e-Invoice Interoperability Framework: e-Delivery Network Feasibility Assessment

Prepared by the Business Payments Coalition
e-Invoice Work Group

November 2019

Business Payments Coalition

Table of Contents

List of Figures

List of Tables

1. Executive Summary

The Business Payments Coalition (BPC)[1] is coordinating a multi-year initiative with industry stakeholders to assess and provide recommendations for an electronic invoice (e-Invoice) interoperability framework for the U.S. market. The desired outcome of this initiative is to increase the exchange of e-Invoices by U.S. businesses, which is an important driver to increase adoption of electronic payments and improve overall business-to-business (B2B) payment efficiency with straight-through processing.

U.S. businesses are striving to increase the adoption rate of e-Invoicing for both their own business and their supply chains. While there are significant challenges to facilitate broad exchange of e-Invoices, there are promising models emerging from other countries based on the establishment of electronic delivery networks and e-Invoice semantic models. In Europe, and elsewhere, e-Invoice frameworks are using common standards and protocols between federated networks of access points, creating a scalable ecosystem that is easier and more cost effective to implement, thus enabling broader adoption. The United States can leverage the learnings and implementation strategies from those frameworks to create an interoperable ecosystem of access points. To achieve the same results, a U.S. framework will enable service providers and accounting technology systems to provide sellers and buyers a service to connect once, and seamlessly exchange e-Invoices with anyone across the network.

An e-Invoice interoperability framework is a set of policies, standards and guidelines that enables the exchange of e-Invoices, documents and messages independent of the payment, accounting and enterprise resource planning (ERP) systems. Access points leverage electronic delivery standards and an e-Invoice semantic model can facilitate document delivery among an open network of providers and significantly reduce the cost and complexity to send and receive invoices.

In 2018, the Business Payments Coalition (BPC) initiated two work groups to study the components of existing e-Invoice interoperability frameworks:

- Semantic Model Work Group assessed the e-Invoice semantic models defined
- Technical Feasibility Work Group to assessed existing e-Delivery network technical architecture

This report presents the findings and recommendations of the Technical Feasibility Work Group.[2]

The Business Payments Coalition (BPC) is a volunteer group of organizations and individuals working together to promote greater adoption of electronic business-to-business (B2B) invoices, payments, and remittance data.

Several key findings from the assessment include:

- Establishing interoperability standards between access points significantly reduces typical integration efforts required to support e-Invoicing.
- Many service providers and networks in the United States also operate in global regions where frameworks exist, which could ease adoption of a U.S. Interoperability framework.

[1]Views expressed here are not necessarily those of, and should not be attributed to, any particular Business Payments Coalition participant or organization. They are not intended to provide business or legal advice, nor are they intended to promote or advocate a specific action, payment strategy, or product. Readers should consult with their own business and legal advisors.

[2]See 7.1 Appendix A – Work Group Members.

- The frameworks assessed are based on a four-corner model architecture creating a network through a series of federated access points securely connecting the community of service provider platforms and networks. The access points bring together standardized components of the e-Delivery network architectural design, which leverages, rather than supplants, existing investments in technology infrastructure and service relationships between sellers and buyers.
- Access points leverage proven technologies and tools readily available that provide the necessary security and scalability for the U.S. market.
- An e-Delivery network can reside outside of payment systems; is payment method agnostic; and does not hold sensitive payment and account information.
- The recommendation for the message transport protocol calls for supporting both Applicability Statement 2 (AS2) and Applicability Statement 4 (AS4). AS4 is the standard message transport protocol used by the frameworks assessed, however AS2 is widely used currently in the United States amongst EDI service providers. Over time, AS4 should become more widely used within the e-Delivery network because of the flexibility and advantages it offers service provider platforms and networks over AS2. Initially, this may add a level of complexity for service providers and networks as they establish access points. However, the tradeoff of flexibility for service providers and networks to establish access points and join the e-Delivery network outweigh initial complexity.
- The frameworks use registries to enable dynamic discovery of a trading party's[3] electronic capabilities and delivery addressing. The registry does not contain confidential information, such as payment information, nor will businesses be required to disclose information about their customer base or competitive data.
- The frameworks assessed rely upon business entity identifiers within the registries and support multiple identifiers. The entity identifiers used by U.S. businesses are very diverse and complex. The framework will need to support multiple entity identifiers; a single entity identifier would be preferred over time.
- The open standards used in the e-Delivery network meet the necessary technical security requirements for creating a secure and trusted environment for exchanging e-Invoices. Additionally, the use of these standards does not require any licensing and are royalty free.
- A governance body will need to determine the business requirements for managing a federated registry and decentralized model, and the issuance of digital security certificates.

The BPC e-Invoice Technical Feasibility Work Group will continue to collaborate with the industry to develop the strategy, policy, and support for the next steps toward establishing a U.S. e-Invoice interoperability framework.

For additional information on this initiative or to share ideas, please contact:

Business Payments Coalition
e-Invoice Work Group
Email: business.payments.smb@mpls.frb.org

For more information about the BPC, visit the website at https://businesspaymentscoalition.org/.

[3]Trading parties refer to any parties involved in exchanging invoices between sellers and buyers.

1.1 Audience

The *BPC e-Invoice Interoperability Framework – e-Delivery Network Feasibility Assessment Report* is intended for technology and business stakeholders in the private and public sector markets involved in the implementation and support of accounting technology systems that process invoices. This report provides technology and business stakeholders with an understanding of the high-level requirements and standards assessed required to establish a framework for the U.S. market.

Business Stakeholders (Primary Audience)

- Individuals who are responsible for implementing and supporting accounting technology systems from the business domain
- Individuals who are responsible for identifying, defining, and supporting business requirements for accounting technology systems that support accounts receivable, accounts payable and electronic exchange of business documents

Technology Stakeholders (Secondary Audience)

- Individuals who are responsible for the design, implementation, and support of accounting technology systems and solutions for electronic exchange of business documents
- Individuals who are responsible for the design, integration and operational support of business applications dealing with invoicing

1.2 Disclaimers, Copyright and Acknowledgments

Views expressed here are not necessarily those of, and should not be attributed to, any particular Business Payments Coalition participant or organization. They are not intended to provide business or legal advice, nor are they intended to promote or advocate a specific action, payment strategy, or product. Readers should consult with their own business and legal advisors.

Readers are free to republish this report in whole or in part without further permission, as long as the work is attributed to the BPC, and in no way suggests the BPC sponsors, endorses or recommends any organization or its services or products. Other product names and company names referenced within this document may be either trademarks or service marks of their respective owners.

The BPC would like to acknowledge the work of the e-Invoice Technical Feasibility Work Group and other contributors, including the Pan European Public Procurement Online (PEPPOL) and the European e-Invoice Service Provider Association (EESPA), for their contributions during the assessment process.

2. Background

The BPC seeks to facilitate discussion with the broader industry by framing industry challenges and business recommendations and suggesting next steps to achieve broader adoption of e-Invoicing and straight-through processing for the United States. The following work led the BPC to identify e-Invoice interoperability frameworks in other parts of the world and the recommendation to further assess the feasibility of establishing a similar framework within for the U.S. market.

The BPC and Federal Reserve Bank e-Invoicing publications to date include[4]:

- *U.S. Adoption of Electronic Invoicing: Challenges and Opportunities*[5], a Federal Reserve Bank white paper study of the business environment and e-Invoicing adoption in the United States and internationally.
- *Catalog of Electronic Invoice Technical Standards in the U.S.*[6] , a BPC workgroup report that documents e-Invoice technical standards that exist in the U.S. market. The report describes the current fragmentation in the U.S. market usage of e-Invoices and the interoperability challenges among the standards.
- *Summary Report from the e-Invoice Interoperability Framework Preliminary Assessment Work Group*[7], a 2018 BPC report that reviewed interoperability framework concepts and assessed the appropriateness of developing a similar framework for the United States.
- *Overview of an e-Invoice Interoperability Framework*[8], a 2019 BPC report that introduces the concept of an e-Invoice interoperability framework as well as market challenges and benefits of addressing them, and a path forward for the BPC work assessing U.S. market needs.

Globally, countries with similar e-Invoice adoption challenges have successfully connected the community of service provider platforms and networks through e-Invoice interoperability frameworks designed to leverage, rather than supplant, existing investments in technology infrastructure and service relationships. In the United States, approximately 75 percent of invoices submitted to buyers are paper-based[9]. For the most part, established B2B networks successfully deliver e-Invoices. However, these networks currently suffer from limited reach and little interoperability, which prevents broader adoption of e-Invoices. An evolution towards an interoperable eco-system of service providers and networks is required for sellers and buyers to exchange invoices and related documents with each other cost effectively. Reducing setup,

[4]Documents cited here are available at businesspaymentscoalition.org, in the e-Invoicing section.

[5]*U.S. Adoption of Electronic Invoicing: Challenges and Opportunities,* Payments, Standards and Outreach Group, Federal Reserve Bank of Minneapolis, June 2016.

[6]*Catalog of Electronic Invoice Technical Standards in the U.S.*, Business Payments Coalition and Federal Reserve Bank October 2017.

[7]*Summary Report from the e-Invoice Interoperability Framework Preliminary Assessment Work Group,* Business Payments Coalition, June 2018.

[8]*Overview of an e-Invoice Interoperability Framework,* Business Payments Coalition, November 2019

[9]*U.S. Adoption of Electronic Invoicing: Challenges and Opportunities,* Payments, Standards and Outreach Group, Federal Reserve Bank of Minneapolis, June 2016.

connection management, and integration costs are critical success factors for an e-Invoice interoperability framework.

An e-Invoicing interoperability framework refers to a set of policies, standards and guidelines that address four essential layers of interoperability (Table 1) enabling U.S. businesses to exchange e-Invoices, documents and messages independent of the accounting and ERP systems they use. Much like email, which is globally interoperable due to its standards-based format and delivery, the framework will enable document delivery among an open network of service providers, B2B networks and platforms through standards with the flexibility to preserve existing connections and operations with customers, and meet a variety of business needs.

Table 1
The Four Essential Layers of an Interoperability Framework

Layer	Description
Legal	Addresses the requirements at the business, network, legislative and policy levels
Business	Describes the business processes, capabilities and discovery process to facilitate the exchange of a document
Semantic	Standardizes the meaning of the data creating a common understanding among trading parties involved in the exchange
Technical	Defines the delivery standards and protocols enabling secure and reliable exchange of documents between trading partners via a federated network

An e-Invoice interoperability framework would foster wider adoption of e-Invoicing and further motivate adoption of electronic payments. Moreover, it provides the following additional business benefits:

- Reduced operating expenses by eliminating paper and manual data entry, and automating workflow such as invoice routing, purchase order matching, and approval
- Increased likelihood of on-time payments[10]
- Optimized cash management by speeding up processing workflow to enable buyers to take advantage of early payment discounts and/or to enable sellers to provide invoices in a timelier manner leading to improved cash flow and working capital
- Minimized risk of overpayments, duplicate payments, and fraudulent payments
- Improved real-time, on-line view and traceability of all invoice-related documents and ability to archive online
- Improves data quality and accuracy, and reduces the time to access business information
- Reduced complexity of working with trading parties in multiple countries through enhanced, standard processes that improve compliance with tax requirements and other country or regional directives

[10] *2016 Data Capture and Mailroom Technology Insight Report*, PayStream Advisors

2.1 Terms and Definitions

For the purpose of this report, important terms and definitions are listed below.

Access point: Access point describes a node on a delivery network connecting two service providers (corners 2 and 3) in a four-corner model and providing trading partners (corners 1 and 4) with access to that network.

Connecting Europe Facility (CEF): The EU Connecting Europe Facility (CEF) supports initiatives in the sectors of transport, telecommunications and energy. Within this, CEF e-Invoicing provides funding, tools and capabilities to support the roll-out of e-Invoicing to public administrations.

CEF e-Delivery: The EU e-Delivery building blocks help public administrations, citizens and economic operators exchange electronic data and documents over a network in an interoperable, secure, reliable and trusted way. It is based on a distributed model, allowing direct communication between participants without the need to set up bilateral channels.

Digital Business Council (DBC): The Digital Business Council (DBC) developed an eInvoicing interoperability framework in Australia that is based on international standards.

Directory: An optional service that provides a variety of business information about a trading party that typically includes information on identifiers, attributes, routing and capabilities to support business discovery and successful e-Invoice exchange. In the context of interoperability frameworks, directories do not contain electronic payment information or other sensitive business information.

Discovery mechanisms: The processes and technology used to discover (e.g. look-up) the capabilities of another party, where and how to send an invoice and/or other message, and validate and authenticate credentials. This includes registry services and other decentralized discovery mechanisms.

e-Delivery Network: Refers to the components of the technical interoperability layer to deliver documents electronically across the Internet.

Electronic Address Identifier: Unique digital address used by a trading party for the routing of digital documents and messages from and to its systems.

Electronic invoice: An invoice issued by the seller, transmitted and received by the buyer in a structured digital format that allows for automated processing.

Electronic Routing Address: Defines the electronic address of a service provider platform that routes digital documents and messages on behalf of a trading party; it is associated with the Electronic Address Identifier.

