nehta

National Authentication Service for Health (NASH)

Concept of Operations

Version 1.0 — 28 March 2012

Final

National E-Health Transition Authority Ltd
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

Document Information

Change History

Version	Date	Comments
1.0	28 March 2012	Final

Document Authorisation

Name	Title	Signature
Stephen Johnston	Head of Products and Solutions Development	

Table of Contents

Preface

Document Purpose

The purpose of this Concept of Operations is to provide an overview of the National Authentication Service for Health by:

- Describing the current state of healthcare authentication
- Describing the National Authentication Service for Health (NASH) in such a way that key stakeholders can visualise how the NASH should be used and how it should work
- Documenting key concepts and their usage
- Illustrating the impact on today's situation.

Information on the current progress towards fulfilment of the Concept of Operations will be carried through in the NASH Business Use Cases and NASH Service Catalogue documents.

Intended Audience

This document should be read and understood by:

- Reference groups and committees who advise or oversee the design and policy framework within which NASH is intended to operate. This includes:
  - National Health Chief Information Officer Forum (NHCIOF)
  - NASH Governance Authority (GA)
  - Identification Authentication and Access Reference Group (IAARG)
  - Clinical Leads Unit
  - Other relevant NEHTA reference groups
  - Australian Government Information Management Office (AGIMO)
- It may also be valuable to others in the eHealth space who have an interest in the overall eHealth program, including:
  - Chief Information Officers
  - Program and Product managers
  - Business analysts
  - Consultants
  - Software developers
  - Policy officers
  - Standards bodies
  - Clinical representatives
  - Healthcare consumer representatives
  - Health informaticians
  - Professional bodies
  - Potential builders, operators and users of eHealth systems.

While this document may have a broader application, it is not directed at readers outside the community identified above.

eHealth Document Map

Figure 1 represents the relationship between this document and other relevant NASH documents.

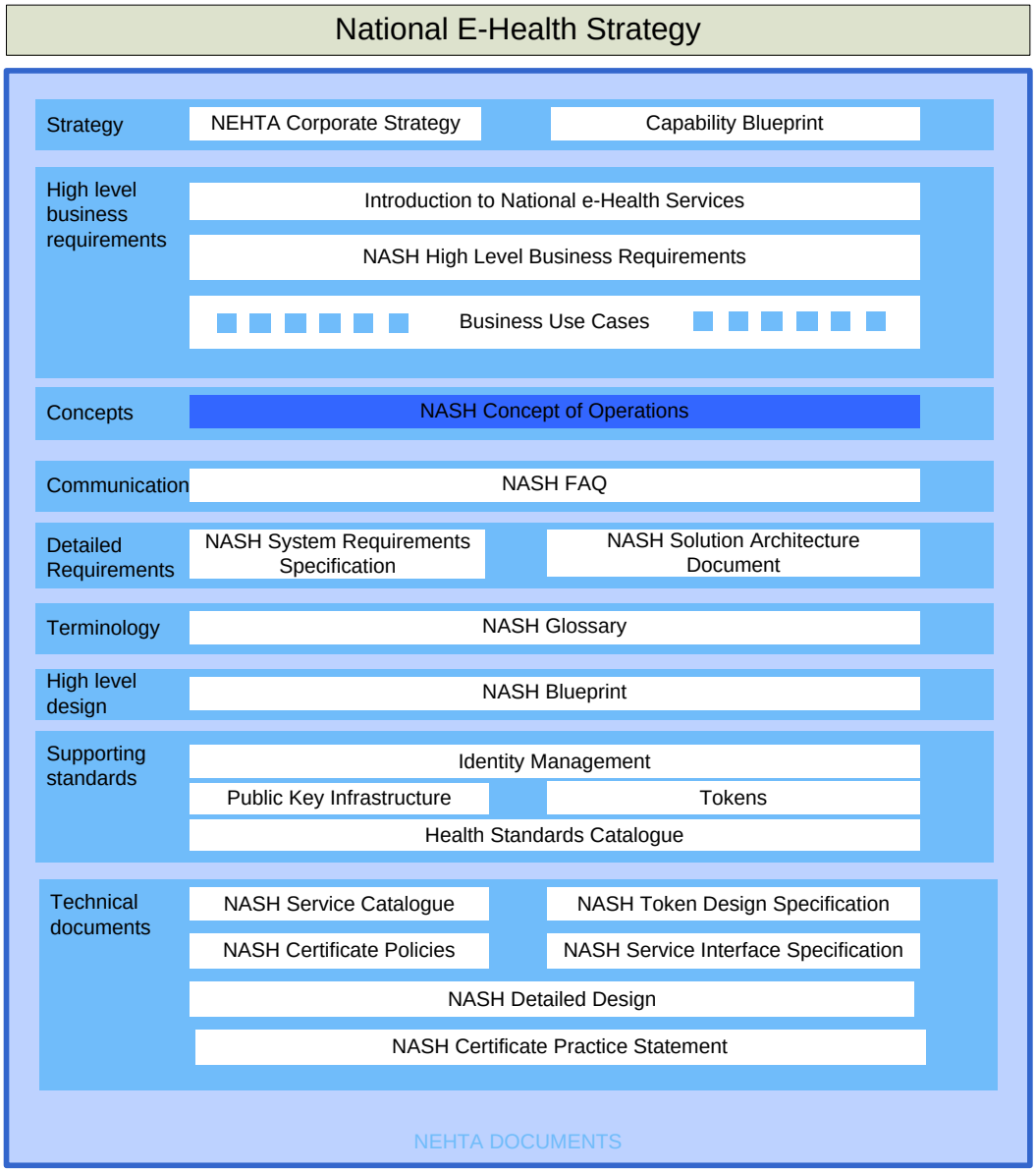


Figure 1 - Document Map

Definitions, Acronyms and Abbreviations

For lists of definitions, acronyms and abbreviations, see the Definitions section at the end of the document, on page 62.

References and Related Documents

For lists of referenced documents, see the References section at the end of the document, on page 67.

1 Scope

1.1 Document overview

1.1.1 Purpose

The subject of this Concept of Operations document is the National Authentication Service for Health. The purpose of the Concept of Operations is to:

- Describe the current state of authentication across the Australian healthcare sector
- Describe the core capabilities and services of the NASH program in relation to its impact on key stakeholders
- Describe NASH in such a way that key stakeholders can understand:
  - What the service is
  - Why the service is required (from a high level)
  - How it should work
  - How it should be implemented
- Describe the key privacy, security and policy underpinnings
- Describe how NASH should support the communities of interest (COI) participating in its authentication framework
- Document key concepts and their usage
- Illustrate the impact relative to today's situation, as it relates to the proposed services and solution.

1.1.2 Format

The general format follows an International Standard (IEEE 1362-1998) for describing the "Concept of Operation" of a software intensive business system.

A Concept of Operations is a user-oriented document that describes system characteristics from a user point of view.

- It is used to:
  - Communicate overall system characteristics to a user, buyer, developer, and other organisational elements (for example, training, facilities, staffing, and maintenance)
  - Describe the user organisation(s), mission(s), and organisational objectives from an integrated system's point of view.

The IEEE format has been expanded to include other descriptive material to provide additional coverage of the application of NASH within typical healthcare delivery business processes.

1.2 System overview

The NASH is a system that provides authentication credentials for healthcare provider organisations, healthcare provider individuals and other healthcare delivery organisations that may be issued with a Healthcare Identifier.

The NASH:

- Enables healthcare providers to assert their Healthcare Identifier (HI) based identity accurately, securely and consistently within a healthcare

delivery context. This includes use within electronic communications such as the Personally Controlled Electronic Health Record (PCEHR), Referrals, Diagnostic Services, Discharge Summaries, Medications Management and other clinical packages.

- Provides a framework in which credentials for other Healthcare authentication purposes may be implemented in a consistent way which enables those credentials to be interoperable with NASH credentials.

To provide an overview of the system, this section will describe the NASH in terms of:

- Purpose
- General nature
- Project sponsors
- The role of NEHTA
- Users of the NASH
- Associated organisations
- Graphical overview.

1.2.1 Purpose of the NASH

The purpose of the NASH is to provide an enabling capability for a variety of national authentication purposes, within healthcare delivery. Compliance with national Gatekeeper standards for authentication mechanisms will provide confidence in the overall security approach for eHealth delivery and encourage the participation of healthcare individuals in eHealth initiatives.

E-health is the means of ensuring that the right health information is provided to the right person, at the right place and time, in a secure electronic form. It aims to optimise the quality and efficiency of health care delivery.

The National eHealth Strategy[1] notes that eHealth will:

- Ensure the right consumer health information is electronically made available to the right person at the right place and time to enable informed care and treatment decisions
- Enable the Australian health sector to more effectively operate as an inter-connected system overcoming the current fragmentation and duplication of service delivery
- Provide consumers with electronic access to the information needed to better manage and control their personal health outcomes
- Enable multi-disciplinary teams to electronically communicate and exchange information and provide better coordinated health care across the continuum of care
- Provide consumers with confidence that their personal health information is managed in a secure, confidential and tightly controlled manner
- Enable electronic access to appropriate health care services for consumers within remote, rural and disadvantaged communities
- Facilitate continuous improvement of the health system through more effective reporting and sharing of health outcome information

[1] National eHealth Strategy, p.26

- Improve the quality, safety and efficiency of clinical practices by giving care providers better access to consumer health information, clinical evidence and clinical decision support tools
- Support more informed policy, investment and research decisions through access to timely, accurate and comprehensive reporting on Australian health care system activities and outcomes.

The NASH will provide an enabling authentication framework for use across the Australian healthcare sector, and will support the Council of Australian Government's (COAG) initiative to accelerate the adoption of eHealth technologies in Australia.

1.2.2 General nature of system

The NASH is more than just business services and technology. It combines technology under enabling legislation, policy and operational services that work together to facilitate consistent use of authentication for healthcare providers with healthcare delivery.

NASH will provide a strong authentication service for the Australian healthcare sector and contribute to providing a capability that "...ensures that transactions are private, traceable and only conducted by known identities...".[2]

The NASH framework will provide:

- An overarching set of authentication policies and procedures to define and endorse the issue and management of trusted digital credentials to all participants in the healthcare sector, enabling the traceability of eHealth transactions with trusted identities whilst respecting appropriate privacy and confidentiality
- A centralised source of authentication Credentials for healthcare providers, based on the use of Public Key Infrastructure (PKI) and Tokens (such as Smartcards)
- A PKI hierarchy dedicated to eHealth in which healthcare communities are able to issue and manage authentication credentials locally, supported by national infrastructure
- A governance approach for the NASH PKI
- Authentication Credentials that are based on well-established standards that are supported by existing systems and applications. This will mean that the NASH credentials will be usable with little or no extra coding required by implementers.

Currently there is no national capability within the Australian healthcare delivery sector that provides standardised trusted digital credentials for the purposes of reliably identifying and authenticating any eligible party across the entire sector. Without the accurate identification and authentication of healthcare provider individuals and organisations, eHealth systems are only able to operate across limited communities within the overall sector.

1.2.3 Project sponsors

In 2006, COAG agreed to a national approach to developing, implementing and operating key systems, including for individual and healthcare provider identifiers, as part of accelerating work towards a national electronic health records system. An authentication service was initially incorporated with the scope of the HI Service, however, it was recognised that the authentication service should have broader applicability for eHealth delivery. In late 2007, NASH was therefore broken-out from the HI Service as a separate service.

[2] NEHTA Strategic Plan 2009/10 to 2011/12, November 2009, p.13

Through the Australian Health Ministers' Conference (AHMC), and latterly the Standing Council on Health (SCoH), the NASH is sponsored by the Commonwealth, state and territory governments, which have been investing, through NEHTA, in key building blocks for a national eHealth system.

1.2.4 Role of NEHTA

The role of NEHTA is to project manage the design, development and delivery of eHealth enabling technologies and services.

The development of the NASH is a foundation component of NEHTA's work program.

1.2.5 Users of the NASH

The NASH will provide an enabling authentication framework for use across a complex network of public and private healthcare provider individuals and organisations, including:

- Public and private sector hospitals
- General practice
- Clinical specialist
- Community health
- Healthcare administrators
- Allied health
- Aged care settings.

1.2.6 Associated Organisations

The NASH will work co-operatively with a number of other organisations in the healthcare sector, including:

- Development organisations
- Standards bodies
- Professional bodies
- Regulatory bodies.

1.3 Graphical overview of system

The following diagram provides a context for the NASH within the National eHealth Infrastructure.

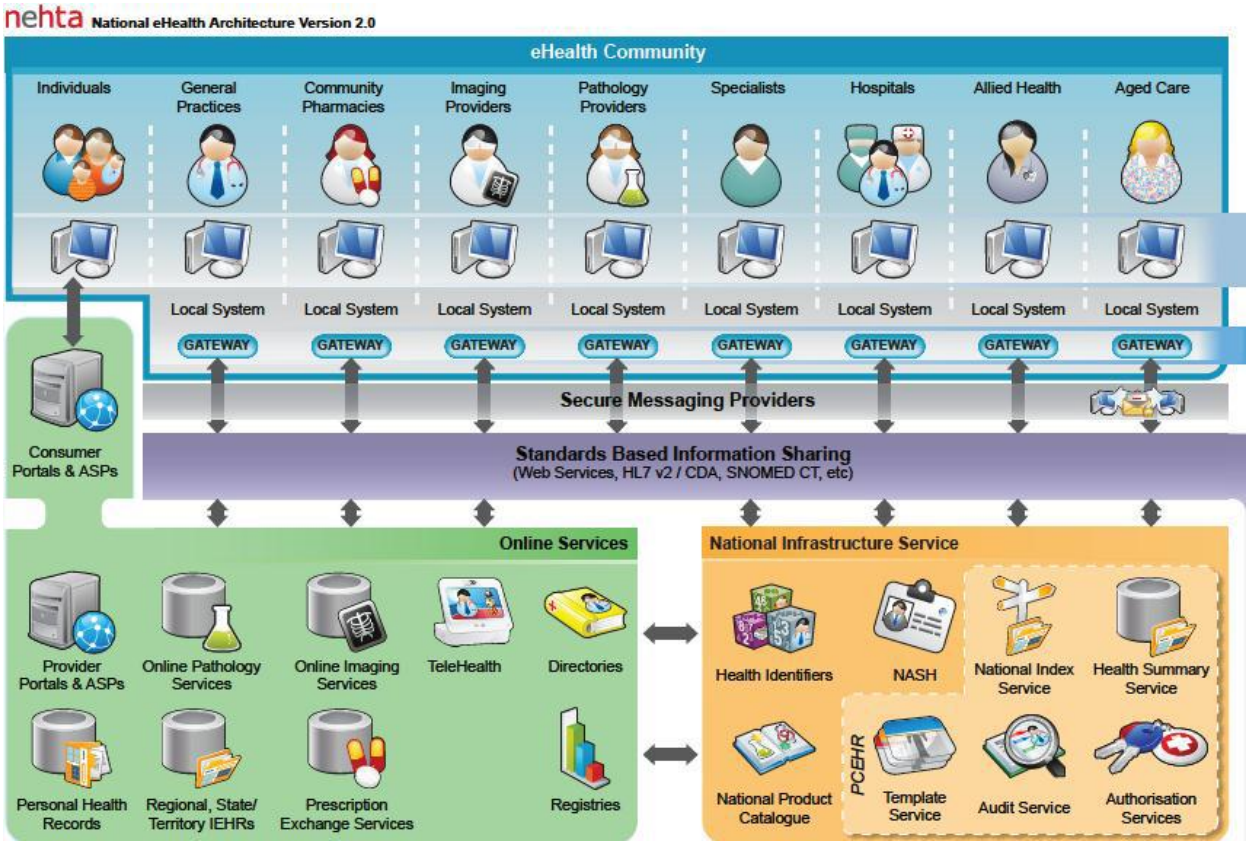


Figure 2 - National eHealth Architecture

The following solution overview diagram shows the NASH and its indicative relationship with associated systems and organisations.

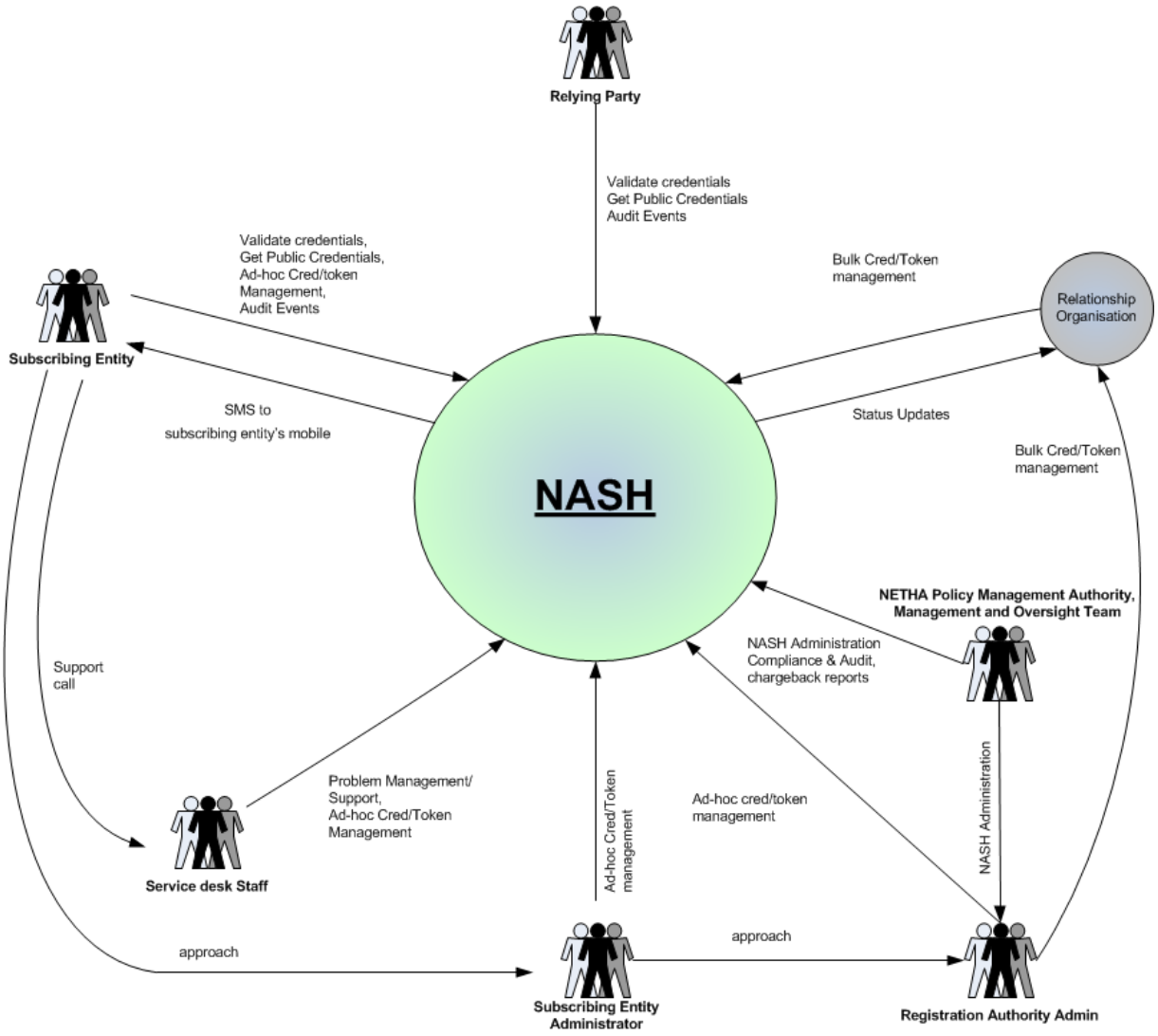


Figure 3 - NASH Relationships

The following diagram shows examples of how NASH will be involved in typical authentication scenarios.

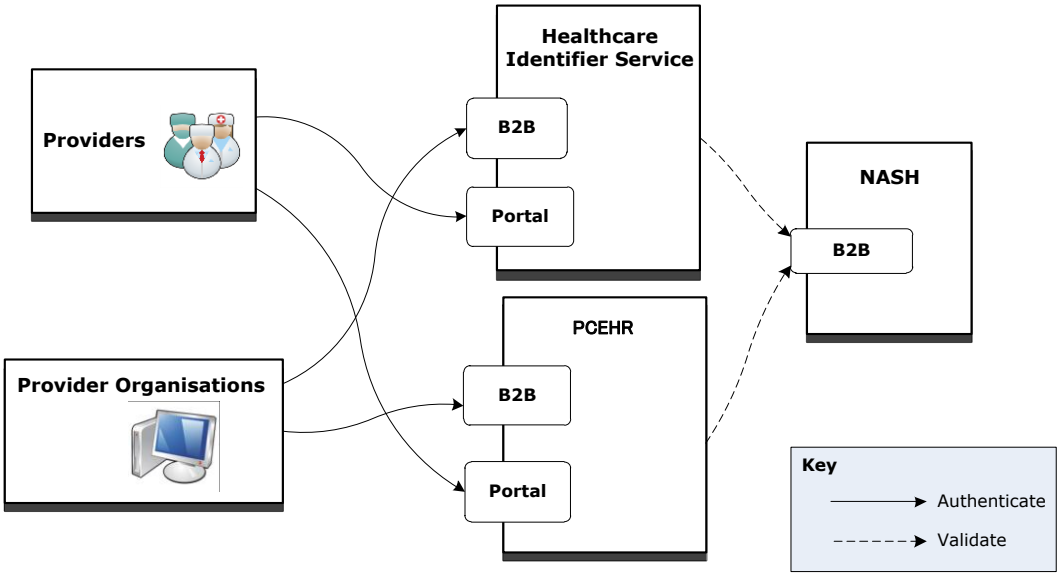


Figure 4 - Authentication using NASH

Healthcare providers will be able to use their NASH credentials to authenticate to Relying Parties (e.g. National eHealth services). NASH will issue Gatekeeper compliant credentials that can be used to access federal government services such as Healthcare Identifier service and PCEHR. The eHealth service provider will determine which NASH credentials can be used to access their services. The National e-Authentication Framework (NeAF) provides guidance in this area.

For details about how healthcare provider individuals and healthcare provider organisations can obtain and manage their NASH credentials refer to Sections 4.4.30.1 and 4.4.30.3.

2 Current situation

This section provides an overview of the existing capabilities for authentication within the Australian healthcare delivery environment.

