Australian Government
Australian Digital Health Agency

National Secure Messaging Network Blueprint

27 June 2023 v1.0

Approved for external use

Document ID: **DH-3568:2023**

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

Acknowledgements

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

HL7 International
This document includes excerpts of HL7™ International standards and other HL7 International material. HL7 International is the publisher and holder of copyright in the excerpts. The publication, reproduction and use of such excerpts is governed by the HL7 IP Policy and the HL7 International License Agreement. HL7 and CDA are trademarks of Health Level Seven International and are registered with the United States Patent and Trademark Office.

National Secure Messaging Network (NSMN) - Blueprint

Key information

Owner	National Chief Digital Officer
Contact for enquiries	Australian Digital Health Agency Help Centre Phone 1300 901 001 Email help@digitalhealth.gov.au

Product or document version history

Product or document version	Date	Release comments
1.0	27 June 2023	Initial version

Table of contents

1 Introduction

The National Secure Messaging Network (NSMN) blueprint describes the proposed operation of a national standards-based network of interoperable systems to allow any healthcare provider in Australia to discover any other healthcare provider and securely deliver clinical messages to them. The blueprint describes the key roles within the secure messaging national network and the capabilities required of each role, as well as providing examples of how specific implementations might fulfil those roles.

1.1 References

- References using URL links are to current drafts of specifications and standards provided for information purposes only.
- The NSMN Interoperability Specification (IS) should be used for details on approved and static references to specifications and standards.

2 Purpose

The purpose of this blueprint is to provide clarity and a consistent and confirmed viewpoint about the proposed secure messaging roles and their required capabilities. As part of the NSMN Interoperability Specification, the Blueprint will serve as the vehicle for agreement and ongoing governance of the solution design for the NSMN. It will also provide policy makers, information system managers and product strategists with clarity and context for decision making.

3 Participation

The NSMN Managed Operating Deed (MOD) outlines principles for behaviours in how NSMN participants are expected to engage and operate with each other for the purpose of secure messaging interoperability.

Each NSMN participant will be required to sign a MOD as it applies to the NSMN role sought.

To support the successful functioning of a national, interoperable messaging network the MOD is required to govern the connectivity between all roles in the network.

4 Roles

The key solution roles in the NSMN are:

- Core Node
- Sending Edge Node
- Receiving Edge Node
- Sending System (aka Sending Client)
- Receiving System (aka Receiving Client)
- Provider Directory