Entity Identifier: The unique digital identifier of a trading party or business entity expressing the identity of a legal or fiscal entity, or a natural person. It may form a component or a path to discover an electronic address or routing address.

European E-invoicing Service Providers Association (EESPA): A trade association for European e-Invoicing service providers.

European E-invoicing Service Providers Association (EESPA) Model Interoperability Agreements: Bilateral or multilateral agreements utilized by EESPA members to establish interoperable connections for exchanging invoices and related documents.

Four-corner model: A networking model that connects four parties to deliver electronic documents and messages: the sender (corner 1), the sender's access point (corner 2), the receiver's access point (corner 3) and the receiver (corner 4).

Message envelope: A container or structured header that contains an embedded message.

Message payload: The semantic content and machine-readable syntax of the actual business message or document.

Message transport protocols: Technical transmission protocols used to create network connections between endpoints to deliver the message payload, such as an invoice and other documents.

Non-repudiation: One party to a transaction cannot deny having received a message about the transaction nor can the other party deny having sent a transaction.

OpenPEPPOL Association: A European membership organization that is responsible for the PEPPOL Network that enables businesses to communicate electronically with any European government institution in the procurement process.

Organization for the Advancement of Structured Information Standards (OASIS): Non-profit consortium that drives the development, conversion, and adoption of open standards for the global information society.

Pan European Public Procurement Online (PEPPOL): A set of artifacts and specifications enabling cross-border eProcurement as well as the operation of a transport infrastructure.

Registry: Is the process (i.e. registry services) and storage of network participant identifiers such as identity, location, and routing information used in automated messaging.

Semantic model: Defines the components of a document including actors and roles; business functions, processes, rules, and terms; and represented information elements (e.g. an invoice).

Semantics: The meaning of the data or information elements used in digital exchanges.

Service Metadata Location (SML): A registry that contains the8 location of the endpoint recipient SMP record used in automated messaging in a network.

Service Metadata Publisher (SMP): Registry that contains the identifier of an endpoint and exchange capabilities of a receiving access point used in automated messaging in a network.

Service Provider: An organization that typically provides its customers with services for the creation, delivery and processing of e-Invoices and other related e-business transactions as well as supporting software and services.

Syntax: The means by which semantic information elements are expressed in machine-readable technical languages (e.g. XML).

3. The e-Invoice Interoperability Framework: e-Delivery Network Feasibility Assessment

The BPC is undertaking a multi-year project to assess existing e-Invoice interoperability frameworks from other markets to determine the applicability to the U.S. market. The objective of the assessment is to determine the feasibility, high-level requirements and recommendations for establishing an e-Invoice interoperability framework in the United States. This work specifically focuses on the ***technical delivery layer*** of an interoperability framework that creates the electronic-delivery network. A separate report focused on the e-Invoice data semantic model that is another essential layer of the framework.

The BPC e-Invoice Technical Feasibility Work Group focused on unified e-Invoicing standards, processes, and common automated tools that support:

- Identifying electronic document exchange and delivery methods and processes for transmitting B2B documents to support technical interoperability while using accepted industry standard security methods and protocols
- Originating and receiving e-Invoice information based on standardized and uniform semantic models, using one or more technical syntaxes that easily integrate into existing software (including ERP systems), platforms and service-provider systems

This report articulates the findings and recommendations of an assessment of frameworks and e-Delivery networks by the BPC e-Invoice Technical Feasibility Work Group.[11] The report does the following:

- Articulates the guiding principles used by the work group members
- Lists the fundamental business and technical requirements
- Describes the assessment process
- Describes the fundamental components
- Summarizes the findings and shares recommendations for each component
- Describes access point and registration technology considerations
- Explains the proof of concept (POC) model used by the work group
- Summarizes recommendations, topics that should be addressed in the future and proposed next steps

3.1 Guiding Principles

Work group members adhered to guiding principles for analyzing existing global interoperability frameworks to determine whether the technical specifications, tools, models, standards and practices could be implemented in the United States. Below is the set of guiding principles:

- A broad cross-section of industry stakeholders were to be involved to vet and validate the required business and technical requirements and specifications for standards and practices for a U.S. e-Delivery network.
- The frameworks assessed had a set of published and transparent technical specifications.[12]

[11] The BPC Technical Feasibility Work Group is a group of experts representing corporations, industry associations, standards bodies, service providers, and others.

[12] Links to specifications and reference documents can be found in Appendix E.

- The components incorporated in the e-Delivery network had to meet current U.S. market capabilities and industry direction for adoption.
- The framework and the e-Delivery network components had been successfully implemented and are actively driving adoption in another country.
- The frameworks used standards that are open, royalty-free and vendor-agnostic; they should not require a singular platform or solution for the exchange of electronic business documents, but rather support a federated network of access points and service providers.
- The frameworks were independent of any payment systems and are payment method agnostic.

3.2 Business and Technical Requirements

The work group identified the following 18 fundamental and critical business and technical requirements for establishing a U.S. framework. The framework should support:

1. Ability for trading parties and their service providers to connect in an interoperable way, **while preserving the flexibility for co-existence of models deployed in the current eco-system.**
2. **Fit-for-purpose network infrastructure** that is robust, secure and ensures end-to-end message delivery without duplication of messages and with non-repudiation.
3. **Delivery assurance** regardless of whether the receiving gateway is available at the time of delivery.
4. **Scalability** to support large numbers of connected parties.
5. **High volume messaging throughput** and the ability to transmit large messages (up to 50 MB).
6. Diverse means for identifying parties and discovering routing addresses to enable the **broadest possible reach.**
7. **Trusted authentication procedures** that ensure confidentiality of customer information when accessing addresses of trading parties and access points.
8. Adequate capability for a **secure message envelope** to carry e-Invoices, associated structured and unstructured documents and attachments.
9. Network attributes that protect **authenticity** and provide **tamper-proof integrity** of information transmitted.
10. **Data privacy protections** that preserve the confidentiality of customer information.
11. **Encryption** for both documents and the delivery channel.
12. A range of **response, status and servicing messages** to permit a dynamic flow of information and asynchronous interactions.
13. **Cost-effective tools and solutions to support implementation by small and medium-size businesses.**
14. **Agreements**, operating procedures and a governance model with the flexibility to meet U.S. market complexity.
15. Well-established **non-proprietary standards**, protocols and operational tools deployed and maintained without significant technology development or adaptation.
16. **Extensibility and flexibility to address gaps and future requirements** without burdensome rework or costly investment.
17. **Integration with existing automated processes without disruption**.
18. **Incorporates lessons learned and best practices from established frameworks.**

3.3 Assessment Process

The work group established a process to assess the frameworks that could together meet the above 18 business and technical requirements while adhering to the guiding principles.

The assessment was conducted through collaborative discussions held weekly over several months. Along with these discussions, a technical architect participated to create an ad-hoc experimentation environment (the POC). The goal of the POC was to gain hands-on experience in a non-production, but functional, network between access points to understand the available tools, and level of complexity to implement an access point, both of which play a vital role enabling interoperability. The work group undertook a broad technical assessment of existing e-Delivery networks from the following frameworks:

- Australian Digital Business Council (DBC)
- Connecting Europe Facility (CEF) e-Delivery specifications[13]
- European E-invoicing Service Providers Association (EESPA) Model Agreements
- Pan European Public Procurement Online (PEPPOL)

The following fundamental logical components of the e-Delivery network within each interoperability framework were evaluated:

1. **Overall architecture:** How the technical components are assembled to create an e-Delivery network.
2. **Message transport protocols:** Transmission protocols used to create e-Delivery network connections between endpoints to deliver the message payload such as an invoice and other documents.
3. **Message envelope:** A container or structured header that contains an embedded message.
4. **Message payload:** The semantic content and machine-readable syntax of the actual business message or document. Messages also include a range of response statuses and servicing messages.
5. **Identifiers:** The way parties and their attributes are identified and discovered.
6. **Discovery mechanisms:** The processes and technology used to discover (e.g. look-up) the capabilities of another party, where and how to send an invoice and/or other message, and validate and authenticate credentials. This includes registry services and other decentralized discovery mechanisms.
7. **Security:** The means by which the framework provides security to its participants.
8. **Access point and registry providers:** Providers that utilize standards and software to make the framework operational.

Each of the eight components was analyzed to:

- Gain an understanding of the requirements of each component
- Evaluate/describe the solutions or combination of solutions, assessed as proven or likely to deliver the component or attribute required
- Provide a summary of the rationale for each recommendation, including an assessment of benefits and drawbacks
- Identify any gaps for the U.S. market and how they might be addressed
- Determine if they followed open standards or had proprietary IP

[13]The Connecting Europe Facility (CEF) e-delivery specifications provided the building blocks of components for PEPPOL's e-delivery network specifications. EESPA is currently evaluating the adoption the CEF e-delivery specifications.

4. Framework Assessment and Recommendations

This section summarizes the work group's assessments, recommendations and supporting rationale for each component evaluated.

4.1 Overall Architecture

Recommendation 1: Base the overall architecture of the e-Invoice Interoperability Framework on a four-corner model.

A four-corner model of an e-Invoicing network is analogous to the phone network. In the phone network, people own landlines or cell phones that have a unique identifier, the phone number. The phones connect to the phone carrier, and the carriers deliver calls over a network utilizing standards that enable interoperability regardless of the type of phone or the carrier. The calls are routed over the phone network from the carrier of the call initiator to the carrier of the call receiver.

The table below describes how an e-Invoice e-Delivery network compares to a phone network.

Table 2
Comparison between a Phone Network and an e-Invoice e-Delivery Network

Phone network	e-Delivery Network
Phone owner	The sender and receiver, identified using a Business Entity Identifier
Phone number	The Electronic Address Identifier used to route the document to the endpoint. Just as individuals and businesses can have multiple phone numbers, one business entity can have multiple Electronic Addresses – such as for different divisions, regions, projects or accounting functions.
Phone carrier	The service provider/access point, whose platform is identified using an Electronic Routing Address.
Phone network	Internet-based e-Delivery network between service providers.
Phone network standards, e.g. CDMA and GSM	The standards and protocols applied to support open exchange, such as transport, envelope, identifiers, security, and registry standards.

As with phone network interoperability, the e-Invoice exchange senders and receivers only need to concern themselves with the identifiers of their trading parties (Business Entity Identifier and Electronic Address Identifiers), leaving service providers to use discovery services through registries and directories to route information between end users.

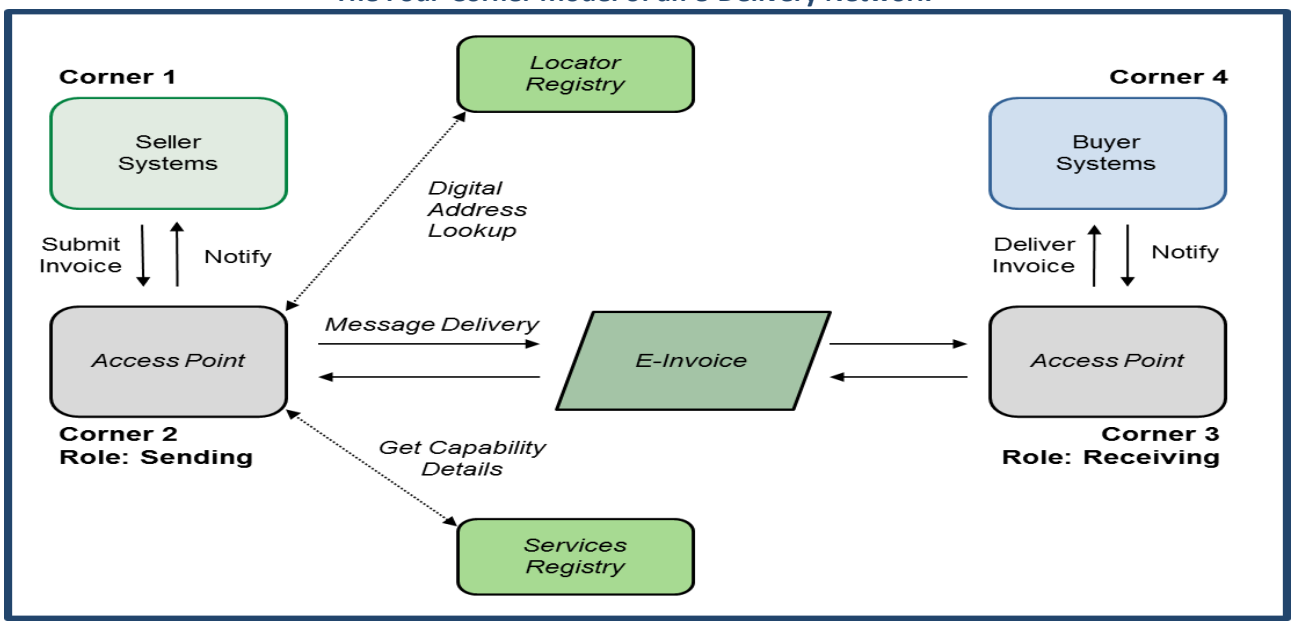
The four-corner model helps achieve the interoperability found in the phone system for the invoice senders and receivers who use different service provider platforms. Senders usually connect to one service provider solution to send all e-Invoices. Some of these e-Invoices may be directed to receivers present on the same platform (three-corner model[14]), but many will be directed to other platforms used by other receivers. Under interoperability agreements, two service providers become access points and connect to

[14] A connection mode where a single service provider or platform connects both the seller and the buyer to its platform to offer and coordinate e-Invoicing and other supply chain services.

each other and transmit or accept invoices on behalf of their customers. Three-corner and four-corner models co-exist within the same e-Delivery network. The Interoperability Framework does not preclude corporates from becoming an access point in an e-Delivery network, but it is the exception rather than the norm. It is usually less work and more cost effective for corporates to connect into the e-Delivery network through a service provider rather than setting up and maintaining their own access point.