2.1 Background

The challenge of identifying and authenticating healthcare providers is not new, but is a fundamental building block for eHealth. The existing state of authentication in the Australian eHealth environment is comprised of disparate management processes with a variety of mechanisms to authenticate healthcare providers.

The Australian healthcare sector currently does not have a national capability to provide standardised trusted credentials for the purposes of reliably identifying and authenticating healthcare providers, both individuals and organisations.[3] Isolated solutions exist within Australia where there is a high level of confidence required when exchanging information within specific purpose communities of interest. However, when information is exchanged or transmitted electronically outside a specific purpose community of interest, the confidence level is diminished. A standard way to communicate between specific purpose communities of interest within the overall healthcare sector, while maintaining a high level of assurance, does not currently exist.

This has created substantial barriers to the effective sharing of information between healthcare providers. Significant research has been undertaken in a number of healthcare environments, and this has shown that poor information sharing is a major cause of preventable errors that compromise the quality and safety of patient care.[4]

A general concern raised by many users in the healthcare sector is related to the number of different authentication tokens which clinicians may be expected to carry and use on a regular basis.

The major issues with the current state are[5]:

- Local authentication service programs currently being established within health jurisdictions are being developed independently and are not aligned.

  Establishment of a national authentication framework will enable health organisations to more easily align their authentication solutions at a business level. Where this may not be required due to the local nature of the authentication solution being implemented there will be scope at the technical level so that implementation costs are minimised and existing infrastructure is re-used where possible.

- No healthcare provider organisational identity credentials exist that can be properly used to support NEHTA-compliant secure messaging standards.

  The existing location certificates supplied by Medicare Australia can be used in some instances. However, there are some technical limitations that mean they cannot provide all the functionality required. New certificate types will need to be provided.

[3] NASH High level Business Requirements, January 2011, p.9

[4] Australian Health Minister's Conference, *National E-Health Strategy,* September 2008, p.13

[5] NASH Blueprint v1.5, January 2012, p.17

NASH embodies a means to establish a new community of trust that extends between healthcare participants across the country, one not reliant upon piecemeal or de facto agreement between specific parties.

2.2 Operational policies and constraints

The nature of the Australian healthcare system has a number of implications for eHealth in this country. First and foremost is the complex and fragmented nature of the service delivery landscape, which has resulted in the creation of a vast number of discrete silos or islands of information across all parts of the health system. This has created significant barriers to the effective sharing of information between healthcare participants and has posed real challenges when trying to understand and report on what is really happening in the Australian healthcare system.[6]

The complexity of Australia's health funding and accountability arrangements and the lack of alignment across public and private sector healthcare providers, and across jurisdictional boundaries, have often resulted in political and governance barriers, as well as technical barriers, being placed in the way of national eHealth progress.

2.2.1 Legislation, guidelines and standards

Legislative controls on identification of healthcare providers include:

- *Healthcare Identifiers Act 2010*
- *Healthcare Identifiers (Consequential Amendments) Bill*
- *Healthcare Identifiers Regulations 2010*
- *Health Practitioner Regulation National Law Act 2009*[7]
- Freedom of Information (FOI) legislation
- Information and privacy legislation
- Public health notifications required under law.

Current legislation, guidelines and standards that impact nationally on information security and authentication include:

- *Gatekeeper PKI Framework*, Australian Government Information Management Office (AGIMO), Federal Department of Finance, February 2009
- *Electronic Transactions Act 1999 (Cth)*, section 10 – outlines requirements that must be met for an electronic signature to be valid
- Australian Standard AS4860-2007, *Knowledge-based identity authentication – Recognising Known Customers* facilitates the deployment of a range of authentication credentials appropriate to the needs of government agencies and their clients
- *National e-Authentication Framework* (NeAF), AGIMO, January 2009 – assists agencies, jurisdictions and sectors in authenticating the identity of the other party to a desired level of assurance or confidence
- *Protective Security Policy Framework* (PSPF), V1.2, Attorney General's Department, January 2011. The PSPF is designed to help agencies identify their individual levels of security risk tolerance, achieve the mandatory requirements for protective security expected by Government, and develop an appropriate security culture to securely meet their business goals

[6] Australian Health Minister's Conference, *National E-Health Strategy,* September 2008, p.9

[7] As enacted in State and Territory Jurisdictions – refer to http://www.ahpra.gov.au/Legislation-and-Publications/Legislation.aspx

- *Australian Government Information Security Manual* (ISM), Defence Signals Directorate, 2012 – provides a framework for agencies to address new and existing security risks to their systems.
- *Report to the Council of Australian Governments on the elements of the National Identity Security Strategy*, April 2007
- *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals*, The Office of the Federal Privacy Commissioner, December 2001
- *Handbook 174: Information security management – implementation guide for the health sector*, Standards Australia 2003
- *Targeted Cyber Intrusions – Mitigation Strategies Matrix* – CERT Australia and the Cyber Security Operations Centre, Defence Signals Directorate
- *International Standard ISO 27799: Health informatics – Information security management in health using ISO/IEC 27002*. This International Standard has been recommended for adoption as an Australian Standard by the IT-14-04 Health Informatics Information Security Sub-Committee
- *NESAF – National eHealth Security Access Framework* – Release 3, NEHTA.

2.2.2 National e-Authentication Framework (NeAF)

NeAF has been developed by the Australian Government Information Management Office (AGIMO) as a whole of government approach to providing a framework for electronic authentication between agencies and jurisdictions, which focuses on the electronic authentication of the identity of individuals and businesses. NeAF provides principles that can be applied by government agencies for standardised implementation of e-authentication approaches. Its intent is to minimise duplication of effort, and achieve a more standard and consistent authentication approach.

The NeAF provides a systematic way to:

- Classify the sensitivity of information used in each online transaction
- Analyse the potential damage that might ensue if the identity accessing that information could not be assured
- Assign a minimum necessary assurance level for each transaction
- Determine the necessary authentication approach – e.g. password, PIN, one-time password, digital credential, digital credential on smartcard.

The NeAF is widely used within government agencies and jurisdictions and is frequently mentioned in any discussion of authentication services. The nature of the NASH is that it will enable the assessment of authentication approaches within the NeAF

NeAF assurance levels are dependent on the context of the issuance and usage of authentication components, such as those provided by the NASH, within a business system. NASH in itself should not automatically provide any particular NeAF level of assurance for a business process or application, though it may enable the achievement of a specific NeAF assurance level when applied together with other attributes of the process or application.

2.2.3 National eHealth Security and Access Framework (NESAF)

The NASH should align and harmonise with NESAF. The vision for the NESAF is to:

- Ensure that access to consumer health information is consistently controlled and monitored as it transitions through independent organisations, business processes and systems in the Australian health sector.
- Ensure that the provenance of all electronic health information is traceable from its creation at a verifiable trusted source through its transition and possible augmentation on route to its destination.

The NESAF sets out a risk-based approach and process to assist analysing risk in relation to participation in the Australian eHealth environment and identify appropriate security and access controls. The process assists businesses to identify appropriate methods – that may include policies, practices, procedures or software and other technical solutions - for protecting healthcare information within their organisation, and the information that they may access and share with other healthcare organisations in the national eHealth environment.

2.2.4 Privacy

Australia's current privacy landscape is complex and fragmented due to differing privacy schemes that apply to health and eHealth infrastructure across the Commonwealth, states and territories. This mix of legislation and administrative arrangements across the Australian health sector has resulted in:

- Increased compliance costs, particularly where business is being conducted across jurisdictional boundaries, or public and private sectors
- Confusion about which regimes regulate particular businesses
- Uncertainty among healthcare individuals about their rights
- Uncertainty among healthcare providers about their responsibilities.

Changes are currently being considered to the national privacy legislation following the Australian Law Reform Commission review of Australian privacy laws.

The major intersection between privacy of legislation and administrative arrangements and the NASH concerns the information which could appear in the directories necessary to operate a PKI service. The NASH design should minimise any exposure of personal information.

2.2.5 Common law duty of confidentiality

In addition to legislative privacy obligations, a common law duty of confidentiality also applies to health care providers with respect to their patients. This duty requires that healthcare providers ensure the confidentiality of the personal information of their patients is maintained when collected and transmitted as part of a healthcare interaction.

The NASH will provide credentials which support the use of encryption of data in transmission.

2.2.6 Healthcare professional requirements and standards

Requirements are imposed on certain healthcare providers under the various healthcare registration schemes. Healthcare and clinical standards are also issued by a range of expert bodies.

2.3 Users and other involved personnel

Current healthcare authentication schemes are provided at a local level and are primarily used to support the clinical and business processes of healthcare providers within their communities of interest.

The individuals and services that are currently involved in authentication processes include:

- Administrators and clerical staff who work for healthcare providers
- IT System Administrators
- Secure Messaging Services
- Jurisdictional and local service directories, including
  - Victoria HealthSMART
  - ACT eHealth
  - Western Australia Identity Management Initiative
  - Northern Territories Continuity of Care (CoC)
- Software vendor organisations
- Certification Authorities (CAs)
- Various PKI directories.

2.4 Technology limitations

There is a relative lack of maturity of information technology within the Australia healthcare sector, with the inconsistent application of national eHealth standards on which to base the development of hardware and software. This has been compounded by a lack of national governance over certification and compliance with standards.

Across Australia, the lack of enforceable standards for data and interoperability in the health sector has contributed to an environment of uncertainty for IT vendors. This had contributed to the implementation of vendor-led eHealth solutions based on proprietary systems, with limited flexibility and interoperability.

Although the health sector is one where information is central to all aspects of care management and delivery, spending on the underlying IT infrastructure has been significantly less than for other information-centric consumer industries such as the financial services and communications sectors. The core infrastructure and systems for many health organisations is not sufficiently mature and reliable.[8]

2.5 International eHealth Implementations

Globally, eHealth has been viewed as an important enabler of health sector reform, particularly in the areas of identification and authentication. Some examples of international adoptions of PKI solutions include:

2.5.1 Denmark

The Danish national eHealth portal, sundhed.dk ("sundhed" means "health"), helps drive the optimisation of the healthcare sector by providing a shared infrastructure for healthcare participants. It enables all parties in the healthcare sector to collaborate across professional and IT-related boundaries

[8] Australian Health Minister's Conference, *National E-Health Strategy,* September 2008, p.20

and makes it possible for healthcare recipients and professionals to access information and communicate with each.

The portal uses a PKI framework for security and authentication. Digital credentials are issued to healthcare recipients and providers to assert identity when accessing the portal.

2.5.2 Ontario (Canada)

In the province of Ontario, Canada the development of a province-wide electronic
information network will ensure the integration of a transformed health system
providing security and confidentiality of personal health information. The scope of the PKI solution includes the development of a PKI governance model, certificate policies and certificate practices, as well as the complete architecture, design and implementation of a highly available PKI in all operating environments.

2.5.3 United Kingdom

In the United Kingdom, the National Health Service (NHS) has established a PKI framework to facilitate access to patient information. Access to the NHS summary care record is controlled using smartcards and Personal Identification Numbers (PINs). These smartcards are configured to allow the user the correct level of access according to their role. The issuance of smartcards is through one of the many Registration Authorities established. Healthcare Provider Individuals are granted access, via their smartcard, to patient information based on their work role and their involvement in patient care.

3 Justification for and nature of changes

3.1 Justification for change

Appropriate eHealth foundations, in the form of computing infrastructure and consistent information standards, rules and protocols, are crucial to effectively sharing information across geographic and health sector boundaries. These foundations represent the core infrastructure that will underpin the national eHealth work program and it is considered too risky and costly to try and establish this infrastructure other than by means of strong national coordination.[9]

In any electronic transmission of health information, there are potential impacts to organisations, but more importantly to healthcare individuals, if assurance of the identity of the person or organisation accessing or sending information is not possible. The risk can range from moderate to substantial and may occur when the incorrect person receives incorrect information or is incorrectly identified. It is imperative to be able to accurately and reliably ascertain and identify both provider individuals and provider organisations within healthcare environments. This provides trust in the electronic communication and exchange of information between healthcare providers. In establishing trusted authentication across the healthcare sector, potential efficiency gains and clinical benefits to healthcare individuals will be realised.

The National E-Health Strategy included identification and authentication as one of the five key national foundations required for eHealth:

> *There is a need to design, build and implement an identification and authentication regime for health information as soon as possible as this work will be absolutely fundamental to the nation's ability to securely and reliably access and share health information. This requires:*
>
> - *Identification - the provision of functions to uniquely identify consumers, care providers and care provider organisations to ensure that information about the right person is going to be sent to the right care provider. Identification services should include the allocation and management of unique identifiers and the provision of directories that allow care providers to be located by name and by the type of services they provide.*
> - *Authentication - the provision of functions to securely address, authenticate and transfer messages from one care provider to another to ensure that the information gets to the right provider in a secure manner.*[10]

A fundamental shift in the way information is accessed and shared across healthcare systems is required. Healthcare providers need to access and share health information reliably and securely across geographic and health sector boundaries. This can only be achieved by implementing a world class eHealth capability and one of the foundation building blocks for the delivery of this is accurate strong identification and authentication of those facilitating healthcare in a healthcare setting.

[9] Australian Health Ministers' Conference, *National E-Health Strategy,* September 2008, p.35

[10] Ibid, p.38

3.2 Benefits of a national approach

The full benefits realisation of eHealth cannot be met and delivered without a national approach. There has been a recognition that eHealth in Australia has been moving too slowly and is in a fragmented state. Investments in IT have been uncoordinated and have offered little interoperability for the exchange of messages and information. Multiple identifiers have also been used for patients and providers across primary and acute healthcare sectors.

There have been a number of eHealth projects that have delivered positive outputs, in localised areas. Unfortunately, while the benefits of these projects may be realised in a community of interest, they are often not able to exchange information with other systems. There is no trust as to who may be communicating with whom, and there is incompatibility between IT Systems. This potentially restricts any current capability in nationally providing equity in provision of some health services.

The realisation of a national approach will provide standardisation, efficiency, and avoid unnecessary duplication and will allow for greater progress due to the coordination of both funds allocated to eHealth and alignment of plans.

The NASH provides one of the fundamental building blocks to enable wider national eHealth initiatives such as personally controlled electronic health record, e-referrals, e-pathology, e-discharge and e-prescriptions. NASH will deliver strong authentication of all healthcare providers participating in the national eHealth scheme in Australia. It underpins NEHTA's core connectivity, is a pathway to national services, and is a key enabler for eHealth services requiring authentication.

The NASH will build on the national Healthcare Identifiers (HI) service and provide healthcare provider organisations and individuals with authentication credentials that assert their HI Identifier. This means that the parties they transact with will be able to have trust in their identity without having to establish separate trust relationships.

4 Concepts for the proposed system

4.1 Background, Objectives and Scope

The NASH will provide a national authentication framework that supports communication of health information more securely and reliably than is possible in the current environment.

This section articulates a high-level description of the NASH and explains how it should operate.

4.1.1 Background

To build a world class eHealth solution, Australia needs frameworks and infrastructure components that can be leveraged at national, state and territory, regional and local levels to deliver solutions that are able to be integrated and share data across geographic and health sector boundaries. To improve patient outcomes, the islands and pockets of information that currently exist across the healthcare sector need to be able to securely exchange information and have trusted relationships with those they are exchanging information with.

The NASH will provide the necessary strong authentication required by the Australian healthcare sector to support a safer, better connected and more sustainable healthcare system.

4.1.2 Objectives

The NASH will provide services that:

- Establish a national framework to define and endorse the issue and management of trusted digital credentials to all entities in the healthcare sector, enabling the traceability of eHealth transactions with trusted identities respecting appropriate privacy and confidentiality.
- Deliver suitable authentication services for access to the HI Service, comprising credentials, smartcards and support services to deliver appropriate levels of authentication of healthcare providers, both individuals and organisations.
- Accredit local PKI services operated within local healthcare communities to manage the issue of authentication credentials within their local environments, delivered through strong and robust processes capable of being supported by national and local infrastructure
- Enable and support the transition of existing systems to use NASH digital credentials that meet NEHTA standards.
- Provide foundation services to other NEHTA initiatives, such as secure messaging, to enable delivery of major new eHealth services like the Personally Controlled Electronic Health Record, electronic referrals, diagnostic services, discharge summaries, medications management and other clinical packages.

The NASH Services will:

- Be separable and transferable from / between service operator(s): The NASH services will be independent of the service provider and not tied, or locked to any inherent or incumbent service provider through technology process or operations. The NASH services will support and promote service provider diversity and transparency.

- Be loosely coupled: The NASH will be a coordinated suite of services, orchestrated in a manner that allows multiple users and service providers to operate seamlessly. The NASH services should be able to be decoupled from each other, while allowing orchestration across organisational boundaries.
- Be delivered using a phased and incremental delivery. The delivery of NASH services will support incremental service delivery, and provide outcomes in a phased release, to support the progression of eHealth.
- Leverage existing investment and assets where appropriate. Existing government and eHealth sector investment should be built upon for the delivery of NASH where business and technologically feasible.
- Deliver services as quickly and as cost-effectively as practicable to the eHealth sector.
- Enable the same token to store credentials from multiple Registration Authorities. This will minimise the number of different authentication tokens that a healthcare worker should only require, and promote the goal of requiring only a single token.
- Have an open solution architecture, to promote uptake. The NASH services will be designed to be open, interoperable, adaptable to change and aligned with international and national standards. This will enable flexibility, longevity of the NASH and provide integration with existing and yet to be developed credential and token infrastructure.
- Have ongoing operational costs for NASH, which should be kept as low as practicably possible, in order to be palatable and sustainable for the healthcare sector.

4.2 Scope of NASH

The NASH will provide a national supply of trusted digital credentials available to all eligible participants in the healthcare sector, allowing the traceability of eHealth transactions to trusted identities.

- The NASH solution is defined in terms of the following elements:
- Credential Management Orchestration
- Policy, Practices, Standards and Governance
- Directory/Order Processing Services
- Certificate Management Services
- Token Management Services
- Fulfilment Services
- Reporting & Audit Service
- Help Desk Service.

4.3 Operational policies and constraints

4.3.1 NASH Governance Authority

The NASH Governance Authority (GA) provides policy and strategic direction to the NASH, and through this body to the participating Certification Authorities and entities. The governance organisation must address technical and business context as well as legal and policy issues of relevance for understanding, specifying and deploying eHealth systems.

The NASH GA will endorse and ensure consistency of all Gatekeeper documentation, which may extend beyond the Certificate Policy (CP) and similar documentation to include, for example, the privacy policy. It will also provide continuity of high level policy assurance as NASH moves into operational activity.

The NASH GA will provide assurance against stakeholder requirements, by ensuring key users provide oversight and direction of the NASH PKI approach and operation. A stakeholder advisory group should be appointed to report and propose strategic initiatives on specific topics to the NASH GA.

The NASH GA may devolve responsibility to subordinate bodies and organisations to act on its behalf. The diagram below is reference model for PKI governance which should be used to inform the specific governance arrangement for the NASH.

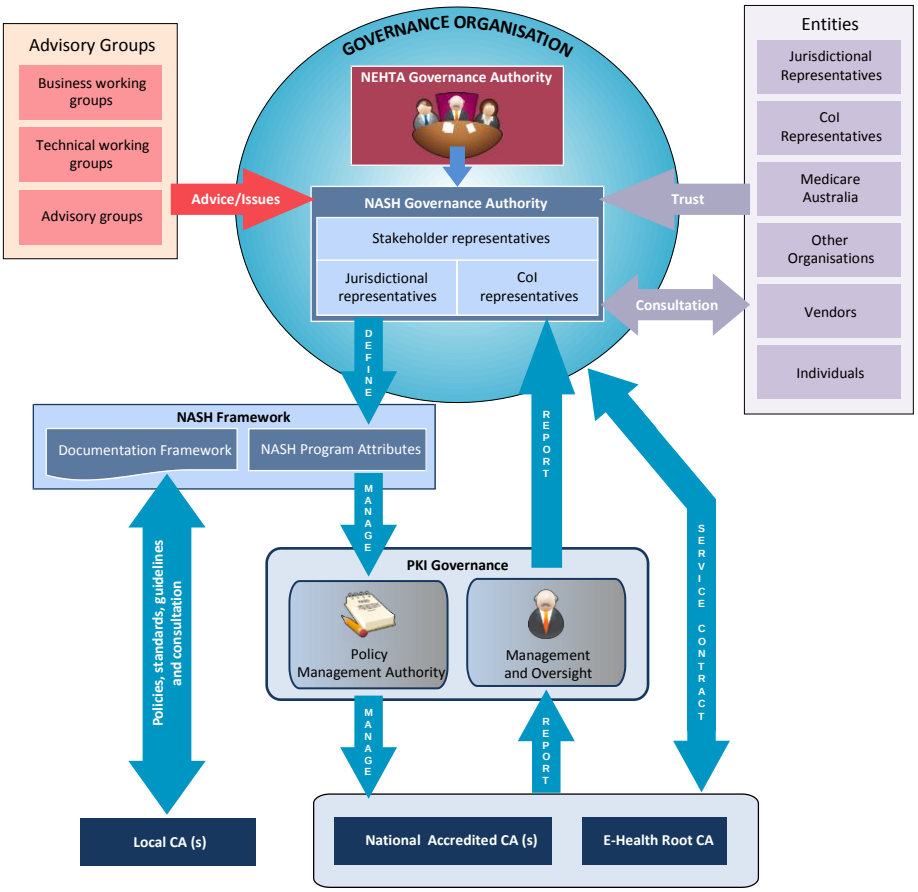


Figure 5 - Indicative Governance Reference Model

4.3.2 Strategic Oversight

The body with responsibility for strategic oversight of NASH will be the Board of the legal entity under which the NASH is established. Key responsibilities of this body will be to determine high level policies and the strategic direction of NASH, including its scope and authorised participants, institutional arrangements and monitoring of those arrangements to ensure they continue to be suitable for purpose.

4.3.3 NASH PKI Policy Management Authority

The NASH PKI Policy Management Authority (PMA) is small working group that will provide specialist technical assurance under the oversight of the GA. The PMA will be responsible for:

- The creation of policies and standards unique to the operation of the NASH PKI and the related Certification Authority (CA) operating within it
- Operational service governance for NASH. Service governance covers the broad range of activities required to maintain operations of the service. Some of the key areas are policy management, operational funding and liability management
- Ensuring that the NASH PKI is consistent with Gatekeeper accreditation requirements.