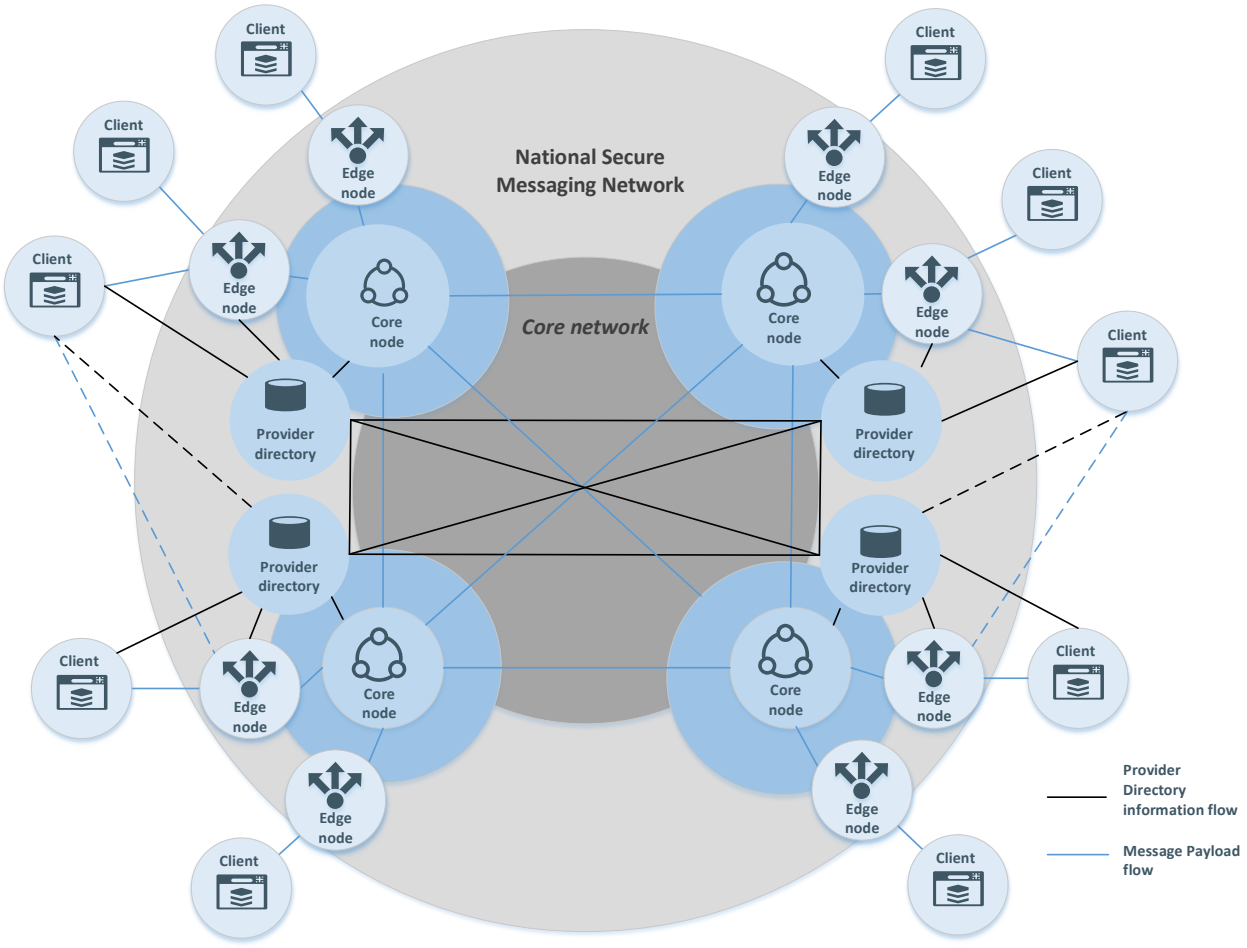


Figure 1 - NSMN Solution Roles

Note:

1. *Participating CIS typically play both the Sending System and Receiving System roles. They are shown as "Client" in Figure 1.*
2. *Participating Edge Node systems typically play both the Sending Client and Receiving Client roles. They are shown as "Edge Node" in Figure 1.*
3. *Clients may have relationships and use more than one Edge Node to send and receive messages (although overtime it is expected that this flow will become redundant)*

4.1 Core Node

The foundation of the NSMN is a core network of fully interconnected Core Nodes. A Core Node is responsible for exchanging messages securely with other Core Nodes in the NSMN and providing message sending and receiving services for their connected Edge Nodes. A Core Node is also responsible for maintaining and exposing a Provider Directory containing address information for its Edge Nodes.

A Core Node is defined as a node that is capable of directly connecting to every other Core Node in the network.

4.2 Sending Edge Node and Receiving Edge Node

An Edge Node is the interface between a Core Node and a healthcare provider organisation's internal systems.

An Edge Node is a delivery point in the network with a logical address where a healthcare provider organisation can receive and/or send messages.

There are two types of Edge Node roles:

- **Sending Edge Node**: responsible for the signing, encryption and transmission of outbound messages to a Core Node. The Sending Edge Node receives message payloads to transmit via an interface with a Sending System.
- **Receiving Edge Node**: responsible for the receiving, decryption and validation (digital signature check) of inbound messages from a Core Node. The Receiving Edge Node transfers received message payloads to a Receiving System. A Receiving Edge Node is represented in a provider directory by one or more endpoint entries.

4.3 Sending System and Receiving System

Sending Systems and Receiving Systems are authoring and rendering systems that uses the NSMN to exchange messages securely. In general, they should only need to connect to one Edge Node.