The four-corner model depicted in Figure 1 delivers the essential architecture for pervasive reach for all parties.

Figure 1
The Four-Corner Model of an e-Delivery Network[15]



The rules and interoperability requirements for a successful framework predominantly focus on the linkages between access point providers in corners 2 and 3. The linkages between trading parties and the access points (corners 1 to 2 and corners 3 to 4) are outside the scope of the framework and under the control of the parties concerned. Access point service providers deliver additional value-added services to clients.

Without a four-corner-based e-Delivery network in place, there is the need for individual bilateral agreements between service providers addressing interoperability conditions, which are often slow to be agreed upon and implemented, and are not scalable. An interoperability framework addresses the inefficiency of bilateral agreements and point-to-point connections, replacing them with a standardized agreement for all participants within the e-Delivery network and one connection that supports many external points. Standardized models for interoperability, such as CEF, PEPPOL and EESPA in Europe, lower the entrance barrier for market participants and the costs to set up interoperability connections between service providers. This model helps increase market penetration by simplifying the implementation, maximizing business endpoint reach through a single connection that allows connecting with many, and increasing the affordability for small and medium-size businesses (SMBs).

[15]Adapted from the e-Invoice Interoperability Framework, Digital Business Council, Version 1.0, July 27, 2016.

In the evaluation process, the work group did not identify any persuasive viable alternative architecture to a trusted four-corner model. However, a four-corner model is demanding and requires collaboration to orchestrate governance, precise rules, technical specifications, and efficient change management.

There are industry voices who see the growth of cloud solutions, blockchain, and distributed ledger technology as opportunities for an environment for permission-based access rights to shared data rather than sending/receiving structured documents. The work group concluded that these ideas are not yet represented in practical or scalable solutions that can be recommended at this time, but they should be monitored as they evolve and mature.

4.2 Message Transport Protocols

Recommendation 2: Support both the AS2 and AS4 message transport protocol models for access points.

The message transport protocols for the framework should enable the exchange of e-Invoices or any type of digital documents between two access points in an interoperable, secure, reliable and trusted manner. Message transport protocols in use today vary in the way that they meet these requirements. Refer to Appendix B for a comparison of some protocols currently used.

The work group reviewed three messaging protocol models:

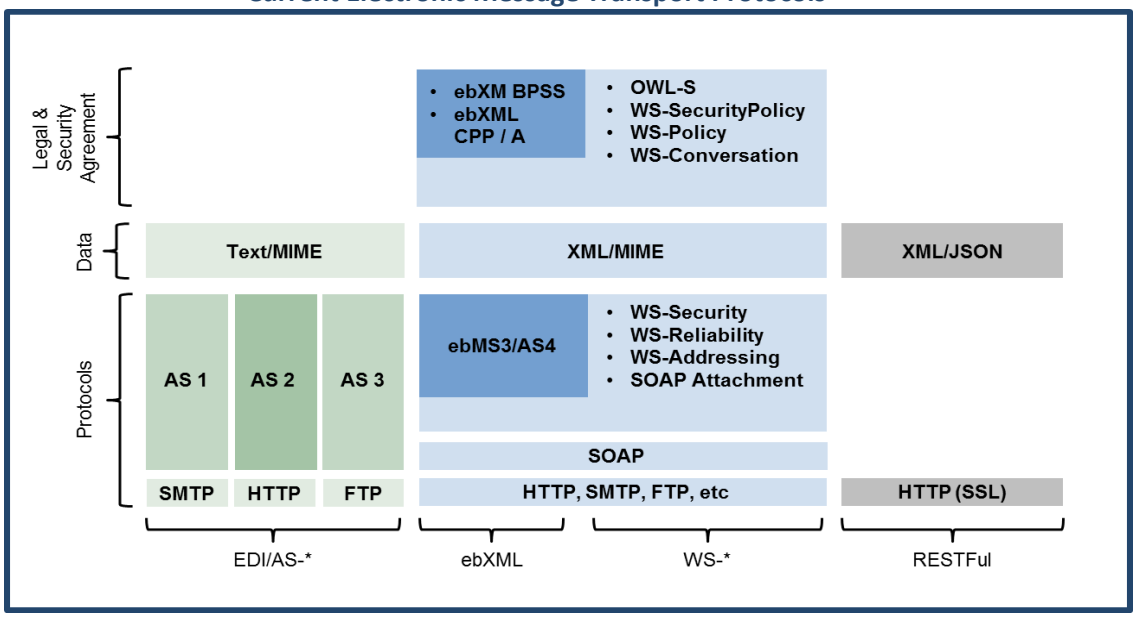
Table 3
Message Transport Protocols

	Description
EDI/AS*	Applicability Statement (AS*) is the specification for Electronic Data Interchange (EDI) communications between businesses. AS2 uses Hypertext Transfer Protocol (HTTP) to transfer EDI data. It supports both EDI and XML syntax.
ebXML - ebMS3/AS4 and WS*	ebXML is a global standard for electronic business document exchange. ebMS3 is a Web Services specification messaging protocol, which consists of 2 parts – a core and advanced features. Applicability Statement 4 (AS4) has features to simplify implementations. Web Service (WS*) refers to a collection of standardized web services specifications.
REST	Representational State Transfer (REST) is a lightweight messaging protocol used in machine-to-machine communications.

There are advantages and disadvantages to all three models, but the EDI/AS2 model (when coupled with external legal and security requirement considerations) and the ebMS3/AS4 and WS model are best suited to support wide-scale standardized interoperable document exchange. REST is best suited for simplified exchange of information in a JavaScript Object Notation (JSON) syntax through Application Program Interfaces (APIs) limiting the amount of information that can be exchanged in comparison to other protocols.

Figure 2 below represents a comprehensive collection of current electronic message transport protocols considered. It should be read as a vertical stack from bottom to top, built in progression from the base protocol to the data layer to the legal and security agreement layer. As shown, not every horizontal grouping has an equivalent representation in the vertical view.

Figure 2
Current Electronic Message Transport Protocols[16]



While the EDI/AS and RESTful columns appear to have a gap at the legal and security level, compared to the middle stack of ebXML or WS, the security aspects of those protocols are bilaterally agreed to, as opposed to standardized. For security, AS2 file transfers typically require both sides of the exchange to trade X.509 certificates and specific trading party names before any transfers can take place. Both AS2 and AS4 use X.509 certificates for authentication security.

The PEPPOL Network which uses AS2, utilizes the OpenPEPPOL legal and security policies for the otherwise bilateral component.

AS2 and AS4 are very similar but have different technical attributes. Currently, AS2 is widely used by EDI Value Added Networks (VANs) in the United States for e-Invoicing message transport. AS4 is a newer protocol that offers synchronous trade, additional logging, and metadata and header capabilities. CEF e-Delivery uses AS4. PEPPOL is migrating to AS4 to align with CEF. Given that many current implementations use AS2, access points must support both protocols for a period. However, all PEPPOL access points are required to support AS4 by February 2020[17]. EESPA currently uses AS2 and is open to an industry migration to AS4.

The work group recommends support for both the EDI/AS2 and ebMS3/AS4/WS models in the U.S market to start. Support for both allows access points the option of migrating to AS4 in accordance with their business needs. Over time, new connections should use ebMS3/AS4/WS.

[16] *Message Protocols for Enabling Digital Services: A Report for the Australian Government on Message Protocols for Enabling Digital Services,* National ICT Australia Limited, CSIRO.

[17] *Support for the PEPPOL AS4 profile mandatory in the PEPPOL eDelivery Network from 1 February 2020.*

4.3 Message Envelope Standards

Recommendation 3: Support both SBDH and XHE envelope technology standards for message exchange while advocating for wide adoption of XHE as the desired long-term approach.

Current e-Delivery networks use either envelopes or headers to address messages to their delivery destination. An envelope is technically different from a header. A message envelope is like a postal envelope that has a delivery address and can contain multiple documents inside that are not visible to those involved with the delivery, unless they know how to open it. A message header is like a postcard, where there is a delivery address and content that is visible to anyone handling the postcard (although the contents are not limited in size).

A message envelope is the container or header that contains an embedded message. Although a lot of document exchange takes place without it, a message envelope is important technology that supports message integrity and confidentiality. For example, access points in corners 2 and 3 can route documents without seeing content. A header does not enable either integrity or confidentiality. It also supports delivering attachments and different message types at the same time.

Uses for an envelope include:

- Privacy and confidentiality
- Ability to send multiple documents in one message
- Ability to send attachments and response messages

UN/CEFACT Standard Business Document Header (SBDH) specification is a header technology commonly used instead of an envelope. SBDH has not been formally adopted as a standard and requires customization prior to implementation.

The Exchange Header Envelope (XHE) is a new joint OASIS and UN/CEFACT specification, which supports both a header and an envelope and supersedes the two prevailing header/envelope standards (OASIS Business Document Envelope (BDE) and SBDH). XHE is currently the only envelope technology standard available that provides end-to-end envelope technology to support a four-corner model.

The work group recommends the XHE specification envelope technology for the uses noted above, while allowing the SBDH specification to support current exchanges until the XHE specification is widely adopted.

4.4 Message Standards

4.4.1 Message Payload

Recommendation 4: Use a single semantic model (under development in the Semantic Model Work Group) and the ISO/IEC 19845 - OASIS UBL v2.x syntax for payload messages.

One of the primary challenges in the market today is the usage of many different e-Invoice standards. The resulting complexity slows adoption and decreases interoperability because it creates overhead and additional cost to manage multiple data integration maps.

Message payload refers to the semantic content and expression in machine-readable syntax. Semantics is the meaning of the data, and syntax is how the computer reads and interprets the data. An analogy with written or spoken language: semantics is the definition of a word, and syntax is how it is spelled.

For example, different languages have a common understanding of a “door,” but they spell the word differently.

Common pieces of information used in an invoice may be referred to using different terminology, but the meanings are constant and commonly understood. The semantic model defines what the common pieces of information mean and the business rules about how to use them in processing. The BPC e-Invoice Semantic Model Work Group is developing a semantic model for the United States. The work group recommends that the framework use this single standardized semantic model for business and semantic interoperability and reduced complexity.

The ISO/IEC 19845 - OASIS Universal Business Language (UBL) syntax is in widespread use globally and adoption is growing. UBL is in common use in the frameworks that were examined. For example, PEPPOL established the Business Interoperability Specification (BIS)[18] with the OASIS UBL 2.1 common directory of data elements and syntax, which helps reduce costs and increase speed of implementation. Currently, EESPA also uses UBL 2.1 syntax based on the semantic model of CEN BII2 for interoperability exchanges and is exploring alternative formats for future adoption.

The European Committee for Standardization (CEN) European Norm (EN) 16931 standard has one semantic model with three syntax options. While they have valid reasons for this implementation, multiple syntaxes result in greater complexity to manage system mappings.

The work group recommends OASIS UBL 2.x[19] due to its common data dictionary and use of a single syntax.

4.4.2 Message Response

Recommendation 5: Adopt message responses compatible with those under development in Europe.

Message responses cover the status, treatment and servicing of the payload in support of the underlying document flows. The status information within these messages may include a number of structured sections and code lists, such as:

- Status (e.g. invoice or transaction under query; invoice approved for payment)
- Reason for the status (e.g. prices or quantities incorrect; approval process completed)
- Action codes (e.g. request to provide information; await remittance advice)
- Detailed clarification or additional information

A common set of message responses is currently under joint development by EESPA and OpenPEPPOL. The response messages, built from an OASIS UBL common directory of data elements, will support exchange of multiple document types.

[18]The PEPPOL standard for the semantic model and its syntax binding, now aligned with the new European standard for a core invoice.

[19]The Work Group did not recommend a specification version of UBL at this time because the OASIS UBL Technical Committee is updating UBL v2.2 to v2.3.

4.5 Business Discovery Process

Recommendation 6: Establish a discovery model that allows trading parties and their service providers to connect and operate in a fully interoperable and flexible way based on standard components while maintaining commonly used practices.

One of the challenges in an interoperable framework is identifying how and to what extent that trading parties and service providers are participating. *Discovery* refers to the processes and technology used to look-up trading party capabilities, how to send electronic invoices or other messages and how to authenticate credentials. Another discovery process challenge is determining the structure and permitted use of the actual identifiers and related information. In this section, both areas are described at a high level in preparation for the detailed analysis and recommendations provided in section 4.6.

