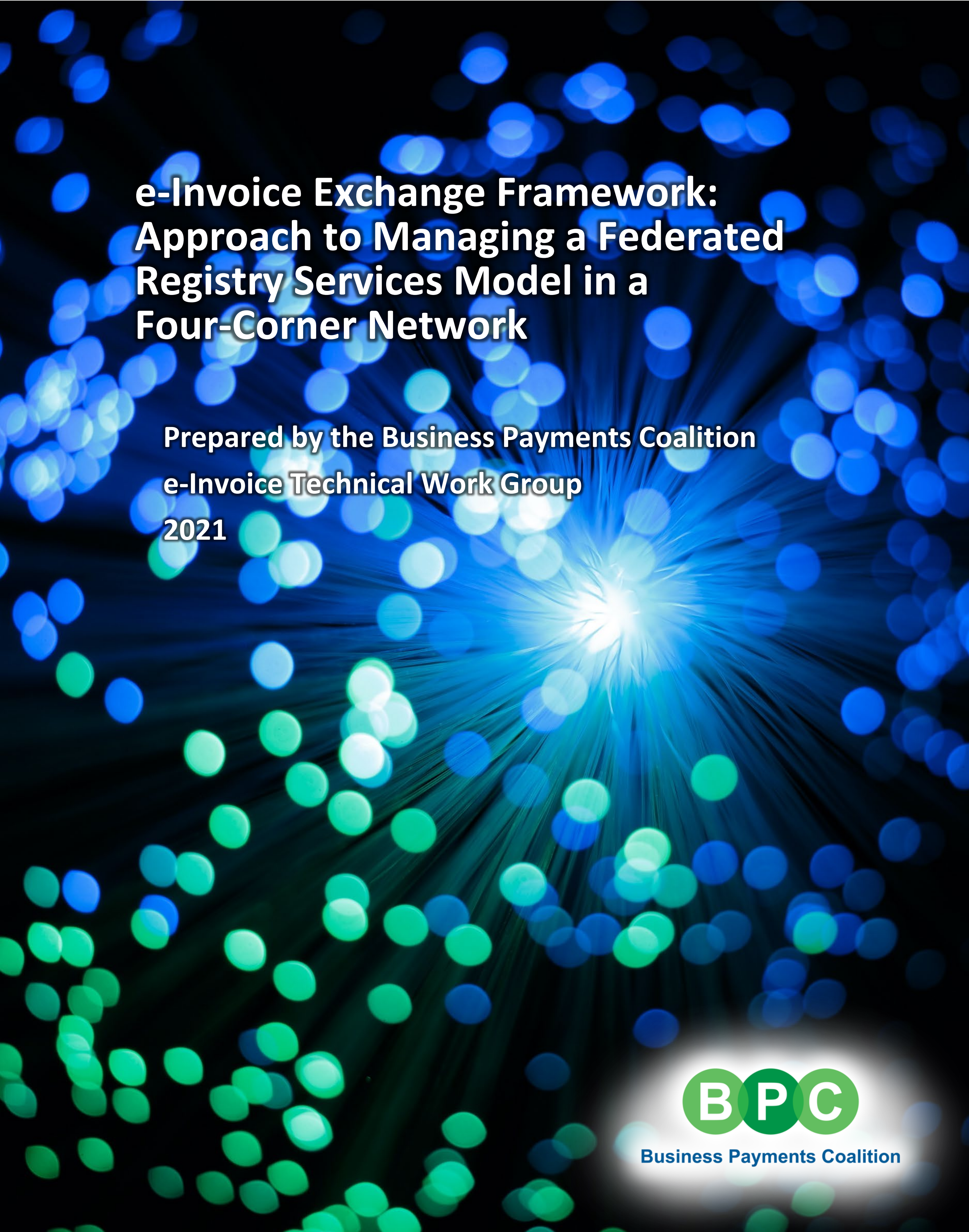


e-Invoice Exchange Framework: Approach to Managing a Federated Registry Services Model in a Four-Corner Network

Prepared by the Business Payments Coalition

e-Invoice Technical Work Group

2021

Business Payments Coalition

Table of Contents

1 Executive Summary

The electronic exchange of invoices (e-Invoices) between businesses requires an approach that reliably identifies where and what to send, in a consistent format, and supports a minimal number of connections to many independent systems and platforms. Multiple markets have implemented e-Invoice exchange frameworks incorporating a set of prescriptive standards which address these hurdles that businesses face.

Current e-Invoice exchange frameworks operating in Europe and elsewhere use a single registry service and central registry service management model. The Business Payments Coalition (BPC) technical feasibility assessment concluded that a federated registry services approach would be required for the U.S. market, and would also provide the foundation to support a North American exchange framework if Mexico and Canada choose to implement an exchange framework for their markets.