- **Sending System**: responsible for the creation, management and release of outbound message payloads.
- **Receiving System**: responsible for validating incoming clinical documents, rendering their contents and importing them into the patient record.

4.4 Provider Directory

A Provider Directory is responsible for containing and exposing structured information about Providers participating in the NSMN.

5 Capabilities

The NSMN requires the following capabilities:

- Public key infrastructure
- Directories
- Addressing
- Transmission and carriage
- Payload authoring
- Payload processing and rendering

5.1 Public key infrastructure

A key capability of the NSMN is to ensure that the identity of participants can be established, and that all participants trust that appropriate processes have been undertaken to assure identity. Public key infrastructure (PKI) is used for this purpose.

The most widely accepted and trusted Certificate Authority for healthcare organisations is the National Authentication Service for Health (NASH), which issues PKI certificates to healthcare providers and supporting organisations in the HI Service.

NASH PKI certificates support the encryption and signing of message payloads (as per ATS-5821[23] E-Health XML Secured Payload Profiles).

Participants may use NASH or commercially issued PKI certificates for mutual (client and server) x509 authentication (as per ATS-5820 E-Health Web Services Profiles).

Other identity providers and authentication protocols exist but are subject to local private agreements and trust models.

(Note: Provider Digital Access (PRODA) is a national online identity verification and authentication system that supports the authentication of healthcare individuals. PRODA can only be used to authenticate access to government systems and is not an alternative to PKI in secure message delivery and is not compatible with existing PKI-based signing and encryption.)

5.2 Directories

To address a message, a Sending System must find the appropriate Receiving Edge Node for delivery to the intended recipient. This is facilitated through an Australian profiled Provider Directory FHIR based API that federate the results of directories across the NSMN and presents the results to enable the message to be appropriately addressed.

Each Core Node in the network provides a directory of all Receiving Edge Nodes in the network so that a Sending System can find all potential recipients by executing a search against *one* Core Node's provider directory.

5.3 Addressing

The Secure Message Addressing - Implementation Guide provides implementation guidance and clarity on how directory identifiers and secure message addressing interact.

Secure messages generally include the following addresses:

- An address (identifier) for the Edge Node in the secure messaging network where the intended recipient of the message can be reached (mandatory in all messages, used to populate message segment MSH-6)
- An address (identifier) for the Edge Node in the secure messaging network where the sender of the message can be reached (mandatory in all messages, used to populate message segment MSH-4)
- An address (identifier) for the intended recipient of the message (included in many messages, used to populate PRD intending recipient or PV1.9 segment of MDM-T02 and ORU^R01)
- An address (identifier) for a software application where the intended recipient of the message can receive it (optional, this is used to populate message segment MSH-5)

Intended recipient

A clinical user will first typically search an address book or directory for the intended recipient of a message. Secure messaging standards support the following kinds of intended recipient:

- A practice or clinic (represented as a Healthcare Service in the FHIR Provider Directory API) or
- An individual practitioner at a practice or clinic (represented as a Practitioner Role in the FHIR Provider Directory API)

Edge Node

Edge Nodes are the handover point between the messaging network and the receiving organisation. Once an Edge Node delivers a message to a receiving organisation's System, the organisation takes responsibility for delivering the message to the intended recipient.

5.4 Transmission and carriage

Core Nodes must implement the ATS-5822 [1]E-Health Secure Message Delivery standard as their interface for connecting to other Core Nodes in the network.

A Core Node and Edge Node should also choose to implement ATS-5822[1] E-Health Secure Message Delivery interfaces when interacting with each other, unless agreed by both parties to use a proprietary interface. The use of ATS-5822[1] is recommended for any Edge Nodes that are intended to connect to multiple Core Nodes.

The transmission and carriage capabilities of Edge Nodes that implement ATS-5822[1] E-Health Secure Message Delivery also depend on the public key infrastructure capability for signing and encrypting sealed messages as per the ATS-5821[2][3] E-health XML secured payload profile standard.

