




Australian Government
Australian Digital Health Agency



NASH SHA-2 PKI Certificate Readiness Assessment

2 August 2021 v1.0

Approved for external information

Document ID: DH-3511-2021

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



Acknowledgements

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

Disclaimer

The Australian Digital Health Agency (“the Agency”) 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. The Agency 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 and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Copyright © 2021 Australian Digital Health Agency

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 the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

OFFICIAL

Document information

Key information

Owner	Director Conformance and Assurance
Contact for enquiries	Australian Digital Health Agency Help Centre
Phone	1300 901 001
Email	help@digitalhealth.gov.au

Table of contents

1	Introduction	5
1.1	Purpose	5
1.2	Intended audience	5
1.3	Scope.....	5
1.4	Overview	6
2	NASH SHA-2 readiness assessment approach	7
2.1	NASH SHA-2 readiness assessment process	7
	Step 1: Test your enhancements	7
	Step 2: Sign and scan the NASH SHA-2 readiness test specification	7
	Step 3: Provide evidence to the Australian Digital Health Agency	8
	Step 4: Agency assessment of SHA-2 readiness.....	8
2.2	Ongoing quality assurance	8
3	Requirements for software product	9
3.1	Use Cases for NASH SHA-2 implementations	9
3.2	Technical requirements for NASH SHA-2 implementation	10
4	Services provided by the Agency	11
	Acronyms	12

1 Introduction

1.1 Purpose

This document describes the process to assess software implementing support of National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) SHA-2 certificates.

It summaries the use cases, technical requirements, testing approach and processes that are required to undertake a NASH SHA-2 readiness assessment.

Any reference to 'developers' in this document should be interpreted as a reference to any organisation that develops a software system with Healthcare Identifiers (HI) Service, My Health Record (MHR) system or secure messaging capability.

1.2 Intended audience

This document is intended for:

- Current and new software developers and implementers that are/will be connecting to:
 - HI Service;
 - the MHR system.
- Current and new software developers developing mobile applications connecting to the MHR system using an intermediary server
- Software developers implementing secure messaging with NASH certificates
- Secure messaging vendors
- Contracted service providers (CSP)
- The Agency teams responsible for NASH SHA-2 readiness assessment

1.3 Scope

The scope of NASH SHA-2 readiness assessment is for assessing software that supports the use of a NASH SHA-2 certificate.

The NASH SHA-2 readiness assessment applies to current and future software developers and implementers who currently or will be using a NASH SHA-2 certificate within their software product(s).

This includes (but not limited to):

- Authenticating for a digital health service (e.g. HI Service, MHR system, FHIR provider directory);
- Authoring and digitally signing clinical documents;
- Implementing secure messaging.

This document does not apply to the software product that is not using NASH certificate.

1.4 Overview

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
- Encrypt health information for secure exchange

Services Australia will no longer issue SHA-1 PKI certificates after 13 March 2022. Medicare PKI site certificates will be decommissioned in March 2022 and connection to the HI Service will require the use of a NASH SHA-2 certificate after 13 March 2022.

From September 2021, Services Australia will commence issuing SHA-2 production certificates, subject to sites readiness. From 14 March 2022, Services Australia will only issue NASH SHA-2 PKI certificates, which must be supported by the CIS and installed by healthcare provider organisations.

In order to continue to receive and publish information for digital health services, all software products that are in-scope (see section 1.3) will need to be upgraded to support NASH SHA-2 prior to March 2022 to retain ongoing business continuity.

Developers will need to ensure their sites (i.e. healthcare organisations) have updated to SHA-2 compatible software prior to March 2022. If the software is not SHA-2 compatible, the software's interface with these digital health services will be affected.

These NASH enhancements will provide enhanced security protection for healthcare information and reduce the need for healthcare organisations to manage multiple certificates.

2 NASH SHA-2 readiness assessment approach

The NASH SHA-2 readiness assessment provides a mechanism to ensure software developers have built the appropriate functionalities within their software product(s) to support the new NASH SHA-2 certificates and to ensure the software product is (including but not limiting to):

- Capable of authenticating a digital health service, e.g. HI Service, MHR system, FHIR provider directories; and/or
- Capable of authoring and digitally signing clinical documents; and/or
- Capable of encrypting and decrypting messages.

Any connecting software systems that is in-scope (see section 1.3) is requested to submit their NASH SHA-2 readiness test specification to the Agency for assessment of their software's readiness to use the new NASH SHA-2 certificate.

If your existing software product is SHA-2 ready, the oldest SHA-2 ready version of the software product should be used to complete the NASH SHA-2 readiness test specification. Once the software product has achieved NASH readiness for the oldest SHA-2 ready version, it is assumed that subsequent software versions are also SHA-2 compatible. The Agency has the option to request further assessment for the subsequent software versions if required.

2.1 NASH SHA-2 readiness assessment process

This section summarises the process of NASH SHA-2 readiness assessment process.

Step 1: Test your enhancements

Software developers who are in-scope (see section 1.3) for the NASH SHA-2 readiness assessment ensures the applicable technical requirements have been correctly implemented in their software product(s). See section 3 for requirements in details.

Step 2: Sign and scan the NASH SHA-2 readiness test specification

The NASH SHA-2 readiness test specification provides the details of test to be performed during the readiness assessment.

The NASH SHA-2 readiness test specification includes:

- Use cases
- Technical requirements
- Test cases
- Declaration for SHA-2 readiness

As part of the internal self-assessment, software developers are required to complete the NASH SHA-2 readiness test specification for the applicable use case(s) and requirements and provide evidence to the Agency for assessment. The software developer will also declare to the Agency that their software product is NASH SHA-2 ready.