4.3.4 Management and Operation

The operational policies that will govern the general management and functions undertaken within NASH will be set by NASH Governance Authority.

Day to day general management of the NASH services will provide administrative, technical support, and policy input, to the Policy Management Authority. This includes ensuring administration of certificate policies, standards and criteria. It will also administer and oversee any contracts with external service providers such as:

- Establish a suitable regulatory and policy framework to manage operations in an eHealth authentication environment
- Develop an accreditation program to allow commercial suppliers of authentication services to be nationally recognised
- Develop an accreditation program to endorse the participation of suitable local authentication services in the national eHealth authentication environment.

Management of operational liability is an area which will require careful governance controls to be in place. For example, if credentials from one community of interest will be recognised and used by others, it will be important to have clarity on where service and usage liability will rest.

4.3.5 Gatekeeper

The Commonwealth Government Gatekeeper Strategy governs the use of PKI in government for the authentication of external clients. The Gatekeeper PKI Framework incorporates the Gatekeeper Strategy, reducing the cost and complexity of Gatekeeper for both business and government.[11]

As Gatekeeper is a formal process for the certification of providers, recognised compliance with Gatekeeper will demonstrate the technical and operational competence of the NASH's capabilities.

As the NASH will be used for access to data sets which fall into the management domain of the Australian Government, it is a specific requirement on the NASH that it is compliant with the Gatekeeper PKI Framework. There are several possible models within the Framework. As there is a distinct community of Healthcare Providers established through participation in the Healthcare Identifiers Service, a Community of Interest model based on a Relationship Organisation should be implemented, based on that affinity.

A Relationship Organisation is one that has an established relationship with its subscribers which it and the Community of Interest (COI) considers adequate as the basis for requesting or authorising the issuance of digital credentials.

In its simplest form, the Relationship Organisation (RO) will request/authorise the issuance of a Relationship Certificate to its subscribers (known as Clients) who will use their Relationship Certificates to conduct transactions with the Relationship Organisation (i.e. the Community of Interest comprises the Relationship Organisation and its Clients).

The process of gaining Gatekeeper accreditation is rigorous and thorough. Establishing the compliance of the NASH with Gatekeeper will provide assurance that products and methods for delivery have been evaluated to ensure that the requirements for security have been met.

4.3.6 Privacy

The NASH program will adhere to privacy best practice through documented processes and policies and observation of the National Privacy Principles (NPPs) under the Privacy Act 1988 (Commonwealth).

[11] *Gatekeeper Public Key Infrastructure Framework,* February 2009, p.5

Gatekeeper also requires compliance with the Information Privacy Principles, including that compliant Certification Authorities ensure that:

Privacy protection is provided for personal information published in publicly accessible lists/registers (Controls over how personal information is accessed, searched and used)

- *No personal information shall be made publicly available in Certificate Revocation Lists (CRLs) and other directory services.*
- *Certification Authorities shall collect and hold minimal personal information when logging accesses to CRLs or other directory services.*
- *Certification Authorities should not disclose personal information collected by logging access to CRLs or other directory services, except in circumstances where, if that information were protected telecommunications information, they will be authorised or required to disclose the information under Part 13, Division 3, Subdivision A of the Telecommunications Act 1997 (Cth).*[12]

Adherence to these privacy requirements is assessed through a formal Privacy Impact Assessment and ongoing privacy compliance is documented in a NASH Privacy Policy..

4.3.7 Information Security

The Information Security Framework for the NASH will operate within the context of the National eHealth Security and Access Framework (NESAF). It covers the principles, policies, processes and tools that are to be used to achieve this aim.

The NESAF will contribute to the success of the NASH by assisting in identifying appropriate controls for safeguarding the information required to operate the Service.

A multi-layered approach will safeguard the NASH, and accordingly the Security and Access Framework incorporates both technical and non-technical controls. These include:

- Digital credentials to facilitate the accurate identification and authentication of individuals accessing any NASH management portals
- Robust audit trails, and proactive monitoring of access to any NASH portals
- Role-based access control policies
- Rigorous security testing, to be conducted both prior to and after commencement of operation of the NASH
- Ensuring users of the NASH are adequately trained, through provision of educational programs and other training mechanisms.

The NESAF will be applied within the NASH to ensure that the privacy, confidentiality, integrity and availability of information within the Service are not compromised.

Security needs to be operationally realistic for stakeholders, meaning that it must support, rather than hinder, the NASH. As such, security will be designed to be 'fit for purpose', and to address policy objectives. Appropriate security controls are therefore being implemented in order to meet the NASH objectives.

The objective of the Information Security Framework for the NASH is to:

- Minimise the risk of unauthorised access to the NASH

[12] *Certification Authority Accreditation Criteria,* Gatekeeper PKI Framework, February 2009, p.18

- Enable detection of unauthorised information access or modification, and any other breach of information security (including privacy)
- Facilitate appropriate response to, and investigation of, any such breaches
- Assure the continued availability of the NASH
- Provide a means to continually improve security protections (including protection of privacy, confidentiality, integrity and availability).

Information security generally operates within broader information regulatory frameworks. Any breach of security would be a breach of privacy and may also be subject to further penalties under the appropriate regulatory regime.

4.3.7.1 Risk Management

A risk management approach should be taken that aligns and complies with appropriate information standards, such ISO/IEC 27001, AS/ANZ ISO 31000:2009 and NESAF requirements.

The achievement of Gatekeeper accreditation will also ensure the NASH is appropriately protected whilst meeting the needs of the healthcare community.

4.3.7.2 Confidentiality

While the NASH holds minimal information of a confidential nature, none the less it is essential to ensure that information held is not made available or disclosed to unauthorised individuals, entities or processes. Confidentiality is not limited to, but includes, personal information, as well as commercially sensitive information.

Information confidentiality should be assured by restricting access to information in the NASH to only those users who are authorised to access it, and also through logging all access.

4.3.7.3 Integrity

Integrity of information is concerned with ensuring that the NASH data cannot be changed without detection. Safeguarding the accuracy and completeness of information is vital for maintaining the integrity of the NASH. Data quality management techniques should be used to regularly assess and maintain the quality and integrity of the NASH information.

4.3.7.4 Availability

The NASH Service must be readily available and usable upon demand by any authorised user. Healthcare delivery events may occur at any time, and it is not readily possible to predict when the circumstances associated with the event could lead to a need to access the NASH management services, e.g. a need to replace a lost or damaged token at a point of care. High operational availability must be assured by using a highly resilient production platform which includes geographically diverse components.

The general availability goal for the NASH components which are critical for operation of the service should be 99.99%. On an annual basis, this targets a maximum of ~53 minutes in total of unscheduled outages. Some brief scheduled outages may be periodically necessary for system maintenance and upgrade purposes, and should be advised well in advance.

The specific availability profile and notification mechanisms should be determined as part of the operational contract.

4.3.8 NASH Framework

The NASH Framework will define a set of minimum policies and requirements that must be met by NASH participants. This standardisation should create a common playing field among each additional Community of Interest that establishes itself within the NASH Framework, over time. The framework will be based on Gatekeeper, particularly the risk based approach to determining:

- Authentication strength requirements
- That a Community of Interest relationship exists, with a level of confidence related to the strength of the credential
- Credential mechanism strength required.

The parameters of the NASH Framework are described in further detail in the NASH Blueprint document.

4.3.9 Compliance

The NASH PMA is responsible for ensuring that the NASH PKI is operated in accordance with the Certificate Policies (CPs) and Certification Practice Statement (CPS) and other operational policies and documents. The PMA will commission annual and ad hoc audits of the NASH PKI. The PMA will also conduct periodic reviews of the audit reports of RAs and subordinate CAs in relation to their compliance and in accordance with contractual agreements.

The PMA will engage external auditors as required. The PMA is required to follow-up any action on recommendations from audit reports and other reviews, and must publish substantial portions of any NASH PKI audit report, including any matters of particular importance or significance.

4.4 Description of the NASH Solution

The NASH service will:

- Provide a national, standards based deployment of digital credentials for healthcare providers based on PKI digital credentials and tokens, such as smart cards
- Provide the ability for a registration organisation, e.g. the operator of the HI Service, to manage the request for credentials by, and their consequent issuance to, trusted healthcare provider organisations and individuals
- Provide token and card reader fulfilment and logistics services
- Provide digital credential authentication and lifecycle management via a self-service web portal and a 24x7 service desk
- Provide usage and service level agreement monitoring and reporting services
- Provide specifications, frameworks and infrastructure to allow eHealth participants to validate NASH-compliant credentials
- Enable the rapid adoption of NASH-compliant credentials by releasing a Software Developers Kit (SDK) for use by healthcare software vendors.

The NASH Solution also supports diverse communities of interest which include:

- Early adopters, within jurisdictions, communities of interest and other organisations including DHS Medicare
- Health industry organisations from sole providers to large multi-location, multi-jurisdictions entities

- Healthcare providers, professionals and other entities that have no supporting infrastructure
- Organisations that own or utilise their own supporting infrastructure
- Organisations that do not want the overhead of managing their own PKI solution(s), and would prefer rather to purchase as a service from an accredited supplier.

The NASH Solution uses existing token deployments by DHS Medicare and emerging token deployments by jurisdictions to establish a service based on Australian and International standards to improve consistency, interoperability, reduce costs and improve service delivery.

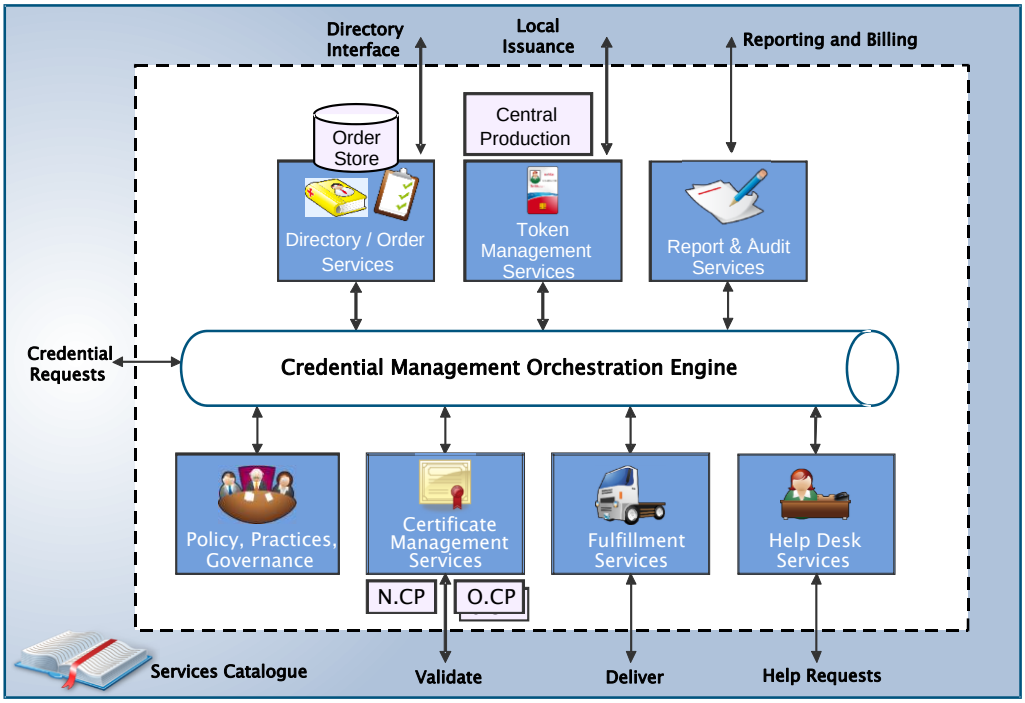
The NASH solution is based on the establishment of one or more accredited Certificate Authorities which are responsible for managing the life-cycle of Individual and Organisational credentials. Establishing nationally accredited Certificate Authorities results in the following improvements over the current state of authentication services commonly used in the heath sector in Australia:

- Higher assurance levels on credentials issued, allowing wider and greater business use
- A nationally endorsed solution reduces complexity, promotes interoperability, and makes authentication services straightforward for users to understand and use
- Supports the end state of a single identifier for all healthcare professionals and users
- Cost savings through common provisioning of services
- Improved availability, accountability and auditability of services
- Provides both a source for nationally recognised credentials, whilst at the same time allows local Certification Authority's to manage their own credentials independently without having to undergo onerous compliance programs.

The NASH solution is defined in terms of the following elements:

- Credential Management Orchestration
- Policy, Practices, Standards and Governance
- Directory/Order Processing Services
- Certificate Management Services
- Token Management Services
- Fulfilment Services
- Reporting & Audit Service
- Help Desk Service.

These elements are shown in the following diagram and are explained in following sections.



N.CP = National Certificate Policy
O.CP = Organisational Certificate Policy

Figure 6 -Overview of the NASH solution

4.4.1 NASH Technical Services Catalogue

The NASH should establish of a set national infrastructure services intended to be used by healthcare provider organisations and e-heath infrastructure service operators. The relying parties may utilise NASH services to find and validate NASH credentials, and could include:

- Access control systems
- Client server applications
- Enterprise applications
- Identity management systems
- Messaging applications
- Operating systems
- Single Sign On
- Web applications
- Web services applications.

NASH services that are intended for external users are defined in a NASH Services Catalogue. These services should provide a point of abstraction that shields users from the intricacies of complex credential and token implementations. That is, users should see the implementation of NASH as a 'black box' with which they transact, via these services.

The key services defined in the NASH Technical Service Catalogue are listed below.

4.4.1.1 Credential Management Administrative Services

Credential Management Administrative services are management services that should be provided in support of key issuance and key recovery processes.

Service Name	Description
Archiving	This service allows a user to save a copy of their private keys to a secondary repository. This allows a user to recover from the loss or damage to a token that has destroyed their credentials/keys.
Cross Certification	This service allows the national Certification Authority to digitally sign the public key of a subordinate Certification Authority, i.e. one belonging to a healthcare service provider.
Certificate Issuance TLS certificates	This service requests the generation of a Transport Layer Security (TLS) certificate to be issued for an authorised domain name, i.e. www.nehta.gov.au. TLS certificates are necessary component of the NEHTA secure messaging security strategy.
Escrow	This service supports the copying of the user or entities private encryption key to be securely stored under an industry wide escrow public key
Escrow Key Recovery	This service allows an escrowed key to be retrieved and allow it to be passed in clear (to a secure token) or encrypted (under a key controlled by the owner of the key)

4.4.1.2 Credential Management Operational Services

The Credential Management Operational Services (see table 2 below) should identify the daily key management services and activities that would be requested or expected of the national Certification Authority and the Card Management System.

Service Name	Service Description
Certificate Issuance Request	Service initiates the generation of a digital credential/token from the national Certification Authority. Other parameters in the request will determine what type of key, where the key will be generated, what type of token, or no token if soft token selected.
Certificate Revocation Request	Service request to revoke a certificate/credential. CA will update the Certificate Revocation list. Note: that some services will be bundled together so that the revocation due to a lost card will also trigger a request for new credential to be issued.
Certificate Renewal Request	Service requests will typically be performed automatically by the system, i.e. reissue credentials a predefined period of time before the old credentials expire. Other automated service requests may also be defined within the CPS
Token Issuance request	Service that allows an authorised user to request a token. The token must at some point in time have a credential provisioned to it. Users will also use this token for other local services.
Token Revocation Request	Service allows a token to be reported lost or stolen. All credentials known to be on the token will be revoked. This transaction can be linked to a

Service Name	Service Description
	provisioning service request that will attempt to replace any credentials the CMS controls or knows about on another token.
PIN Generation	Service that allows the generation of a pin to unlock a set of credentials or tokens
PIN Reset	Service that allows a pin on a token to be reset to a known value
Load Application	Service that allows an application to be loaded onto a token
Update Application	Service request that allows an application to be updated on a token
Key Certification	Service that allows a user or entity to submit a credential for certification by the Certification Authority

4.4.1.3 Directory Services

Additional support services or interfaces will need to be developed for the management of directory information and services required for the identification and validation of credentials (see table below).

Service Name	Service Description
Directory Lookup	Service to support access to the credential directory to identify the public key associated with a Healthcare Provider Identifier Individual (HPI-I) or Healthcare Provider Identifier Organisation (HP!-O).
Validate Certificate	Service that queries the current status of a credential
Validate Token	Service that queries the current status of a token

4.4.2 Credential Management Orchestration

4.4.2.1 Credential Management Orchestration Engine

The credential Management Orchestration engine (cMOE) should manage and co-ordinate all activities from the different services, devices and systems to provision credentials. On receipt of data or service requests (e.g. from the Relationship Organisation), the cMOE will refer to business and policy rules to validate the request and to identity the actions needed to be performed to complete the request. Service requests can initiate credential provisioning either centrally or remotely. Each delivery channel will entail the orchestration of different services to satisfy the request. The cMOE will manage all requests.

The cMOE should also be capable of providing different services for different organisations, i.e. use of different branding, logos and support numbers on the card. Business logic within the system may also order different cards based on system parameters, service configurations and service level agreements.

The Certification Authority Repository should store a copy of the enrolment data necessary for the delivery of credentials in a secure and private data store. Individual or organisational private data (i.e. secret questions, or passwords) will only be used to authenticate credential holders accessing the help desk or Card Management System, usually to assist in authenticating users when they have lost or forgotten their credentials.

4.4.2.2 Enrolment Administration

An enrolment role will be able to submit organisation digital credential requests on behalf of a Community of Interest (COI). For example, the Organisation Maintenance Officer role (OMO) holders that operate within the HI Service would be able to add, retire and manage Organisational Identifiers and credentials. They would be able to request digital credentials for organisational processes (e.g. a web service end point) and individuals (e.g. an employee).

4.4.3 Policy, Practices and Governance

4.4.3.1 Governance Operations

A NASH Governance entity will be responsible for all aspects of NASH as described in Section 4.3.1.

The governance organisation must address technical and business context as well as legal and policy issues of relevance for understanding, specifying and deploying eHealth systems.

Where the Governance organisation is a separate legal entity to the organisation that operates the eHealth Root CA, this organisation should enter into a contract that defines the policies under which the eHealth Root CA operates. Under this contract the eHealth Root CA should be required to sign nationally accredited CA certificates when requested to do so by the Governance Organisation.

A working relationship between the NASH Governance entity and any implementation partner organisations should be developed so that a common understanding or a shared governance model is developed that will provide a complete overview of the eHealth initiatives.

All parts of the governance organisation should have written and agreed terms of reference that are reviewed periodically to ensure that changing needs are understood and addressed and are still relevant.

A Governance and Privacy Management Framework should underpin the operations of the NASH program within the Australian health sector. Responsibility for governing the service will rest with three main bodies:

The NASH Governance entity should set the strategic direction for the national authentication service, define expectations for the establishment and operation of the service, define performance standards and oversee the creation or amendment of certificate policies. The Governance entity should devolve responsibility to subordinate bodies and organisations to act on its behalf. The Governance entity would need to determine the appropriate future ownership of the Root Certificate Keys, upon which all other keys and credentials are trusted.

The Policy Management Authority (PMA) should formulate new policies or change existing policies and should ensure that revised policies are implemented. A formal constitution for the PMA should be provided to set out the functions and operating procedures.

The PMA will provide Service governance for NASH. Service Governance covers the broad range of activities required to maintain operations of the service. Some of the key areas are policy management, operational funding and liability management.

A Management and Oversight (M&O) function should perform day to day management of the NASH services through the provision of administrative, technical and policy support to the Policy Management Authority. This should include maintenance of certificate policies, standards and criteria. It should administer and oversee any contracts with external service providers such as:

- Administer and oversee any contracts with external service providers

- Develop an accreditation program to allow commercial suppliers of authentication services to be nationally recognised.
- Develop an accreditation program to endorse the participation of suitable local authentication services in the national eHealth authentication environment.

Management of operational liability is an area which will require careful governance controls to be in place. For example, if credentials from one community of interest will be recognised and used by others, it will be important to have clarity on where service and usage liability will rest.

4.4.3.2 Policies and Procedures

The success of the NASH Program operations will be largely dependent upon the development, implementation, awareness, acceptance and compliance with robust and well-written support documentation. Adequate and appropriate policies will be required very early in the development process.

The NASH should develop a document framework that will identify what optional and mandatory documentation should be developed and maintained. The document management framework should include processes and procedures for the management and review of documents within the framework.

4.4.3.3 Binding Identity

The binding of a NASH approved token to the rightful individual or organisation should be achievable in two ways:

- The first binding method should allow an HI Service issued identifier to be included inside of the token/credential
- The second method of binding identities to credentials should allow an existing DHS Medicare Australia (or other Gatekeeper accredited) credential to be linked to an identifier via directory services. This method would require a token/credential holder to perform a directory inquiry of the token/credential registry to determine the validity and binding of the token/credential with the identifier. Implementation of this solution would mean that ~70,000 plus credentials issued by DHS Medicare do not have to be reissued.

4.4.3.4 Legal Framework

The legal framework for communities of interest PKI should be contractually based. Legal relationships are between known but legally distinct entities, suitable for governing through formal written agreements. These should include Subscriber Agreements and possibly agreements between the Root CA and issuing CA(s), and CA/RA Agreements. This would be dependent on the registration model and whether the Root CA and issuing CA(s) are the same legal entity.

Registration Authorities would be greatly assisted if core legal documents with model contents are centrally developed and then used to provide templates. The templates should allow quick and efficient operational deployments with a robust and appropriate legal framework in place.

4.4.3.5 Service Levels

Service Level Agreements (SLAs) should define a common understanding about services, priorities, responsibilities, guarantees, and warranties between NASH and eHealth participants. Each area of service should have a "level of service" defined. The SLA should specify the levels of availability, serviceability, performance, operation, and may include other attributes of the service. The "level of service" should also be specified as "target" and "minimum", to inform participants of what to expect, while providing a

measurable average target value that shows the level of organisation performance.

The "agreement" should relate to the services the customer receives, and not how the service provider delivers that service. SLAs should be put into place for all entities that provide NASH related eHealth services to healthcare and allied communities. This should include SLAs for response times, availability for key certification, helpdesk response, vendor support, token supply, provisioning, or enrolment. Certification authorities and subordinate certification authorities should also put into place agreements covering the minimum service levels each will provide.

The NASH Governance entity should be responsible for establishing the initial SLAs for the national Certification Authority and helpdesk services. Other participants would negotiate their own SLA's with NASH service providers.