[1] Recognising the need to update TLS to a current minimum of v1.2
[2] Recognising the need to update signatureMethod and digestMethod to a current minimum of RSA-SHA256
[3] Recognising the need to update encryption from RSA 1.5 to the currently recommended mandatory minimum AES-128 GCM

5.5 Payload authoring

Sending Systems have the capability to create, manage and release outbound message payloads to an Edge Node which then signs and encrypts the payload for delivery. Sending Systems generate outbound referral, discharge summary and other clinical documents, then pass them to a Sending Edge Node for digital signing, encryption and transmission. Receiving Systems generate responses/acknowledgements and pass them to a Receiving Edge Node for digital signing, encryption and transmission.

There are two broad categories of widely interoperable message payloads that Sending Systems may support:

- A packaged CDA document conforming to the Agency's clinical document specifications, encapsulated within an HL7 v2 Medical Document Management (MDM) message.
- An HL7 v2 message conforming to HL7AUSD-STD-OO-ADRM-2021.1 - HL7 Australia. For example, a patient referral (REF I12) or observation result (ORU R01).

Payload authoring also depends on the public key infrastructure capability for signing CDA packages as per the Agency's CDA Package v1.0 standard.

Other payload types may be supported where there is localised agreement between senders and receivers.

5.6 Payload processing and rendering

Receiving Systems have the capability to process incoming message payloads (transferred from an Edge Node), render their contents and optionally import them into the patient record.

This includes Receiving Systems extracting the packaged CDA document from within an MDM message and validating the signature applied to the CDA package.

They must also be capable of rendering the contents of the message payload (either the CDA document or the contents of a HL7 message) in an appropriate format for end users.

A receiving organisation's systems are also responsible for "internal routing" of a message to its intended recipient, as described in the 'Directories and Addressing' capability.

6 Required standards

6.1 Core Node

The following table provides a summary of the capabilities and related standards for a Core Node:

Capability	Related standards
Public key infrastructure	**X.509**: for certificates that are used for transport-level encryption (as per ATS-5822 Secure Message Delivery). Certificates must be issued by a Certificate Authority that is trusted by all other Core Nodes in the secure messaging national network.
Directories	**AU-FHIR-PD**[4]: for invoking lookups of a provider directory *(Note: other proprietary APIs may be invoked for address directory lookups in addition to AU-FHIR-PD)* **ATS-5820 E-Health Web Services Profiles**: for mutual x509 authentication to the provider directory
Transmission and carriage	**ATS-5822**[1] **E-Health Secure Message Delivery**: for communicating with other Core Nodes and optionally with Edge Nodes *(Note: other proprietary APIs and services may be used to support transmission between core and Edge Nodes by agreement)*

6.2 Edge Node

The capabilities and related standards for an Edge Node are listed below:

Capability	Related standards	Applies to
Public key infrastructure	**X.509**: for certificates that are used to encrypt and sign message payloads (as per ATS-5821[23] E-Health XML Secured Payload Profiles). Certificates must be issued by a Certificate Authority (usually NASH, but others by agreement) that is trusted by other Edge Nodes in the NSMN.	Sending Edge Node Receiving Edge Node

[4] Recognising that this version of PD needs to be updated to v2.1 when ballot is complete. PD 2.1 will be based on AU Base 4.1.0

Capability	Related standards	Applies to
Directories	**AU-FHIR-PD**: for invoking lookups of a provider directory *(Note: other proprietary APIs may be invoked for address directory lookups in addition to AU-FHIR-PD)* **ATS-5820 E-Health Web Services Profiles**: for mutual x509 authentication to the provider directory *(Note: other proprietary protocols (such as IP whitelisting, API keys) may be supported (based on private agreements) for authentication in addition to mutual x509).*	Sending Edge Node Receiving Edge Node
Transmission and carriage	**ATS-5822**[1] **E-Health Secure Message Delivery**: for communicating with Core Nodes using standardised interfaces (via the sender and receiver roles) *(Note: proprietary APIs and services may be used to support transmission between Core and Edge Nodes that are operated by the same messaging provider)* **File Drop:** The exchange of standard HL7 V2 payloads via a local file system is a common convention for the exchange of messages between Edge Nodes and Clients.	Sending Edge Node Receiving Edge Node

