
# HealthLink Messaging System
# Message Security

## Version 1.2

## Document Control

| | |
|---|---|
| **Version** | 1.2 |
| **Last Saved** | 21 Jan 2014 |
| **Author** | Lars Becker |
| **Filename** | HMS Message Security v1.2 20070904.doc |

## Approvals

| **Development** | **Signed** | **Date** |
|---|---|---|
| | | |
| **Service Delivery** | | |
| | | |

## Document History

| **Version** | **Date** | **Author** | **Comment** |
|---|---|---|---|
| 1.0 | 10 Oct 2006 | Lars Becker | Initial creation |
| 1.1 | 11 Oct 2006 | Lars Becker | Review results Graeme Stretch included |
| 1.2 | 04 Sep 2007 | Lars Becker | Minor corrections |
| 1.2 | 01 Jan 2014 | Nick Rowland | Publish document to website |

## Related Documents

| **Document** | **Source** |
|---|---|
| | |
| | |

# Table of Contents

**1 Introduction ..... 5**

**2 HealthLink's PKI Infrastructure ..... 5**

2.1 Channel Encryption ..... 5
2.2 Message Encryption ..... 6
2.3 Digital Signature ..... 6
2.4 Encryption Algorithms ..... 6

**3 Message Tracking ..... 6**

**4 Security Evaluation ..... 7**

4.1 Identification ..... 7
4.2 Authentication ..... 7
4.3 Authorisation ..... 8
4.4 Confidentiality ..... 8
4.5 Integrity ..... 8

# 1 Introduction

The purpose of the HealthLink Messaging System (HMS) is to reliably and securely transmit messages in the health sector. All health-related information is highly sensitive as it is closely related to the privacy rights of patients. Its transmission through electronic data networks, hence, has to meet high standards in terms of information security.

The HealthLink Messaging System is designed to meet these requirements. This document describes the information security aspects of the HMS. Chapter 2 gives an overview over the various security mechanisms implemented in HMS; chapter 3 compares these mechanisms with an accepted set of criteria for the evaluation of messaging systems security.

# 2 HealthLink's PKI Infrastructure

The security architecture of the HealthLink Messaging System is based on a Public Key Infrastructure (PKI). PKIs rely on pairs of long numbers (key pairs) generated using special algorithm that have two unique characteristics:

- Even when the generation algorithm for a key pair is well-known, it is (within any reasonable timeframe) not possible to compute the second key when only one key is known.
- A message encrypted with one key can only be decrypted with the other key of the same key pair. The encryption mechanism is commutative, i.e. each key of a key pair can be used for encryption and decryption.

From any generated key pair, one key is treated as the private key, only accessible by its owner, and a public key, freely distributable to and publicly accessible by any interested party. In order to ensure that any public key, actually, belongs to its owner, the public key is signed by a mutually trusted certification authority. This digital signature together with the public key is wrapped into a digital certificate using the X.509 certificate standard.

HMS supports the Australian Gatekeeper standard, which requires the usage of two different key pairs (hence, two private keys and associated digital certificates) per user. One of the key pairs is used for generating and verifying digital signatures, the other key pair is used for encrypting and decrypting messages.

## 2.1 Channel Encryption

All communication performed over the open internet is protected against eavesdropping and manipulation using the SSL encryption standard. This standard uses symmetric encryption within each session, based on a session key that is

dynamically established between the communicating parties. This establishment process is based on the parties' asymmetric key pairs.

In addition to that, connections can also be protected using IPSec tunnels.

## 2.2 Message Encryption

Each message to be submitted to the HMS messaging infrastructure is automatically encrypted by the sending HMS Client using the recipient's public key. As only the message recipient has access to the private key necessary to decrypt the message, this mechanism ensures that only the message recipient is able to decrypt the message.

## 2.3 Digital Signature

Each message also gets digitally signed by the sending HMS Client using the sender's private key. This ensures the authenticity of the message sender. All parties involved, including the message recipient and the HMS infrastructure components, are able to verify the authenticity of the message by verifying its digital signature.