4.4.3.6 Business Continuity

Business continuity should be designed to ensure that critical business functions will be available to jurisdictions, communities of interest, healthcare professionals, organisations, vendors and customers that have access to those functions even when the technology fails or is unavailable.

The development of eHealth systems and services reliant on digital credentials or assertions will impact or potentially even stop business or eHealth services should central services not be available. The training, education and vendor support should reinforce the need for Business Continuity Planning in the development of any solution that uses digital credentials or encryption to ensure fall back processing options exist where appropriate.

The foundation of business continuity should be the policies, guidelines, standards, and procedures implemented by NASH, jurisdictions, communities of interest and organisations Technical aspects will be covered by disaster recovery plans.

4.4.4 Identity Management Services

The Identity Management Services should manage the authentication of all movement of data from the HI Service (or other Trusted Data Sources of Identity Data) into a secure data store. The order store should also be responsible for the replication of data to other repositories both within the national Certification Authority and to the Relationship Organisation.

The Relationship Organisation should provide all of the information necessary for the provisioning of credentials, including personal details such as user name, address, contact numbers and may also contain answers to security questions, if required. The answers to security questions would be registered with the order store and would be used when users needed to contact the help desk, or when interacting with the Card Management system when they do not have access to their credential. This would typically be used when users were requesting either an emergency or replacement credential.

The order store would also be used to manage other data that is provided over time as users interact with the Card Management system e.g. order additional services, cards, tokens, maintain history of user credentials.

4.4.4.1 Relationship Organisation

The following provides a brief overview of the Relationship Organisation process that will feed information to the provisioning service.

On receipt of an enrolment request and associated data the Relationship Organisation would validate that the data is complete i.e. all mandatory fields are completed.

The Relationship Organisation may collect additional information from the requester so that the national Certification Authority or the Card Management System can action the credential provisioning request. The credential request process should determine if the requester has an existing token or credentials that can be reused (and bound to their HPI-I) or if online or central provisioning of a new digital credential is required.

The Relationship Organisation enrolment data and provisioning service requests should be forwarded to the credential Management Orchestration Engine (cMOE) for passing to the Directory/Order Processing Services.

4.4.4.2 Provisioning and De-Provisioning

The Directory and Order Processing Services (DOPS) should also be responsible for the replication of necessary data from other repositories including national Certification Authorities, the Relationship Organisation and other trusted data sources. As such, automated provisioning and de-provisioning of credentials and tokens would be achieved.

For example, the order store would contain the results of a provisioning request that was initiated through the cMOE for a local credential to be loaded onto a nationally issued token. As a result of a directory change (user being removed) within the local context, the change would be pushed to the DOPS, which in turn would instruct the card management system to remove the credential from the token upon next presentation.

4.4.5 Certificate Management Services

4.4.5.1 Authentication Hierarchy

The following diagram illustrates an indicative authentication hierarchy that should be used to deliver the trust network required to support the NASH.

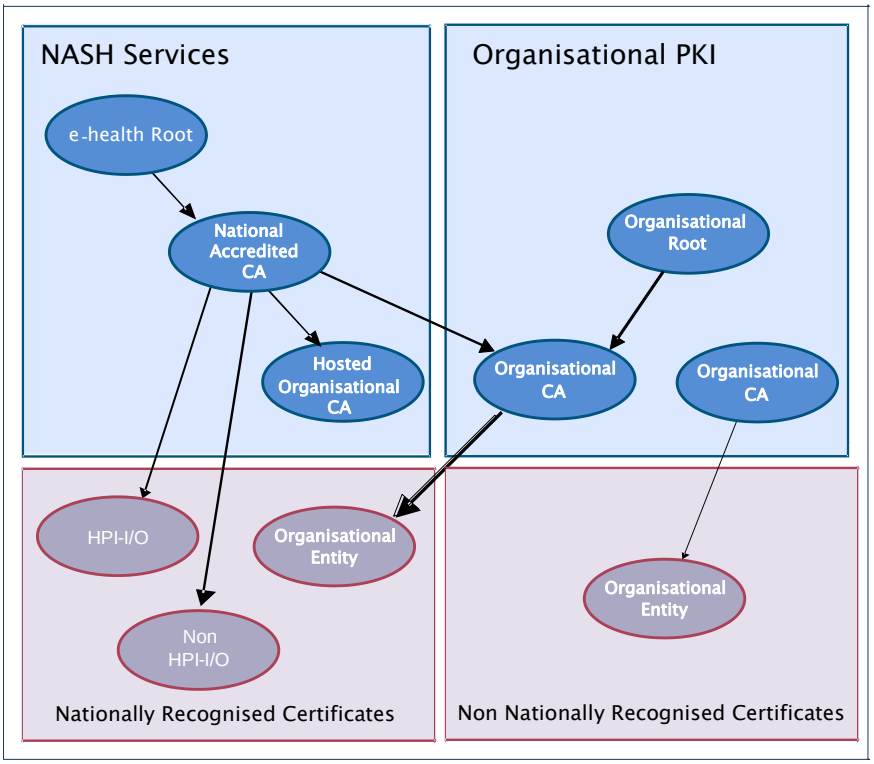


Figure 7 - Indicative PKI Hierarchy

Pivotal to the hierarchy should be an eHealth Root certificate. It would be the trust anchor for all nationally recognised digital credentials. The eHealth Root would be available to cross certify any National Certification Authority, which

would then be available to cross certify Organisational Certification Authorities provided these Certification Authorities meet the criteria for entry as defined by the NASH Governance entity.

A national Certification Authority may provide Certification Authority hosting service(s) whereby a health organisation can have a logical Certification Authority established within a National Certification Authority's service boundaries and still maintain control of the credentials it issues.

4.4.6 National eHealth Root

A National eHealth root key is the anchor for all certificates/credentials issued by subordinate Certificate Authorities. It will therefore be relied upon by all organisations involved in eHealth in Australia.

The eHealth root key is, however, an asset that must be "owned" by one organisation. Stakeholder organisations therefore need to be satisfied that any risks that result from having a dependency on the organisation that owns the eHealth root key are managed.

The result is that the organisation that "operates" the e-heath Root CA should ensure that the eHealth root key is (and continues to be):

- Fit for purpose
- Available when required
- Secure
- Used only in accordance with appropriate policies (which only change by mutual agreement).

In the NASH target state, these requirements would be satisfied by requiring the organisation that "owns" the eHealth root to use and manage it as a service provided by it to the NASH Governance Organisation under a binding legal contract.

4.4.6.1 Acceptance of the eHealth root

In order to promote acceptance, and secure the eHealth root the Governance Authority should maintain ultimate responsibility for the eHealth root. This would involve:

- Establishing a Governance entity to assume responsibility for the governance of the root certificate
- Stewarding the process of contracting a suitable service provider to become the "service operator", who securely holds and maintains the eHealth root
- The Service Operator should commence service operations as soon as practicable.

4.4.7 Certification Authorities

A Certification Authority is responsible for everyday certification processes. A Certification Authority's public key would be signed by the eHealth root key.

The certification (or recognition) of the eHealth root by a trusted Commercial Certification Authority would allow a Certification Authority to issue any certificate type it requires and should allow it to authorise subordinate Certificate Authorities to do likewise. This would allow a Certification Authority or subordinate Certification Authority's to issue web service certificates. This would assist in providing trust to healthcare workers when accessing health care sites.

The signing of a Certification Authority's keys would provide a trust chain down to any credential issued. This would also allow transport level (SSL etc.)

certificates to be provisioned by Certification Authorities or sub-ordinate Certificate Authorities to support web site trust.

While a national Certification Authority's primary responsibility is the provisioning of Individual or Organisational credentials it should also be capable of issuing additional credentials that local jurisdictions or the eHealth sector may require.

4.4.8 Hosted Certification Authorities

A national Certification Authority may provide a hosted Certification Authority service. This would allow communities of interest (COI), jurisdictions or health organisations to have a hosted subordinate Certificate Authority established to meet their own specific needs.

The primary benefit of a hosted Certification Authority service would be that entities will manage their own credentials without having to build and operate their own secure PKI systems.

A hosted Certification Authority service may also appeal to organisations who no longer wish to host their own Certification Authority but still want to utilise any credentials or services that a local Certification Authority once offered.

4.4.9 NASH Healthcare Identifiers COI Hierarchy and Terminology

"Relationship PKI" is a relatively new approach to digital credentials intended for use only within a defined Community of Interest (COI). By restricting certificate usage to an established context, under existing business rules and liability arrangements, all problems of cross-recognition and standardising levels of identity proofing disappear.

The total cost of ownership is greatly reduced, registration processes are streamlined, and legal complexities eliminated. The Relationship Certificates are still regular X.509 public key certificates, processed and maintained as usual, but instead of being interpreted as vouching for the identity of the subject, they are used to assert a specific relationship, which is embodied through the use of a Healthcare Identifier between the registering entity and the subscriber.

Gatekeeper accommodates Relationship Certificates in the "Special Purpose" category. To distinguish Relationship Certificates from orthodox "General Purpose" Identity Certificates, Gatekeeper coined the term "Relationship Organisation" (RO) for the entity that enrols subjects in the COI, typically issuing them with a unique reference number. In the case of the initial NASH COI, this is a Healthcare Identifier issued by the HI Service. The RO is similar in function to a conventional Registration Authority (RA) except that under Gatekeeper, the RO follows enrolment protocols that are specific to the COI, and so the NASH Relationship Certificates should not be used outside the Healthcare Provider COI.

According to the Gatekeeper Relationship Certificate Guidebook:

> Relationship Certificates are issued to Clients of a Relationship Organisation according to business rules local to the Community of Interest (COI) and are intended for use in applications only within the same COI.
>
> They are a departure from historical Gatekeeper identity certificates. The real world experience of PKI, includes the fact that successful PKIs tend to be "closed" and therefore subject to localised business rules rather than global identification rules. Relationship Certificates will be easier to obtain and deploy, and will be better matched to their

intended applications, meaning that PKI enabled software should be easier to use.[13]

A Relationship Certificate issued within a COI and bearing a certain identifier means nothing more and nothing less than the fact that the Subject is associated with that identifier, under the auspices of the Community Rules.

NASH certificates specifically convey the fact that a healthcare provider has been issued with a unique Identifier by the HI Service which informs the Relationship Organisation. The possession of an NASH certificate allows the subject to assert their HI in eHealth transactions, according to the provisions and sanctions of the Healthcare Identifiers Act.

4.4.10 Subordinate Certificate Authorities

Subordinate Certificate Authorities would be operated by an organisation provided that it has entered into a subordinate trust relationship with a national Certification Authority. This trust relationship would then extend to all credentials that they issue.

The use of Subordinate Certification Authorities would allow organisations to manage their own credentials but to have these credentials recognised as being issued from the jurisdiction. This may be used for the issuance of new credentials or for the maintenance of existing credentials typically to support local systems. In general, entities would seek to be subordinate only if they wish credentials they issue to be recognised outside of their own domains. Subordinate Certificate Authorities should meet defined security criteria based on the level of assurance/recognition they are seeking for their credentials.

4.4.11 Assurance Levels

All NASH credentials should be capable of being bound to a NeAF assurance level at the point they are utilised in an eHealth software application.

Assurance levels are determined on the security controls and relationship that the credentials were issued under, and should be consumed under.

Assurance levels are defined based on the security controls and EOI that the credentials were issued under. There are four NeAF levels ranging from low to high. A minimum security and compliance program should be developed for each assurance level. The binding of an assurance level to a credential would allow the relying party to decide if the level of assurance of the identity is sufficient for the application or service they offer.

One of the major benefits in using assurance levels is that different Certification Authorities can continue to be built and deployed based on their own local security needs.

4.4.12 Secure Token Service

A Secure Token Service (STS) would, on authenticating a user's credential, issue the user with a security assertion that could be used in one or more local or national eHealth systems or services. Assertions may be valid for a period of time similar to Kerberos tickets, and may also be used to pass additional information, or less information, to a service. Enabling an anonymous logon to an eHealth system would be an example of an assertion allowing a session to be authorised without passing the system user details.

A Secure Token Service could be established under a subordinate Certification Authority to operate inside or outside of the NASH defined PKI infrastructure. Given the need for high availability such a solution maybe more suited being

[13] Gatekeeper Relationship Certificate Guidebook, Executive Summary, AGIMO, 2009.

placed within two or more jurisdictional data centres. This would provide greater distribution and place services close to some of the main user groups. The need for a Secure Token Service should be reviewed as part of the National Security Access Framework (NESAF) program.

4.4.13 Policy

The eHealth Root and national Certification Authorities should have a comprehensive suite of policy, legal, operational and technical documentation. These should be based on industry best practice and compliance with the Gatekeeper model, and should consist of at least the following:

- Certification Practice Statement
- Certificate Policy and/or PDS for each type of certificate published
- Subscriber Agreement
- CA/RA Agreement
- Root CA/CA Agreement if issuing CA(s) and Root CA are distinct legal entities
- Privacy Policy and Privacy Impact Assessment
- CA Operations Manual (unless CA is already in existence and has documentation in place)
- Disaster Recovery and Business Continuity Plans
- Security Profile: the exact contents will vary depending on whether an existing accredited CA is leveraged but some combination of the following may be needed:
  - Security Policy
  - Security Plan
  - Threat and Risk Management
  - Key Management Plan.

4.4.14 Certificate Policy & Certification Practice Statement

PKI activities performed by Certification Authorities should be governed by the rules and statements defined in the Certificate Policy and their Certification Practice Statements. Together, these two documents define the operational framework of the Certification Authority.

- The Certificate Policy specifies what a credential is used for and the liability assumed by the Certification Authority for this use
- The Certification Practice Statement specifies the practices that the Certification Authority employs to manage the credentials it issues. It describes how the requirements of the certificate policy are implemented in the context of the operating policies, system architecture, physical security and computing environment of the organisation. For example, a certificate policy may specify that the private encryption key can be exported, in which case the CPS describes how this is accomplished.

From time to time, new or changed certificate policies would be required to meet changes in the eHealth environment. Certificate Policies describe:

- The types of digital credentials to be produced under NASH services
- Any hardware used to store digital credentials and their associated keys
- The process for enrolling to obtain digital credentials.

In addition, the Certificate Policy would reference supporting PKI documents such as the Certification Practice Statement, any PKI disclosure statements and any agreements between parties in the service.

4.4.15 Directory services

As part of the NASH service a Health PKI Directory or 'X.500 white pages' should be provided. This service should be designed for wide availability. The directory should be available on the Internet and include a copy of all active credentials and public keys.

Relying parties can browse the directory by searching on key words or utilise software to automatically retrieve required credentials for use. The directory service will support the establishment of a publishing and access controls regime that will enable communities of interest to control what information is published and what information is available to whom, i.e. communities of interest may restrict access to its credential to members of the communities of interest only.

A set of standard practices should be provided to allow relying parties to determine if a digital credential has been revoked. The directory services should support the use of Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) responders.

A Digital Certificate Directory Interface will allow relying parties to retrieve a set of one or more digital credentials from the directory based on given search criteria (e.g. the name of the digital credential holder or a digital credential identifier).

Directory services should include:

- The provision and maintenance of Certificate Revocation Lists (CRLs)
- Digital Credentials, current and expired
- Online Certificate Status Protocol (OCSP) Responder
- Lightweight Directory Access Protocol (LDAP) and Hypertext Transfer Protocol (HTTP) to support system or application queries
- Additional information related to the individual, entity, or organisation.

Sub-ordinate Certification Authorities that are not hosted within the NASH PKI would need to provide directory and certificate/credential revocation service for any credentials they issue, though it may be possible for these services to also reflect their directories up to the National directory.

As web authentication, authorisation and identity framework standards mature the NASH Governance entity will be best placed to respond to the needs of the Australian health sector and deliver on its stated objectives through its advisory committees and service governance model.

The NASH Governance entity would identify relevant standards and inter-operability touch points for use of credentials and will deliver recommendations and national services where required to facilitate broad use of NASH endorsed credentials in relying party systems.

The use of multiple certificate authorities within eHealth will benefit from the federation of all of the relevant directories, i.e. all Certification Authorities post to the same CRL and directory site.

4.4.16 Certificate Revocation

Certification Authorities should be responsible for providing certificate directory services, this includes Certificate Revocation Lists (CRL's) which need to support multiple query types to support automated application validation processes, manual user validation and partial and full directory replication.

4.4.17 Key Generation

Key generation would be performed by National Certification Authorities, Subordinate or Hosted Authorities or it can be performed on the token itself, if it provides the functionality.

Certification Authorities would also issue soft tokens. The keys associated with soft certificates will normally be generated by the National Certification Authority and delivered via post on CD, DVD or memory sticks. An alternative solution would be to provide a mechanism whereby users can securely generate their own key pair and have their public keys signed by an online service. This would improve the speed of delivering credentials and provide greater assurance that the credentials have not been tampered with or copied whilst in transit.

The private keys on soft tokens are able to be copied so are not as secure as keys held in a secure token. A PIN key to the unlock token, which is delivered separately from the token, should be used as this improves the delivery security of the token. Alternatively the use of SMS messaging to deliver a PIN or PUK (Personal Unblocking Key) to a customer where possible would improve the security, cost and speed of enabling access. The possible use of one time challenge responses which require an SMS password each time keys are copied would also reduce the potential misuse of tokens.

4.4.18 Token applications

Applications on a token would provide a means of tailoring the functionality of the token so as to provide a business function to the token holder. The main application that the NASH would provide on its tokens is an electronic identity application that supports the storage and use of digital credentials for the purposes of establishing the token holder's identity electronically.

4.4.19 Escrow/Key Archiving

A key escrow or key archiving solution capability should be provided. This would allow private keys used for encryption to be recovered should a hardware token be lost or become inoperable.

The Governance Authority should define when and where key escrow and key archiving would be allowed to be used, and would set the minimum standards and guidelines for the recovery of keys. Key recovery would need clearly defined authorisation processes and audit trails.

The validation of digital credentials maybe required long after keys have expired, to support a legal position or action. A long term archiving solution should be provided that allows healthcare workers to validate expired digital credentials on historical documents or transactions. Archival services also support escrow service archiving. Archiving services would:

- Have clear guidelines on the duration that keys are retained. This may include different time frames for online and offline storage
- Processes and authorisation regimes for the retrieval of archived keys
- Index services to identify archived keys.

4.4.20 Password Protected Credentials (PPC)

A password protected credential should be encoded in a PKCS#12 file. The length of the password used should be in accordance with Information Security Manual (ISM). The Password Protected Credential (PPC) can be delivered by mail on a CD or using an electronic means that provides equivalent confidence in the identity of the recipient. An example of this is via a browser based online registration process, where the recipient has proven their identity to the issuing system.

The PIN should be delivered separately to the PPC itself. For example it may be mailed in a separate envelope on a separate day so that the interception of one day of mail delivery will not result in both the token and the PIN being lost.

4.4.21 Soft Tokens

A soft token consists of keys stored on a device that is readable or accessible, i.e. stored on an electronic media such as a DVD or memory stick. Organisational credentials may be issued as soft tokens to allow keys to be shared between multiple systems or users. All soft tokens would be protected by a PIN to provide a level of security over their misuse or duplication. The movement to electronic delivery of soft tokens or local generation of soft token keys should provide cost savings over the traditional physical delivery methods and their associated costs.

4.4.22 Token Management Services

The token and smart card architecture should support the existing DHS Medicare customers, as well as new communities of interests (e.g. jurisdictions). The primary difference between these two areas is that DHS Medicare has been an early adopter of smart card technology, while many jurisdictions are still 'green field' sites.

Credentials should be made available in a variety of standard forms and formats to suit different business environments and needs. The types of credentials that will be available include the following:

- Tokens (including Smart cards)[14]
- Password protected credentials (i.e. soft tokens).

4.4.23 Token Standards

The NASH should provide a catalogue of approved tokens, interfaces and protocols that are endorsed, in order to promote interoperability. A choice of tokens should be offered to match the predominate needs of token holders.

The initial tokens in the catalogue should include both Contact smart cards, Dual Mode (Contact plus Contactless) smart cards and USB PKI tokens.

The underlying architecture for the NASH should be extensible to support installation of certificates in other suitable devices over time. As an example, this may include mobile devices with an appropriately secure credential store capability, and appropriate communications capabilities to interact with those token readers that are suitable for healthcare settings.

4.4.23.1 NASH Compliance Standards

In order to promote the wide usability of tokens by clinical host systems NASH has selected a basic suite of standards or industry specifications for smart cards. These standards selection should be updated over time, to cater for change and adoption of market technologies.

Initial guidance for suitable token standards for eHealth purposes should be provided in the following areas:

- Security Assurance Standards
- Digital Certificate Interface Standards
- Supported Token Catalogue

[14] Smart cards issued to healthcare workers to hold their personal credentials, used logging on and digital signing.

  - Accepted Card Types
  - Smart Card Token Standards – Physical / Logical
  - Smart Card operating Systems
- Card Management Standards.

The development and adoption of global standards that will replace many proprietary standards will provide greater interoperability. Two standards that are foremost in achieving this are ISO/IEC 24727 and "GlobalPlatform".

- ISO/IEC 24727 is relatively new but is quickly gaining global acceptance. ISO 24727 is a new token standard that provides a complete Application Programming Interface (API) that covers both management of the applications and data on the card and the operational use of the card assets. It also provides a comprehensive authorisation and access control model for a token that enables access to the card assets to be controlled at a fine grained level. This will enable the card to be a common repository of potentially unrelated and increasingly diverse applications and data without compromising their security and integrity.
- GlobalPlatform is a more mature product having been around for a number of years; it has high vendor take-up, support and adoption and has achieved good market penetration. It is recognised that global adoption of these standards will drive down the costs and provide interoperability between vendor's products.

Adoption of new standards by NASH and the Australian eHealth sector will depend on the widespread acceptance and support by card vendors and software platform developers.

4.4.24 Card Management System

A national Card Management System should function as the core of the smart card/token system. It would require connectivity and interfaces with all other system components. It should house the central cardholder database that supports the capture, storage, retrieval, retention, integrity and management of data necessary for the Life Cycle Management (LCM) of tokens. LCM includes: pre-issuance, issuance, status, replacement, renewal, post-issuance capabilities and audit of smart cards/tokens.

The deployment of a national Card Management system will allow both national and local credentials and applications be managed on the same token.

