



Australian Government
Australian Digital Health Agency

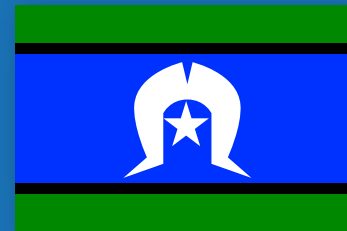
National Authentication Service for Health (NASH) Improvements

Australian Digital Health Agency

7 July 2021



Acknowledgement



The Australian Digital Health Agency acknowledges the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to Elders past, present and emerging.

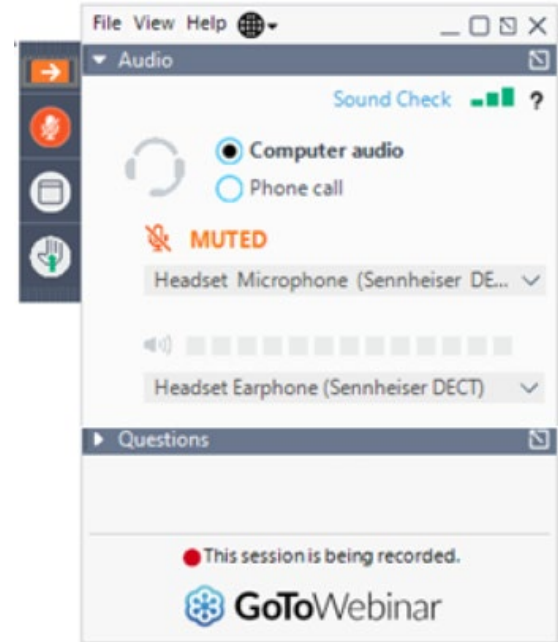


Housekeeping



About GoToWebinar

- Your microphone will be muted throughout the presentation.
- If your screen and sound don't match you may have a poor internet connection.
- This session is being recorded and made available in the Australian Digital Health Agency Developer Centre.



Australian Digital Health Agency Representatives

Facilitator

- **Paul McDonald** – Implementation Support Lead, Partnerships Branch

Presenters

- **Kieron McGuire** – Director, Identity, Authentication & Directory Products
- **Jeffrey Barson** – Senior Business Analyst, Identity, Authentication & Directory Products



Agenda

- Background
- What does this mean for Software Developers?
- How we can support you
- Questions



Background

Kieron McGuire

Director, Identity, Authentication & Directory Products
Architecture, Informatics and Products

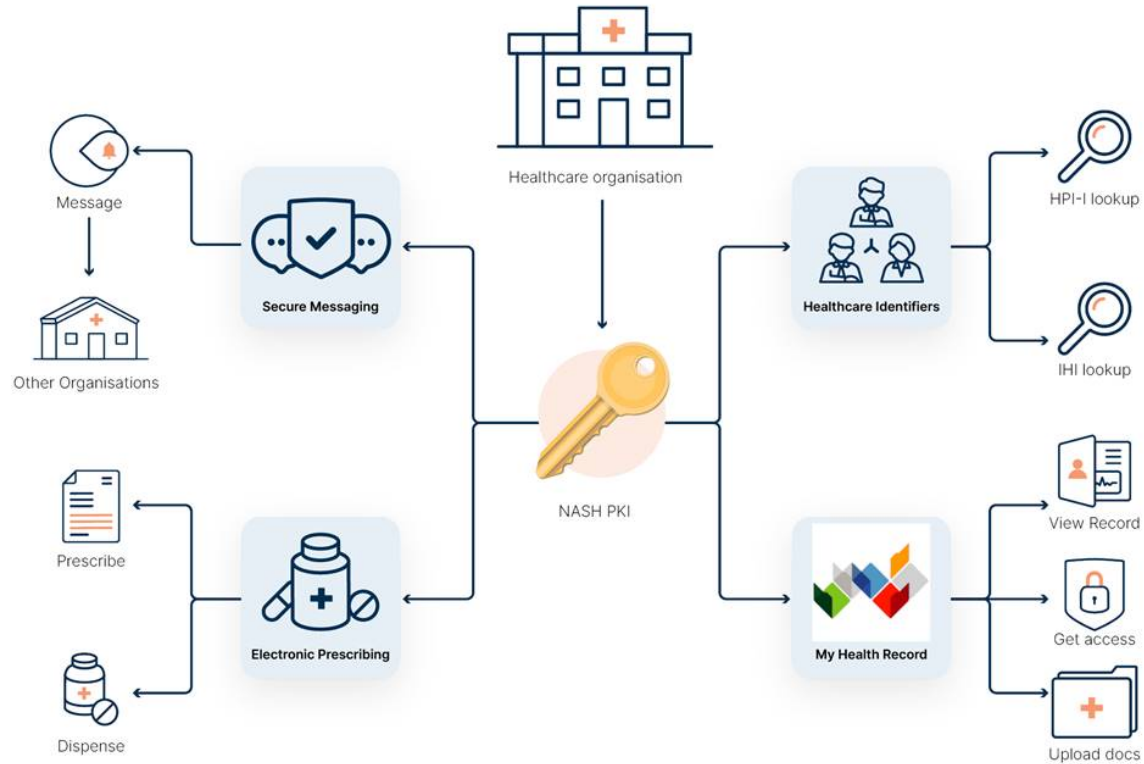
What is NASH?

