Collaboration Protocol Agreement Guide

Public Health Information Network Messaging System (PHINMS)

Version: 1.0.0

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 PHINMS (Public Health Information Network Messaging System) 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.

Creating a Collaboration Protocol Agreement (CPA) is a necessary agreement between two messaging partners.

REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0.0	Wendy Fama	03-07-08	Collaboration Protocol Agreement Guide.
1.0.0	Rajeev Seenappa	04-05-08	Reviewed document.
1.0.0	Wendy Fama	04-15-08	Finalized document.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYM LIST

CDC	Centers for Disease Control and Prevention
CPA	Collaboration Protocol Agreement
ebXML	Electronic Business Extensible Markup Language
OID	Object Identifier
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System

1.0 CPA OVERVIEW

The Collaboration Protocol Agreement (CPA) consists of rules which allow communication between hardware and software. Interoperability is a major concern when different systems attempt to communicate. Both sides must understand the same protocol for the communication to be successful. A communications protocol defines:

- rate of transmission in bits per second,
- whether the transmission is to be synchronous or asynchronous,
- whether the data is to be transmitted in half-duplex mode (data can only be transmitted in one direction at time) or full-duplex mode (data can be transmitted in both directions at once),
- rules for detecting and recovering from transmission errors, and
- rules for encoding and decoding data (data compression and decompression).

Note: Information on importing and exporting CPAs can be located in the PHINMS Implementation Guide.

1.1 CPA Communication

The CPA is a unique identifier providing the information needed to communicate between two or more messaging partners. This includes the transport protocol and security constraints both parties have agreed to use when sending and receiving messages to one another. A CPA is required for every Public Health Information Network Messaging System (PHINMS) installation at each location. Each PHINMS Sender requires a CPA when they are installed at two separate locations.

There are two parts to the CPA, the Sender's and the Receiver's Object Identifier (OID). An OID is generally an implementation - specific integer or pointer uniquely identifying an object. An object can be any organization, a vocabulary code, a PHINMS software installation, or any other entity. The OID indicates the organization running the software and the location at which the software is running.

1.2 CDC OID

The CDC uses a Party Identifier (PartyID) as an OID for PHINMS. A PartyID is used to provide the instance with a unique ID. A PartyID is required for each and every organization sending messages to the CDC and receiving messages from the CDC. A PartyID uniquely identifies a PHINMS installation, also called an instance or node. The PartyID is included with every message informing the recipient of the originator.

Note: A CDC PartyID is an OID but an OID is not necessarily a CDC PartyID.

Instances not sending data to the CDC may create an unofficial PartyID. This is used to test and become familiar with the PHINMS application when multiple installations are configured. Once the site becomes comfortable using the application, apply for a registered PartyID when messages are going to be sent to the CDC. If the servers were installed without a registered PartyID, the PHINMS application software must be removed and re-installed using the registered PartyID.

Contact the PHINMS Help Desk to obtain a PartyID by calling 1-800-532-9929, option 2 or by sending an email to phintech@cdc.gov. Information is required about the organization(s) sending and receiving messages. When complete, the PHIN Help Desk will email the PartyID to the requestor. Contact the PHIN Help Desk regarding any issues encountered with the PartyID.

1.3 Create CPA

Complete the following steps to create a CPA .xml file using any text editing software such as Microsoft Notepad:

Note: The CPA file naming convention for sending messages to CDC is <CDCOID>.<PartnerOID>.xml. Sending and receiving nodes need to have a CPA identically named in order to send messages. This is how PHINMS determines the relationship between the two parties.

1. save the **CPA .xml file**,
2. configure the **CPA .xml file**, and
3. ensure both partners' **CPA .xml file** are identical.

When troubleshooting the route configuration, if a change is made to the CPA .xml file both partners' CPA .xml files need to be updated. Ensure there are no extra spaces or unknown characters in the destination PartyID.

