PHIN

SECURE MESSAGE TRANSPORT GUIDE

Version 2.0

7/31/08

DOCUMENT CHANGE HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
0.1	John Thomas Barry Rhodes	02/10/2005			Initial Draft
1.0	Tom Brinks	05/09/2007	Tim Morris	5/30/2007	Second Draft – compiled document from Cross Functional Components and Secure Messaging Guide
2.0	Tom Brinks	03/26/2008	Gautam Kesarinath	3/26/2008	Third draft o Includes comments from DAMC staff & Dr. Raja Kailar o Updated to reflect PHIN Requirements v2.0
2.0	Tom Brinks	07/31/2008			Included comments from DAMC

TABLE OF CONTENTS

1 INTRODUCTION

1.1 BUSINESS CONTEXT

The electronic transfer of public health data involves the ability to securely and automatically send and receive information between computer systems, to achieve a "live" network for data exchange between partners in public health, i.e. the Public Health Information Network (PHIN).

The Centers for Disease Control and Prevention has advanced a standards-based approach to secure, reliable, bi-directional message transport across the Internet. The resulting Public Health Information Network (PHIN) specification calls for ebXML messaging on top of SOAP web services, XML Encryption, XML Digital Signature, and SSL authentication using client side certificates and/or passwords. The use of these industry standard specifications ensures that public health data is securely, reliably and automatically sent and received between health data systems. To effectively exchange information, both sending and receiving parties must adhere to the same specifications. This provides guidance of how to implement systems that securely send and receive public health data.

1.2 OBJECTIVES

The objective of the *PHIN Secure Message Transport Guide* is to provide:

- Requirements for secure message transport within the PHIN framework

This specification attempts to generalize message transport processing so that existing or proposed public health applications can more easily be integrated into a PHIN compatible public health infrastructure.

1.3 SCOPE

This document describes the processes, data flows, system components, and relevant standards and specifications that constitute the PHIN Secure Messaging. This document provides an architecture view of the work that is performed when an electronic message is created, routed, sent, and received between PHIN partner sites such as labs, public health departments or the CDC.

This specification is not prescriptive as to how specific public health messages, such as an ELR HL7 2.3.x message are created nor does this guide address how messages are routed based on message content. For information on creating specific public health messages, please reference PHIN messaging implementation guides which can be found at *http://www.cdc.gov/phin/resources/guides.html.*

Scope of this specification is limited to high-level requirements of the PHIN Secure Messaging Integration Point. The document does not prescribe specific platforms, technologies or infrastructure components that constitute a physical instance of the integration point. These aspects of system architecture should be further defined in system design documents. The intent of this document is to provide enough specificity to promote rapid and consistent development of PHIN compatible messaging transport systems without unduly constraining the development of such systems.

Implementations based on this guide should be able to interoperate ("over the wire") with CDC's PHIN Messaging System (PHINMS). Detailed interoperability features can be found in the ebXML Messaging Services Specification Version 2.0 (ebMS) at *http://ebxml.org*. However, there is no guarantee of interoperability until an implementation is tested using PHINMS.

1.4 HIGH LEVEL OVERVIEW

Essential functional elements of the PHIN Secure Messaging integration point consist of the ability to securely send and receive public health messages between designated end-points. The following illustration, ***Figure 1-1,*** is a business process diagram of the PHIN Secure Messaging in Business Process Modeling Notation (BPMN).