In order to support discovery within a network, the required information can be:

- Maintained and shared bilaterally between trading parties and their service providers
- Contained in a registry, a directory or both

The bilateral discovery model is common because trading parties are able to exchange information during procurement or contractual activities undertaken prior to invoicing. Although it is not scalable as transaction volumes and trading relationships proliferate, it is likely to remain in use between habitual trading parties, as it is valued by those who are reluctant to join a registry for confidentiality reasons.

Many trading entities take advantage of a registry service operating at the network level and/or use a directory service provided by various entities within a network eco-system. A *registry* contains technical information about identifiers that encapsulates the legal or entity identity, location, and routing instructions of participants in the network. It is used for *technical interoperability* and allows access providers in corners 2 and 3 to create the necessary connections for the delivery of messages. Such registries (or metadata directories) contain a minimum set of metadata elements required to operate and support the required network connections.

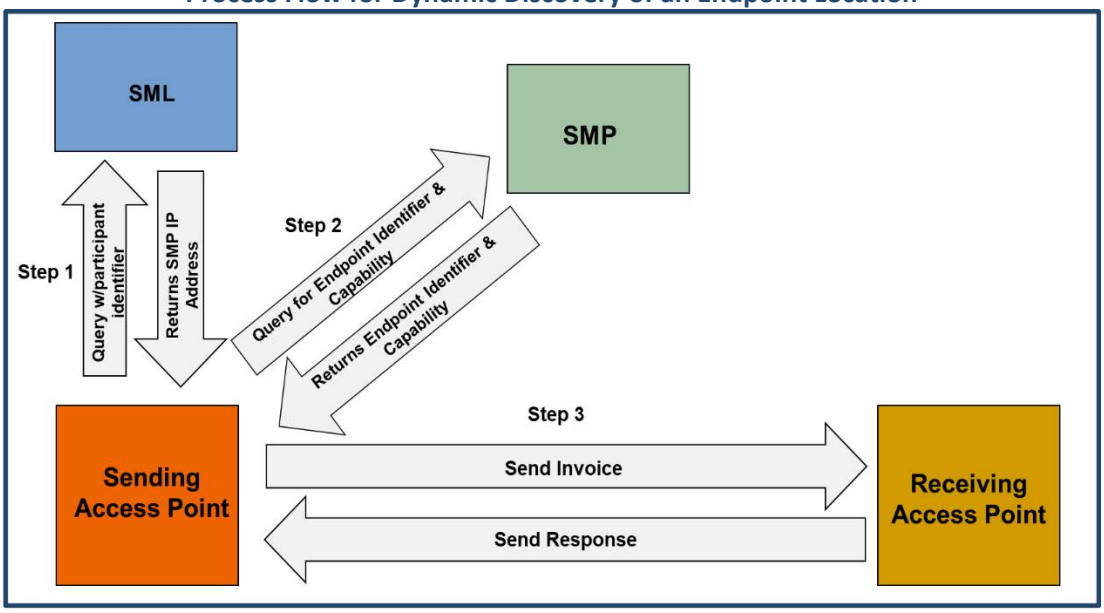
A registry may connect to a *directory* that contains a variety of business information elements about a trading party; it is analogous to the "yellow pages." It is used for *business interoperability* and may also contain information that supports *technical interoperability* (such as identifiers). Service and solution providers of various kinds typically offer and manage these directory services. Such a directory may list document receivers and contain company information, documents supported, contact details, business rules and electronic address identifiers. This facilitates timely and highly automated onboarding and allows business users to discover a receiver's capabilities and initiate document exchange based on fully accessible routing details.

Table 4
Usage Differences between Registry and Directory

Type	Usage	Usage
Registry	Technical	The e-Delivery network uses the registry information for discovery of identity, location and routing (i.e. The essential metadata for automated messaging).
Directory	Business	Directories, similar to the 'yellow pages', are used by businesses users to discover who is on the framework, and related information about trading parties. Directories may also contain metadata that is found in the registry.

For example, the Connecting Europe Facility (CEF) e-Delivery specification creates a four-corner network configuration using standard artifacts. Discovery consists of two components; the Service Metadata Publisher (SMP), which publishes the capabilities of a receiving party, and the Service Metadata Locator (SML), which identifies the location of the Service Metadata Publisher (SMP). These standard components provide the benefit of facilitating dynamic discovery across a four-corner model network, and compared with bilateral discovery, avoids having to maintain multiple routing tables. Figure 3 is a simplified illustration of the process.[20,21]

Figure 3
Process Flow for Dynamic Discovery of an Endpoint Location



Source: Business Payments Coalition

Trading parties exchange documents through access points that connect with many other access points. To locate a trading party end-point on the network, the sending access point first queries (Figure 3, Step 1) the SML using the Entity Identifier to find the Universal Resource Locator (URL) of the Service Metadata Publishing (SMP). The query provides a response informing the sender where the end-point recipient SMP record resides. A second query (Figure 3, Step 2) is initiated to the SMP to retrieve the end-point identifier and confirm the capabilities of the receiver.

The SML and SMP approach has implementations within the e-Invoicing and e-procurement space in PEPPOL and in other public administration use cases in the European Union. PEPPOL largely developed the artifacts that now form part of the generic open source CEF e-Delivery, which is gaining acceptance as a standard for interoperability at the transmission level. It is also used in Australia, and EESPA is planning to pilot CEF e-Delivery to support its Multilateral Interoperability Agreement.

A major design decision with respect to *discovery* concerns whether to deploy registry services on a centralized basis or on a decentralized basis. With centralized discovery, trading parties share information using a common registry service updated and accessed by all trading parties and usually managed by a single authority. Decentralized or federated discovery employs a number of separate registry services that

20 Business Document *Metadata Service Location Version 1.0, OASIS Standard*, August 01, 2017.

21 *Service Metadata Publishing (SMP) Version 1.0, Oasis Standard*, August 01, 2017.

are accessible by trading parties but also conform to a common set of rules and governance principles. A further exploration of this choice and related recommendations is detailed below in section 4.6. Directory services are by their nature commonly decentralized, although a single authority operating a registry may also offer directory services.

In addition to the discovery processes discussed above, the e-Delivery network requires a standard set of entity identifiers, electronic address identifiers and electronic routing addresses. The wide range of identifier types and standards used today reflects the diversity of potential e-Delivery network participants. Section 4.6 describes possible approaches to identifiers and makes specific recommendations for implementation.

4.6 Identifiers and Registries – Implementation Level

The previous section provided a high-level overview of the network discovery process and its implementation in various frameworks. This section provides an analysis and implementation recommendations for the use of identifiers for business and routing addresses, and the deployment of registry services. The work group reviewed the detailed approaches and techniques used by the frameworks. Additional information on each follows.

4.6.1 Identifiers for Business and Routing Addresses

Recommendation 7: The identifier system should have three distinct levels: 1) Entity (and sub-entity) Identifier, 2) Electronic Address Identifier, and 3) Electronic Routing Address.

The primary function of access points is addressing and routing of invoices and related documents, which requires identifiers to determine where invoices are to be sent. The core identifier elements for routing are included in Table 5 below.

Table 5
Core Identifier Elements

Element	Description
Entity Identifier	Unique digital identifier of a trading party or business entity
Electronic Address Identifier	Unique digital address used by a trading party for the routing of digital documents and messages
Electronic Routing Address	Electronic routing address associated with an Electronic Address Identifier that defines the service platform that supports routing digital documents and messages of a trading party

An Entity Identifier may form a component of or a path to discover an electronic address or routing address. Identifiers should support characteristics such as business, location, nationality and levels within an ownership structure.

The Entity Identifier is specific to the business entity and independent of a service provider or any other trading party (except the issuer, which may be a regulator or government entity).

There is no single global identifier in use; each framework uses a slightly different approach as appropriate for their market. For example, the PEPPOL code list of participant identifier schemes contains 78 entries[22]. Table 6 illustrates several identifier scheme examples currently in use.

Table 6
Example Identifiers Used in Other Frameworks

	OpenPEPPOL	DBC
Identifier schemes	• Country specific VAT Number • Global Locator Number (GLN) • Data Universal Numbering System (DUNS) • International Bank Account Number (IBAN)	• Australian Business Number (ABN) • Global Locator Number (GLN) • Data Universal Numbering System (DUNS)

At this time, a single Entity Identifier scheme is not feasible for the U.S. market since many different identifiers are in use and need to be sustained to minimize adoption friction. Migration toward a single identifier such as the Global Legal Entity Identifier (GLEI) would be preferred over time. However, until a single identifier achieves sufficient adoption in the United States it will be necessary to allow the use of multiple identifiers to enable discovery across systems that currently use different identifiers.

The work group recommends the framework support multiple identifier schemes from the ISO/IEC 6523 identifier standards. ISO/IEC 6523, used in the frameworks assessed, defines a structure for uniquely identifying organizations and divisions or subsidiaries. Given the diversity of identifiers in use in the United States, clear rules and practices must be established for the operation of Entity Identifiers, especially as it is likely that a single legal entity may use multiple identifiers in parallel. Identifiers with widespread usage in the United States and those needed for cross-border trade should be considered. Businesses can agree bilaterally on identifiers for their own use and within the e-Delivery network. Entity Identifiers can be used within the framework and for external purposes.

The Electronic Address Identifier is a specific electronic identifier used to enable a trading party to send and receive digital documents and messages to/from another trading party, independent of the specific routing or platforms being used and whether they are provided internally or operated by a third party. A legal entity may use one or more Electronic Address Identifiers. For example, a legal entity may use one Electronic Address Identifier for the receipt of orders and a separate Electronic Address Identifier for the receipt of invoices and other documents. It will often contain information elements derived from the Entity Identifier, but this is not mandatory or exclusively the case. An Electronic Address Identifier may also be linked with digital capabilities and business rule details defining what can be sent or received using this address and how either party will handle such exchange.

The Electronic Routing Address (i.e., a service provider or receiving technical platform address) is linked to the Electronic Address identifier, and used within the e-Delivery network to identify the service providers or technical platforms comprising corners 2 and 3 (Figure 1).

22 *OpenPEPPOL Code Lists - Participant identifier schemes* v6 draft.

These addresses need to be available to end users and all other service providers to support interoperability. If the exchange is bilateral, the relevant electronic addresses are only those of the sending and receiving trading parties. To enable discovery of this and other permutations, registries post identifiers and addresses.

Entity Identifiers and the Electronic Address Identifiers can be easily confused because elements of one may be used as a component of the other. In some situations, the Entity Identifier is a proxy or alias for the Electronic Routing Address, and therefore a discovery process is required.

A governing body should assume responsibilities for decisions about identifiers, starting with documentation of available options and concluding with the establishment of clear and logical rules for deployment. In addition, an assessment of ISO/IEC 6523 standards should be conducted to determine identifiers that are currently in use by U.S. businesses. The assessment should include business end users to determine U.S. market requirements.

4.6.2 Registry Approaches

Recommendation 8: Use a federated registry service using the Domain Name System (DNS) to enable discovery across all access points and participants that choose to use the service.

The work group examined various approaches to manage the registry process itself and information in the registries. The process to register into the frameworks was not assessed; rather, the assessment focused on how access to and control of the information is managed.

4.6.2.1 Technical Features of Registries

DNS provides a global address space needed for any type of network that uses the Internet and requires dynamic discovery of disparate participants. The BDX-Location-V1.0 standard provides a common mechanism to use the DNS namespace in a controlled manner. It also uses NAPTR[23] resource records to route connections from the registry to another point on the Internet. In the e-Delivery network, it routes an access point's connection request to the appropriate Service Metadata Publisher (which ultimately sends it to the target access point). This functionality opens up many options to register participants into the e-Delivery network without having to maintain entries in a central database. DNS, by its nature, is a globally distributed and replicated system, so its use creates an instant distributed environment for the e-Delivery network. Due to this flexibility, it is recommended that whatever standard is adopted includes the use of DNS for registering components.

4.6.2.2 Governance and Deployment Approaches

There are three different governance and deployment approaches to the processes and management of the data in a registry: centralized, federated and fully decentralized. Earlier this document referred to these terms in the context of technical architecture. The following information describes these terms as they relate to approaches to registry governance. The meaning of these terms can be interpreted broadly, however, for this assessment they were defined as follows.

[23] Name Authority Pointer (NAPTR) is a type of resource record in the Domain Name System of the Internet.

Centralized

Centralized has one authority that handles all participant registrations. This includes managing and owning the infrastructure to support the e-Delivery network and explicitly controlling participant enrollment. It is suitable for a regulator that wants to control participation and can mandate the approach.

Advantages of a centralized approach include ensuring the accuracy and integrity of data; allowing for deployment of a single technical environment (which can offer coherence of information); ease of maintenance; and lower costs. A disadvantage of this model is that it can be a single point of failure.

For example, in order to participate in the PEPPOL Network, entities must be registered in the PEPPOL DNS[24] name space, meet the specifications, and agree to a legal contract. Registry governance lies with PEPPOL; some registry services are delegated to non-autonomous PEPPOL authorities.

The PEPPOL registry is centralized, public, and query-able, but not searchable. A PEPPOL Authority registers business identifiers and SMP locations into a single PEPPOL Service Metadata Location (SML).