6.3 Provider Directory

The capabilities and related standards for Provider Directories are listed below:

Capability	Related standards
Directories	**AU-FHIR-PD**[4]: for containing and providing access to a healthcare providers directory with support for aggregating information from directories **ATS-5820 E-Health Web Services Profiles**: for mutual x509 authentication to the provider directory

6.4 Sending Systems and Receiving Systems ("Clients")

The capabilities and related standards for Sending Systems and Receiving Systems are listed below:

Capability	Related standards	Applies to
Public key infrastructure	**X.509**: for certificates that are used to sign clinical documents (in CDA). Certificates must be issued by a Certificate Authority (usually NASH, but others by agreement) that is trusted by the receiving organisation.	Sending System

Capability	Related standards	Applies to
Directories	**AU-FHIR-PD**[4]: for invoking lookups of a provider directory *(Note: other proprietary APIs may be invoked for address directory lookups in addition to AU-FHIR-PD)* **ATS-5820 E-Health Web Services Profiles**: for mutual x509 authentication to the provider directory *(Note: other proprietary protocols (such as IP whitelisting, API keys) may be supported (based on private agreements) for authentication in addition to mutual x509).*	Sending System
Transmission and carriage	**ATS-5822**[1] **E-Health Secure Message Delivery**: for communicating with Edge Nodes using standardised interfaces (via the sender and receiver roles) *(Note: proprietary APIs and services may be used to support transmission between Clients and Edge Nodes that are operated by the same messaging provider)* **File Drop:** The exchange of standard HL7 V2 payloads via a local file system is a common convention for the exchange of messages between Edge Nodes and Clients.	Sending System Receiving System

Capability	Related standards	Applies to
Payload authoring	**HL7 v2**: for creating message payloads according to the relevant specifications: Referrals • HL7 v2.4 REF^I12-L1[5] or • Agency eReferral CDA package wrapped with HL7 v2.3.1 MDM^T02 or • Agency Service Referral CDA package wrapped with HL7 v2.3.1 MDM^T02 • *(Note: that eReferral CDA is retained for compatibility with existing implementations, but new implementations should use Service Referral CDA)* Discharge summaries • HL7 v2.4 REF^I12-L1[5] or • Agency Discharge Summary CDA package wrapped with HL7 v2.3.1 MDM^T02 Specialist letters • HL7 v2.4 ORU^R01[5] or • HL7 v2.4 REF^I12-L1[5] or • Agency Specialist Letter CDA package wrapped with HL7 v2.3.1 MDM^T02 Observation orders (HL7 v2.4 ORM^O01[5]) Observation results (HL7 v2.4 ORU^R01[5]) Application acknowledgements[5] • RRI^I12 or • ACK^T02, ACK^O01, ACK^R01 **CDA/Agency specifications**: for the creation of clinical documents according to the relevant Agency clinical document specifications and signing CDA packages as per the Agency's CDA Package v1.0 standard	Sending System Receiving System

[5] References current draft standard - check for the latest active standard version via this page HL7 Australia Standards Development - HL7 Australia Standards Development - HL7 Australia

Capability	Related standards	Applies to
Payload processing and rendering	**HL7 v2**: for processing incoming message payloads and creating application-level acknowledgements according to the relevant specifications: Referrals • HL7 v2.4 REF^I12-L1[6] or • Agency eReferral CDA package wrapped with HL7 v2.3.1 MDM^T02 or • Agency Service Referral CDA package wrapped with HL7 v2.3.1 MDM^T02 • *(Note: that eReferral CDA is retained for compatibility with existing implementations, but new implementations should use Service Referral CDA)* Discharge summaries • HL7 v2.4 REF^I12-L1[5] or • Agency Discharge Summary CDA package wrapped with HL7 v2.3.1 MDM^T02 Specialist letters • HL7 v2.4 ORU^R01[5] or • HL7 v2.4 REF^I12-L1[5] or • Agency Specialist Letter CDA package wrapped with HL7 v2.3.1 MDM^T02 Observation orders (HL7 v2.4 ORM^O01[5]) Observation results (HL7 v2.4 ORU^R01[5]) Application acknowledgements[5] • RRI^I12 or • ACK^T02, ACK^O01, ACK^R01 **CDA/Agency specifications**: for validating the signatures of CDA packages and rendering clinical documents, according to the relevant Agency clinical document specifications and signing CDA packages as per the Agency's CDA Package v1.0 standard.	Sending System Receiving System

