Secure, Reliable Messaging Comparisons between PHINMS, SFTP, and SSH

Public Health Information Network Messaging System (PHINMS)

Version: 1.0

Prepared by:
U.S. Department of Health & Human Services

Date: April 15, 2008

EXECUTIVE SUMMARY

Public health involves many organizations throughout the PHIN (Public Health Information Network), working together to protect and advance the public's health. These organizations need to use the Internet to securely exchange sensitive data between varieties of different public health information systems. The exchange of data, also known as "messaging" is enabled through messages created using special file formats and a standard vocabulary. The exchange uses a common approach to security and encryption, methods for dealing with a variety of firewalls, and Internet protection schemes. The system provides a standard way for addressing and routing content, a standard and consistent way for information systems to confirm an exchange.

The Centers for Disease Control and Prevention’s (CDC) Public Health Information Network Messaging System (PHINMS) is the software which makes this work. The system securely sends and receives sensitive data over the Internet to the public health information systems using Electronic Business Extensible Markup Language (ebXML) technology.

This document provides a comparison of secure network protocols which provide file transfers over a reliable data stream.

REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0	Raja Kailar	03-20-08	Implemented Comparison of PHINMS, SSH and SFTP.
1.0	Wendy Fama	04-15-08	Edited and updated document.

TABLE OF CONTENTS

ACRONYM LIST

B2B	Business-to-Business
CDC	Centers for Disease Control and Prevention
CPA	Collaborate Protocol Agreement
DMZ	Demilitarized Zone
ebMS	ebXML Messaging Services
ebXML	extensible Markup Language
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IETF	Internet Engineering Task Force
OASIS	Organization for the Advancement of Structured Information Standards
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System
PKI	Public Key Infrastructure
SECSH	Official Internet Engineering Task Force's (IETF) name
SSH	Secure Shell
TCP	Transmission Control Protocol

1.0 COMPARISON

This document provides a comparison of the following secure network protocols:

- Public Health Information Network Messaging System (PHINMS),
- Simple File Transfer Protocol (SFTP), and
- Secure Shell (SSH).

These protocols allow data to be exchanged between two or more computers over secure channels. They all encrypt the data and authenticate the origin.

1.1 Feature

FUNCTION	PHINMS	SSH	S-FTP
Primary Function	B2B Secure and Reliable Messaging	Secure remote login shell	Secure file transfers
Open Standard	ebMS 2.0 (OASIS ebXML)	SSH-1 (obsolete) and SSH-2 (current) (IETF SECSH)	Designed by IETF SECSH, but not yet an Internet standard

1.2 Security

FUNCTION	PHINMS	SSH	S-FTP
Use of PKI for Encrypting files	Yes	Yes	Yes
Use of PKI for Authenticating connections	Yes	Yes	Yes
Point-to-Point Communication Encryption	Yes	Yes	Yes
End-to-End (Payload level) Encryption	Yes	N/A (not a FTP)	No
DMZ Web-Server Proxy (Internet Best Practice)	Supports	Does not support	Does not support

1.3 Reliability

FUNCTION	PHINMS	SSH	S-FTP
Guaranteed delivery (once and only once)	Built-in	N/A (not a FTP)	Not supported
Automated sending, retries, delayed retries	Built-in	N/A (not a FTP)	Not included, needs to be scripted.
Chunking support for very large files	Built-in	N/A (not a FTP)	Not included, needs to be scripted

1.4 Routing and Workflow Support

FUNCTION	PHINMS	SSH	S-FTP
Support for synchronous message handling	Built-in	N/A (not a FTP)	Not part of standard
Collaboration agreement between trading partners	Built-in, and is part of ebMS standard (CPA)	N/A (not a FTP)	Not part of standard (need to be developed)
Metadata for sending to backend business processes behind a receiving node	Built-in, and is part of ebMS	N/A (not a FTP)	Not part of standard (need to be

FUNCTION	PHINMS	SSH	S-FTP
	standard (Service/Action)		developed)
Route-not-Read Capability to support small sites that can only receive by polling a server	Yes	N/A (not a FTP)	Not built-in, needs to be scripted.
Metadata for routing via an Intermediary to a node that receives via polling the intermediary (Route-not-Read)	Built-in	N/A (not a FTP)	Not part of standard (need to be developed)

1.5 Discovery

FUNCTION	PHINMS	SSH	S-FTP
Support within Open Standard for Node Discovery	Part of ebXML Standard (ebXML Registry) but not fully implemented in PHINMS.	Not part of standard	Not part of standard

1.6 Management

FUNCTION	PHINMS	SSH	S-FTP
Queue management	Yes	No	No

1.7 Implementation

FUNCTION	PHINMS	SSH	S-FTP
Ports	Uses standard HTTPS ports (443), supported by most organizational firewalls.	Typically uses TCP Ports (22), hence needs port opening on firewalls.	Typically uses TCP Ports (22), hence needs port opening on firewalls.