Step 3: Provide evidence to the Australian Digital Health Agency

Once the software product is ready for NASH SHA-2 readiness assessment, software developers should submit the NASH SHA-2 readiness test specification and testing evidence to the Agency. The developer may be asked to provide further testing evidence where appropriate.

Step 4: Agency assessment of SHA-2 readiness

The Agency will provide the developer with the results of the NASH SHA-2 readiness assessments review. Upon the successful completion of the assessment, the Agency will provide the NASH SHA-2 readiness assessment outcome for the software product and record the assessment outcome for each in-scope test case.

Pass the success criteria:

- The software product must support the relevant technical requirements that correspond to the relevant use cases; and
- The software developer must complete the required NASH SHA-2 readiness test specification and provide testing evidence to the Agency and declare that their software product is NASH SHA-2 ready; and
- The software developer must achieve 100% pass rate for the test cases corresponding to the relevant requirements, and
- The Agency assesses the testing evidence provided by the developers. If the Agency's assessment does not conclude that the evidence supplied meets requirements, the Agency will work with developers to resolve any issues. This may require developers to submit a new version of their evidence submission.

Once the software developer passes the success criteria, the Agency will add the software product to HPOS to ensure developer's customers can request the correct certificate, and also add the product to the NASH SHA-2 readiness register. Developers can explicitly request to suppress their details from this register.

2.2 Ongoing quality assurance

The Agency will act on advice received regarding potential or confirmed non-SHA-2 compatible software product and work with software developers to address non-compliance within agreed timeframes and to an agreed management plan. The Agency will have the ability to remove non-SHA-2 compatible software product or version from the NASH SHA-2 readiness register as required.

3 Requirements for software product

3.1 Use Cases for NASH SHA-2 implementations

To determine which technical requirements, apply to a software product, developers/implementers need to identify the use cases that apply to their digital health implementation(s). Once the use cases are identified, the mandatory technical requirements corresponding to the relevant use cases are identified.

The table below lists the use cases of implementing NASH SHA-2 certificate within the software product to provide one or more of these digital health services.

	UC. No	Use Case	Use Case Description	Mandatory requirements
General use cases				
CIS/CSP software/consumer application	1	Authenticate a connection with a digital health service	Authenticate a connection with a digital health service, e.g. HI Service, MHR system, FHIR provider directory.	REQ 1
	2	Retrieve information from a consumer's My Health Record	A rendering system provides viewing functionality of the MHR, e.g. CIS, CSP software or mobile application.	REQ 1, 2b
	3	Author and digitally sign a clinical payload to be sent to a digital health service	Author and digitally sign a clinical payload (e.g. CDA document) for a digital health service (e.g. MHR system).	REQ 1, 2a, 2b
Secure messaging use cases				
CIS/CSP software	4	Author and digitally sign a clinical payload to be sent via secure messaging	Author and digitally sign a clinical payload (e.g. CDA document) to be sent via secure messaging	REQ 2a
	5	Verify the digital signature of a clinical payload received via secure messaging	Verify the digital signature of a clinical payload (e.g. CDA document) upon receipt via secure messaging	REQ 5a
Secure messaging developer	6	Send a message via secure messaging	Secure message agent sends messages via secure messaging	REQ 2b, 3
	7	Receive a message sent via secure messaging	Secure message agent receives messages via secure messaging	REQ 4, 5b

3.2 Technical requirements for NASH SHA-2 implementation

Software developers and implementers must demonstrate the functions and transmissions for each of the requirement that is relevant to the software product.

- **REQ 1: Authentication**

The software system shall authenticate and securely access the digital health service using NASH SHA-2 certificate.

- **REQ 2: Generating Digital Signature**

- **REQ 2a:** The software system shall digitally sign a clinical payload with NASH SHA-2 certificate.
- **REQ 2b:** The software system shall digitally sign a message with NASH SHA-2 certificate.

- **REQ 3: Encryption**

The software system shall be able to encrypt a secure message using a recipient's NASH SHA-2 certificate.

- **REQ 4: Decryption**

The software system shall be able to decrypt a secure message using a locally installed NASH SHA-2 certificate.

- **REQ 5: Verifying Digital Signature**

- **REQ 5a:** The software system shall verify a clinical payload signed with NASH SHA-2 certificate.
- **REQ 5b:** The software system shall verify message signed with NASH SHA-2 certificate.

4 Services provided by the Agency

The Agency provides a number of resources to support the NASH PKI readiness assessment:

1. Publications, FAQs and supporting materials

The Agency's Developer Centre website (<https://developer.digitalhealth.gov.au/>) provides developer guide, FAQs, notifications and supporting materials for software developers and implementers to support the NASH SHA-2 readiness assessment.

- National Authentication Service for Health (NASH)
<https://developer.digitalhealth.gov.au/topic/national-authentication-service-health-nash>
- Transition to NASH SHA-2 Certificates
<https://developer.digitalhealth.gov.au/transition-nash-sha-2-certificates>

2. Support for developers and implementers wishing to assess the NASH SHA-2 readiness with the Agency.

The Agency acknowledges that software developers and implementers operate in many different parts of the health sector. The Agency provides advice to developers/implementers on system requirements that need to be met within the context of their target environment. It is the responsibility of the individual developer to conduct self-testing prior to the submission of NASH SHA-2 readiness test specifications to the Agency.

3. Customer support help centre

The Agency operates a customer support help centre (help@digitalhealth.gov.au) to provide assistance and a point of contact for any enquires about the technical requirements and NASH SHA-2 readiness assessment.

Acronyms

Acronym	Description
CDA	clinical document architecture
CIS	clinical information system
CSP	contracted service provider
FHIR	fast healthcare interoperability resource
NASH	national authentication service for health
PKI	Public key infrastructure
SHA-2	Secure Hash Algorithm 2