Functions required of a Card Management System include:

- Integration with card issuance and personalisation services
- Web based customer service User Interface
- Out-of–the-box tool for viewing and managing the content a smart card, with appropriate access controls
- Support for two modes:
  - Customer service agent, which can view and manage any smart card, subject to access controls policies; and
  - Cardholder mode, for self-service management over the internet, of only the cardholder's card.

The deployment of standard token types may allow jurisdictions and local certification authorities using these cards to continue to use support services defined for national cards, i.e. be capable of managing cards via the National Card Management Systems and use the NASH compliant software and drivers.

4.4.25 Digital Certificate Interfaces

Digital credentials would be held either on an approved hardware token or directly in the software based credential store of a system, e.g. Windows desktop, gateway server, common digital credential stores such as Microsoft's System Certificate Store, Java Key store and Netscape's Security Services (NSS) Certificate Store.

4.4.26 Delivery Channels

The PKI infrastructure should be capable of supporting multiple delivery channels. It should allow users to submit credential and token management requests via telephone, SMS, mail, email or via remote web interfaces. Delivery channels should be capable of supporting both ad-hoc requests and bulk requests.

4.4.26.1 Bulk Issuance

The NASH should support large scale distribution of credentials (from several hundred to tens of thousands at a time) via bulk issuance requests from jurisdictions, communities of interest or larger organisations. Typically bulk issuance would be in response to projects or new developments.

Bulk issuance would utilise central distribution services to manage production and any personalisation or token branding. Bulk issuance would be able to deliver large quantities of personalised credentials more cost effectively than local Certification Authorities.

4.4.26.2 Local Issuance

Some communities of interests may wish to issue their own credentials from a standalone Certificate Authority. These entities would not require their credentials to be recognised by any entity or system other than their own. Local Certification Authorities can load their credentials onto NASH sponsored hardware tokens.

The local issuance of credentials may be able to utilise the Card Management System to assist in the management of their credentials if they are on a NASH token known and managed by the CMS.

4.4.26.3 Self Provisioning/Remote Issuance

Users with access to NASH compliant tokens should be able to utilise remote or self provisioning capabilities offered by the national Certification Authority/Card Management Service. Users would authenticate to a web service to allow credentials to be generated or loaded onto their token. Credentials would be digitally signed by the national Certification Authority.

The ability to provide remote provision or self-provision would be dependent on the availability of tokens within an organisation. Inventory management and automated ordering capability should be managed by the National Certification Authority/Card Management System. This would ensure that organisations have a ready supply of spare tokens available. The inventory management system may also suspend lost and stolen tokens and revoke and assist in the reordering of any credentials the system knows about on the token.

Authorised organisational representatives should also be able to remotely provision additional organisational credentials for use in gateways, devices, applications or provided to employees/roles. Organisational credentials would be able to be directly downloaded from the national Certification Authority or will be generated on the local system and be digitally signed by the national Certification Authority.

Self-provisioned credentials/tokens would be distributed either with generic branding, or with partial organisational branding. Post implementation text or graphics printing will allow tokens to be further personalised.

4.4.27 Fulfilment Services

4.4.27.1 Card Readers

Token readers should be provided by the NASH to support the deployment of tokens. The most likely scenario is for the provider of the token/smart card to also ensure that users have a USB PKI token, or have a smart card reader available.

Some jurisdictions may provide keyboard or other integrated smart card readers, including contactless readers. Some communities of interest or small groups of users may also wish to use a combined biometric/smart card reader for enhanced authentication and identification.

4.4.27.2 Token Replacement

The replacement of a token may be due to reissue, loss or because a user has left it at home, all of which may require immediate action to rectify the situation. The ability to re-establish all users' credentials is vital to enable users to return to full service.

The national Card Management System should be used to track and manage the credentials assigned to users. Where a national Token is not available then the replacement of user’s Individual credentials would need to be performed using either a self-service portal or a service desk assisted transaction. The Card Management System should only replace credentials it is aware of and has control of.

4.4.27.3 Personalisation

Smart card or token personalisation should be completed within the national Certification Authority (issuance point), or locally within an organisation depending on the issuance capabilities of the organisation and the level of personalisation required. Issuance points should provide:

- Initial smart card or token setup with defined configurations and applications
- Graphic printing directly on to smart cards or tokens, with details such as the name of the holder
  - Exact personalisation requirements will need to be defined and agreed for each issuing entity. Organisational issuance points will not require a printing capability if they only issue temporary cards.
- PIN mailer or SMS services if delivery of token PIN will be supported.

4.4.27.4 Branding

At a minimum, branding is essential to protect the copyright or registration of logos and other imagery devices. It may also be necessary to register patents if unique ideas are involved.

A central order and provisioning service should be established so that organisations can order tokens with their individual branding. In addition cards required through the central CA may be personalised to meet their communities of interest's requirements. This may include name, or logos required.

Consideration should be given to adding both the organisation approved and NEHTA approved logos to identify cards, application or system as secure and certified as being authentic. A logo may help raise user's security awareness and trust in the products and services to use or not to use.

4.4.28 Reporting & Audit Services

4.4.28.1 Reporting

The NASH solution should provide reporting capability to help assist in determining trends and performance levels so that Service Levels will accurately be measure. Reports would typically go to stakeholders and executives including the M&O and other governance bodies.

The NASH systems may provide additional data to support external billing and management reporting systems.

4.4.28.2 Compliance

NASH should develop compliance programs to measure and monitor NASH participant's compliance with standards, policies, rules and frameworks that need to be followed. These programs may include:

- Certification Authorities compliance program
- Vendor compliance and accreditation programs
- Subordinate jurisdiction compliance and assurance accreditation programs
- EOI compliance programs.

4.4.28.3 Audit

To demonstrate ongoing credibility and to ensure that key service providers are operating within accepted (and documented) rules, an audit and compliance regime would need to be developed.

The use of a national Certification Authority approach greatly simplifies this process. Downstream the certification authorities would be audited by their own jurisdictions and local audit teams primarily to validate that EOI processes are being followed consistently. The national CA will need to ensure that it complies with national standards and with individual state legislation and privacy laws.

A properly governed PKI should institute regular external audits, generally annually, as well as upon any significant changes to PKI policy or infrastructure. For a Gatekeeper accredited CA the audit will be performed through AGIMO.

4.4.29 Client tools

One of the main issues with credentials is the likelihood that users will be provided with a number of credentials that they will need to manage. The development of tools to facilitate the self-management of credentials on users' tokens will make it easier for credential holders to review and manage their credentials.

Additional tools may be developed to support:

- View credentials and keys on a token
- Export credentials from the token in X509 DER format
- Change of PIN
- Unlocking a card (will require the PIN Unlock Code [PUK])
- The addition of certificates and keys to the card from these file formats:
  - Certificates: X509 in Distinguished Encoding Rule (DER) format or Privacy Enhanced Mail (PEM) format, PKCS#12 DER format
  - Private Keys: PKCS#12 DER format.

4.4.30 NASH Business Services

The following services represent the major conceptual models for orchestration of end to end business services, as seen by the user of those services. It does not cover all possible business services but none-the-less should be reasonably representative of the significant business services. The actual orchestration of the services should be determined in the detailed operational design for the NASH.

The services are described here in in terms of being solely NASH services, for the sake of clarity of purpose for the service concerned. As an integrated services view of eHealth business services develops, each of the NASH business services should be capable of being integrated into a higher level orchestration of similar service components from other healthcare service streams and programs.

As an example, when an integrated support desk for eHealth is implemented, to provide a single point of user contact for issue resolution, the support desk services of NASH should be able to form part of the integrated support desk.

The services are described primarily in terms of those required for the initial Relationship Organisation for the healthcare delivery Community of Interest that is based on national Healthcare Identifiers issued by the HI Service. Similar services would need to be provided within other Communities of Interest which may operate within the NASH Framework, and should be specified at the time those communities come into being.

4.4.30.1 Establish NASH COI relationship for HPI-O

This service describes the process for a Healthcare Provider Organisation to enrol with the healthcare delivery Community of Interest and to receive a NASH PKI credential. The enrolment process is necessary to satisfy the Evidence of Identity for the Community of Interest, which underpins each credential.

- A Healthcare Provider Organisation needs to hold an HI Service *Healthcare Provider Identifier – Organisation* (HPI-O) identifier in order to participate in the healthcare delivery Community of Interest which underpins the NASH.
  - If the organisation does not already hold an HPI-O identifier, an application will need to be made to the HI Service Operator to acquire one. This application will include an option to automatically initiate the process for the issuing of a NASH credential, described below.
  - If the organisation currently holds an HPI-O identifier but has not previously been issued with a NASH digital credential, the organisation will need to make an application to the Relationship Organisation for the credential. This is expected to be in the form of a simple request, as the majority of the information required for NASH enrolment should be obtained by NASH from the HI Service Operator.
- The Healthcare Provider Organisation will need to assign the NASH administration roles within their organisation. The Gatekeeper Framework, suggests that the following titles are used.
  - Authoriser
    - In the normal course of events this role would be assigned to the Responsible Officer that the organisation needs to nominate for HI Service purposes
  - Credential Managers

- In the normal course of events these roles would be assigned to the Organisational Maintenance Officers that the organisation needs to nominate for HI Service purposes.

Digital credentials to identify individuals in the above administration roles will be issued by the NASH. These administrative credentials are intended explicitly for administration tasks associated with national healthcare delivery services, such as the NASH and the HI Service, which the organisation may be engaged with.

The NASH will produce and deliver a NASH credential for the organisation, and administrative credentials as appropriate for the organisation concerned. The organisation credential with be a Soft Token (see Section 4.4.21). Electronic delivery of the Soft Token will be available. The Soft Token can be easily installed into local certificate and key stores that support PKCS#12. Credentials managers will be able to use their administrative credentials to authenticate to the NASH web portal and perform credential lifecycle management functions (e.g. revoke and replace) of the organisational credentials they are responsible for.

4.4.30.2 Establish NASH COI relationship for other known Organisations within the Community of Interest

The service for enrolling other organisations which are known within the healthcare delivery Community of Interest, such as Contracted Service Providers (and any additional roles that may be necessary to support other eHealth programs), should generally be similar to that for HPI-Os.

4.4.30.3 Establish NASH COI relationship for an HPI-I

There is no explicit NASH business service for this, however for the sake of completeness of covering the overall Relationship Organisation approach, the description below covers the method by which a relationship between the healthcare delivery Community of Interest and Healthcare Provider Individuals is established.

- Healthcare Provider Individuals - who have been issued with an HI Service Healthcare Provider Identifier – Individual (HPI-I) - are therefore eligible to receive NASH credentials, following:
  - Registration with at least one of the national Medical Boards covered by the Australian Healthcare Practitioner Registration Authority
  - Direct application to the HI Service Operator, if they are able to satisfy the requirements in the Healthcare Identifiers Act 2010.
- There is no action required for eligible individuals to undergo a further Evidence of Identity process with the CA. Verification of Identity processes are managed by the Relationship Organisation.

The initial general model for this end to end process, which crosses numerous organisational boundaries in the healthcare sector, should be:

- Healthcare Provider Individual registers with AHPRA if eligible, and request NASH token as part of the registration application, or
- Healthcare Provider Individual who is not eligible to register with APHRA but it otherwise eligible under the provisions of the HI Service legislation, applies to the HI Service operator (DHS Medicare) for an HPI-I and request a NASH token as part of the registration application
- AHPRA, or the HI Service Operator, forwards the NASH token request to the NASH Service Operator.
- The NASH Service Operator arranges the timely fulfilment of the token request. This may be through a variety of different methods, depending on the specific circumstances applying to the Healthcare

Provider Individual concerned. These could include physical delivery of a token with certificates for activation or personal collection of token from a local supply held by a point of care, or similar.

- The Healthcare Provider Individual receives the token, and uses a web portal provided by the NASH Service Operator to activate the token in a straightforward manner.
- The Healthcare Provider Individual conducts some simple tests with the web portal to assure that that the token and certificates have been activated.
- The Healthcare Provider Individual is then able to use the token in eHealth applications which have been enabled to utilize NASH tokens.
- The Healthcare Provider Individual will be able to use the NASH web portal to perform self-service functions related to the ongoing management of their token. This includes functions such as resetting their PIN and reporting a lost or stolen token.

4.4.30.4 Credential Management Services for an HPI-I

The following services apply to Healthcare Provider Individuals, and in this case the term credential is used to cover both the relevant digital credentials and the Smartcard token on which they will be issued for the initial production release of the NASH.

Acquisition of NASH credential

At the point in time, when a Healthcare Provider Individual needs to initially acquire NASH Credentials, an order to supply the credentials should be placed with the NASH by the Relationship Organisation. The order is likely to take one of two forms:

- A request from an individual to the Relationship Organisation to supply the credential. It is expected that request should be able to be made through an appropriate electronic channel, such as a web portal, in straightforward way. In business-as-usual scenarios, the request for an initial NASH Credential should be incorporated in the overall healthcare sector registration processes for an HPI-I.
- A policy decision related to a specific eHealth implementation program which would result in a request to supply credentials to a nominated group, or class, of Healthcare Provider Individuals, in order to support operation of a relevant healthcare service or application.

Once the order has been received, the credential will be produced by the NASH and delivered to the individual in a timely manner.

Replacement of a NASH credential

There are three services related to replacement of a NASH credential which has been lost or is damaged.

- Temporarily lost credential
  - This service is intended to cover the circumstance where a credential has been misplaced rather than lost outright, and there is a high likelihood that it can be recovered within a reasonable time.
  - A temporary credential should be issued locally to the individual with a short term expiry, as defined in in the Certificate Policy. For this to occur, local administrative support would be necessary.
  - After expiry, the temporary token should be returned to a local administrator, such as the OMO, for future reuse.
- Permanently lost/damaged credential

  - This service is intended to cover the circumstance where a credential has been definitively lost, or is damaged, so there is no hope of recovery.
  - A temporary credential should be issued locally, as described above, as well as an order for a replacement permanent credential placed with the NASH. When the replacement permanent credential has been received and acknowledged, the temporary credential should be deactivated and the new permanent credential activated.
  - For this to occur, local administrative support would be necessary.
- Scheduled renewal
  - This service is intended to cover the periodic circumstance, where a credential is due to automatically expire in accordance with the Certificate Policy. The NASH should automatically issue a new permanent credential in adequate time to deliver it to the individual prior to it expiry.
  - When the replacement permanent credential has been received and acknowledged, the about-to-expire credential would be deactivated and the new permanent credential activated.
  - This process should not normally require local administrative support, with the acknowledgement and activation being able to be performed through a self-service web portal.

Retirement of an NASH Individual credential

There are two services related to retirement of a NASH credential.

- Automatic retirement
  - If the HPI-I for an individual is deactivated or retired in the HI Service, the associated NASH credential should also be permanently retired.
- Voluntary retirement
  - Where an individual is ceasing to have a use for NASH digital credentials, they should advise the Relationship Organisation. This should be able to be performed through a self-service web portal.

4.4.30.5 Credential Management Services for an HPI-O

In the normal course of events the credentials issued to Healthcare Provider Organisations should not need the same level of services as those issued to individuals. The digital credentials issued to organisations should be able to be backed up and restored through normal Information Technology data management practices. If a digital credential is permanently damaged or destroyed such that it is unrecoverable, the Credential Manager for the organisation should be able to reacquire the digital credential from the NASH.

Retirement of a NASH Organisation credential

There are two services related to retirement of a NASH credential.

- Automatic retirement
  - If the HPI-O for an organisation is deactivated or retired in the HI Service, the associated NASH credential should also be permanently retired.
  - If there is a merger or acquisition of one HPI-O organisation by another HPI-O, the Responsible Officer of the continuing organisation would need to determine which NASH credentials may need to be utilised in the future.
- Voluntary retirement

- Where an organisation is ceasing to have a use for a NASH digital credential, they should advise the Relationship Organisation. This should be able to be performed through a self-service web portal.

4.4.30.6 NASH Credential Management Services

There are two Credential Management Services which are internal NASH processes.

Assurance of delivery at issuance

This service is intended to provide assurance that any credential which has been issued has in fact been received by the intended recipient. This assurance should be satisfied by the recipient performing an explicit action on receipt of the credential which would confirm to the NASH that the credential has indeed been received correctly.

The exact mechanism to provide the assurance may vary depending on the circumstances and policies in place at the time, but should not be onerous and should be able to be carried out through a self-service web portal.

Management of NASH credentials on a non-NASH Token

There will be a need for an additional management service, internal to the NASH, as this capability becomes supported. The nature of this service would be determined at that time.

4.4.30.7 Token Management Services

For the initial release of the NASH, the digital credentials for Healthcare Provider Individuals should normally only be delivered on a NASH token, therefore the management of tokens is congruent with the management of credentials described in section 4.4.30.4.

Management of multiple credentials on a NASH Token

NASH should support hosting of multiple compliant credentials, issued by other Certificate Authorities, on NASH supplied tokens. There will be a need for an additional management service, internal to the NASH, as this capability becomes supported. The nature of this service would be determined at that time.

4.4.30.8 Token Activation

The activation of the NASH credentials on a NASH issued token should be achieved through a web portal service in a straightforward manner. On receipt of the physical token, the token holder, or an appropriately authorised delegate, should use the portal to identify themselves, acknowledge receipt of the physical token and activate the NASH credentials associated with the token.

Where NASH credentials are carried on a physical token issued by another Certificate Authority, the activation of the NASH credentials on the token should as far as possible be consistent with the activation approach described in the above, but in any case should follow a straightforward activation process.

4.4.30.9 NASH Usage Services

This group of services is related to supporting the uptake of the NASH. There are three groups of services, with each group targeted at a different part of the overall community of users of the NASH.

End Users

The direct end users of the NASH are Healthcare Provider organisations and individuals, who will use NASH issued credentials within a growing range of clinical transactions in the eHealth eco-system. While the overall approach to using NASH credentials will effectively be driven by the way that eHealth

applications and systems are designed and implemented, there will be a need for instructional material to introduce the credentials to clinicians, and to provide training for administrative staff in their specific roles.

The business services for this user sector should:

- Deliver User Guides
  - This service should determine the end user needs for information about how to use NASH credentials and tokens.
- Deliver Training Material
  - This service should determine the needs for support staff users for information about how to perform the administrative tasks related to the use of NASH credentials within a Healthcare Provider organisation.

Both services should publish this information in appropriate forms, which may include paper and electronic media, and maintain the currency of the user information as the NASH service develops and as new eHealth applications which require the use of NASH credentials go into production over time.

Developers

Developers of software systems which require authentication credentials within their operations will have access to information about implementing NASH credential support in their systems.

The business services for this user sector should:

- Deliver a Software Development Kit (SDK)
  - This service should create and deliver a range of materials which should support the inclusion of NASH credential capability in application and other software systems. The NASH SDK should include:
    - Sample Source Code organised into appropriately named files to facilitate easy navigation and viewing by developers
    - Test software that provides full coverage of the sample source code
    - Test results
    - Build support files for each platform
    - Output of running the samples
    - Output of testing the software
    - Error codes and responses
    - File Structure formats
    - Documentation, developer guides
    - Utilities
    - All Token middleware necessary to interface with a NASH Token.

The service should also maintain the currency of the SDK information and contents as the NASH service develops, as new eHealth services become available, and as contemporary IT infrastructure evolves over time.

- Deliver Implementation Guide
  - This service should determine the needs of business planers to understand the role and value of NASH authentication in clinical system design. The implementation guide, or guides, would typically be supplied with the SDK, but also have a broader role in terms of business planning.

- Compliance, Conformance and Accreditation
  - This service should provide a mechanism for determining that any software system that implements the use of NASH credentials demonstrates appropriate standards of interoperability, security and clinical safety in the way it handles and exchanges information using these credentials.
  - It is anticipated that CCA activity for NASH credentials should occur concurrently with CCA activities for other aspects of a healthcare software system, through NEHTA's overall CCA program.

The services should also maintain the currency of the information for developers as the NASH service develops and as new eHealth applications which require the use of NASH credentials go into production over time.

Integrators

Integrators of software systems that want to integrate NASH compliant authentication services into the overall enterprise architectures will be consumers of information about how to implement authentication support into their deployed systems. This would include using NASH credentials as part of the Identity Management approach within an enterprise, using NASH credentials on non-NASH supplied tokens, or using local PKI credentials on a NASH Supplied token, etc.

The business services for this user sector should:

- Deliver Professional Services
  - This service should provide professional consulting services to facilitate the integration of NASH authentication with an enterprise environment, through working with the integrators own IT staff to transfer knowledge and build internal capability to implement with PKI authentication solutions.
- Deliver Integration Guidance
  - This service should determine the needs of business planers to understand the role and value of authentication of NASH in enterprise solutions. It should cover a range of material including:
    - NASH technical and business guides and white papers
    - NASH adoption plans and guidelines
    - Implementation guides
    - Technical implementation guides
    - Business Case Templates.
- Compliance, Conformance and Accreditation
  - Where appropriate, elements of the NASH CCA approach may be utilised to assure that interoperability, security and clinical safety of the integrated authentication approach are appropriately achieved in a deployed system. This would normally done with professional services assistance.

The services should also maintain the currency of the information for integrators as the NASH service develops.

4.4.30.10 Fulfilment Service

The NASH requires a fulfilment service that is able to deliver authentication service artefacts to users. The service should be able to handle both physical and electronic delivery of artefacts, as appropriate to the circumstances.

Given that authentication service artefacts are critical components in the NESAF, secure and assured delivery to the nominated entity (organisation or individual) should be provided.

The fulfilment service should be able to deliver authentication service artefacts on demand in a timely manner, and also en masse against program schedules, as appropriate to program settings.

The artefacts that are typically handled by the fulfilment service include:

- Digital credentials
- Tokens
- FIPS 2.1 compliant card readers and device drivers.

4.4.30.11 Service Desk (Support) Services

The NASH Service Desk should provide support services to two broad classes of users. While both classes have similar needs for support, the context of the support request should be significantly different for each class, and require a different entry level into the support processes.

End Users

End users support requests should primarily be around the use of NASH credentials in healthcare settings. The NASH Service Desk support for end users should include:

- Initial point of contact for NASH issues
  - This should involve responding directly to issues which can be addressed in a straightforward manner, and escalating issues which require further support service to resolve.
- Problem Resolution
  - All support calls should follow processes that assure the problem is resolved, including through any subsequent support steps.
- Persistent problem lifecycle management
  - For support calls where a user or users are encountering recurring issues which indicate there may be a persistent problem which appears across multiple calls, appropriate lifecycle management for the resolution of the problem should be instigated until it is resolved.
- Change request management
  - End users may request changes in the way the NASH operates within their usage context. The support desk should capture these requests for change for assessment in ongoing NASH product development.