EESPA currently uses a minimum centralized database of routing addresses for EESPA members. All trading party information is maintained at the member level and exchanged bilaterally. EESPA is planning a pilot of the CEF e-Delivery specifications which could lead to a membership wide adoption.

Federated

Federated means authorized groups (e.g. service providers) register participants directly into the network. DNS with the NAPTR resource record can support this federated registration process. It allows registration entries to be stored in any DNS name space, but uses a specialized textual lookup to ensure redirection into an authorized e-Delivery network. This eliminates the need for a centrally managed registry. Additional analysis of this technology is needed to further validate how well it supports federated registration while also ensuring integrity and trust.

A federated model requires a level of oversight from a governance group that maintains the standards and approves participants through legal agreements. Stakeholders, including access point and SMP providers, end users and neutral parties need to participate in the governance of a federated model. Another important aspect in a federated model is the need to ensure trust. The participants within the e-Delivery network need to ensure those in it are legitimate endpoints. There may also be a need for minimal infrastructure maintenance support for the e-Delivery network and some level of accountability oversight, yet also a high level of autonomy. This model is appropriate for a highly diverse, unregulated e-Invoice environment like the U.S. market.

Advantages of a federated approach include the ability to attract participation by empowering entities to provide e-Delivery network services; avoidance of a single point of failure; and coherence of information when standards are used. A disadvantage of this model could be the distributed nature of registries and greater complexity to maintain. However, it is possible that maintenance of the registry information locally, rather than centrally, could increase the information integrity as long as there is some form of accountability.

The PEPPOL and CEF e-Delivery environments deploy aspects of the federated model with SMP registries. In practice, centralized registries used by certain frameworks could still be present in a federated model (as one instance of a registry service) provided it conforms to the common rules. The phone networks are other examples of a successfully federated model in which service providers assign a phone number to their users.

[24] PEPPOL has a registered Domain Name Space (DNS) which controls access to the PEPPOL network.

Decentralized

Decentralized means there is no control over who can register as a valid participant within the network, but there is a defined standard that each participant is presumed to follow and no governance body exists to oversee accountability.

A fully decentralized approach shares advantages and disadvantages of a federated approach. Oversight that is absent or poorly implemented can present security vulnerabilities. However, the architecture of the network reduces the number of connections that need to be managed by the endpoints making it easier to monitor and mitigate risk.

Examples of decentralized approaches are file sharing or instant messaging networks.

The work group determined that a decentralized approach is not recommended initially for the proposed Interoperability Framework because it would bring major challenges in the early stages of the operation of a registry service. However, it could be a longer-term objective when standardization and operational maturity of the framework is well established.

For clarity, this determination does not rule out or deter the use of bilateral discovery processes on a decentralized basis by network participants, whereby the required information is maintained and shared between the trading entities and their service providers. Frameworks that offer a centralized or decentralized registry service invariably do not rule out this practice for discovery, as the use of registry services is optional.

Governance Model Conclusions

The work group concluded that without a central authority and mandate for e-Invoicing, a federated model would best fit the U.S. market. The United States would need an organization to manage the federated model, such as a member-driven consortium.

The work group recommends that when developing final requirements for the registry process, the United States monitor the efforts by OpenPEPPOL, EESPA, and ConnectONCE[25] and consider approaches that will enable a future Global Interoperability Framework (GIF). The GIF is a neutral vehicle intended to facilitate collaboration on global or regional e-Invoicing interoperability.

4.6.3 Discovery Conditions

Recommendation 9: Support conditional permission levels for trading party access.

The discovery process must support defined rights and responsibilities for end-users and service providers to establish exchange across the e-Delivery network in accordance with the requirements of the end-users. Service providers can assign rules to the receiving or sending of transactions across the e-Delivery network as required by the end-user.

End-users may be open to receive e-Invoices from anyone on the Network; they may want to apply conditions such as restricting receipt of invoices from only one region; or they may want to prevent discovery of their connection without specific approval. As outlined in Figure 7, these conditions are a vital component of the overall framework, given the commercial and competitive nature of the information.

[25] ConnectONCE is a trade organization that provides B2B e-Commerce marketplace operators, their suppliers and customers, service providers and others a collaborative forum to advance global trade.

The business directory, registry, and service provider all need to support the permission levels required by the end-user. The business directory would only publish non-confidential information. The service provider can build rules to block unwanted transactions. The registry may need to prevent access to network routing details unless an authorization code has been provided or the receiving party has specifically added the sender ID to a managed list of senders able to access their routing details within the registry.

These conditions are critical to the end user for functions such as fraud prevention. For example, the e-Delivery network may need to support different conditions for connections to be established. Table 7 provides the types of connection conditions that may need to exist.

Table 7
Connection Conditions

Level	Description
Open	Open connection where the receiving party is open to receive all classes of transactions and documents supported by the e-Delivery network, from any trading party with a business relationship, and through any channel with the required access capabilities. This is analogous to a public phone number that accepts all calls.
Conditional	Conditional connection whereby the connection is open to any trading party but there are limitations on the transaction and document types or processes supported. This is analogous to call blocking on a phone.
Pre-authorized	A connection can only be established following pre-authorization by the receiving end-user and communicated directly or through its nominated service provider. This is analogous to call screening on a phone.

PEPPOL uses conditional attributes whereby the connection is open to any trading party, but there are limits (controls) on the documents that can be exchanged. For example, PEPPOL only allows for the transport of an e-Invoice that strictly follows the BIS.

4.6.4 e-Delivery Network Registry Standards

Recommendation 10: Use the OASIS SML and SMP specifications for the registry infrastructure.

Registries store identifiers, routing and capabilities information. A registry is a vital component to support dynamic discovery. OASIS is the only organization that has developed a set of open, non-proprietary standards for dynamic discovery, the OASIS Business Document Metadata Service Location 1.0 (SML) and OASIS Service Metadata Publishing 2.0 (SMP) specifications.

OASIS refers to its registry as a metadata directory. The metadata directory enables dynamic discovery for connections between trading parties in contrast to static EDI routing tables.

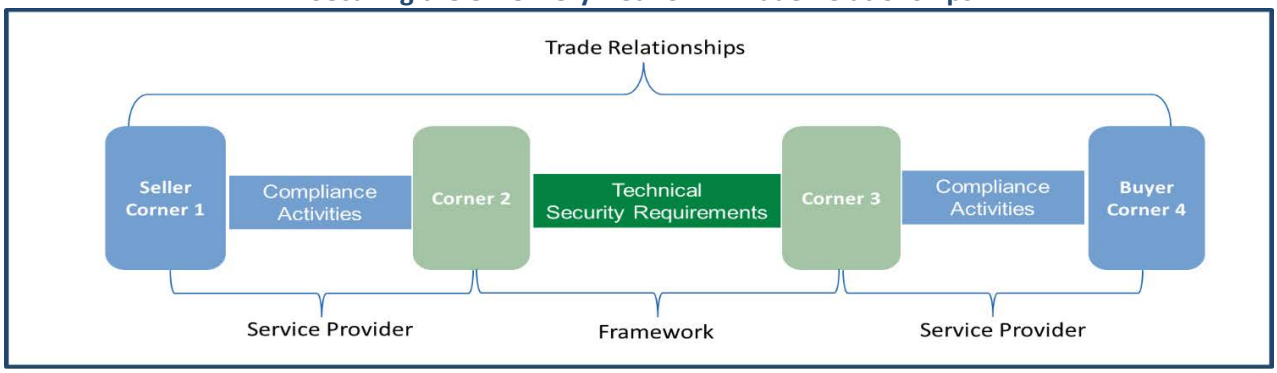
4.7 Security

Recommendation 11: Support a variety of security options within a defined set of minimum technical requirements that meet current industry security standards. A governance organization should address legal requirements for e-Delivery network participation and define the technical security standards and protocols that establish an appropriate balance between interoperability and security to promote adoption.

An Interoperability Framework requires both technical security within the e-Delivery network and supporting business agreements. The framework security model must enable confidence and maintain trust by setting high security standards. Trust is a shared responsibility and must be established at both the business and technical levels.

From the business standpoint, security requirements start with the agreements between trading parties (corners 1 and 4) and between service providers and their customers (corners 1 and 2 and 3 and 4) when performing compliance activities such as Know Your Customer (KYC) and Anti-Money Laundering (AML) during onboarding.

Figure 4
Securing the e-Delivery Network – Trade Relationships



Source: Business Payments Coalition

All interoperability frameworks require agreements that define access point responsibilities, requirements, and liabilities. For example, to gain access to the e-Delivery network, service providers enter into an agreement with the operator of the framework. The agreements may also include compliance requirements established by the governance body overseeing the framework. For example, EESPA has model interoperability agreements amongst its members that define the responsibility of each party, contractual and business issues, as well as transmission modes. OpenPEPPOL requires service providers to enter into a Transport Infrastructure Agreement (TIA), which covers the roles and responsibilities of access points. A U.S. market governance body should address the appropriate legal agreements required by the proposed e-Delivery network.

Technical security requirements for corners 2 and 3 (Figure 4) must prevent fraudulent invoices from actors outside of the e-Delivery network and prevent attacks such as Denial of Service that erode the confidence and trust of participants. For transport layer security, the message transport protocols must be maintained to ensure confidentiality between access points. Message layer security is provided by the system on a per message basis; it should be independent of the transport layer security. In the four-corner model, message layer security ensures integrity, confidentiality, authenticity, and non-repudiation at all times. These are inherited by use of the standards that support envelope and message transport protocols.

The work group concludes that infrastructure security rests on the following key tenets:

- Leverage established approaches that scale well and use proven technology for secure communication protocols. AS2 and ebMS3/AS4 transport or exchange standard, for example, inherently meet the requirements for secure communications.

- Use x.509 public key infrastructure (PKI) certificates. This provides authentication technology to assure that both sender and receiver participants are communicating with valid e-Delivery network members.
- Register participants into the network using a controlled process (section 4.6.2 Registry Approaches) to ensure accurate discovery and document transport.

If the United States pursues a federated registry model, with decentralized governance, careful consideration would be necessary to achieve security and trust. A core component of the recommended security is the use of X.509 security certificates, which rely upon a trusted certificate issuance process. In a centralized architecture, there can be a central certificate issuance authority. In a federated architecture, a governance body will need to determine the certificate issuance and process for exchange.

Finally, the work group recommends the framework security be flexible to support a variety of options within a defined set of minimums that meet current industry security standards. A governance organization should establish a balance between interoperability and security to promote adoption.

4.8 Standards

Recommendation 12: Base the e-Delivery Network on the open standards listed in Table 8.

For the most part, the existing frameworks assessed use open, non-proprietary standards for their e-Delivery networks. The importance of building the framework on open, non-proprietary standards cannot be overstated. Without open standards, interoperability would be hard to achieve, resulting in continued fragmentation of the market. Table 8 lists the open standards recommended for use in defining the framework. Using this set of standards creates a level playing field for service providers.

Table 8
Recommended Open Standards for the U.S. Framework

Component	Standard	Reference Link
Message Transport Protocol	OASIS Applicability Statement 4 (AS4 Profile) of ebXML (ebMS 3.0) version 1.0	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html
	Applicability Statement 2 (AS2) for Business Data Interchange Using HTTP	https://www.rfc-editor.org/info/rfc4130
Message Envelopes	UN/CEFACT and OASIS Exchange Header Envelope (XHE)	https://docs.oasis-open.org/bdxr/xhe/v1.0/xhe-v1.0-oasis.html
	UN/CEFACT Standard Business Document Header (SBDH)[26]	https://www.gs1.org/docs/gs1_un-cefact_%20xml_%20profiles/CEFACT_SBDH_TS_version1.3.pdf
Message payload syntax	OASIS Universal Business Language (UBL) v2.x (ISO/IEC 19845:2015)	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl

26 The specification has not been approved nor published by the UN/CEFACT (its official status is "draft").

Component	Standard	Reference Link
Service Registry (Location)	OASIS Business Document Metadata Service Location (SML) version 1.0	http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html
Service Registry (Capability Publishing)	OASIS Service Metadata Publishing (SMP) version 2.0	https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/bdx-smp-v2.0.html
Entity Identifiers **Network identifiers (routing addresses)**		To be specified by a governance group

5. How the Framework Comes Together and Proof of Concept

Service providers, which offer services and Software as a Service (SaaS), provide connections to an interoperability network as access points. The services include integration with client business application systems, processing services, and access to the network. The access point *software* provides an interface into the network and its discovery mechanisms.

In the four-corner model (Figure 1), access points are located at corners 2 and 3. In an e-Invoicing interoperability network they provide the necessary means to deliver documents and messages.

The access point software at corner 2 packages and validates payload business data received from corner 1, and access point software at corner 3 unpacks and prepares it for transmission to corner 4. An access point consists of two main components:

- Integration with client applications such as ERP systems that send or receive payload across the network
- The standard message service handler interface with other network access points

As discussed in section 4.2, the standard message service handler uses a standard message transport protocol between corners 2 and 3. This ensures interoperable, secure, and consistent data exchange within the network. The functions of the message service handler are configured during the implementation of the access point.