[6] References current draft standard - check for the latest active standard version via this page HL7 Australia Standards Development - HL7 Australia Standards Development - HL7 Australia

7 Implementations

This section provides an overview of how different software product deployments may implement the logical roles involved in secure messaging.

7.1 Roles

Different software products in different deployments may implement the capabilities of one or more of the logical roles in the National Secure Messaging Network. Some examples include:

Core Node

- A messaging gateway product provided (and hosted) by a secure messaging vendor that has entered into the Core Node Agreement to communicate with all other Core Nodes in the network
- A cloud-based CIS / EMR / PMS product that has implemented secure messaging functionality and entered into the Core Node Agreement to communicate with all other Core Nodes in the network

Sending Edge Node and Receiving Edge Node

- A messaging agent product provided by a secure messaging vendor, usually installed on-premises
- A cloud-based CIS / EMR / PMS product that has implemented secure messaging functionality and can communicate with one or some, but not all Core Nodes in the network[7]

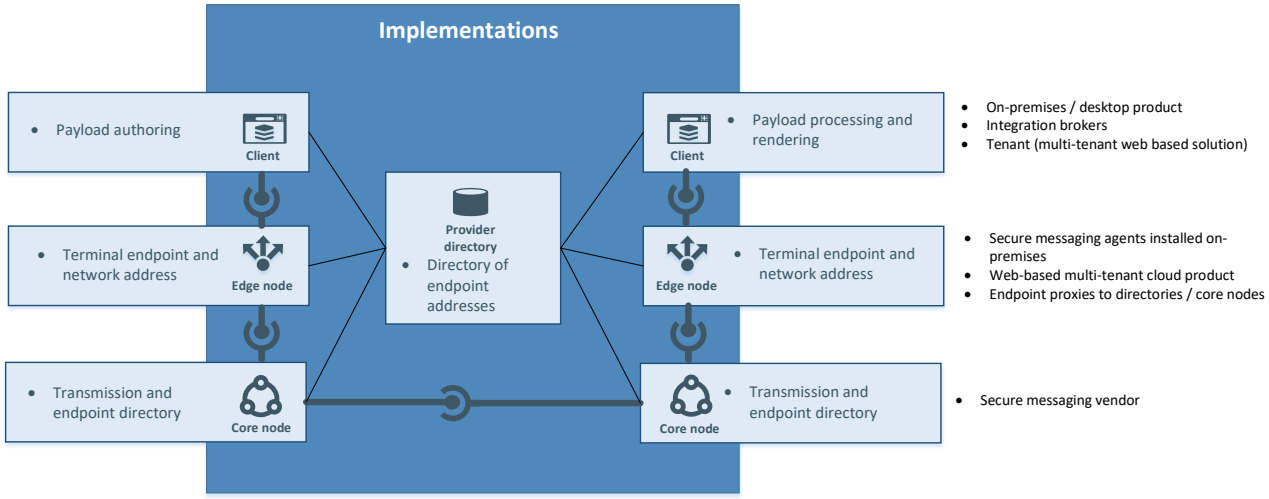
Sending System and Receiving System

- A desktop CIS / EMR / PMS product installed on-premises
- A cloud-based CIS / EMR / PMS product connects to the secure messaging network through a software product from another supplier that acts as a Sending Edge Node and Receiving Edge Node[1]
- An integration broker managing payload creation / processing for other client products

Provider Directory

- A Provider Directory may be implemented independently and contain consolidated provider addressing information (e.g., NHSD)
- A Provider Directory shall be implemented by a Core Node and only contain Edge Node addressing information relevant to a Core Node