## 2.4 Encryption Algorithms

HMS uses the following ciphers:

| | |
|---|---|
| Symmetric cipher: | DESede/CBC/PKCS5Padding |
| Asymmetric cipher: | RSA/ECB/PKCS1Padding |
| Session key generation algorithm: | DESede |
| Public/private key pair algorithm: | RSA |

# 3 Message Tracking

The HMS infrastructure components automatically track each message transmitted. Each message is uniquely identified by its message identifier and the EDI account names of sender and recipient. The tracked information also includes the application type, message type, timestamp, message size etc.

The message recipient is required to generate a (positive or negative) response message when receiving the message (for HL7 messages, this behaviour is already part of the HL7 standard). This response message is automatically matched with the original message by the HMS message tracking system.

HealthLink provides a web-based application (HealthLink User Online; HUO) for online access to its message tracking database. Messages acknowledged by the recipient cannot effectively be repudiated by the recipient as the HUO application provides all parties with the necessary non-disputable tracking information.

# 4 Security Evaluation

A secure messaging system must provide the following features:

- Identification
- Authentication
- Authorisation
- Confidentiality
- Integrity

The following sections describe the relevant requirements for each of these features and their implementation by the HealthLink Messaging System. Please refer to chapter 2 for a thorough description of the HMS security infrastructure.

Please note that the term *user* used throughout this document applies to every user entity that is participating in the exchange of messages in the HealthLink Messaging System, e.g. individuals, providers, facilities as well as infrastructure and server components.

## 4.1 Identification

*How does the messaging system accurately identify the users involved?*

Each user has to apply with HealthLink (or any other trusted certification authority) for the issuing of a unique digital certificate. The application and certificate issuing process ensures the unambiguous identification of each applying user.

As a result of this process, HealthLink assigns a unique EDI account name to the user and issues a digital certificate. The private key generated as part of this process is only accessible by the user themselves. The digital certificate containing the public key is stored by HealthLink in a centralised repository (please refer to chapter 2 for details). All HMS components access this repository for retrieving digital certificates based on their users' EDI account names.

## 4.2 Authentication

*How does the messaging system confirm the credentials of a user's claimed identity?*

Each user's private key is securely stored in a passphrase-protected PKCS-12 key store. Every time the user starts their local HMS Client, the system requires the user to enter this passphrase. The HMS Client uses the private key for generating the user's digital signature.

Other components of the HMS use the user's digital certificate for verifying the user's digital signature, thus effectively and securely authenticating the user. This mechanism is used for both, channel security (using SSL with client authentication) and message security.

Along with each message, the HMS Client always submits the sender's digital signature to the recipient. By verifying the digital signature using the sender's digital certificate, the message recipient ensures the sender's authenticity.

## 4.3 Authorisation

*How does the messaging system ensure that users are able to perform the tasks that they are permitted to, and that they are prevented from performing tasks that they are not permitted to?*

The functionality of the HMS Client (sending, receiving, processing and de-processing messages) is available to all users who have successfully been authenticated.

Elaborate, role-based authorisation mechanisms are in place for the HealthLink-operated HMS infrastructure components. These mechanisms are based on and integrated with HealthLink's centralised certification management system.

## 4.4 Confidentiality

*How does the messaging system ensure that information is not exposed to unintended parties?*

HMS uses asymmetric encryption based on private keys and digital certificates. Each outgoing message is automatically encrypted by the HMS Client before it is submitted to HMS components outside of the user's premises.

The HMS Client uses the digital certificate of the message recipient to encrypt the message. It can hence only be decrypted with the private key of the recipient. As this private key is only accessible by the message recipient, no other user can access the message content. This includes all HMS infrastructure components.

## 4.5 Integrity

*How does the messaging system ensure that information is not unintentionally altered?*

HMS uses digital signatures for both, authenticating the message sender and ensuring the message integrity. The HMS Client automatically generates a digital signature for the encrypted message before it is submitted to HMS components outside of the user's premises. It uses the user's private key for generating the signature. The signature is submitted together with the encrypted message content.

The recipient verifies the signature using the message sender's digital certificate. This verification ensures that the message has not been modified.