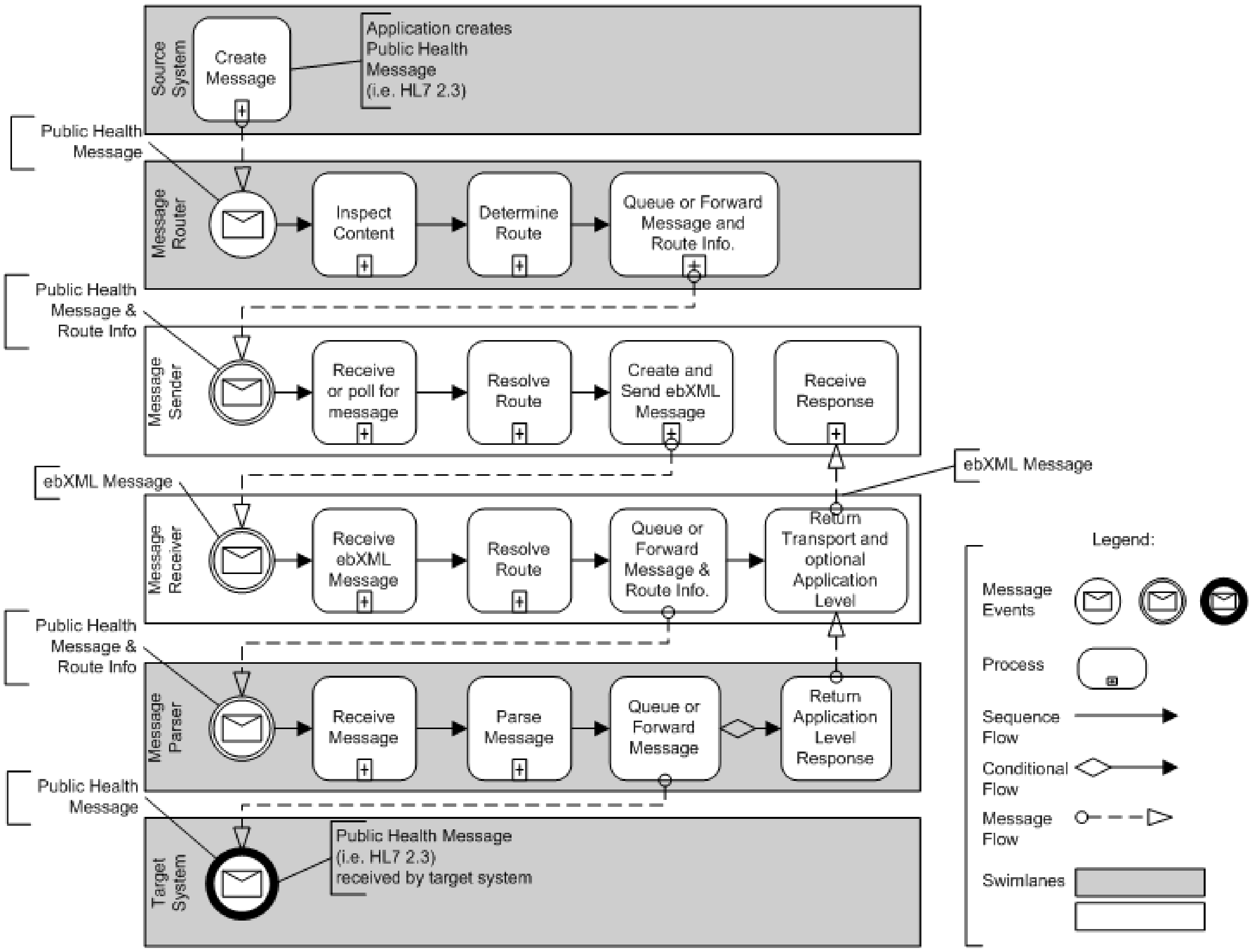
Source System
Create Message
Application creates Public Health Message (i.e. HL7 2.3)
Public Health Message
Message Router
Inspect Content
Determine Route
Queue or Forward Message and Route Info.
Public Health Message & Route Info
Message Sender
Receive or poll for message
Resolve Route
Create and Send ebXML Message
Receive Response
ebXML Message
ebXML Message
Message Receiver
Receive ebXML Message
Resolve Route
Queue or Forward Message & Route Info.
Return Transport and optional Application Level
Public Health Message & Route Info
Message Parser
Receive Message
Parse Message
Queue or Forward Message
Return Application Level Response
Public Health Message
Target System
Public Health Message (i.e. HL7 2.3) received by target system
Legend:
Message Events
Process
Sequence Flow
Conditional Flow
Message Flow
Swimlanes

Figure 1-1: PHIN Secure Messaging

All PHIN Secure Message processing occurs in the Message Sender and Message Receiver swim-lanes. The Source System, Message Router, Message Parser and Target System swim-lanes and the processes that occur within them are not within scope of PHIN Secure Messaging integration point. PHIN Secure Messaging starts upon acceptance of the public health (HL7) message and associated routing information from a Message Router. PHIN Secure Message processing ends upon receipt of the Public Health Message and associated routing information by the receiver-side Message Parser.

Message Sender and Message Receiver processing is based on the ebXML Messaging Service specification (ebMS) version 2.0. The ebXML specification extends XML based Simple Object Access Protocol (SOAP) specifications with essential capabilities to securely and reliably send messages over the Internet. EbXML's flexible enveloping technique allows payloads of any format type to be securely transported over the Internet.

The ebXML specification also provides a reliable messaging function which defines an interoperable protocol where any two Message Service implementations can reliably exchange messages guaranteeing "once-and-only-once delivery."

2 MESSAGE TRANPORT FUNCTIONAL REQUIREMENTS

The requirements in the section describe the baseline functionality for secure message transport within the PHIN framework. These secure message transport requirements address: securely and reliably exchanging messages over the Internet using the ebXML protocol, and security controls to prevent unauthorized access to systems and data.

2.1 SECURE MESSAGE TRANSPORT

Secure Message Transport refers to the secure, reliable, bi-directional exchange of information between public health partners. Security and privacy requirements necessitate that information generally be encrypted and that communications be performed in a way which ensures delivery to the intended recipient(s) only. Messages are securely transported over the Internet using standards such as ebXML, Public Key Infrastructure (PKI), and Secure Socket Layer (SSL), which are described in the following sections.

The CDC has developed PHIN Messaging Service (MS) as an implementation of the standards supporting secure message transport. Exchange partners must use a secure transport protocol that is compatible with PHIN MS. PHIN MS fully implements PHIN standards for secure messaging and is available from CDC. More information about PHIN MS is available at *http://www.cdc.gov/phin/phinms*. However, the use of PHIN MS is not required as long as PHIN data exchange requirements can be met using a PHIN MS compatible solution.