The interface between client applications and the service provider (corners 1 and 2 and/or 3 and 4) can use any message transport protocol, as this is part of the service provider value-added client services. Corner 2 receives invoices or invoice data from corner 1's application and transforms the data to the agreed-upon syntax to send through the network. Corner 3 receives and transforms the network data into a syntax compatible with corner 4's business application and sends the invoices to that application.

Access points are typically set up and managed by service providers that provide a variety of services to clients. For e-Invoicing, these services may include:

- Document creation
- Document enrichment
- Data formatting
- Data mapping, translation/transformation
- Data archiving
- User access portals
- Data validation for corners 1 and 4
- Delivery of documents
- Compliance with established network rules and interoperability standards

Client integration is more complex for service providers than only building connections between access points. Service providers customize the integration with business applications by building specific interfaces for the various ERP systems they support. Individual client configurations may require customization. These integrations are typically part of a larger suite of services such as operational support and other value-added services to clients as mentioned above. These functions lie outside the standardization efforts of the framework.

Service providers may also host registry and/or directory functionality as described in sections 4.5 and 4.6. Service providers typically enroll their clients into the registry/directory with information about the endpoint identifiers and the receiving access point's capabilities.

An interoperability framework presents opportunities for access point providers to offer clients additional value-added services, and scale their business by offering clients an exponentially growing number of trading parties for document exchange. They also ease adoption of e-Invoicing for their clients by handling technical connectivity and data transformation to meet the exacting open exchange message standards.

5.1 Proof of Concept (POC) for e-Delivery Network Technology

Recommendation 13: The final step for the work group is to conduct a broader validation exercise of the recommendations (Table 10) for an e-Delivery network for the U.S. market.

5.1.1 POC Purpose

At the beginning of the assessment process, the work group determined that it would be valuable to develop a simple, yet functional, representation of a typical e-Delivery network that was isolated from any live production systems or other networks. This would create a POC for the findings and concepts developed in the technical assessment.

The objective of the POC was to utilize a baseline of recommended standards and practices for a U.S. Framework (Table 8) to help the work group better understand:

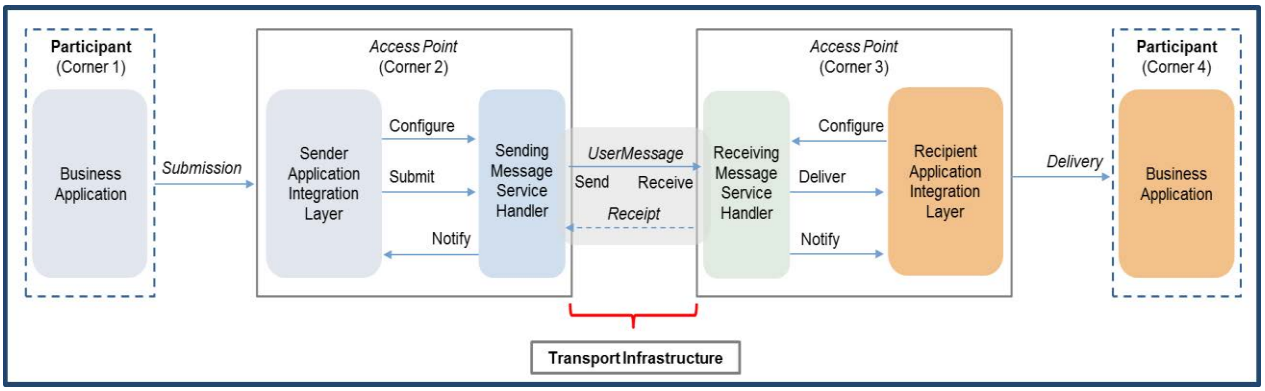
- The network functions
- The degree of complexity in implementing access point functionality
- The tools available to assist in development
- Typical use of the network by participants

5.1.2 POC Scope

The POC established a small-scale network that could demonstrate the flow of messages between two access points, and how those access points could discover each other prior to message transmission. As described in section 5.1.3 below, the network was configured using the open-source artifacts forming the CEF e-Delivery building blocks.

Figure 5 illustrates the high-level business functions in the end-to-end process. The scope of the POC focused on building a message transport interface, or the *message service handler,* and establishing *connectivity* within the e-Delivery network.

Figure 5
Workflow within the Four-Corner Model[27]



[27] *PEPPOL Transport Infrastructure AS4 Profile Version: 1.0:* OpenPEPPOL AISBL, August 12, 2017.

The POC did not attempt to create the integration layer between the access points and corners 1 or 4 (end-customer ERP systems) (Figure 5). This would require integration into potentially many client application environments in which a high degree of discretion applies regarding services and capabilities. The POC therefore incorporated a simple emulation of corner 1 and 4 systems, which were not representative of a true production-level access point integration with service provider and client business applications.

Table 9
Business Process Steps and POC Scope

Business process step	POC scope
1. ERP application (corner 1) creates an invoice and sends to the corner 2 access point.	Emulated the business application with XML.
2. Corner 2 access point evaluates and validates the invoice (including transformation to meet standards).	Installed software to create access point.
3. To locate an endpoint on the e-Delivery network, the sending access point first queries the SML using the Entity Identifier to find the Universal Resource Locator (URL) of the Service Metadata Publishing (SMP). The query returns the location where the endpoint recipient SMP record resides.	Created an SML. Access point connected to the SML.
4. A second query is initiated to the SMP to retrieve the endpoint identifier and confirm the receiving access point's capability.	Created an SMP. Access point connected to the SMP.
5. The SMP relays back to the corner 2 access point both the Internet location of the corner 3 access point and the type of documents and standards required by the end customer (corner 4).	SMP connected to the access point.
6. Corner 2 access point connects with the corner 3 access point and sends the invoice.	Created the corner 3 access point. Corner 2 access point connected with corner 3 access point and sent document.
7. Corner 3 access point evaluates the invoice, validates that it meets requirements (as defined by corner 4) and accepts the invoice.	Tested against dummy rules.
8. Corner 3 access point transforms the invoice into the specifications required by the corner 4's business application and sends the invoice to corner 4.	Created XML file and sent from corner 3 access point to corner 4.
9. Corner 4 (end customer business application) receives the invoice and moves it into internal processing.	Validated the XML file.

5.1.3 The POC Setup

CEF e-Delivery, an existing open source solution, was used[28] to avoid lengthy and expensive development. The Connecting Europe Facility (CEF) Digital Unit open source software provides end-to-end capability for electronic document delivery over the Internet based on OASIS standards. These artifacts also form the basis of the PEPPOL specifications and are used in a range of other applications within the European Union and elsewhere. Implementation guides and open source tools[29] are available to assist service and software providers during the set-up of access point components. In addition, certification[30] and testing tools[31] are available to ensure the access point conforms to the requirements of the network.

Building the access point software (corners 2 and 3) was straight forward. Corners 1 and 4 were simple emulations using XML documents. The access point software is the critical component that interfaces into the network to send and receive messages; in this case, invoices. The business application was emulated with an XML file containing information that defined the document type and recipient, along with arbitrary but plausible information representing the payload (invoice). The access points were built using an open source product called Domibus.

In order to undertake the discovery process, access points need to discover their target's identifiers and capabilities prior to allowing message exchange. Typically, a centralized repository is used for discovery. However, because registration mechanisms are, by nature, centrally defined and managed, there are relatively few software packages or systems established to use as examples for a decentralized model (4.6.2 Registry Approaches). Based on a decentralized design, the OASIS standards group created a registration standard called Business Document Metadata Service Location (BDX-Location-V1.0- BDXL). OpenPEPPOL uses a controlled DNS namespace, where registering into that name space is strictly controlled through an authority using an SML. The CEF Digital team created an SML software package that can be configured to use either the OASIS BDXL standard or the PEPPOL SML standard. The POC used this software and configured it for the BDXL standard.

---

[28] Technology Used: Windows Server ® 2016; Windows® DNS; ApacheTomcat® Java® Web Servers (https://tomcat.apache.org/); MySQL™ Database (for SMP and APs) (https://www.mysql.com/); SoapUI™ (for emulating back end business transactions) (https://www.soapui.org/); CEF Digital SML (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+software); CEF Digital SMP (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+software); CEF Digital Domibus (access point) (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus)
Standards used: OASIS BDX-Location-1.0 (for Meta-data Location (SML)) (http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html); OASIS BDX-SMP-V1.0 (for Meta-Data Publisher (SMP)) (http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html); EBXML EBMS V3.0 (for Semantic and Syntax of the XML files used in the message and envelope) (http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html); AS4 transport protocol (used as the transport between Corners 2 and 3) (http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html)

[29] For example, CEF has a list of tools available to establish an access point. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software?preview=/82773366/82798324/(CEFeDelivery).(AccessPoint).(COD).(v1.09).pdf. PEPPOL guidelines. http://peppol.eu/downloads/ap-guidelines/

[30] For example, CEF points to the Drummond Group to help access points get their AS4 certification of conformance. https://drummondgroup.com/applicability-standards/

[31] *OpenPEPPOL Test and Onboarding,* OpenPEPPOL AISBL, November 26, 2018.

Access points also need a mechanism to register their specific capabilities and discover the capabilities of other access points. These capabilities include specific product and document types and other information based on the agreed-upon standard, defined by the governance group responsible for that network instance. The SMP stores this access point capability information and endpoint location. OASIS publishes a common standard for SMP (BDX-smp-1.0) and the CEF Digital group created open source software designated with the same name. The POC used the CEF provided SMP software to create the final component needed for an end-to-end POC test. Service providers may also host registries (the OASIS BDXR standard refers to them as Service Metadata Publishing).

All components (e.g. message transport protocol, message envelope, identifiers, and registry) use certificates to establish authenticity and avoid false registrations and unwanted connections. In CEF e-Delivery, these certificates are provided/registered by an authority. This centralized management results in a system with tight controls that reduces the risk of fraudulent activity. The POC tested functionality, not security, so certificates were not required to complete the test.

Setting up the SML and SMP functionality without establishing a DNS namespace for the POC environment proved challenging. DNS namespace is critical to the core functioning of the components, and the access point software options had dependencies that required DNS integration. See section 4.6.2, Registry Approaches, for an explanation of the DNS namespace. It quickly became apparent that any standard developed using BDX-Location-V1.0 as a base will also have to establish how the DNS namespace will be used and managed. This aspect will require work on governance and deployment in a future phase of the project.

5.1.4 Findings and Recommendations

The POC proved to be invaluable in understanding how a secure and fit-for-purpose e-Delivery network can be created using open source software tools. The client integration layer was not extensively emulated and tested, nor was the full functionality associated with discovery processes. Main findings and recommendations are as follows:

<u>e-Delivery network performance and access</u>

- Creating the access point and the ability to participate in the network is relatively easy. Message flows between corners 2 and 3 are also easily accomplished.
- Although the POC scope was limited, it is clear that there are significant complexities for business application integration between corners 1 and 2 and 3 and 4. This is typical in any network integration situation.
- The well-scoped access point definition with its message handler interface drastically reduces the number of integrations per trade party creating a “connect once, exchange with many” environment.
- A thriving service provider industry is required to establish competitive and well-positioned platforms for delivering business application integration and providing a range of value-added services. These services can range from basic to complex.
- The environment needs to be managed through establishing a cooperative governance framework which delivers network user rules and practices which ensure delivery of the essentials for interoperability, surrounded by a highly competitive market-place for solutions and services.

Discovery

- Using the SMP model for hosting the access point metadata is recommended. The BDX-smp-1.0 specification has proven to be effective; it fully supports a distributed model, and appears to work well for CEF e-Delivery (and OpenPEPPOL). Adoption of this standard mechanism does not unduly limit options for access points or the registration mechanisms, as it can be adapted to meet a variety of requirements.
- Hosting an SMP model can be complex and requires management and support resources. At the same time, a noted benefit of SMP hosting is the ability to expand service provider business offerings, increasing competition and client choice through multiple SMP hosts.
- Using the NPATR standard Name Address Pointer with DNS is recommended. It is a proven method of handling discovery of endpoint locations on the Internet, and is a distributed, fault-tolerant system used globally. It is flexible and avoids creating a new mechanism to support the distribution of participant addresses.
- It is clear that a federated, decentralized SML model will require considerable thought on organization rules and governance.
- Based the key findings of the POC, it is clear that the necessary technology exists today to support a fit-for-purpose interoperable network. A next step is to conduct a validation exercise of the work group's above recommendations of the network technology for an e-Delivery network for the U.S. market.

6. Recommendations and Next Steps

In conclusion, the BPC e-Invoice work group found the technology components and tools required for an e-Delivery network exist today and provide the necessary security and scalability for the U.S. market.

6.1 Recommendations

The work group's comprehensive assessment of the business and technical requirements of the U.S. market yielded the recommendations recapped in Table 10.