National Authentication Service for Health (NASH) is a Public Key Infrastructure (PKI) solution introduced in 2012 and is used by healthcare provider organisations and supporting organisations to:

- Authenticate and securely access digital health services
- Digitally sign documents and other transactions
- Encrypt health information for secure exchange



Where is NASH used?



Chain of Trust

- NASH PKI Certificates are issued through a chain of trust operated by Services Australia.
- Digital health systems must have this chain of trust installed so that they can validate NASH PKI certificates.
- Services Australia's Chain of trust (CoT) is made up of:
 1. Medicare Australia Root Certification Authority (RCA) Certificate
 2. Medicare Australia Organisation Certification Authority (OCA) Certificate
- So CoT = RCA+OCA.



What is changing?

- NASH PKI certificates are currently signed by the Services Australia OCA using a SHA-1 hash.
- All NASH PKI certificates issued from March 2022 will be signed with a SHA-2 hash.
- SHA-2 PKI certificates will be issued through a new Services Australia SHA-2 chain of trust – which must be installed by healthcare provider organisations.
- Medicare PKI site certificates will no longer be issued from 13 March 2022. All digital health systems must be using NASH PKI prior to this.



SHA-2 Timeline

✓ October 2018	HI Service commenced accepting NASH PKI certificates in preparation for decommissioning of Medicare PKI
	Commenced online issuance of NASH PKI certificates (instead of CD)
✓ April 2019	Advised software industry of requirement to complete transition to SHA-2 by March 2022
	Services Australia NASH SHA-2 Certificates available in the SVT Test environment
✓ Apr 2021	Advised software industry to include SHA-1 OCA (2026) and SHA-2 chain of trust in product updates in preparation for transition to SHA-2
✓ 16 May 2021	Services Australia issued new SHA-1 OCA (2026) certificate with expiry in 2026 (NASH certificates issued from 16 May 2021 carry a 2 year expiry from date of issue).
September 2021	Commence issuing SHA-2 NASH certificates subject to site readiness.
14 March 2022	SHA-1 NASH certificates will no longer be issued and all organisations must have updated to SHA-2 compatible software. Existing SHA-1 NASH certificates will remain valid until expiry.
Future roadmap	NASH Simplified renewal



SHA-2 Transition Key Points

SHA-2 certificates can be issued from September 2021 subject to site readiness.

Sep. 2021

All certificates issued from 14 March 2022 must be SHA-2.

14 Mar. 2022

All sites must have updated to SHA-2 compatible software prior to 14 March 2022.

14 Mar. 2022



SHA-1 Renewal

- Services Australia SHA-1 OCA certificate was expiring 13 March 2022.
- Consequently, we have 10,000+ NASH PKI Certificates expiring 13 March 2022.
- 16 May 2021 - Expiry was updated to 2026 to provide continuity through the transition.
- NASH SHA-1 PKI certificates issued since have a 2 year expiry.