1.4 CPA .xml Files

This section explains the tags within the CPA .xml files for both Sender and Receiver. PartyInfo Segments

1.4.1 Sender CPA .xml File

The default location for the PHINMS 2.8.00 Sender CPA .xml file is C:\Program Files\PhinMS2.8.00\config\sender\CPA. The Sender CPA .xml file is shown in Figure 1 and explained after the figure.

```
<?xml version="1.0" encoding="UTF-8"?>
<tp:CollaborationProtocolAgreement tp:cpaid="uri:phmsg-cdc-ssl" tp:version="1.2"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:tp="http://www.ebxml.org/namespaces/tradePartner" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:schemaLocation="http://www.ebxml.org/namespaces/tradePartner
http://ebxml.org/project_teams/trade_partner/cpp-cpa-v1_0.xsd">

<tp:Status tp:value="proposed"/>
<tp:Start>2001-05-20T07:21:00Z</tp:Start>
<tp:End>2002-05-20T07:21:00Z</tp:End>
<tp:ConversationConstraints tp:concurrentConversations="100" tp:invocationLimit="100"/>

<tp:PartyInfo>

  <tp:PartyId tp:type="zz">PHINMSSender</tp:PartyId>
  <tp:PartyRef xlink:href="http://www.cdc.gov/about.html" xlink:type="simple"/>

  <tp:Transport tp:transportId="N35">
      <tp:SendingProtocol tp:version="1.1"> </tp:SendingProtocol>
      <tp:ReceivingProtocol tp:version="1.1"> </tp:ReceivingProtocol>
      <tp:Endpoint tp:type="allPurpose" tp:uri="phmsg.cdc.gov/evalebxml/receivefile"/>
      <tp:TransportSecurity>
          <tp:Protocol> </tp:Protocol>
          <tp:CertificateRef> </tp:CertificateRef>
          <tp:authenticationType> </tp:authenticationType>
          <!-- basic, custom, sdn, clientcert -->
          <tp:basicAuth>
            <tp:indexPage> </tp:indexPage>
            <tp:basicAuthUser> </tp:basicAuthUser>
            <tp:basicAuthPasswd> </tp:basicAuthPasswd>
          </tp:basicAuth>
       </tp:TransportSecurity>
</tp:Transport>

</tp:PartyInfo>

<tp:PartyInfo>

  <tp:PartyId tp:type="zz">CDCRegistration</tp:PartyId>
  <tp:PartyRef xlink:href="http://www.cdc.gov/about.html" xlink:type="simple"/>

  <tp:Transport tp:transportId="N35">
      <tp:SendingProtocol tp:version="1.1"> </tp:SendingProtocol>
      <tp:ReceivingProtocol tp:version="1.1"> </tp:ReceivingProtocol>
      <tp:Endpoint tp:type="allPurpose" tp:uri="phinmsping.cdc.gov:443/receiver/receivefile"/>
      <tp:TransportSecurity>
          <tp:Protocol>HTTPS</tp:Protocol>
          <tp:CertificateRef> </tp:CertificateRef>
          <tp:authenticationType>clientcert</tp:authenticationType>
          <!-- basic, custom, sdn, clientcert -->
          <tp:basicAuth>
            <tp:indexPage> </tp:indexPage>
            <tp:basicAuthUser> </tp:basicAuthUser>
            <tp:basicAuthPasswd> </tp:basicAuthPasswd>
          </tp:basicAuth>
          <tp:customAuth>
            <tp:customLoginPage> </tp:customLoginPage>
            <tp:publicParams> </tp:publicParams>
            <tp:secretParams> </tp:secretParams>
          </tp:customAuth>
          <tp:netegrityAuth>
            <tp:sdnPassword> </tp:sdnPassword>
            <tp:sdnLoginPage> </tp:sdnLoginPage>
            <tp:keyStore> </tp:keyStore>
            <tp:keyStorePasswd> </tp:keyStorePasswd>
          </tp:netegrityAuth>
          <tp:clientCertAuth>
            <tp:keyStore>C:/Program Files/PhinMS2.8.00c/security/sender/cdc_reg.pfx</tp:keyStore>
            <tp:keyStorePasswd>CPA_keyStorePasswd27</tp:keyStorePasswd>
          </tp:clientCertAuth>
      </tp:TransportSecurity>
</tp:Transport>

</tp:PartyInfo>

<tp:Comment xml:lang="en-us">send/receive agreement between cdc and messaging partner</tp:Comment>

</tp:CollaborationProtocolAgreement>
```