2.1.1 Transport Standard

The ebXML Messaging Service (ebMS) is the industry standard used by PHIN for message transport across the Internet for the exchange of sensitive health data information between partner organizations. It supports a neutral format for carrying messages between different systems, such as between legacy systems and web services applications. It is designed to work with any communications protocol, and the content of messages carried over ebMS can be in any format. The ebMS standard is a set of layered extensions on the Simple Object Access Protocol (SOAP) to support business-to-business transactions. More information on ebXML and ebMS is available at http://www.oasis-open.org/home/index.php.

2.1.1.1 Systems must transport messages across secure channels using the ebXML protocol.

2.1.1.2 Systems should be able to handle common network failures and should be able to deliver undelivered messages automatically when network connectivity has been restored using retries and delayed retries.

2.1.1.3 Systems should detect and handle duplicate message submissions.

2.1.1.4 Systems should guarantee the "once and only once" delivery of messages.

2.1.1.5 System should support small sites that only have an outbound connection to the Internet by allowing them to receive messages by polling a server.

2.1.2 Secure Transport

2.1.2.1 Hypertext Transfer Protocol (HTTP) over Secure Socket Layer (SSL), or HTTP over SSL (HTTPS), is required to ensure secure communication. HTTPS is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the web server. HTTPS is the use of SSL as a sub-layer under its regular HTTP application layering.

2.1.2.1.a For system-to-system communication over the Internet, the HTTPS protocol must be used to protect communication confidentiality at all times.

2.1.2.1.b HTTPS should be used for communication between DMZ components and Intranet components. DMZ, or "demilitarized zone", refers to a computer or sub network that sits between a trusted internal network and an untrusted external network.

2.1.2.2 Strong authentication mechanisms must be applied to data exchange partners, as described in section *2.2 System Security and Availability* of this document.

2.1.2.3 Stored data from messages should be protected using strong authentication and authorization as described in section *2.2 System Security and Availability* of this document.

2.1.2.4 Messaging partners must be authorized to send data, as described in section *2.2 System Security and Availability* of this document.

2.1.2.5 The XML Encryption standard should be used to represent the encrypted content and the information that enables an intended recipient to decrypt it. This standard makes use of Public Key Infrastructure (PKI) so that only the intended receiver can read the message. The public key of the intended message recipient is used to encrypt the message. Upon receipt, the recipient decrypts the message using their private key. More information on XML Encryption is available at *http://www.w3.org/TR/xml-encryption-req*.

2.1.2.6 The XML Digital Signature standard should be used to insure message integrity and non-repudiation. Digital signatures are created by performing an operation on information such that the receiver of the message can confirm that the message originator created the message and that the signed message was not subsequently changed. More information on XML Digital Signature is available at *http://www.w3.org/TR/xmldsig-core*.

2.1.2.7 System must maintain detailed logs of messages sent and received, success and error conditions.

2.1.2.8 Systems should transport payloads encrypted end-to-end not just point-to-point.

2.2 SYSTEM SECURITY AND AVAILABILITY

Systems and data supporting PHIN must be protected from sabotage, corruption, and unauthorized access, and must be available subsequent to a catastrophic event. System security should also assure that processes cannot be initiated or controlled by unauthorized individuals.

2.2.1 User Authentication and Authorization

2.2.1.1 A user authentication mechanism must be used to validate that the user is registered to use the system and has signed on with the appropriate user name and password or other identifiable key.

2.2.1.2 Strong authentication mechanisms, such as X.509 certificates or secure token based technology, are recommended.

2.2.1.3 User authorization levels must be supported to manage access to system functions and data. Authorization levels can include user based, role based and/or context based (e.g., work hours vs. after-hours; on-site vs. remote; during investigation vs. normal business) authorization.

2.2.1.4 Access control rules must be implemented to enforce authorization levels and control user access to the system. For example, access control should allow a jurisdiction to view its own data but should not allow access to data for other jurisdictions, unless expressly permitted.

2.2.1.5 System access by users must be audited.

2.2.2 Secure System Management

2.2.2.1 A firewall must be employed to protect resources from external threats.

2.2.2.1.a Firewalls will need to securely provide access to an ebXML SOAP receiver to present a service for secure Internet receipt of public health information as well as secure access to restricted access web sites.

2.2.2.2 System integrity mechanisms like intrusion detection software and/or virus scanners should be employed to protect resources from both external and internal threats.

APPENDIX A – PHIN SECURE MESSAGE TRANSPORT STANDARDS

The following standards relate to PHIN Secure Message Transport.

Standard	Version
ebMS (ebXML Message Service)	2.0
FIPS 140-2 (Cryptographic Module Validation Program)	
FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems)	
HTTPS (SSL over HTTP)	
XML Digital Signature	RSA-1.5 and SHA-1 (digest algorithm)
XML Encryption	RSA-1.5 and Triple-DES-CBC
PKI / X.509 Digital Certificates	
SOAP	1.1
Two-way SSL (using client certificates)	3.0
TLS	1.0
CPA (Collaboration Protocol Agreement)	1.0
LDAP (Lightweight Directory Access Protocol)	
TCP/IP, DNS	
HTTP Basic Authentication	