Developers and Integrators

End users support requests should primarily be around the integration of NASH into application and enterprise systems. In some cases it may act as second level of support to a support desk operated directly by the developer or integrator, which has prequalified a support issue for escalation. The NASH Service Desk support for developers and integrators should include:

- Initial point of contact for NASH issues
  - This will involve responding directly to issues, and escalating issues which require further support service to resolve. It is expected that support requests have been pre-qualified by someone who has more than an elementary level of competence with authentication systems and can articulate the issue, and initial analysis, clearly.

- Problem Resolution
  - All support calls should follow processes that assure the problem is resolved, including through any subsequent support steps.
- Persistent problem lifecycle management
  - For recurring issues which indicate there may be a persistent problem which appears across multiple calls, appropriate lifecycle management for the resolution of the problem should be instigated until it is resolved.
- Change request management
  - Developers or integrators may suggest changes in the way the NASH operates within application and enterprise systems. The support desk should capture these requests for change for assessment in ongoing NASH product development.

4.4.30.12 Market Communication & Reporting

The NASH Communications service should provide market collateral to support the use of NASH authentication in Healthcare. The market collateral may be delivered by multiple channels as appropriate to its particular target audience.

Typical examples of market collateral include:

- Explanation of the NASH
  - Explanations, directed at various user groups, of how authentication works in healthcare settings, the benefits it provides and outcomes it enables.
- FAQ
  - Answers to frequently asked questions about various aspects of the NASH. This should be informed by user feedback and analysis of service desk issues.
- Change notification
  - Advise of changes to the range of authentication services delivered by the NASH over time.
- NASH news
  - Information about how NASH is being used, where it will be going in the future, and user experiences with the service, etc.

The NASH Reporting service should deliver information on the operation of the service to relevant stakeholders for Governance of the NASH. The reporting service should produce scheduled reports and ad hoc reports as required for governance purposes.

5 Summary of Impacts

The NASH is a new, national, healthcare authentication service that does not replace any existing national healthcare authentication service. The NASH will facilitate authentication between entities where there has been limited capability or means to establish a strong electronic trust relationship.

Some effort will be required to initially prepare healthcare individuals and organisations to participate. The main impacts will be in the introduction and adoption of NASH. Once participation is established, there should be little ongoing impact as the processes involved should be relatively straight forward and seamless.

The impact on NASH participants would vary depending on a variety of factors, including:

- Type of healthcare services provided
- Organisation size and structure
- Existing eHealth capability (IT systems and software)
- Level of participation
- Existing documentation, processes and procedures.

This section describes the expected start-up and ongoing operational impacts that are likely to arise from participation in NASH.

5.1 Start-Up Impacts

Some of the considerations for an organisation and an individual when preparing to authenticate using NASH credentials are:

- Acquiring NASH digital credentials
  - Evidence of Identity (EOI) enrolment information for participants
  - Application/registration process for credentials (noting there will be initial lead time for issuance)
- Changes to organisation policy and process
  - Implement business system changes
  - Implement/update existing organisation policy and procedures
  - Update documentation
  - Provide training and education for users (as required)
  - Budgeting for cost implications
  - An assessment would need to be undertaken to identify impacts and dependencies for the organisation to participate in NASH
- Changes to IT systems
  - Upgrade or obtain new software
  - Obtain reliable internet access
  - Configure smartcard readers
  - Integrate with existing IT systems
  - Integration/replacement with existing authentication mechanisms.

5.2 Operational Impacts

Once credentials have been obtained, and IT Systems are configured and updated appropriately, the operational impacts on organisations would include:

- Maintenance of credentials and tokens (re-issuance, revocation etc.) within the organisation
- Managing any IT upgrades (with consideration to impact on NASH credentials)
- Ensuring users are appropriately trained
- Maintaining internal records and documentation
- Managing new staff requirements, and staff departures.

6 Analysis of the NASH

This section provides an analysis of the benefits, new and enhanced capabilities, and the limitations and trade-offs that have been considered in the initial design of NASH.

6.1 Benefits

Implementation of eHealth across the Australian healthcare sector will deliver a safer more sustainable health system through:

- More secure, convenient and coordinated interactions across the many different parts of the healthcare system
- Providing greater accuracy and completeness of health information
- Provisioning for coordinated access to healthcare information, leading to improved clinical safety
- Facilitating the availability of more timely, up–to-date and accurate information at the point of care
- Establishing a trust community to securely transfer health related information between healthcare providers.

NASH supports this by:

- Higher assurance levels on credentials issued, allowing wider and greater adoption across the healthcare sector
- Providing a nationally endorsed solution that reduces complexity, promotes interoperability and makes processes simpler for providers to understand, implement and use
- Enhancing the end state of a single identifier for all healthcare providers and users
- Providing cost and efficiency savings through common provisioning of services
- Improved availability, accountability and auditing of services
- Providing both a source for nationally recognised credentials while at the same time allowing local CAs to manage their own credentials independently, without having to undergo onerous compliance programs
- Facilitating the ability to have one single token with local and national credentials
- Gatekeeper accreditation providing a level of recognised assurance in the capability of NASH.

The NASH program has identified a range of benefits from actions that the program will address. Benefits maybe Strategic, Clinical, Operational or Technical in nature.

No.	Rational	Benefit
1	An integrated Certificate Authority approach is closely aligned to NEHTA's strengths in orchestrating the use of systems and services under its frameworks rather than as a builder/operator of large national systems	Strategic Benefit - Allows interoperability and recognition of locally issued certificates
2	There is a natural complement between the HI and NASH programs; the PKI service operated for HI will align to the NASH specifications, and will be widely available to healthcare professionals and organisations across the sector	Strategic Benefit – Greater alignment and adoption of NASH specification and standards
3	The timing of HI service delivery will allow jurisdictional development of local authentication systems to be informed by the initial operations of the HI program.	Strategic Benefit - Building local systems to align with the national approach will be simplified once the NASH framework and approach is documented and understood by the jurisdictions
4	The NASH Framework will support the secure transfer of electronic information between authorised entities.	Clinical Benefit – Increased accuracy of patient data as electronic data is forwarded and shared instead of being written or re-keyed.
5	A national set of identifiers underpinned by NASH authentication solution.	Operational Benefit - Will improve the speed with which information can be securely passed between health professionals and services improving service reliability and responsiveness. Clinical Benefit – Improved speed of delivery and reliability may result in increased patient wellbeing and healthcare responsiveness.
6	The NASH program will assist in the delivery of a high grade national service issuing hardware tokens and digital certificates to healthcare professionals and users.	Operational benefit - This could eventually equip over 800,000 health professionals including state and local authentication programs with high assurance authentication credentials.
7	The NASH Framework provides a national alignment path and for new locally developed authentication services (such as those being established by Queensland Health, DHS Victoria and South	Operational Benefits - Allows jurisdictions to control ownership and local service delivery

No.	Rational	Benefit
	Australia Health)	
8	Development of national eHealth authentication architecture.	Operational Benefits – Will allow commercial security software vendors to develop targeted service offerings that meet the specified standards. The availability of 'off the shelf' services will increase the pool of commercial bidders, and reduce procurement risk for healthcare organisations. Strategic Benefit – Drive down costs Technical Benefit – Simplifies the development and improves the interoperability of vendor software.
9	The use of digital certificates and hardware tokens is widely recognised as a high grade mechanism for the delivery of authentication services within healthcare.	Technical Benefit - Establishing a user or organisational credential that is widely available, accepted and trusted through HI and supporting the development of local services will lay strong foundations for the ongoing NEHTA work program
10	Services delivered by the NASH program will be a significant focal point in the development, uptake and support of a high grade authentication services in eHealth. This is a complex area, and having a service which provides operational services and technical resources will be valuable in enabling a consistent and thorough approach.	Technical Benefit - Local eHealth application developers benefits from availability of a local knowledge repository and reference implementations that can be leveraged as required.
11	The identity services established through HI and NASH programs will be important underpinnings for further work being undertaken in the area of access control.	Technical Benefit - A standardised smart card platform will be assist in delivering access control services for sensitive health information where needed.

6.2 Limitations

NASH has a number of limitations that will need to be considered during its development and adoption within the healthcare sector. These include:

- The adoption of NASH is not mandatory. It is not compulsory for COIs to take up any services offered by NASH. Healthcare providers will take time to build trust and confidence in NASH.
- NASH will be affected by inherent PKI and smartcard limitations. Perceptions that PKI deployments have faced in the past include:
  - Limited software application support; and
  - Poor conceptual models for understanding PKI.

6.3 Alternatives and trade-offs considered

The accreditation and assurance model chosen for NASH is Gatekeeper, which will be an enabler for application systems to employ a NeAF based authentication model. Gatekeeper accreditation is an Australian Government requirement for authentication of access to national data sets under its control. Although no alternatives were considered as suitable for the healthcare sector, within NeAF there are alternative models for service delivery and authentication.

Although PKI based credentials have been chosen as the initial credential type to be supplied by NASH, other credential types such as Security Assertion Markup Language (SAML) credentials have also been considered and will be explored further during adoption. Similarly, although smartcards have been chosen as the initial token type, other tokens such as USB security keys will be considered during the adoption process.

7 Operations Services

7.1 Catalogue

The table below reflects an indicative operational service catalogue for the NASH.

These services are discrete operational components to perform specific functions with the NASH. Many are business-as-usual services that will be regularly used, however, some are expected to be only used very occasionally.

Request Services	SC.01.01	Request information and apply to become an RA
	SC.01.02	Add, modify and enable RA in NASH, provision credentials
	SC.01.03	Create and maintain Certificate Policies
	SC.01.04	Define and maintain Provisioning Profiles
	SC.01.05	Define and maintain token Profiles
	SC.01.06	Request information and apply to become a CA
	SC.01.07	Add and enable CA in NASH, provision credentials
	SC.01.08	Create and maintain Certificate Policies (CP)
	SC.01.09	Define and maintain Certification Practice Statement (CPS)
	SC.01.10	Request a Credential
	SC.01.11	Request token
	SC.01.12	Order Hardware (Blank tokens, card readers, etc.)
Revoke Services	SC.02.01	De-register an RA
	SC.02.02	De-register a CA
	SC.02.03	Revoke Credential
	SC.02.04	Cancel token
Replace Services	SC.03.01	Recover Credential
	SC.03.02	Renew token
	SC.03.03	Renew Credential
	SC.03.04	Issue a temporary token
Manage Services	SC.04.01	Change Credential Manager
	SC.04.02	Change token PIN
	SC.04.03	Reset token PIN
Local Services	SC.05.01	Add [local] credential to NASH managed tokens
	SC.05.02	Install Credential (Soft Certificate)
Use	SC.06.01	Access the NASH Services Catalogue (public)

Services	SC.06.02	Access the NASH Service Desk (public)
	SC.06.03	Publish RA Contact Details (public)
	SC.06.04	Get Credential Status and Public Key (public)
	SC.06.05	View Credentials on NASH token
	SC.06.06	Get Reports (Service Level & Compliance)

7.2 Mapping of BUCs to SCs

The table below shows an indicative mapping between the NASH Business Use Cases (BUC) identified at the time of writing this Con-ops and the indicative NASH Operational Services Catalogue (SC).

	Use Case	UC.Number	Service Catalogue
Registration Authority (RA) / Relationship Organisation (RO) related Use Cases	UC.001.001 Request RA Application Pack	UC.001.001	SC.01.01
	UC.001.002 Submit RA Application	UC.001.002	SC.01.01
	UC.001.003 Approve RA Proposal	UC.001.003	SC.01.01
	UC.001.004 Build and Self Assess RA Solution	UC.001.004	SC.01.01
	UC.001.005 Obtain formal NASH RA accreditation	UC.001.005	SC.01.01
	UC.001.005.01 Engage with NASH Assessor	UC.001.005.01	SC.01.01
	UC.001.006 Provision RA Digital Credentials	UC.001.006	SC.01.02
	UC.001.008 Define Digital Certificate Policy	UC.001.008	SC.01.03
	UC.057 De-register a NASH Registration Authority (RA)/ Relationship Organisation (RO)	UC.057	SC.02.01
	UC.058 Define Provisioning Profile.	UC.058	SC.01.04
	UC.074 Manage Provisioning Profile	UC.074	SC.01.04
	UC.006 Define Token Profile.	UC.006	SC.01.05
	UC.073 Manage Profile of a NASH managed Token	UC.073	SC.01.05
	UC.052 Publish RA Contact List	UC.052	SC.06.03
Certification Authority (CA) related Use Cases	UC.055.001 Request Certification Authority (CA) Application Pack	UC.055.001	SC.01.06
	UC.055.002 Submit CA Application	UC.055.002	SC.01.06
	UC.055.003 Approve CA	UC.055.003	SC.01.06

	Proposal		
	UC.055.004 Build and self assess CA Solution	UC.055.004	SC.01.06
	UC.055.005 Obtain formal NASH CA accreditation	UC.055.005	SC.01.06
	UC.055.006 Provision CA Digital Credentials	UC.055.006	SC.01.07
	UC.055.007 Define CA Digital Certificate Policy	UC.055.007	SC.01.08
	UC.055.008 Define CA Certification Practice Statement (CPS)	UC.055.008	SC.01.09
	UC.055.009 De-Register Certificate Authority	UC.055.009	SC.02.02
	UC.072 Manage Digital Certificate Policy (CP)	UC.072	SC.01.08
	UC.007.001 Request Digital Credential	UC.007.001	SC.01.11
	UC.007.002 Validate Digital Credential Request	UC.007.002	SC.01.11
	UC.007.003 Generate Digital Credential	UC.007.003	SC.01.11
	UC.007.004 Dispatch/Issue Digital Credential	UC.007.004	SC.01.11
	UC.007.005 Receive Digital Credential	UC.007.005	SC.01.11
	UC.017 Install Digital Credential	UC.017	SC.05.02
Credential Management System (CMS)	UC.021 Obtain Digital Credential Status	UC.021	SC.06.04
	UC.023 Recover Digital Credential	UC.023	SC.03.01
	UC.028 Revoke Digital Credential	UC.028	SC.02.03
	UC.035 Change Credential Manager	UC.035	SC.04.01
	UC.046 Renew Digital Credential	UC.046	SC.03.03
	UC.022 Obtain Certificate (Public Key)	UC.022	SC.06.04
	UC.067 Add local Digital Credential(s) to NASH managed Token(s).	UC.067	SC.05.01
	UC.071 Obtain National e-Authentication Framework (NeAF) level.	UC.071	SC.06.04

Token Management System (TMS)	UC.009.001 Request NASH managed Token with Credential	UC.009.001	SC.01.12
	UC.009.002 Validate NASH managed Token Request	UC.009.002	SC.01.12
	UC.009.003 Generate NASH managed Token	UC.009.003	SC.01.12
	UC.009.004 Dispatch NASH managed Token	UC.009.004	SC.01.12
	UC.009.005 Receive NASH managed Token	UC.009.005	SC.01.12
	UC.018 Activate NASH managed Token	UC.018	SC.01.12
	UC.032 Revoke NASH managed Token	UC.032	SC.02.04
	UC.036 Change NASH managed Token PIN	UC.036	SC.04.02
	UC.037 Reset NASH managed Token PIN.	UC.037	SC.04.03
	UC.038 View Credentials on a NASH managed Token.	UC.038	SC.06.05
	UC.063 Remotely renew Digital Credential on NASH managed Token.	UC.063	SC.03.02
	UC.064 Issue NASH temporary managed Token	UC.064	SC.03.04
	UC.065 Purchase NASH managed blank Tokens	UC.065	SC.01.13
Other Use Cases	UC.039. Generate reports	UC.039	SC.06.06
	UC.041 Access the NASH Service Catalogue	UC.041	SC.06.01
	UC.060 Contact NASH Service Desk	UC.060	SC.06.02
	UC.061 Compliance auditing for NASH RAs and CA’s	UC.061	SC.06.06

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
CC	Core Connectivity
CI	Clinical Information
CT	Clinical Terminology
EHR	Electronic Health Record
ICT	Information and Communication Technology
NASH	National Authentication Service for Health
SIL	Service Instance Locator
SNOMED CT	Systemised Nomenclature of Medicine, Clinical Terminology
UHI	Unique Healthcare identifiers

Glossary

This table lists specialised terminology in alphabetical order.

Acronym/term	Definition
AGIMO	Australian Government Information Management Office.
AHMAC	Australian Health Ministers' Advisory Council
AHMC	Australian Health Ministers' Conference
AHPRA	Australian Health Practitioner Regulation Agency
AS	Authoritative Source. The role of an organisation which collects a healthcare entity's details, confirms them against a known customer database or by sighting paper EOI documents.
Authentication	The act of establishing or confirming something (or someone) is authentic, that is, claims made by or about the subject are true. This should involve confirming the identity of a person, tracing the origins of an item, ensuring that a product is what it claims to be, or assuring that a computer program is trusted.
B2B	Business-to-business software interface, allowing pre-arranged information exchange between computer systems.
Business Day	Means any day other than a Saturday, Sunday or public holiday (including public service holidays) throughout Australia, promulgated in the Commonwealth of Australia Gazette.
Business Hours	8.30 AM to 6:00 PM in any Australian time zone on a Business Day.
CA	Certification Authority. The CA creates and signs PKI credentials at the request of a Digital Credential Manager / Token Manager Registration Authority. The trust provided by a PKI system depends upon the security policies practiced by the CA. Its private key must be kept secret otherwise all the credentials it has signed become compromised. The CA publishes a directory of credential holders

Acronym/term	Definition
	and a CRL which contains a list of revoked credentials.
CMS	Credential Management System. A system operated by the Certification Authority for the purpose of providing a direct interface for Registration Authorities to request and revoke authentication credentials.
COAG	Council of Australian Governments
COI	Community of Interest. A community of entities that have a need to electronically communicate with each other. The community is considered closed in that its members have no need to communicate with any entity outside the community. Any given member may belong to more than one community.
Confidentiality	Defined by the International Organisation for Standardisation (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorised to have access" and is one of the cornerstones of information security. Confidentiality is one of the design goals for many cryptosystems, made possible in practice by the techniques of modern cryptography.
CP	Certificate Policy. A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of credential to the authentication of electronic data interchange transactions for the exchanging of confidential health information
CPS	Certification Practice Statement. A statement of the practices, which a certification authority employs in issuing digital credentials.
Credential	A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant authority that in principle or in fact is assumed competent to do so.
CRL	Certificate Revocation List. A list maintained by the issuing Certification Authority (CA) that details each digital credential that is no longer valid, even though it has not yet expired. It can also be seen as a credential black list. Once expired, a digital credential is typically removed from the CRL.
CSP	Contracted Service Provider. A provider who provides business services on behalf of an HPI-O, and requires an Healthcare Identifier to assert in conjunction with an HPI-O identifier in eHealth transactions.
DHS	The Australian Government Department of Human Services. Specifically in the context of this document, that part of the DHS which was previously known as Medicare Australia
Digital Credential	An attachment to an electronic message used for security purposes. The most common use of a digital credential is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply
Digital Credential	Used specifically in the PKI sense i.e. the encapsulation of a public key along with a set of attributes that pertain to the owner of the corresponding private key that is signed by a CA. Digital Credentials issued by the NASH will conform to the X.509 Standard.
DSD	Defence Signals Directorate.
E-Health	E-Health Is the process of employing the combined use of electronic communication and information technology in the health sector
Entity	An individual or organisation that may be issued with a credential

Acronym/term	Definition
EOI	Evidence of Identity. Also known as Proof of Identity (POI). A set of documents that authenticate the identity of an individual or organisation
e-Pathology	The secure transmission of pathology results between healthcare professionals.
e-Prescribing	The secure transmission of prescriptions from a GP's desktop to the dispensing pharmacy.
e-Referrals	The secure transmission of patient information from one treating healthcare provider to another.
ETP	Electronic Transfer of Prescription - E-prescriptions are computer-generated prescriptions created by healthcare providers and made available to pharmacies at the time of dispensing.
GA	Governance Authority.
Gatekeeper	Gatekeeper is the Australian Government's strategic framework for the use of Public Key Infrastructure (PKI) as a key enabler for the delivery of online government services.
Healthcare Entity	This is a person or 'subject' who can be uniquely identified in a particular context. The entity does not have to have a physical form; it can be a company or a piece of digital equipment.
HI	Healthcare Identifier is a 16 digit unique reference number used to identify various classes of participants in the delivery of Australian healthcare. There are different number groups for each major class of participant.
HI Service	Healthcare Identifiers Service is a range of business services that enable the identification, allocation, access control, disclosure, maintenance and retirement of national healthcare identifiers for healthcare individuals and providers
HI Service Operator	The organisation that operates the HI Service, including performing registration for some classes of HI Service users. The HI Service operator is currently the DHS Australian Government Department of Human Services
HPI-I	Healthcare Provider Identifier – Individual for individual healthcare providers (HPI-I) is a 16 digit unique reference number used to identify individuals who deliver Australian healthcare.
HPI-O	Healthcare Provider Identifier – Organisation is a 16 digit unique reference number used to identify healthcare organisations who deliver Australian healthcare.
IAARG	Identification, Authentication and Access Reference Group.
Integrity	The assurance that recorded information has not been altered since the time it was recorded
Jurisdiction	Refers to the Australian public health departments at federal, state and territory levels
Marketing collateral	The textual and diagrammatic materials that describe a business and its products and services. Marketing collateral includes web sites, brochures, newsletters, fact sheets, press releases, and other related materials produced to support a product in the market place.
NASH	National Authentication Service for Health.
NEAF	National E-Authentication Framework. An authentication framework setup by AGIMO for Australian Government Agencies to use when engaging in online transactions. It defines a risk based approach to

