papiNet

Global Standard for the Paper and Forest Products Supply Chain

Interoperability Overview

papiNet Standard

October 2016

Copyright

Use of Documents in papiNet Implementations

Documents may be used as templates for a papiNet implementation. The Presenters grant the right to modify and edit them to fit an actual implementation project provided all copies display the copyright and any other proprietary notices contained in this document. Such modified documents must not be distributed beyond the trading partners implementing or maintaining a papiNet connection.

Table of Contents

Interoperability Vision

The papiNet Standards Group has the vision of enterprises of any size and in any geographical location meeting and conducting the business of Paper and Forest Products with each other through the exchange of XML based e-business documents. The intent is to define a neutral method (one that is open and non-proprietary) for exchanging these electronic business documents. In addition to being neutral the exchange process has to guarantee safe, secure delivery.

The goal of this vision is to replace paper documents with electronic documents; eliminating the paper documents. It is through this upgrade process that improved data accuracy, more timely information, and cost reductions will be achieved.

These interoperability objectives can be summarized in the following way:

- Participants in the messaging transfer process should be able to choose the technology they desire to use to communicate e-Documents independent of other participants in the communications network.
- Errors in transmission to the destination must be communicated.
- Security must be assured:
  - Privacy - Protect against information being disclosed or revealed to any entity not authorized to have that information by permitting the use of encryption techniques (for example, payload encryption using S/MIME techniques).
  - Authentication - Authenticate the claimed identity of the originator.
  - Authorization - Protect against the threat that unknown entities enter into the system and ensures that an entity performs only authorized actions within the system.
  - Integrity - Protect against the threat that the value of a data item might be changed en route.
  - Non-repudiation - Protect against one party to a transaction or communication later falsely denying that the transaction or communication occurred.

Aspects of Interoperability

When we talk about e-business document communication there are many aspects to consider. The process starts with an individual reviewing the output from a business application and initiating some sort of action that can be communicated using a papiNet e-business document.

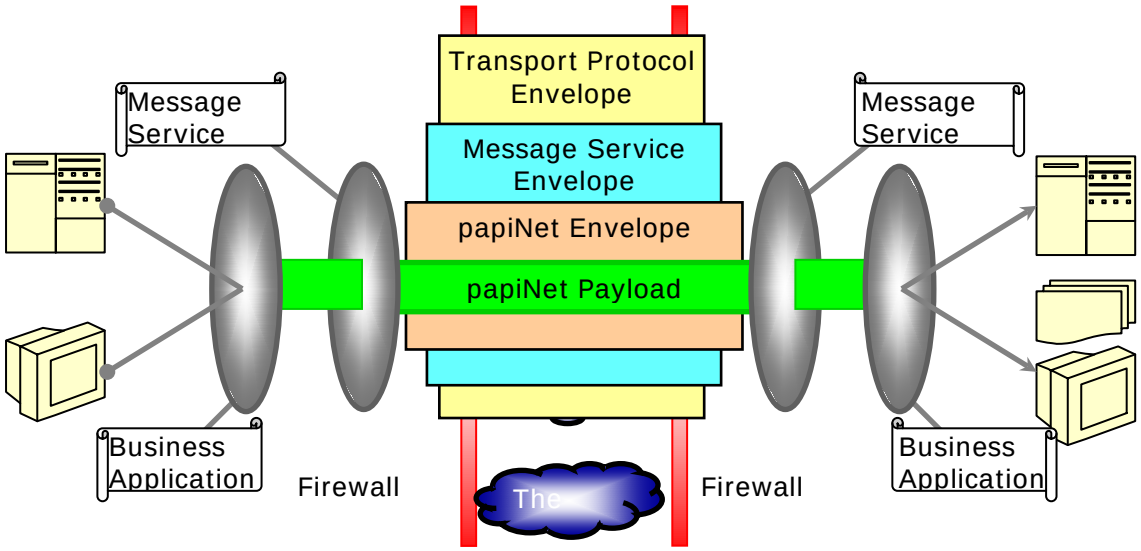

Figure 1: The Interoperability Horizon

The papiNet e-business document is sent from your location to the recipient's location over the internet via one of several possible transfer methods. The payload is wrapped in several electronic envelopes that provides identification and supports security features.

The papiNet Payload

In the diagram above the papiNet e-business document is labelled as the papiNet payload. The standardized format of the papiNet payload provides a common view of the business document across trading partner boundaries.

The papiNet Envelope

The papiNet Standards Committee has found that there is a consistent group of information that is beneficial for XML processing programs to have readily available. Grouping this information into an envelope that contains the papiNet payload means that this information is always in the same location and provides a hook for the XML processing programs to use when beginning to process a given transmission.

You do not need to use the papiNet Envelope. However, it is recommended that it is used as this makes it possible to clearly define the technical aspects of communicating the e-Document.

Message Service and Transport Protocol Envelopes

We'll cover these two items together because, in many cases, the transport protocol envelope and the message service envelope are so closely related that it is hard to distinguish them.

In the papiNet world we deal with the HTTP, FTP, and SMTP transport protocols. From an allegorical standpoint you could think of the transport protocols in the following way:

- SMTP – as secure as your postal mail and with the same issue of junk mail.
- FTP – a package delivery service that delivers the package to your front door step but does not wait for someone to provide a signature of receipt. Sometimes they ring the doorbell. You can secure your front door step but you cannot ensure that a receipt is provided.
- HTTP/HTTPS – (think of HTTPS as an armoured car delivery) Depending on the nature of the message service you use HTTP can be implemented so that it provides delivery similar to a personal high-security courier who personally delivers the message to you, provides the security cipher, and guarantees that the message has not been tampered with and is from the party indicated. You can also run HTTP/HTTPS in such a way that it provides the same level of capability as with SMTP or FTP.