Table 10
Summary of Recommendations

	Section	Component	Recommendations
1	4.1	Overall architecture	Base the overall architecture of the e-Invoice interoperability framework on a four-corner model.
2	4.2	Message transport protocols	Support both the AS2 and AS4 message transport protocol models for access points.
3	4.3	Message envelope	Support both SBDH and XHE envelope technology standards for message exchange while advocating for wide adoption of XHE as the desired long-term approach.
4	4.4.1	Message payload	Use a single semantic model (under development in the Semantic Model Work Group) and the ISO/IEC 19845 - OASIS UBL v2.x syntax for payload messages.
5	4.4.2	Message response	Adopt message responses compatible with those under development in Europe.
6	4.5	Discovery process	Establish a discovery model that allows trading parties and their service providers to connect and operate in a fully interoperable and flexible way based on standard components while maintaining commonly used practices.
7	4.6.1	Identifiers	The identifier system should have three distinct levels: 1) Entity (and sub-entity) Identifier, 2) Electronic Address Identifier, and 3) Electronic Routing Address.
8	4.6.2	Registry approaches	Use a federated registry service using the Domain Name System (DNS) to enable discovery across all access points and participants that choose to use the service.
9	4.6.3	Discovery conditions	Support conditional permission levels for trading party access.
10	4.6.4	Registry standards	Use the OASIS SML and SMP specifications for the registry infrastructure.
11	4.7	Security	Support a variety of security options within a defined set of minimum technical requirements that meet current industry security standards. A governance organization should address legal requirements for e-Delivery network participation and define the technical security standards and protocols that establish an appropriate balance between interoperability and security to promote adoption.
12	4.8	Standards	Base the e-Delivery network on the open standards listed in Table 8.
13	5.1	Proof of concept	The final step for the work group is to conduct a broader validation exercise of the recommendations (Table 10) for an e-Delivery network for the U.S. market.

6.2 Framework Governance Key Considerations

As with the other e-Invoice interoperability frameworks throughout the world, a governance body plays an essential role and would need to be established for the U.S. market. The recommendations within this document are intended for use by the governance body. Additionally, the work group identified the following topics for that body to address. These topics are all addressed within established e-Delivery networks and while this document provides guidance and insights, a governance body should make final implementation determinations for the U.S. market.

Table 11
Framework Governance Key Considerations

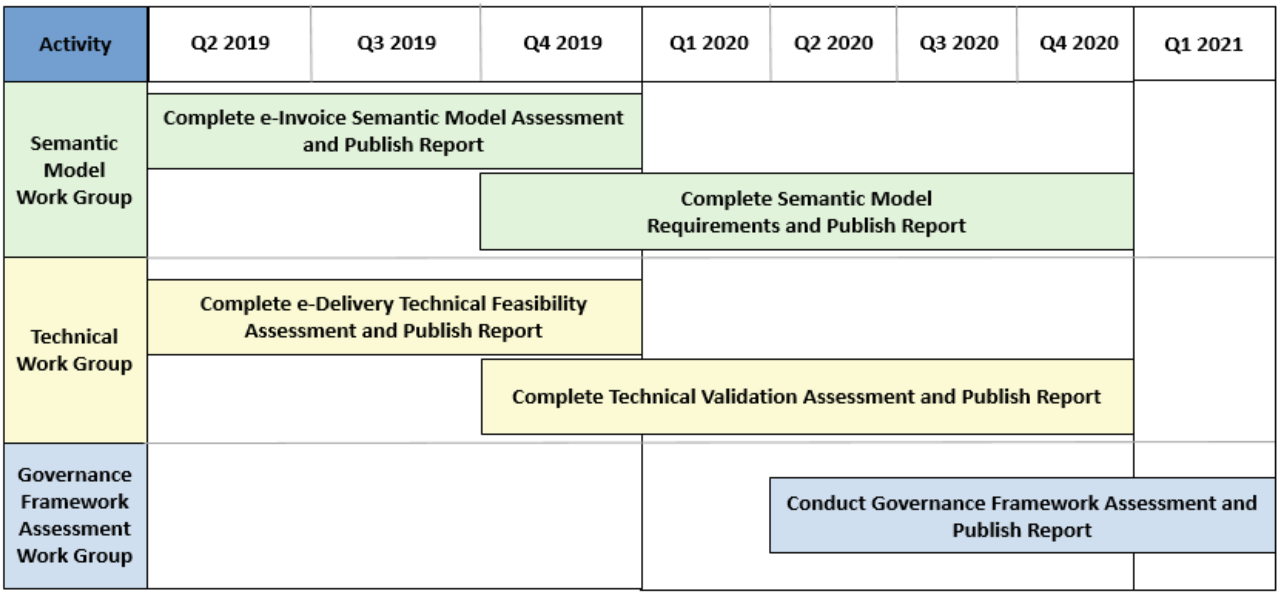
Topic	Key Consideration
Registries	• Determine the degree of technical and governance centralization for the registries. • Conduct further research and industry dialogue to determine elements and considerations of a federated model for owning and updating DNS namespaces. The method for validating trust in such a model is a critical element.
Operations	• Develop standardized legal agreements between various participants in the e-Delivery network. • Finalize and publish operating rules for participants such as handling of documents that fail data validation, do not comply with business rules, or are received from an unrecognized sender.
Access to e-Delivery Network	• Finalize access point identification, vetting, and certification/accreditation. • Establish access point registration process and related controls. • Determine the appropriate permission level and access rights options available and granted to users.
Identifiers	• Establish Identifiers for addressing and routing to support dynamic discovery. • Publish/State clear rules and practices for the use of Entity Identifiers. It is likely that a single legal entity may use multiple identifiers in parallel. • Consider/assess ISO / IEC 6523 standards for identifiers.
Security	• Develop legal agreements to support security considerations. • Determine the appropriate balance between interoperability and security to promote adoption.

6.3 Next Steps

The BPC e-Invoice Technical Feasibility Work Group recommends the following next steps:

- The BPC should initiate a validation test of the requirements for establishing an e-Delivery network. The validation will allow for a rigorous analysis of the recommendations from this report and determine the final technical requirements for an e-Delivery network utilizing a federated registry model (see recommendation 8).
- The BPC should complete the Semantic Model assessment, and develop and publish the U.S. Semantic Model requirements. This assessment report refers to the Semantic Model Work Group and recommends a single Semantic Model and Syntax for the message payload (see recommendation 4).
- The BPC should establish a new work group to assess how interoperability frameworks are governed and their approach to manage the e-Delivery network. This report, the results of the validation test and the Semantic Model requirements are foundational artifacts as inputs for that assessment.
- The BPC will continue to initiate work group efforts and foster industry dialogue to increase e-Invoice adoption in the United States.

Figure 6
Interoperability Framework Initiative Work Group Timelines



Source: Business Payments Coalition

7. Appendices

7.1 Appendix A – Work Group Members

The BPC would like to thank all work group members who contributed to the assessment.

Table 12
Work Group Members

Name	Organization
Ahti Allikas	Opus Capita
Alberto Toledo	ATEB Servicios SA de CV
Bard Langoy	Pagero
Charles Bryant	European E-Invoicing Service Providers Association (EESPA)
Chris Welsh	OFS Portal
Daniel Liesenfeld	Basware
Daniel Sanchez	Indicium Solutions
David Hixon	IBM
Ger Clancy (Chair)	IBM
German Peguero	Edicom Group
Janos Toberling	Partner Hub
Jesus Pastran	ATEB Servicios SA de CV
Jose Luis Ortiz	Indicium Solutions
Kenneth Bengtsson	eFact
Katalin Kauzli	Partner Hub
Liviu Rodean	IBM
Matt Vickers	Xero
Omar Martinez	Factura Facilmente de Mexico SA de CV
Omar Valencia	Ekomercio
Pal Efstrom	Pagero
Peter Malaczko	Partner Hub
Robert Gallo	Edicom
Tim Cole	Causeway Technologies, EESPA
Todd Albers (Convener)	Federal Reserve Bank of Minneapolis
Patti Ritter	Federal Reserve Bank of Minneapolis
Dennis Weddig	Federal Reserve Bank of Minneapolis
Chris Ellingworth	Federal Reserve Bank of Minneapolis
Britta Holland	Federal Reserve Bank of Minneapolis

7.2 Appendix B - Message Transport Protocols

Appendix B contains information on message transport protocols (section 4.2) assessed by the work group in their analysis. This information refers to message delivery, not the content of the invoice itself.

Table 13
Common Messaging Components[32]

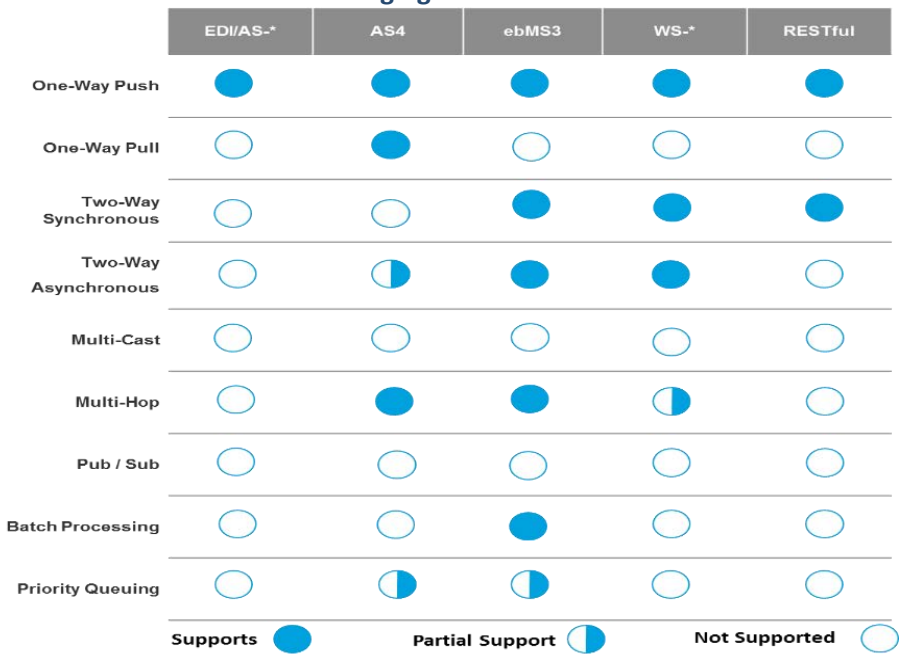
Term	Description	Example
Security	Capabilities to provide data protection	Data needs to be encrypted before placed onto an e-Delivery network
Reliability	Capability guaranteeing delivery to its designated destination	Ensure the document is received by the intended recipient
Ordering	Capability guaranteeing messages are received in the order they were sent	Allows for sequencing of the documents according to the intended order between trading parties
Priority	Capability for the messaging layer to group messages and deliver them in different ways using different resources and order	Allows for messages to be prioritized over other messages (i.e. an express versus regular delivery)
Multi-cast	Capability to send one message to multiple destinations	Allows for sending one message to multiple recipients
Multi-hop	Capability to route a message through intermediary nodes until it reaches its final destination	Allows for messages to move to multiple parts of an organization for processing
Publisher/ Subscription	Capability of sending a message to a number of parties who have subscribed to the topic subject of the message	Allows for a broadcasting of a document to multiple recipients
Non-Repudiation	Capability verifying that a message was sent or received	Helps resolve disputes whether a message was sent or received
Traceability	Capability allows a sender to query and view the current state of a message during posting. Refers only to traceability between corners 2 and 3, not end to end (corner 1 to 4).	Allows for checking the progress of a document during transport to its destination
Batch Processing	Capability of sending a message triggering a batch process on the destination side	Allows for bulk processing of messages at a predetermined time
Large Message	Capability to send a large amount (50 MB) of data	Allows for large documents to be sent

[32] Adapted from *Message Protocols for Enabling Digital Services: A Report for the Australian Government*, June 2015, National ICT Australia Limited CSIRO.

Messaging Patterns Supported by Messaging Protocols

A variety of methods are used to exchange messages. Figure 7 identifies the message protocol that supports each message exchange pattern. The information was used during the assessment to help guide discussions about messaging and messaging protocols.

Figure 7
Messaging Patterns[33]

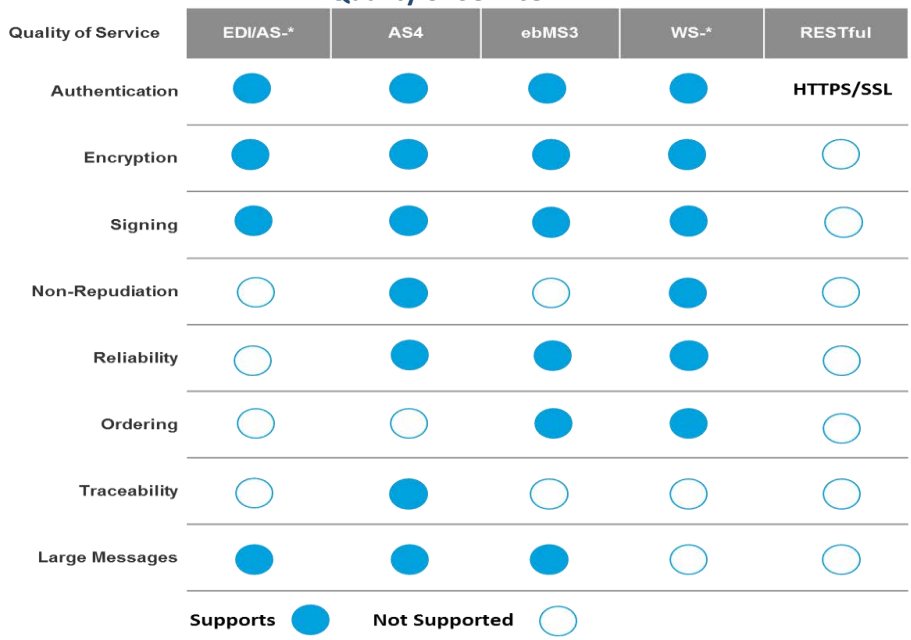


[33] *Adapted from Message Protocols for Enabling Digital Services: A Report for the Australian Government*, June 2015, National ICT Australia Limited CSIRO.