Acronym/term	Definition
	assessing the authentication strength required for a given online transaction.
NESAF	National eHealth Security and Access Framework. A framework that ensures that health information is consistently controlled and monitored and that provenance of all electronic health information is traceable from creation from a verifiable source through its transition and possible augmentation to its destination.
NEHIPC	National eHealth and Information Principal Committee
NEHTA	National eHealth Transition Authority.
NHCIOF	National Health Chief Information Officer Forum
Organisation Maintenance Officer	A role within an Healthcare Provider organisation which provides day to day administrative support for with national eHealth services .
PDS	Provider Directory Service - will enable the search and location of healthcare providers and facilitate communication and information exchange between them, such as referrals, test orders and results.
PIN	Personal Identification Number. A number known only to the owner of a token that is required to enable access to private information or functionality of the token.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority. An organisation that is responsible for determining membership of a COI. This may be based on an existing relationship the organisation has with the members of the COI or require the collection of suitable EOI at the time of joining the COI. Once membership is determined an RA can then issue its members with a credential. Once a member ceases to belong to the COI then it is the responsibility of the RA to revoke their credential.
RCA	Root Certification Authority.
Relationship Organisation	A Gatekeeper role under the special purpose provisions of the Gatekeeper Framework.
Relying Party	An individual or organisation that relies upon a Digital Credential in a business transaction which may include digital signing, authentication or encryption.
Responsible Officer	A role within a Healthcare Provider organisation which manages the relationship with national eHealth services.
Smartcard	A plastic card about the size of a credit card, with an embedded microchip that can hold and can process data.
Soft Certificate	A digital credential for which the private key is stored in a soft store or a password encrypted file.
Strong authentication	The means of positively identifying a person, an organisation, or one of its assets to a system. In NEAF terms this corresponds to an authentication assurance of level 3 or higher. NASH has chosen the use of PKI and smartcard technology in order to achieve these levels.
Subscriber	End users or individuals who have been issued with a token and/or digital credentials for eHealth electronic services.
TDS	Trusted Data Source is a managed repository of valid or trusted data that is recognised as an authoritative external source of data that meets an appropriate set of criteria and contains a set of

Acronym/term	Definition
	attributes that covers the requirements of another business system. Leveraging existing data from an approved TDS occurs through technical processes, always ensuring that personal information is safeguarded
Token	A cryptographic device (e.g. smartcard) that can be used to securely contain one or more of an entity's private keys and its associated digital credentials.
Token Holder	An individual or organisation that has been issued a NASH token.
TMS	Token Management System - a system that automates the personalisation of tokens prior to being issued and also enables post issuance updates to the token. It is used by the Token Manager to create and import new private keys and import credentials as they are needed by the token holder. If the token supports multiple applications its can also be used to load and unload applications onto the token. Also known as Card Management System (CMS) and Smartcard Management System (SCMS)

References

Reference Documents	
Document Name	Publisher
AS 3523-1:2008 Australian Standard, Identification Cards-Identification of issuers, Part 1: Numbering system, 2008	Australian Standards Association, 2008
AS4846-2006 Healthcare Provider Identification, 2nd edition,	Australian Standards Association, 30 June 2006
Certification Authority Accreditation Criteria, Gatekeeper PKI Framework	Australian Government Information Management Office, Department of Finance and Deregulation, February 2009
Gatekeeper Public Key Infrastructure Framework,	Australian Government Information Management Office, Department of Finance and Deregulation, February 2009
Metadata Online Registry (METeOR)	Australian Institute of Health and Welfare, 2006
AS5017-2006 Healthcare Client Identification	Australian Standards Association, 30 June 2006
Better Health for all Australians Action Plan Attachment D, 10 February 2006,	Council of Australian Governments (COAG) http://coag.gov.au/meetings/100206/attachment_d_better_health.pdf (password required)
Healthcare identifiers and privacy: Discussion paper on proposals for legislative support	Australian Health Ministers' Advisory Council, July 2009
HI Service Concept of Operations, version 1.0	National E-Health Transition Authority, 19 November 2009
HI Service Security and Access Framework, version 1.0	National E-Health Transition Authority, 13 November 2009
IEEE 1362-1998, IEEE Guide for Information Technology - System Definition – Concept of Operations (ConOps), Software Engineering	Standards Committee of the IEEE Computer Society, USA, 19 March 1998
Introduction to National eHealth Services, version 1.0	National E-Health Transition Authority, 1 November 2009
ISO/PDTS 22220, Healthcare Informatics – Identification of subjects of healthcare	International Standards Organisation, 18 January 2005
ISO7812-16/IEC 7812-1:2000(E), Identification Cards – Identification of Issuers	International Standards Organisation, 15 September 2000
National E-Health Strategy	Australian Health Ministers' Conference, September 2008
NEHTA Strategic Plan 2009/10 to 2011/12	National E-Health Transition Authority, November 2009
NASH Blueprint, version 1.4	National E-Health Transition Authority, July 2010
NASH Project Initiation Document	National E-Health Transition Authority, May 2011

Appendix A: Business Scenarios

A.1 Establish HI (Healthcare Identifier) Service as a Relationship Organisation (RO)

Scenario	The HI Service requires trusted interaction and use of the NASH to provide strong authentication for its users when they access the HI Service. This scenario refers to the HI process.
Assumptions	1. The NASH GA has defined the processes and policies to become an RA, including the RA accreditation process and core Digital Credential Policy requirement. 2. An agreement between the NASH GA and the HI Service is required to ensure both parties know their roles and responsibilities. 3. The terms under which an RA executes the agreement may differ from RA to RA. 4. The issuance of NASH managed Digital Credentials and Tokens for the RA to use when accessing the NASH is part of the establishment process. 5. The HI Service has updated their systems to integrate with the NASH.
Main Flow	1. The Duly Authorised Officer of the HI Service applies to the NASH GA to become a NASH RA. 2. The NASH GA assesses the HI Services' application against the set of eligibility criteria based on the National eHealth Authentication Framework and the Gatekeeper Community of Interest (COI). 3. The NASH GA confirms that the HI Service can be a NASH RA and informs the HI Service of the outcome of the assessment process. 4. The NASH GA and the Duly Authorised Officer of the HI Service sign the agreement. 5. The HI Service defines one or more Digital Credential Policies derived from the National eHealth Authentication Framework (NeAF) under which to issue Digital Credentials to its Subscribers. 6. The HI Service is now a RA and can commence issuing Digital Credentials and NASH managed Tokens to its Subscribers.
Alternate Flows	This scenario would also be applicable to all organisations that wish to issue Digital Credentials to their Subscribers.
Associated Requirements	BR.2010.07.100 Provide services to enable organisations to become NASH RA.
Associated Business Use Cases	1. UC.001.001 Requested RA Application Pack 2. UC.001.002 Submit RA Application 3. UC.001.003 Approve RA

	4. UC.001.004 Build and Self Assess RA Solution 5. UC.001.005 Obtain formal accreditation 6. UC.001.005.01 Engage with NASH Assessor 7. UC.001.006 Provision RA Credentials 8. UC.005 Define Digital Certificate Policy 9. UC.006 Define Token Profile 10. UC.058 Define Provisioning Profile 11. UC.007.002 Validate Digital Credential Request 12. UC.007.003 Generate Digital Credential 13. UC.007.004 Dispatch/Issue Digital Credential 14. UC.007.005 Receive Digital Credential 15. UC.017 Install Digital Credential 16. UC.009.003 Generate Token 17. UC.009.004 Dispatch Token 18. UC.009.005 Receive Token 19. UC.018 Activate Token

A.2 The HI Service issues a Digital Credential to a registered HPI-O

Scenario	A registered HPI-O requires a Digital Credential to authenticate to a system or protect electronic data. For example, the HPI-O needs to access the HI Service.
Assumptions	1. A facility to establish one or more secondary authentication mechanisms to access the NASH is provided in the event of a lost or faulty Digital Credential. 2. This scenario is applicable to a Seed Healthcare Provider Organisation. 3. The HI Service is a NASH accredited RA.
Main Flow	1. A healthcare provider organisation applies for a NASH credential. 2. The RO establishes a secondary authentication mechanism to access the NASH directly in case of lost or faulty HPI-O Digital Credential. 3. The Organisation's Responsible Officer (RO) requests a HPI-O Digital Credential for the healthcare provider organisation through the HI Service officer. 4. The HI Service officer enters the request into the HI Service. 5. The HI Service validates and submits the request to the NASH. 6. The NASH validates the request. 7. The NASH generates the HPI-O Digital Credential and saves a backup copy of the Digital Credential. 8. The NASH issues the HPI-O Digital Credential to the RO via the channel as specified by the recipient. 9. The NASH dispatches the password for the HPI-O Digital Credential separately. 10. The RO receives the HPI-O Digital Credential. 11. The RO receives the password for the HPI-O Digital Credential and installs the Digital Credential onto their local system(s).
Alternate Flows	1. The NASH may dispatch the HPI-O Digital Credential and the associated password via the HI Service. 2. A registered HPI-I requires a Digital Credential to access the HI Service.
Associated Requirements	BR.2010.07.090 Provide online services to support Local, Central and Remote issuance and management of NASH Credentials.
Associated Business Use Cases	1. UC.007.001 Request Digital Credential 2. UC.007.002 Validate Digital Credential Request 3. UC.007.003 Generate Digital Credential 4. UC.007.004 Dispatch Digital Credential 5. UC.007.005 Receive Digital Credential

	6. UC.017 Install Digital Credential

A.3 A healthcare provider organisation needs to send a secure message to another healthcare provider organisation

Scenario	A general practitioner working in a general practice needs to send an e-referral to a specialist clinic.
Assumptions	1. The secure message is being transmitted between two healthcare provider organisations. 2. Both healthcare provider organisations have active HPI-Os. 3. The HPI-O Digital Credentials have been issued to both healthcare provider organisations. 4. Both healthcare provider organisations have access to the NASH. 5. Both healthcare provider organisations have implemented the Secure Messaging standards and the e-Referral specifications. 6. Both of the healthcare provider organisations have opted to be in the HI Provider Directory Service. 7. This is the first time the healthcare provider organisations have communicated with each other using the Secure Messaging standards. 8. Both healthcare provider organisations have systems which are compliant with the HI Service and the NASH.
Main Flow	1. The general practitioner logs on to their general practice application and securely accesses the HI Service to retrieve the secure messaging details of the specialist clinic from the HI Provider Directory Service (HPDS) using the organisation's HPI-O Digital Credential. 2. The HI Service authenticates the HPI-O Digital Credential of the general practice and returns the required details which include a reference to the specialist clinic's HPI-O Digital Credential. 3. The general practice system uses the reference to access the NASH to obtain the public component of the specialist clinic's HPI-O Digital Credential and confirm that it is valid. 4. The general practitioner completes the referral and sends it. 5. The general practice system signs the referral document with the organisation's HPI-O Digital Credential and encrypts using the public component of the specialist clinic's HPI-O Digital Credential. 6. The general practice system securely sends the message to the specialist clinic referral receiving system. 7. The specialist clinic referrals system receives the referral and decrypts it using the private component of their HPI-O Digital Credential. 8. The referrals system accesses the NASH to ensure that the general practice credential used to sign the

	message is valid. 9. The referrals system actions the referral according to the business rules of the specialist clinic.
Alternate Flows	1. The healthcare provider organisations will be able to cache Digital Credential information so that they are not accessing the NASH every time they need to validate the Digital Credential to send or receive a message. In this case, Steps 1, 2, 3 and 8 can be omitted, provided that the healthcare provider organisations will also be able to cache the secure messaging details from the HPDS. 2. This scenario would also be applicable to all SMD messaging patterns where relevant.
Associated Requirements	BR.2010.07.005 Provide a foundation service to enable Healthcare Providers to securely and reliably access and share health information.
Associated Business Use Cases	1. UC.021 Obtain Digital Credential Status 2. UC.022 Obtain Public Component

A.4 Healthcare provider organisation has lost their Digital Credential

Scenario	A healthcare provider organisation has misplaced or lost their HI Service Digital Credential. The healthcare provider organisation has no backup of the Digital Credential, and therefore needs their Digital Credential to be replaced.
Assumptions	1. The NASH is able to use other authentication mechanisms to authenticate the healthcare provider organisation's registered representative, e.g. Responsible Officer (RO), in the absence of a Digital Credential. 2. The NASH has approved that the NASH RA (HI Service) can request replacement of Digital Credentials.
Main Flow	1. The healthcare provider organisation has lost access to their HI Service Digital Credential and has no backup stored locally. 2. The healthcare provider organisation has lost access to their HI Service Digital Credential and has no backup stored locally. 3. The healthcare provider organisation's representative (authorised individual at the healthcare provider organisation) notifies the NASH of the lost Digital Credential, using a secondary authentication mechanism. 4. The NASH authenticates the healthcare provider organisation representative and processes the lost Digital Credential notification. 5. The NASH revokes the Digital Credential and generates a replacement Digital Credential. 6. The NASH delivers the replacement Digital Credential to the healthcare provider organisation via the channel specified by the HI Service.
Alternate Flows	1. The healthcare provider organisation representative contacts the HI Service to report the lost Digital Credential. 2. The healthcare provider organisation has lost access to their HI Service Digital Credential and has no backup stored locally. 3. The NASH sends the notification of the replacement Digital Credential to the HI Service instead of the healthcare provider organisation.
Associated Requirements	BR.2010.07.090 Provide online services to support Local, Central and Remote issuance and management of NASH Credentials.
Associated Business Use Cases	1. UC.028 Revoke Credentials

A.5 HI Service issues Tokens to healthcare provider individual

Scenario	A healthcare provider individual needs a HPI-I Credential to reside on a Token.
Assumptions	1. The healthcare provider individual agrees to the terms and conditions of use for the HPI-I Digital Credential and Token. 2. An issued Token will include installation software and documentation. 3. The software at the healthcare provider organisation has been configured to use the NASH. 4. Tokens are issued with Digital Credentials uploaded onto them. 5. The HI Service is a NASH accredited RA.
Main Flow	1. The healthcare provider individual contacts a HI Service officer and requests for a HPI-I Digital Credential. 2. The HI Service officer authenticates the identity of the healthcare provider individual. 3. The HI Service officer submits the request to the NASH with the healthcare provider individual's details and details of the Digital Credential and NASH managed Token to be issued. 4. The NASH validates and confirms the receipt of the request. 5. The NASH generates the Digital Credential, saves a backup copy of the Digital Credential and loads it onto a new NASH managed Token. 6. The NASH issues the NASH managed Token to the healthcare provider individual. 7. The NASH issues the PIN for the Token separately. 8. The healthcare provider individual receives the NASH Token and confirms receipt. 9. The healthcare provider individual receives the Token PIN. 10. The healthcare provider individual activates the NASH managed Token using the provided PIN. 11. The NASH notifies the HI Service that the request was successfully processed.
Alternate Flows	The HI Service can request for Tokens via the NASH web portal. The request can be a single request or a bulk request.
Associated Requirements	BR.2010.07.135 Provide NASH Tokens to support strong authentication for the healthcare sector.
	1. UC.009.001 Request Token with Digital

	Credential 2. UC.009.002 Validate Token Request 3. UC.009.003 Generate Token 4. UC.009.004 Dispatch Token 5. UC.009.005 Receive TokenUC.018 Activate Token

A.6 A Local Organisation adds Local Digital Credential onto a NASH managed Token

Scenario	A healthcare provider individual, who already has a NASH managed Token, begins employment at a new Local Organisation and requires local system access using the same Token.
Assumptions	1. The Local Organisation token reader/writer is compatible with the NASH Token reader/writer. 2. The local organisation systems are compatible with NASH Tokens. 3. The NASH managed Token can store multiple Digital Credentials. 4. The Local Organisation has authenticated the identity of the healthcare provider individual. 5. The Local Organisation has a facility to generate and upload Local Digital Credentials onto the NASH managed Tokens. 6. The healthcare provider individual has agreed to the terms and conditions of use for the NASH managed Token.
Main Flow	1. The Local Organisation's authorised officer: 2. Collects the Token from the healthcare provider individual; 3. Logs on their local system; 4. Enters the healthcare provider individuals details to create a new Local Digital Credential; 5. Creates the Local Digital Credential; 6. Saves the Local Digital Credential to their local system directory; 7. Inserts the healthcare provider individual's Token into a Token reader/writer and uploads the Local Digital Credential onto the NASH managed Token; 8. Returns the token to the healthcare provider individual.
Alternate Flows	If the NASH Token is full and cannot hold any more Digital Credentials then the local organisation will issue the healthcare provider individual with a new NASH Token from blank stock on hand and load the local Digital Credential onto that Token.
Associated Requirements	BR.2010.07.090 Provide online services to support Local, Central and Remote issuance and management of NASH Credentials.
Associated Business Use Cases	1. UC.067 Add local Digital Credentials to NASH managed Tokens 2. UC.065 Purchase blank Tokens

A.7 The HI Service issues a Digital Credential onto a Local Organisation Token

Scenario	A healthcare provider individual with a local token requires their HPI-I Digital Credential to be added on the local organisation token.
Assumptions	1. The local Token accepts multiple Digital Credentials. 2. The local Token is NASH compliant. 3. The local organisation token reader/writer is compatible with the NASH Token reader/writer. 4. The healthcare provider individual agrees to the terms and conditions of use for the local Token and their HPI-I Digital Credential. 5. The local organisation has been approved by the HI Service to perform the appropriate Evidence of Identity (EOI) checks on healthcare provider individual. 6. The local organisation token management practices have been assessed and accredited under the National eHealth Authentication Framework and the results have been forwarded to the NASH. This is necessary so that the NASH can assign the appropriate Digital Credential strength level to Digital Credentials loaded onto local organisation tokens.
Main Flow	1. The local organisation performs the necessary EOI checks on the healthcare provider individual as approved by the HI Service. 2. The local organisation authorised officer obtains the local Token from the healthcare provider individual. 3. The local organisation authorised officer contacts the HI Service and requests HPI-I Digital Credential. 4. The HI Service validates and submits the request for the HPI-I Digital Credential to the NASH. 5. The NASH validates the request. 6. The NASH generates the HPI-I Digital Credential. 7. The NASH dispatches the Digital Credential to the local organisation via the channel as specified by the HI Service. 8. The local organisation authorised officer receives the HPI-I Digital Credential and loads it onto the local organisation token. 9. The local organisation authorised officer returns the Token to the healthcare provider individual.
Alternate Flows	The local Organisation Token is full and requires a new

	token.
Associated Requirements	BR.2010.07.125 Support multiple channels for secure Credential management requests, despatch and delivery.
	1. UC.007.001 Request Digital Credential 2. UC.007.002 Validate Digital Credential Request 3. UC.007.003 Generate Digital Credential 4. UC.007.004 Dispatch Digital Credential 5. UC.007.005 Receive Digital Credential

A.8 A healthcare provider individual lost or had their NASH managed Token stolen

Scenario	A healthcare provider individual's NASH managed Token has been lost or stolen and needs to be revoked and replaced.
Assumptions	1. The NASH is able to use other authentication mechanisms to authenticate the healthcare provider individual in the absence of their HPI-I Digital Credential. 2. The healthcare provider individual agrees to the terms and conditions of use for the NASH managed HPI-I Digital Credential and Token. 3. The Local Organisation has a facility to request and upload HPI-I Digital Credentials to NASH managed Tokens. 4. The Local Organisation has a temporary NASH approved Token that can be issued to the healthcare provider individual for immediate use until a permanent replacement Token arrives. 5. The healthcare provider individual requires Tokens to be replaced within half an hour of it being reported lost or stolen. 6. Local organisations that have embedded their local credentials onto the NASH managed Tokens will need to periodically check the NASH Public Directory or download the NASH Certificate Revocation List (CRL).
Main Flow	1. The healthcare provider individual informs its local organisation authorised officer that their Token has been lost or stolen. 2. The local organisation authorised officer revokes any local Digital Credentials on the Token. 3. The local organisation authorised officer requests the NASH to revoke and replace the NASH managed Digital Credential and Token. 4. The NASH authenticates the request; 5. The NASH revokes the existing Digital Credentials and updates the NASH CRL; 6. The NASH revokes the Token; 7. The NASH generates the replacement Digital Credentials and Token; 8. The NASH updates the NASH Public Directory. 9. The NASH dispatches the Digital Credential on the NASH managed Token to the local organisation. 10. The NASH dispatches the PIN to the local organisation. 11. The local organisation authorised officer issues a local temporary token with local and NASH Digital Credentials for the healthcare provider individual to use while they await delivery of the permanent replacement Token from the NASH.

	12. When the replacement Token arrives, the local organisation authorised officer receives the Digital Credential(s) on the NASH managed Token; 13. When the PIN arrives, the healthcare provider individual activates the NASH managed Token; 14. The local organisation authorised officer uploads the Local Digital Credential on the NASH managed Token. 15. The local organisation authorised officer exchanges the temporary token given to the healthcare provider individual with the NASH managed Token.
Alternate Flows	The NASH receives a request to revoke and replace the token directly from the healthcare provider individual. If the healthcare provider has access to a temporary token then the NASH can load it with a temporary Digital Credential while they await delivery of the NASH managed Token.
Associated Requirements	BR.2010.07.130 Provide processes and services to support Local, Central and Remote issuance and management of NASH issued Tokens.
Associated Business Use Cases	1. UC.028 Revoke Credentials 2. UC.032 Revoke Token

A.9 A healthcare provider individual's NASH managed Token is damaged

Scenario	A healthcare provider individual's NASH managed Token was damaged and needs to be revoked and replaced.
Assumptions	1. The NASH is able to use other authentication mechanisms to authenticate the healthcare provider individual in the absence of their HPI-I Digital Credential. 2. The NASH has sufficient Token in stock for immediate dispatch and use. 3. The healthcare provider individual agrees to the terms and conditions of use for the NASH issued HPI-I Digital Credential and Token. 4. The local organisation has a facility to create and upload Local Credentials on NASH managed Tokens. 5. The local organisation has a token management facility to check the types of Digital Credentials that are on the NASH managed Token. 6. The local organisation token reader/writer is compatible with the NASH Token reader/writer. 7. The healthcare provider individual requires their Token be replaced within half an hour of it being reported damaged. 8. For damaged tokens, the saved copy of the Digital Credential can be loaded onto a replacement token.
Main Flow	1. The healthcare provider individual contacts their local organisation authorised officer and informs that their NASH managed Token was damaged. 2. The local organisation authorised officer checks the Token and finds it damaged. 3. The local organisation authorised officer revokes any local Digital Credentials. 4. The local organisation authorised officer requests the NASH to revoke the NASH managed token and the HPI-I Digital Credential on it. 5. The NASH authenticates the request. 6. The NASH revokes the existing HPI-I Digital Credential. 7. The NASH updates the NASH Credential Revocation list. 8. The NASH generates a replacement HPI-I Digital Credential and Token. 9. The NASH updates the NASH Public Directory. 10. The NASH dispatches the HPI-I Digital Credential and the Token to the local organisation. 11. The NASH dispatches the PIN to the local organisation. 12. The local organisation authorised officer receives the HPI-I Digital Credential on the Token.