Figure 1. Sender Collaboration Protocol Agreement .xml File

The first part of the Sender CPA .xml file is the beginning tag for the CPA.

```
<?xml version="1.0" encoding="UTF-8"?>
<tp:CollaborationProtocolAgreement tp:cpaid="uri:phmsg-cdc-ssl"
tp:version="1.2" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:tp="http://www.ebxml.org/namespaces/tradePartner"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:schemaLocation="http://www.ebxml.org/namespaces/tradePartner
http://ebxml.org/project_teams/trade_partner/cpp-cpa-v1_0.xsd">

<tp:Status tp:value="proposed"/>
<tp:Start>2001-05-20T07:21:00Z</tp:Start>
<tp:End>2002-05-20T07:21:00Z</tp:End>
<tp:ConversationConstraints tp:concurrentConversations="100"
tp:invocationLimit="100"/>
```

The next part identifies the PHINMS Sender's PartyID, type, reference transport ID, sending protocol, receiving protocol, protocol version, and encryption certificate.

```
<tp:PartyInfo>

  <tp:PartyId tp:type="zz">PHINMSSender</tp:PartyId>
  <tp:PartyRef xlink:href="http://www.cdc.gov/about.html"
xlink:type="simple"/>

  <tp:Transport tp:transportId="N35">
   <tp:SendingProtocol tp:version="1.1"> </tp:SendingProtocol>
   <tp:ReceivingProtocol tp:version="1.1"> </tp:ReceivingProtocol>
   <tp:Endpoint tp:type="allPurpose"
tp:uri="phmsg.cdc.gov/evalebxml/receivefile"/>
   <tp:TransportSecurity>
       <tp:Protocol> </tp:Protocol>
       <tp:CertificateRef> </tp:CertificateRef>
       <tp:authenticationType> </tp:authenticationType>
       <!-- basic, custom, sdn, clientcert -->
       <tp:basicAuth>
         <tp:indexPage> </tp:indexPage>
         <tp:basicAuthUser> </tp:basicAuthUser>
         <tp:basicAuthPasswd> </tp:basicAuthPasswd>
       </tp:basicAuth>
       </tp:TransportSecurity>
</tp:Transport>

</tp:PartyInfo>
```

The section which follows the PHINMS Sender's PartyID identifies the CDC Registration's PartyID, type, reference transport ID, sending protocol, receiving protocol, protocol version, and encryption certificate:

```
<tp:PartyInfo>

  <tp:PartyId tp:type="zz">CDCRegistration</tp:PartyId>
  <tp:PartyRef xlink:href="http://www.cdc.gov/about.html"
xlink:type="simple"/>

  <tp:Transport tp:transportId="N35">
```

```
      <tp:SendingProtocol tp:version="1.1"> </tp:SendingProtocol>
      <tp:ReceivingProtocol tp:version="1.1"> </tp:ReceivingProtocol>
      <tp:Endpoint tp:type="allPurpose"
   tp:uri="phinmsping.cdc.gov:443/receiver/receivefile"/>
      <tp:TransportSecurity>
          <tp:Protocol>HTTPS</tp:Protocol>
          <tp:CertificateRef> </tp:CertificateRef>
          <tp:authenticationType>clientcert</tp:authenticationType>
          <!-- basic, custom, sdn, clientcert -->
          <tp:basicAuth>
            <tp:indexPage> </tp:indexPage>
            <tp:basicAuthUser> </tp:basicAuthUser>
            <tp:basicAuthPasswd> </tp:basicAuthPasswd>
          </tp:basicAuth>
          <tp:customAuth>
            <tp:customLoginPage> </tp:customLoginPage>
            <tp:publicParams> </tp:publicParams>
            <tp:secretParams> </tp:secretParams>
          </tp:customAuth>
          <tp:netegrityAuth>
            <tp:sdnPassword> </tp:sdnPassword>
            <tp:sdnLoginPage> </tp:sdnLoginPage>
            <tp:keyStore> </tp:keyStore>
            <tp:keyStorePasswd> </tp:keyStorePasswd>
          </tp:netegrityAuth>
          <tp:clientCertAuth>
            <tp:keyStore>C:/Program
   Files/PhinMS2.8.00c/security/sender/cdc_reg.pfx</tp:keyStore>
            <tp:keyStorePasswd>CPA_keyStorePasswd27</tp:keyStorePasswd>
          </tp:clientCertAuth>
        </tp:TransportSecurity>
   </tp:Transport>

   </tp:PartyInfo>
```

The last section indicates the language and the description of the agreement between the CDC and the messaging partner.

```
   <tp:Comment xml:lang="en-us">send/receive agreement between cdc and
   messaging partner</tp:Comment>

   </tp:CollaborationProtocolAgreement>
```