Quality of Services versus Messaging Protocols

Businesses may need different Quality of Service (QoS) in messaging exchange patterns and protocols. For e-Invoicing exchange, authentication, encryption (and decryption), non-repudiation, and the ability to support large messages are important. Figure 8 was used during the assessment to help guide discussions about messaging and message protocols.

Figure 8
Quality of Service[34]



7.3 Appendix C – Comparison of AS2 and AS4 Message Transport Protocols

This appendix compares the AS2 and AS4 message protocols and supports the recommendation in the main document.

Table 14
Comparison of AS2 and AS4[35]

Requirement	AS2	AS4
Interoperability • Message metadata • Multiple deployment models • Message exchange patterns	• Message header data is separate from the protocol • Message exchange patterns supported are one-way inbound and one-way outbound	• Several options to include metadata in message header • Message exchange patterns supported are one-way push, one-way pull, inbound two-

34 *Adapted from Message Protocols for Enabling Digital Services: A Report for the Australian Government*, June 2015, National ICT Australia Limited CSIRO.

35 Digital Business Council – eInvoicing work group materials.

Requirement	AS2	AS4
• API must be document/ message agnostic		way/sync and two-way/push – pull • Functional superset of AS2
Security and Assurance • Security • Transmission integrity • Confidentiality • Non-repudiation of receipt and origin	• Transport layer (SSL /TLS) • X.509 certificates • Confidentiality – MIME Multipart / Encrypted • Non-repudiation of origin – MIME Multipart / Signed • Non-Repudiation of Receipt – Signed Messages Disposition Notification	• Transport layer (SSL/TLS) • X.509 Certificate, Any security token that's part of XML encryption including SAML 2.0 • Confidentiality – WS – Security Encryption • Non-repudiation or origin – WS-Security • Non-repudiation of receipt – Signed Receipt Signal Message
Robustness • Guaranteed once and only once • Large documents • High throughputs • Varying number of access points and nodes	• When Message Delivery Networks are used • AS2 Restart must be used • Implementation specific	• A-Least-Once, At-Most-Once, In-Order delivery • Large documents supported including GZIP • Implementation specific • MultiHop support

7.4 Appendix D – Registries

The Digital Business Council eInvoicing Working Group looked at registries during their assessment (January 2016). The following table summarizes their findings.

Table 15
Comparison of Registries[36]

Capability Lookup	What it is	What is it used for	Advantages	Disadvantages
OASIS BDX Service Metadata Publishing (SMP) and Service Metadata Location (SML)	An open specification that defines the method to retrieve the capability metadata associated with a trading/communication partner within a four-corner network	It is used to discover the interoperability capabilities of a particular trading/communication partner The metadata conveys information such as ability to receive a particular document type over a specific transport, which business processes the document can	Open standard and open source available Could be implemented by any number of providers or access points – does not require centralized infrastructure Supports multiple service definitions per entity and	Every participant must maintain its metadata directly or via a service provider

[36] Digital Business Council – eInvoicing work group materials.

Capability Lookup	What it is	What is it used for	Advantages	Disadvantages
		participate in, and various operational data such as activation and expiration times For recipients that want to use more than one SMP, the metadata may include a redirect for specific document types	promotes a standardized method of publishing Improves interoperability (local and international) Supports a dynamic/metadata driven approach to interoperability including production and test parameters Promotes 'openness' and can be used beyond e-Invoicing	
OASIS ebXML RegRep ebRS with ebRIM	An open standard for software that manages diverse content such as documents, images, services, devices, assets, schemas, WSDL, ontologies, records (medical, justice, immigration, tax, …) Consists of a Repository to manage the content and a Registry to manage the metadata that describes the content (hence the term RegRep)	Generic metadata and content management. It is capable of managing diverse content such as documents, images, services, devices, assets, schemas, WSDL, ontologies, records	Promotes data quality, integrity by enforcing validation rules Supports synchronized replication and federation of data Uses secure federated queries Enforces governance policies defined by Community of Practice Developed as part of the ebXML framework	Because of its generic nature the sophisticated data model requires detailed profiling (technically complex). Relatively low level of adoption – limited sets of tools and experience
Web Service UDDI	The Universal Description, Discovery and Integration protocol	Enables businesses to publish service listings and discover each other, and to define how the services or software applications interact over the Internet	Supports organizational, business classification and web service metadata An OASIS Web Service standard	UDDI has not been as widely adopted as its designers had hoped. IBM, Microsoft, and SAP announced they were closing their public UDDI nodes in January 2006 The OASIS TC responsible for UDDI has also closed

7.5 Appendix E – Global Interoperability Framework

As trade expands globally, U.S. businesses seek to meet the invoicing requirements of their international trading partners. The BPC Framework is an opportunity to align United States requirements with other jurisdictions. The BPC technical and semantic analysis should take into consideration how to support a Global Interoperability Framework (GIF), which is described below:

- The GIF is a neutral vehicle intended to facilitate cross-association collaboration on common issues and, where possible, agree on common documents and artifacts that should be supported on a global or regional basis.
- Three organizations are leading the development of the GIF in the e-Invoicing and supply chain space. ConnectONCE is an established global forum for C-level executives in digital commerce. EESPA, the European E-invoicing Service Providers Association, has fostered a fully interoperable network based on its model agreements. The OpenPEPPOL Association enables multilateral interoperability between trading parties in their procurement and invoicing processes.
- The GIF initiative is timely, as it develops an interoperable ecosystem to support the rollout of public sector e-procurement and e-Invoicing, as required by EU Directive 2014/55/EU.
- The GIF seeks to identify where consensus exists to adopt certain components into the global framework. For example, such components could potentially, over time, include:
    - Data components, covering both semantics and message/payload elements
    - Identifiers and discovery: how companies, services, capabilities and data elements are identified and made accessible to all parties
    - Transmission and delivery
    - Envelope standards
    - Common communication protocols, e.g., response messaging, exchange status, business rules, query handling and rejections
    - Protocols to support interoperability within three- and four-corner exchanges
    - Emerging technology components, such as blockchain, robotics, artificial intelligence, etc.
    - Compliance and security protocols

  As the framework is developed by the BPC Work Groups, it is expected that the stakeholder group will be expanded to ensure relevance to global supply chain communities. The BPC will monitor the development of the GIF and engage directly in it when appropriate.

7.6 Appendix F – Resources Links

Links to more detail about the frameworks assessed are included below.

CEF: Getting Started with eDelivery
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Get+started+eDelivery

ConnectONCE: https://connect-once.com

DBC: The Interoperability Framework http://digitalbusinesscouncil.com.au/interoperability-framework/

EESPA https://eespa.eu/

OASIS Standards https://www.oasis-open.org/standards

OpenPEPPOL e-Delivery Network Specifications https://peppol.eu/downloads/the-peppol-edelivery-network-specifications/

7.7 Appendix G – References

AS4 Profile of ebMS 3.0 Version 1.0, OASIS Standard, January 23, 2013.

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html

Business Document Metadata Service Location Version 1.0, OASIS Standard, August 01, 2017.
http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html

Catalog of Electronic Invoice Technical Standards in the U.S., Business Payments Coalition and Federal Reserve Bank October 2017.

https://fedpaymentsimprovement.org/wp-content/uploads/catalog-electronic-invoice-standards.pdf

CEF Digital Domibus. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

CEF Digital Service Metadata Locator (SML) software.
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+software

CEF Digital Service Metadata Publisher (SMP) software.
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+software

CEF eDelivery Access Point, Component Offering Description: European Commission DIGIT Connecting Europe Facility, September 26, 2018.
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software?preview=/82773366/82798324/(CEFeDelivery).(AccessPoint).(COD).(v1.09).pdf.

Drummond Group B2B MFT Interoperability: Drummond Certified Benefits for Software Vendors.
https://www.drummondgroup.com/interoperability/b2b-mft-interoperability/

eInvoice Interoperability Framework version 1.0: Digital Business Council, July 27, 2016.
http://www.icb.org.au/out/130497/eInvoicing_Interoperability_Report.pdf

Message Protocols for Enabling Digital Services: A Report for the Australian Government, June 2015, National ICT Australia Limited CSIRO.
https://www.sbr.gov.au/sites/g/files/net5641/f/Message-Protocols-for-Enabling-Digital-Government-Services-Final-Report.pdf

The Naming Authority Pointer (NAPTR) DNS Resource Record.
https://tools.ietf.org/html/rfc2915

OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features, Committee Specification 02: OASIS, July 12, 2007.
http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html

OpenPEPPOL Access Point Implementation Guidelines.
http://peppol.eu/downloads/ap-guidelines/

Open PEPPOL Code Lists - Participant identifier schemes v6 draft.xlsx
https://github.com/OpenPEPPOL/documentation/tree/master/Code%20Lists

OpenPEPPOL Test and Onboarding: OpenPEPPOL AISBL, November 26, 2018.
https://peppol.eu/wp-content/uploads/2018/11/PEPPOL-Testbed-and-Onboarding_v1p0.pdf

Overview of an e-Invoice Interoperability Framework, Business Payments Coalition, November 2019
https://businesspaymentscoalition.org/wp-content/uploads/20191031-bpc-overview.pdf

PEPPOL Transport Infrastructure AS4 Profile Version: 1.0: OpenPEPPOL AISBL, August 12, 2017. https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/old/ICT-Transport-AS4_Service_Specification-1.0-2017-12-08.pdf

Service Metadata Publishing (SMP) Version 1.0, OASIS Standard, August 01, 2017.

http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html

Service Metadata Publishing (SMP) Version 2.0, Committee Specification 01, OASIS, May 20, 2019.

https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/bdx-smp-v2.0.html#_Toc9594042

Summary Report from the e-Invoice Interoperability Framework Preliminary Assessment Work Group, Business Payments Coalition, June 2018.

https://fedpaymentsimprovement.org/wp-content/uploads/bpc-e-Invoice-if-assessment-report-june-2018.pdf

Support for the PEPPOL AS4 profile mandatory in the PEPPOL eDelivery Network from 1 February 2020.

https://peppol.eu/support-for-the-peppol-as4-profile-mandatory-in-the-peppol-edelivery-network-from-1-february-2020/

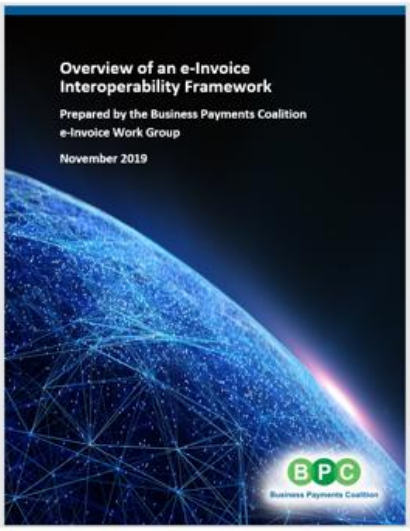
2016 Data Capture and Mailroom Technology Insight Report, PayStream Advisors

U.S. Adoption of Electronic Invoicing: Challenges and Opportunities: Payments, Standards and Outreach Group, Federal Reserve Bank of Minneapolis, June 2016.

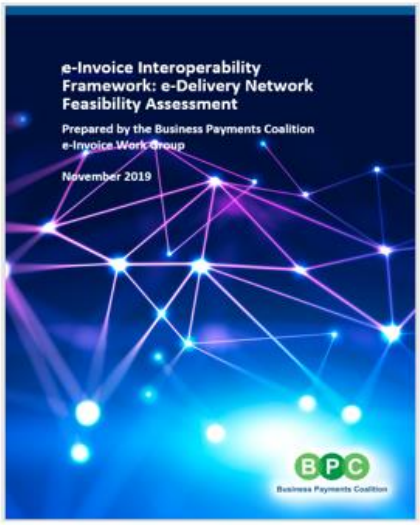
https://fedpaymentsimprovement.org/wp-content/uploads/e-invoicing-white-paper.pdf

7.8 Appendix H – Interoperability Framework Assessment Reports

The *e-Delivery Network Feasibility Assessment* report is the second report as part of a three part series of the Business Payments Coalition e-Invoice Work Group e-Invoice Interoperability Framework assessments.



Overview of an e-Invoice Interoperability Framework



e-Invoice Interoperability Framework: e-Delivery Network Feasibility Assessment

e-Invoice Interoperability Framework: Semantic Model Assessment