	13. The local organisation authorised officer gives the token with the replacement HPI-I Digital Credential to the healthcare provider individual. 14. When the PIN arrives, the healthcare provider individual activates the NASH managed token. 15. The local organisation authorised officer uploads the local credential on the NASH managed token.
Alternate Flows	The healthcare provider requests the Token to be issued and replaced by the NASH. Instead of revoking the existing HPI-I Digital Credential, the NASH recovers the saved component of the Digital Credential and loads it to a replacement token.
Associated Requirements	BR.2010.07.130 Provide processes and services to support Local, Central and Remote issuance and management of NASH Tokens.
Associated Business Use Cases	1. UC.007.001 Request Digital Credential 2. UC.007.002 Validate Digital Credential Request

A.10 A healthcare provider individual misplaced their NASH managed Token

Scenario	A healthcare provider individual's NASH managed Token was misplaced, and a temporary replacement token needs to be issued.
Assumptions	1. The NASH is able to use other authentication mechanisms to authenticate the healthcare provider individual in the absence of their HPI-I Digital Credential. 2. A temporary Token along with the required credentials can be issued in a timely manner. 3. The local organisation has set aside spare tokens for the purpose of temporary use. 4. The misplaced Token and Credentials do not have to be immediately. 5. The temporary Token will only be valid for 24 hours. 6. The temporary Token and Credentials need to be issued within half an hour of it being reported misplaced. 7. The local organisation token reader/writer is compatible with the NASH Token reader/writer.
Main Flow	1. The healthcare provider individual contacts the local organisation authorised officer and informs that they misplaced their Token. 2. The local organisation authorised officer informs the NASH that a temporary token has been issued and that the HPI-I Digital Credential needs to be uploaded onto the token. 3. The NASH authenticates the requests. 4. The NASH issues a temporary HPI-I Digital Credential. 5. The local organisations authorised officer loads the temporary HPI-I Digital Credential onto the temporary token. 6. The local organisation authorised officer receives the temporary HPI-I Digital Credential. 7. The local organisation authorised officer activates the temporary HPI-I Digital Credential. 8. The local organisation authorised officer loads the local credential(s) onto the temporary token. 9. The local organisation authorised officer gives the temporary token to the healthcare provider individual.
Alternate Flows	1. The local organisation authorised officer requests the NASH to issue the temporary token. 2. The validity period of the temporary token can be extended subject to the approved Certificate Policy.
Associated	BR.2010.07.130 Provide processes and services to support

Requirements	Local, Central and Remote issuance and management of NASH Tokens.
Associated Business Use Cases	1. UC.064 Temporary issuance of Tokens

Appendix B: Clinical Scenarios

B.1 Private Provider

Scenario	Samantha presents with an injury at a new GP near her work and is diagnosed or treated and referred for further treatment	
Assumptions	1. This scenario is not using a Contracted Service Provider (CSP). 2. All activities are electronic unless specified otherwise. 3. Individual credentials are used to log in. 4. The e-Signature policy is not yet defined. 5. Stored sessions have been enabled. 6. The credential of the Healthcare Provider Identifier – Individual (HPI-I) and Healthcare Provider Identifier – Organisation (HPI-O) is validated at the start of the session. 7. The patient has a Patient Controlled Electronic Health Record (PCEHR) and has allowed access to their PCEHR by any practitioner involved in her healthcare. 8. All credential transactions need to be validated through policy. 9. Organisational network management policies apply. (session timeout policies)	
Main Flow	**Clinical Scenario Main Flow**	**Associated NASH Actions**
	1. Samantha visits nearest General Practice.	
	2. The receptionist registers Samantha via the Patient Management System (PMS)/Patient Administration System (PAS), including obtaining consent to access her PCEHR.	2. Method of receptionist identification?
	3. The receptionist accesses the HI Service via the PMS/PAS, to access Samantha's IHI.	3. Use HPI-O Credential to access the HI Service.
	4. Samantha sees Dr. Sharma (regular GP at the practice).	3. Use HPI-O Credential to access PCEHR. (NEHTA Action: If there are multiple HPI-O Credentials within the org, which one is used?)
	5. Dr. Sharma accesses the local Electronic Medical Record (EMR) which provides access to the PCEHR record.	5a. Dr. Sharma uses her HPI-I Credential and the HPI-O Credential to access the Samantha's PCEHR.
	6. Dr. Sharma accesses PCEHR and downloads PCEHR content to the local EMR. The consultation occurred and Dr. Sharma adds	5b. The PCEHR system verifies the HPI-I and HPI-O Credentials which have been provided. 5c. The practice EMR

	the information to the local EMR record. 7. Dr. Sharma orders an x-ray. 8. Dr. Sharma issues a prescription by sending an electronic prescription message to a Prescription Exchange Service (PES) conformant repository. (NEHTA Action: Confirm the steps with Electronic Transfer Prescription (ETP) and Secure Messaging Delivery (SMD). 9. The consultation ends. 10. Samantha returns to the practice. 11. Dr. Sharma receives a secure message with the x-ray report. 12. Dr. Sharma receives a secure message notification that the script was issued. 13. At the end of the consultation, Dr. Sharma sends a referral to an orthopaedic surgeon at private rooms, with a copy sent to PCEHR. 14. The local EMR generates an event summary and sends it as a secure message to the PCEHR system. Consultation ends.	validates PCEHR system Credential. (NEHTA Action: question for PCEHR design authority) 7a. The practice EMR ensures the validity of the public certificate of the radiology provider. 7b. Dr. Sharma uses her HPI-I Credential or the HPI-O Credential (NEHTA Action: e-Sig Policy) to sign the message and the HPI-O Credential of the recipient to encrypt it. 8a. The practice EMR ensures the validity of the public certificate of the PES conformant repository. 8b. Dr. Sharma uses her HPI-I Credential to sign the message and the HPI-O Credential of the recipient to encrypt it. 10a. Use HPI-O Credential to access the HI Service. 10b. Use HPI-O Credential to access PCEHR. (NEHTA Action: If there are multiple HPI-O Credentials within the org, which one is used?) 11a. Dr. Sharma uses her HPI-I credential or the HPI-O credential (NEHTA Action: e-Sig Policy) to access the message and the HPI-O credential of the recipient to decrypt it. 12a. Dr. Sharma uses her HPI-I credential to access the message and the HPI-O of the recipient to decrypt it. 13a. The practice EMR ensures the validity of the public credential of the private rooms. 13b. Dr. Sharma uses her HPI-I Credential and HPI-O Credential to sign the referral and encrypts with PCEHR Credential. 14a. Dr. Sharma uses her HPI-I Credential and HPI-O Credential to sign the

		event summary and encrypts with PCEHR system Credential.
Alternate Flows	Samantha is referred to a local public ED.	
Associated Business Use Cases	UC.017 Install/Activate Credential UC.021 Obtain Credentials Status UC.022 Obtain Public Component UC.018 Activate Token	

B.2 Specialist

Scenario	Samantha attends the private rooms of the orthopaedic surgeon.	
Assumptions	1. This scenario is not using a CSP. 2. All activities are electronic unless specified otherwise. 3. Individual credentials are used to log in. 4. The e-Signature policy is not yet defined. 5. Stored sessions have been enabled. 6. The credential of the HPI-I and HPI-O is validated at the start of the session. 7. The patient has a PCEHR and has allowed access to their PCEHR by any practitioner involved in her healthcare. 8. All credential transactions need to be validated through policy. 9. Dr. Sullivan's EMR is not the same as the hospital's EMR. 10. Organisational network management policies apply. (session timeout policies).	
Main Flow	**Clinical Scenario Main Flow**	**Associated NASH Actions**
	1. Samantha presents to the private rooms.	
	2. The receptionist registers Samantha via the PMS/PAS, including obtaining consent to access her PCEHR.	2. Method of receptionist identification?
	3. The receptionist accesses the HI service via the PMS/PAS, to access Samantha's Individual Healthcare Identifier (IHI).	3. Use HPI-O Credential to access the HI Service. 3. Use HPI-O Credential to access PCEHR. (NEHTA Action: If there are multiple HPI-O Credentials within the org, which one is used?)
	4. The receptionist receives the referral through secure messaging.	
	5. Samantha sees Dr.	4a. The practice EMR decrypts the message

	Sullivan. 6. Dr. Sullivan accesses the local EMR which provides access to the PCEHR record. 7. Dr. Sullivan accesses PCEHR and downloads PCEHR content to the local EMR. The consultation occurred and Dr. Sullivan adds the information to the local EMR record. 8. Dr. Sullivan arranges for Samantha to be admitted into hospital. 9. Samantha takes a copy of her e-Referral to the hospital admission desk. 10. The local EMR generates an event summary and sends it as secure message to the PCEHR system. 11. The local EMR generates a specialist letter and sends it as a secure message to the referring GP (Dr. Sharma), Samantha's regular GP and the PCEHR system.	and validates certificates. 6a. Dr. Sullivan uses her HPI-I Credential and the HPI-O Credential to access the Samantha's PCEHR. 6b. The PCEHR system verifies the HPI-I and HPI-O Credentials which have been provided. 6c. The practice EMR validates PCEHR system Credential. (NEHTA Action: Question for PCEHR design authority) 8a. Could an e-Referral be an admission form? 10a. Dr. Sharma uses her HPI-I Credential and HPI-O Credential to sign the event summary and encrypts with PCEHR Credential. 11a. Dr. Sharma uses her HPI-I Credential and HPI-O Credential to sign the specialist letter and encrypts with the HPI-O Credential of the recipient(s) and the PCEHR Credential.
Alternate Flows	N/A	
Associated Business Use Cases	UC.017 Install/Activate Credential UC.021 Obtain Credentials Status UC.022 Obtain Public Component UC.018 Activate Token	

B.3 Public Hospital Admission

Scenario	Samantha presents at the public hospital emergency department, is admitted, undergoes surgery and discharged after 2 days.
Assumptions	1. This scenario is not using a CSP. 2. All activities are electronic unless specified otherwise. 3. Individual certificates are used to log in. 4. The e-Signature policy is not yet defined. 5. Stored sessions have been enabled. 6. The credential of the HPI-I and HPI-O is validated at the start of the session.

	7. The patient has a PCEHR and has allowed access to their PCEHR by any practitioner involved in her healthcare. 8. All certificate transactions need to be validated through policy. 9. Organisational network management policies apply. (session timeout policies) 10. Internal hospital activities do not require external authentication.	
Main Flow	**Clinical Scenario Main Flow**	**Associated NASH Actions**
	1. Samantha arrives at Emergency Department (ED) by ambulance.	
	2. Samantha is admitted to ED. The ED clerk verifies identity and obtains medical history.	
	3. The ED clerk registers Samantha via the PMS/PAS, including obtaining consent to access her PCEHR.	3. Use HPI-O Credential to access the HI Service. 3. Use HPI-O Credential to access PCEHR. (NEHTA Action: If there are multiple HPI-O Credentials within the org, which one is used?)
	4. The ED clerk accesses the HI Service via the PMS/PAS, to access Samantha's IHI.	
	5. Samantha is taken to triage. She is assessed by triage nurse and prioritised for treatment based on severity and history.	
	6. Samantha is taken to treatment room and treated by ED nurse and/or doctor.	
	7. The doctor orders pain medication and x-ray.	
	8. Samantha is admitted to the hospital from ED.	
	9. Samantha is transferred to pre-operation.	
	10. Samantha is transferred to theatre.	
	11. Samantha is transferred to recovery.	
	12. Samantha is transferred to ward.	
	13. Samantha is discharged from hospital.	
	14. The discharge summary is generated from the hospital EMR system.	
	15. The authorised medical	

	officer lodges copy of discharge summary and event summary record in the PCEHR system. 16. The authorised medical officer sends copy of discharge summary to Samantha's regular GP.	15a. The authorised medical officer uses her HPI-I Credential and HPI-O Credential to sign the event summary and encrypts with PCEHR system Credential. 16a. The authorised medical officer uses her HPI-I credential and HPI-O Credential to sign the discharge summary and the HPI-O of the recipient to encrypt it.
Alternate Flows	N/A	
Associated Business Use Cases	UC.017 Install/Activate Credential UC.021 Obtain Credentials Status UC.022 Obtain Public Component UC.018 Activate Token	

B.4 Private Hospital Admission

Scenario	Samantha presents at the private hospital Emergency Department (ED), is admitted, undergoes surgery and discharged after 2 days.
Assumptions	1. This scenario is not using a CSP. 2. All activities are electronic unless specified otherwise. 3. Individual credentials are used to log in. 4. The e-Signature policy is not yet defined. 5. Stored sessions have been enabled. 6. The credential of the HPI-I and HPI-O is validated at the start of the session. 7. The patient has a PCEHR and has allowed access to their PCEHR by any practitioner involved in her healthcare. 8. All credential transactions need to be validated through policy. 9. Organisational network management policies apply, including session timeout policies. 10. Internal hospital activities do not require external authentication.

Main Flow	**Clinical Scenario Main Flow**	**Associated NASH Actions**
	1. Samantha arrives at ED by ambulance.	
	2. Samantha is admitted to ED.	
	3. The ED clerk registers Samantha via the PMS/PAS, including obtaining consent to access her PCEHR.	3. Use HPI-O Credential to access the HI Service. 3. Use HPI-O Credential to access PCEHR. (NEHTA Action: If there are multiple HPI-O Credentials within the org, which one is used?)
	4. The ED clerk accesses the HI service via the PMS/PAS, to access Samantha's IHI.	
	5. Samantha is taken to triage. The triage nurse assesses and prioritises Samantha for treatment based on severity and history.	
	6. Samantha is taken to the treatment room. The ED nurse and/or doctor treat Samantha.	
	7. The doctor orders pain medication and x-ray.	
	8. Samantha is admitted to the hospital from ED.	
	9. Samantha is transferred to pre-operation.	
	10. Samantha is transferred to theatre.	
	11. Samantha is transferred to recovery.	
	12. Samantha is transferred to ward.	
	13. Samantha is discharged from hospital.	
	14. A discharge summary is generated from hospital EMR system.	
	15. The ward clerk lodges copy of discharge summary and event summary record in the PCEHR system.	15a. The ward clerk uses her HPI-I Credential and HPI-O Credential to sign the event summary and encrypts with PCEHR Credential.
	16. The ward clerk sends copy of discharge summary to Samantha's regular	16a. The ward clerk uses her

	GP.	HPI-I to sign the discharge summary and the HPI-O Credential of the recipient to encrypt it.
Alternate Flows	N/A	
Associated Business Use Cases	UC.017 Install/Activate Credential UC.021 Obtain Credentials Status UC.022 Obtain Public Component UC.018 Activate Token	

B.5 Allied Health

Scenario	As part of Samantha's her discharge from the private hospital, she is referred to a physiotherapist.
Assumptions	1. This scenario is not using a CSP. 2. All activities are electronic unless specified otherwise. 3. Individual credentials are used to log in. 4. The e-Signature policy is not yet defined. 5. Stored sessions have been enabled. 6. The credential of the HPI-I and HPI-O is validated at the start of the session. 7. The patient has a PCEHR and has allowed access to their PCEHR by any practitioner involved in her healthcare. 8. All certificate transactions need to be validated through policy. 9. The physiotherapist's EMR is not the same as the hospital's EMR. 10. Organisational network management policies apply. (session timeout policies) 11. Internal hospital activities do not require external authentication.

Main Flow	**Clinical Scenario Main Flow** 1. Physiotherapist receives referral from private hospital or orthopaedic surgeon as a secure message. 2. The physiotherapist registers Samantha via the PMS/PAS, including obtaining consent to access her PCEHR. 3. The physiotherapist accesses the HI Service via the PMS/PAS, to access Samantha's IHI. 4. The physiotherapist accesses the local EMR which provides access to the PCEHR record. 5. The physiotherapist accesses PCEHR and downloads PCEHR content to the local EMR. 6. A consultation occurred and the physiotherapist adds the information to the local EMR record. 7. At the end of every treatment, the physiotherapist lodges event summary to the PCEHR.	**Associated NASH Actions** 3. Use HPI-O Credential to access the HI Service. 3. Use HPI-O Credential to access PCEHR. (NEHTA Action: If there are multiple HPI-O Credentials within the org, which one is used?) 4a. The physiotherapist uses her HPI-I Credential and the HPI-O Credential to access Samantha's PCEHR. 4b. The PCEHR system verifies the HPI-I and HPI-O Credentials which have been provided. 4c. The physiotherapist's EMR system validates the PCEHR system Credential. (NEHTA Action: question for PCEHR design authority) 7a. The physiotherapist uses her HPI-I Credential to sign the message and the HPI-O of the recipient to encrypt it.
Alternate Flows	One event summary lodged at end of treatment.	
Associated Business Use Cases	UC.017 Install/Activate Credential UC.021 Obtain Credentials Status UC.022 Obtain Public Component UC.018 Activate Token	

Appendix C: PKI Overview

C.1 Public Key Infrastructure

Public Key Infrastructure (PKI) provides a solution to a number of possible risks in eHealth transactions. The 4 main pillars of Public Key Infrastructure are; 1) Privacy, 2) Authentication, 3) Integrity and 4) Non-repudiation.

C.2 Privacy

Privacy means that a transaction between parties cannot be viewed or interfered with by an outside party. PKI uses encryption to ensure that transactions are kept private. PKI technology can use encryption to protect the privacy of data in transit and in storage.

C.3 Authentication

Authentication means that access to an eHealth system is limited to those who can provide the proper identity credentials. Authentication is commonly handled through the use of a logon ID and password. This technology is considered a very low level of authentication and is often easy to break. PKI uses a digital certificate as the identity credential.

The idea of a digital credential is similar to the idea of a passport. Nations require that people traveling across international borders must be able to produce an identity credential called a passport. People get passports by proving who they are to their national government. All governments accept a passport as evidence that the issuing national government believes that this person is who they claim to be.

A digital credential is very similar. A person must prove his identity to a Certificate Authority (CA). If the CA can verify the assertion of identity, it will issue a digital credential that states that the issuing CA trusts the identity of this individual.

Programs that require a digital certificate as an identity credential also specify what CA or CAs they accept certificates from. This is an additional level of security. It prevents a person from starting his own CA and issuing fraudulent certificates. It is also a way to specify who it trusts by defining which CAs it trusts.

In the physical world, we keep our ID in a wallet. In the electronic world, there are two common places to store a digital credential. The most common is in a Web browser. You may not be aware of it, but you likely already have several digital credentials stored in the browser and used to access various sites on the Internet.

The next most common place to store digital credentials is on a Smart Card, or in the case of NASH, a token. In this case, the Smart Card is inserted into a reader in order to access a secured system. The secured system reads the digital credential stored on the card and decides whether to permit you access.

C.4 Integrity

Integrity means two things. One meaning of integrity is that the data received is the same as the data sent. That means that the data was not changed in transit either by mistake or on purpose. The other meaning is that at any time in the future, it is possible to undeniably prove whether different copies of the same document are in fact identical or not.

PKI uses a technology called "message digest" or "hashing" to ensure data integrity. It is possible to view any data object as a string of numbers, even if

people view it as a text document. Message digest programs do exactly that - they view all data objects as strings of numbers. A message digest program adds up the numbers in a data object using a specific algorithm. The result is a single number, called the message digest or hash value of the data object. Because of the mathematical technique used in the calculation, the hash value of a data object is unique; no other data object can produce the same hash value. If so much as one character is changed, added, or deleted in a data object (even a blank at the right end of a line), the calculated hash value will be different and a loss of integrity will be detected.

The message digest is a common way of verifying data integrity in transmission. The sender calculates the message digest and sends that value with the file he is transmitting. The recipient calculates the message digest of the received file and compares it to the value that the sender calculated. If they are the same, then the file sent is the same as the file received.

C.5 Non-repudiation

Non-repudiation means that if a discrepancy or dispute arises over an eHealth transaction, there is incontrovertible evidence present within the eHealth system that can be used to prove beyond reasonable doubt just what exactly occurred and why.

The most common way to provide non-repudiation is through the use of digital signatures. A digital signature is the electronic equivalent of a handwritten signature. Many nations now have laws that define how and where digital signatures can be used in the conduct of eHealth. The Australian digital signature laws are some of the world's leading legislation on digital signatures, including the Gatekeeper compliance for the Commonwealth.

PKI technology is based on a cryptological technique that can create a unique pair of numbers. These numbers are used as keys by special encryption programs. If a file is encrypted with one key in a given pair, only the other key can decrypt it, and vice versa. PKI specifies that when a person receives a key pair, one member of the pair will be kept private and the other will be published as the public key. An example will illustrate how the key pairs are used.

Party 1 and Party 2 each have PKI key pairs. They each have access to the other's public key. If Party 1 wants to send Party 2 a private message, they can encrypt the message with Party 2's public key and send it. Only Party 2's private key can decrypt the message, so Party 1 has confidence that only Party 2 can read the message, even if a million people were to receive the message.

Now consider another example. Party 1 and Party 2 want to digitally sign an electronic document and they want to be sure that the document can't be changed later and that neither can dispute that they signed it. Party 1 will do the following:

- Party 1 and Party 2 agree to the exchange of a document.
- Party 1 calculates a message digest or hash value of the electronic document.
- Party 1 encrypts the hash value with their private key.
- Party 1 provides the contract and the encrypted hash value of that document to Party 2.

Party 2 can prove that the hash value is from Party 1 because Party 1's public key can decrypt it. Because no other key in existence can decrypt this hash value, it must have been encrypted using Party 1's private key. Party 2 can tie the decrypted hash value to the document by calculating a hash value of the document themself. Since each document produces a unique hash value, if the value they calculate is the same as the value Party 1 provided, then the document they have is the same as the one Party 1 sent. Now Party 2 will

encrypt the hash value they calculated with their private key. Both parties have digitally signed the document. The proof of this consists of the following:

- The document
- The hash value of the document, encrypted with Party 1's private key
- The hash value of the document, encrypted with Party 2's private key

If there is doubt about the contents of the document, the parties can calculate a hash value of the document and compare it to the original values calculated by both Parties.

If there is doubt about the keys, can Party 1's public key decrypt their version of the hash value? Can Party 2's decrypt theirs? If the answers are "yes," then the only possible argument that can be made is that a private key has been stolen. If this argument is made, then all documents that have been signed or encrypted by the compromised person can be said to be legally void, since the date of theft is probably not known.