SHA-1 OCA (2026)

- Since 2018 COT is not included in NASH Organisation Certificate file.
- Since new SHA-1 OCA (2026) went live 16 May 2021, sites must install this OCA when installing their renewed NASH certificate.
- This SHA-1 OCA (2026) must be presented in the TLS handshake when connecting to the My Health Record system with a NASH certificate issued after 16 May 2021.

Please contact myhealthrecord.otshelpdesk@servicesaustralia.gov.au if your sites are still encountering issues.



What does this mean for Software Developers?

Jeffrey Barson

Senior Business Analyst
Identity, Authentication & Directory Products

What does this mean for Software Developers?

- (If required) Update your software to:
 - If connecting to the HI Service, use NASH to connect to the HI Service
 - Become compatible for NASH SHA-2
 - Provide a Certificate expiry warning for customers
 - If your deployment approach can include the SHA-1 2026 OCA and the SHA-2 COT, consider doing this.
- Test your software for using both NASH SHA-1 2026 and NASH SHA-2 certificates (simple tests to follow).
- Notify the Australian Digital Health Agency about your software readiness. We need this verification before your sites can request a NASH SHA-2 certificate in HPOS.



How we can support you

Paul McDonald

Implementation Support Lead
Partnerships

The TrustChainChecker

The TrustChainChecker is sample code that software developers can use to support their users in verifying that they have got the correct OCA & RA Certificates installed in their windows key store. It will also show if any NASH & Medicare PKI Certificates are installed with that chain of trust.

[Link to the code:](#)

<https://github.com/AuDigitalHealth/nash-chain-of-trust-checker-dotnet>



Key organisations supporting you, their roles and responsibilities

Australian Digital Health Agency Contact

The Agency's Digital Health Help Centre

First level support and escalation to Agency subject matter experts, product and partnership teams

1300 901 001 (Mon-Fri, 8:00-17:00 AEST/AEDT)
help@digitalhealth.gov.au

Services Australia Contacts

Developer Support (Services Australia)

First level support and escalation to technical support and product integration teams

1300 550 115 (Mon-Fri, 8:30-17:00 AEST)
DevSupport@servicesaustralia.gov.au

Test Kit Support

DevSupport@servicesaustralia.gov.au

Online technical support HI service

HI.OTS.HELPDESK@servicesaustralia.gov.au

Online technical support My Health Record system

Myhealthrecord.otshelpdesk@servicesaustralia.gov.au

Other questions

help@digitalhealth.gov.au

For further information please visit the [Developer Centre Home](#), alternatively, please see contact details.



Resources

Transition to NASH SHA-2 Certificates

<https://developer.digitalhealth.gov.au/national-authentication-service-health-nash>

NASH Developer Guide

<https://developer.digitalhealth.gov.au/developer-guide/transition-nash-sha-2-certificates-developer-guide>

NASH FAQs

<https://developer.digitalhealth.gov.au/transition-nash-sha-2-faqs>

NASH Chain of Trust Certificates

<https://www.certificates-australia.com.au/>

Services Australia Developer Portal

<https://healthsoftware.humanservices.gov.au/claiming/ext-vnd/>



Communications to PHNs and Healthcare provider organisations

We will start working with PHNs to support your customers to:

- Ensure your customers have a PRODA individual account.
- Download and install the New SHA-1 OCA and SHA-2 OCA when renewing a NASH certificate.
- Be on the lookout for your software version that is NASH SHA-2 ready.



Recap

1.

SHA-2 is almost here

2.

Ensure your software:

- Uses NASH to connect to the HI Service Supports SHA-2
- Provides alerts for expiring certificates
- Include COT in deployment if possible

3.

Provide us evidence of readiness for SHA-2

4.

Support your customers

- Ensure customers have COTs installed
- Communicate your SHA-2 readiness plans



Questions

ADHA Team

Further information and support

My Health Record

Web: www.myhealthrecord.gov.au

Help line: 1800 723 471 (select 2 for providers)

Australian Digital Health Agency

Web: www.digitalhealth.gov.au

Email: help@digitalhealth.gov.au

Help line: 1300 901 001



[Australian Digital Health Agency](#)



[@AuDigitalHealth](#)



[@AuDigitalHealth](#)