[7] encryption/signing certificates should be managed by the tenant of cloud offering, and be independently revokable by the tenant. i.e. messages created should use a certificate of the tenant rather than certificate of cloud provider

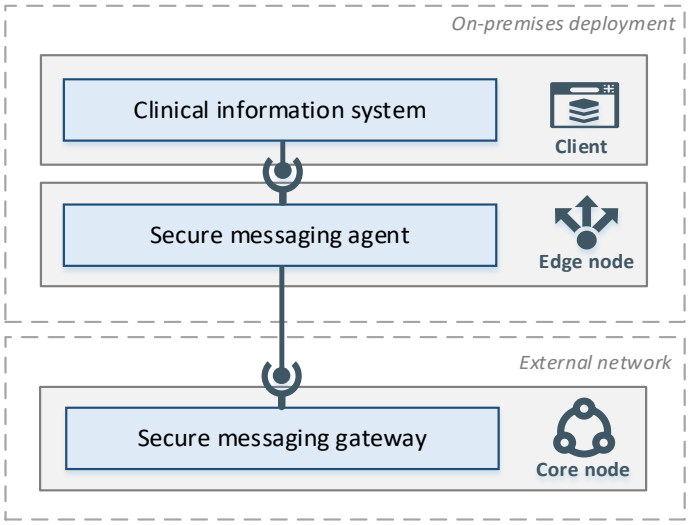


7.2 Deployment examples

The following diagrams provide two examples of typical secure messaging deployments. In all deployments, a Receiving Edge Node will have one or more payload types per endpoint, and the same endpoint may be used for addressing a message to multiple practitioner roles and /or healthcare services.

7.2.1 CIS as on-premises desktop product

A traditional on-premises CIS/EMR/PMS product will implement the *Sending System* and *Receiving System* roles with a secure messaging agent implementing the *Sending Edge Node* and *Receiving Edge Node* roles. The secure messaging agent manages communication with the secure messaging gateway, which implements the Core Node role.

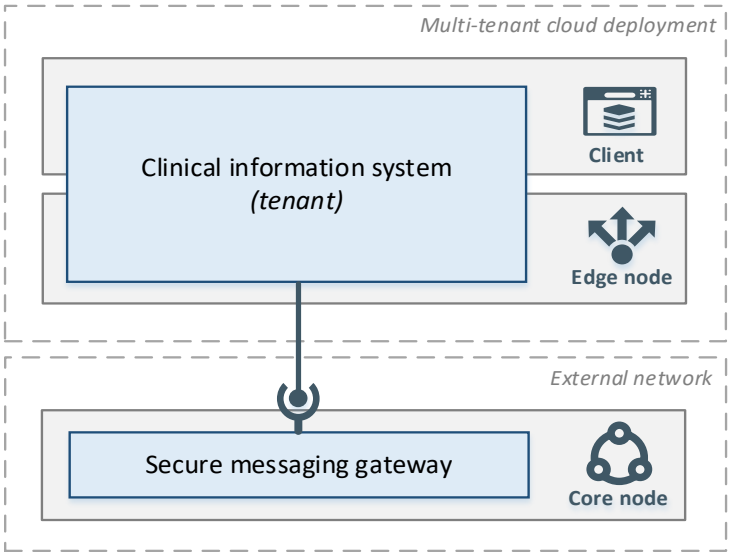


Key notes:

- A client should only need to connect to one Edge Node as all Core Nodes are interconnected.

7.2.2 CIS as web-based multi-tenant cloud

A CIS/EMR/PMS may be a web-based multi-tenant cloud product. In this example, the cloud product implements the *Sending System, Sending Edge Node, Receiving Edge Node* and *Receiving System* roles providing a standardised platform for their tenants to exchange information with an external secure messaging gateway that fulfils the *Core Node* role.



Key notes:

- Each tenant shall have their own PKI certificate, and their own endpoints for their supported payload types (i.e. each tenant has its own logical Receiving Edge Node within the cloud solution).
- The platform connects to a Core Node on behalf of the tenants and implements a separate "logical edge node" for each tenant.