In the HTTP/HTTPS transport protocol environment there are several message protocols that you need to be aware of they are SOAP, AS2, and SOAP-ebXML. The level of functionality provided by the HTTP/HTTPS requires more coordination between the sender and recipient than is required by SMTP and FTP.

Creating Well-formed papiNet e-Document

This document reviews a typical XML e-Document, the sample XML that immediately follows. You might want to place this discussion next to the sample XML, so that you can follow the discussion line-by-line. To validate a papiNet e-Document, verify it against the papiNet xsd schema definition.

Line 1:

The required XML element with attributes for version and encoding is the first line of the XML e-document. There are several encoding approaches. UTF-8 is the approach that is prescribed by the Internet Engineering Task Force (IETF). UTF-8 can handle every character, pictograph languages my take up more space but they can be represented.

Lines 2-44:

These lines are a papiNet e-Document, in this instance, a DeliveryMessage.

Line 3:

This line indicates that this DeliveryMessage lies in the v2r40 namespace which is managed by papiNet. The papiNet namespace prefix is blank.

Line 4:

This line indicates the namespace of W3C XML schema definition.

Line 5:

The namespace and schema location for the DeliveryMessage is shown in these lines. The namespace and schema location are separated by a space character. The schema file is locally stored.

Sample XML – papiNet e-Document: DeliveryMessage

```
1.  <?xml version="1.0" encoding="UTF-8"?>
2.  <DeliveryMessage
3.        xmlns="http://www.papinet.org/v2r40"
4.        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5.        xsi:schemaLocation="http://www.papinet.org/v2r40 DeliveryMessageV2R40.xsd"
6.        DeliveryMessageStatusType="Original"
7.        DeliveryMessageType="DeliveryMessage">
8.     <DeliveryMessageHeader>
9.          <DeliveryMessageNumber>001002456</DeliveryMessageNumber>
10.        <DeliveryMessageDate>
11.            <Date>
12.              <Year>2008</Year>
13.               <Month>03</Month>
14.                <Day>06</Day>
15.             </Date>
16.       </DeliveryMessageDate>
17.       <ShipToCharacteristics>
18.           <ShipToParty PartyType="Buyer">
```

```
                <NameAddress>
                    <Name1>myBuyerName</Name1>
                </NameAddress>
            </ShipToParty>
        </ShipToCharacteristics>
        <DeliveryLeg>
            <DeliveryLegSequenceNumber>1</DeliveryLegSequenceNumber>
            <DeliveryOrigin>
                <LocationParty PartyType="Supplier">
                    <NameAddress>
                        <Name1>mySupplierName</Name1>
                    </NameAddress>
                </LocationParty>
            </DeliveryOrigin>
        </DeliveryLeg>
    </DeliveryMessageHeader>
    <DeliveryMessageLineItem>
        <DeliveryMessageLineItemNumber>1</DeliveryMessageLineItemNumber>
        <Product>
            <ProductIdentifier Agency="Buyer" ProductIdentifierType="SKU">
                1234567890</ProductIdentifier>
        </Product>
            <Quantity QuantityType="Count">
                <Value  UOM="Reel">5</Value>
            </Quantity>
    </DeliveryMessageLineItem>
</DeliveryMessage>
```

Selecting the Proper Environment

The number one or two question that we are continually asked is, “What message service should I use when communicating with my trading partners?” The answer depends on many different factors. We’ll try to group them into groups that will help you to make the proper decision.

In order to achieve the security considerations mentioned at the beginning of this document our first recommendation is always going to be one of the HTTP oriented protocols. However, if security is less of a concern then other choices may be desired.

1. Are you a large company, a medium sized company, or a small company?

Security considerations aside, a small company may feel very comfortable in using SMTP (e-mail) to send papiNet e-Documents. In general most medium and large companies use one of the HTTP oriented protocols. FTP is used by some medium and large companies as it provides a bit more reliability and security than e-mail however; it is not as robust as the HTTP oriented protocols.

2. What are your trading partners doing? What are your customers requiring?

This point gets to the coordination that is required between the sender and recipient and the amount of investment that is required to implement any solution. Obviously you do not want to implement a solution that does not meet your security requirements but all the approaches require a degree of coordination.

3. How sensitive is the information you are communicating?

While all the approaches provide a certain degree of security SMTP provides the lowest and HTTPS with either AS2 or ebXML provides the highest. Of course the coordination requirements are more extensive with AS2 or ebXML.

The Need for Coordination between Trading Partners

When two trading partners decide to exchange electronic business documents they must agree on the parameters for the exchange. Be aware that all communication and all e-Documents do not need to be sent in the same way between all trading partners. You could be receiving e-Documents in one form from a trading partner and sending them in another form. However, both of you must at least agree that you will be “looking out” for e-Documents of a certain type.

Most companies like to reduce the complexity of their infrastructure by reducing the number of communications approaches they have to support. There are two competing factors that prevent a single uniform approach for all companies.

- First, there is the drive to the “lowest common denominator” which would be the solution that is easiest and cheapest to implement. Depending on

who you are this could be email, ftp, or the more prevalent – do nothing solution.

- Secondly, there is the drive to the “highest level of security” which would be the HTTP/HTTPS with AS2 or ebXML.

So, coordination is required between two trading partners. The first time you set-up your environment for one of the more robust solutions there will be some initial steps that you need to perform. These will be one-time steps (obtaining certificates) that will applicable for subsequent implementations.