/sites/default/files/test-nash-certificate-order-form.pdf.

For more information

- Please visit https://developer.digitalhealth.gov.au/resources/faqs/national-authentication-service-health-nash-pki-organisation-certificate.
- Please contact help@digitalhealth.gov.au for more information.
- Please contact hi.ots.helpdesk@servicesaustralia.gov.au for technical issues.

Publication date: 3 July 2020

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000 digitalhealth.gov.au
Telephone 1300 901 001 or email help@digitalhealth.gov.au

OFFICIAL