The BPC 2019 technical feasibility assessment[1] recommended conducting a proof of concept of a federated registry services model using the Domain Name System (DNS) to enable discovery across multiple e-Invoice exchange frameworks[2]. Federated registries services would address several challenges facing the market, including the lack of a central, federal or state governmental authority to establish and administer a framework or a mandate for Business-to-Business (B2B), Business-to-Government (B2G)[3] and Government-to-Business (G2B) e-invoicing.

A ***federated registry services model*** enables authorized (centralized or decentralized) administrators or registrars to register and onboard participants into the e-Invoice exchange framework. Similar to registering a new email address on email systems, onboarding is possible by entering and storing participant's identification and routing information into any DNS namespace with the Name Authority Pointer (NAPTR) resource record[4], enabling a dynamic discovery process through a specialized textual lookup and redirection function.

The proposed federated registry services, decentrally managed, would operate similar to the e-mail ecosystem. It allows multiple registrars to register participants within the e-Invoice exchange framework.

[1] e-Invoice Interoperability Framework – e-Delivery Network Feasibility Assessment Report (PDF) (businesspaymentscoalition.org)

[2] The e-Invoice exchange framework replaced the e-Invoice interoperability framework name in 2020.

[3] The Office of Management and Budget (OMB) of the Executive Branch of the U.S. Federal Government has issued several memorandums providing instructions to agencies that fall under the CFO Act of 1991 to support "e-Invoices". However, the memorandums fail to define what a "e-invoice" is.

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

A **decentralized registry services management model** utilizes multiple registry services (e.g. federated registry services) managed by separate authorities.

A **centralized registry service management model** is a single registry service usually managed by a single authority.

The multiple registry services architecture, although a tried and true technology, has not been implemented within the context of existing e-Invoice exchange frameworks and is a fundamental building block to facilitating global interoperability. To validate it and the discovery function of the proposed e-Invoice exchange framework for the U.S., the BPC successfully performed a proof of concept (POC) by building the functional components required for an operational federated registry services. Once built, a series of tests were performed that validated the proposed architectural approach and operational model recommended for the U.S. e-Invoice exchange framework. This report outlines the approach, observations, results, and recommendations from the validation exercise.

1.1 Registry Background

A **registry** contains technical information about identifiers that encapsulates the legal or entity identifier, location, and routing instructions of participants in the network. In a four-corner network model[5] used within exchange frameworks, it provides *technical interoperability* and allows access providers in corners 2 and 3 to dynamically discover each other and create the necessary connections for secure message delivery.

Registries can be managed either by single or multiple authorities. Current exchange frameworks such as those in Europe, use a centralized registry management model where a ***central registry service*** is managed by a single authority. In contrast, ***federated registry services*** are managed by multiple authorities in a decentralized manner; a new concept for registry management for e-Invoice exchange frameworks. Whether central or federated, both registry services models require participants to conform to a common set of rules, standards, and governing principles for the framework.

Given that this concept is new within the e-invoice space, the BPC conducted a validation exercise to gain an understanding of the technical components required for establishing federated registry services and the potential impacts to the dynamic discovery function used by existing frameworks.

The POC scope performed a specific validation exercise within a limited scale environment comprising of six access points, three service metadata publishers (SMP), and two Service Metadata Location (SML)[6] services, representing the federated registry and management by separate authorities. The SML services maintained a registry under a single DNS, so that the sending Access Point needed only to perform a single query in order to locate the appropriate SMP. This SML services configuration facilitated participants to register through any SML service provider without impacting discovery across the network.

[5] Further definition of a four-corner network model can be found in section 2.1.
[6] Two additional SMLs were developed and tested outside of the validation exercise network. This test used a different approach towards federating the registries, where each registry was created under a DNS subdomain structure managed by a single authority. Further description and the results of the test is described in Appendix B.

The POC successfully demonstrated a path forward for creating an e-Invoice exchange framework with a federated registry services model leveraging a single DNS namespace with the NAPTR resource records. Furthermore, the approach taken for building the federated registry services did not impact the dynamic discovery function that is critical for building a technical bridge across multiple frameworks to deliver and receive messages and e-Invoices.

The observations, results and recommendations from the validation exercise include:

1) Dynamic discovery of end points can be achieved utilizing federated registry services architecture and existing registry and discovery standards[7],[8]. The minimum viable functional components built for the validation exercise proved and support the notion that it is ***technically*** viable to establish and manage a decentralized registry (Section 5.1).
2) The current OASIS BDXL (SML services) standard supports the concept of decentralized management of a federated registry services model under a single DNS structure (Section 5.1). It is recommended that a change to the standard should be proposed for establishing a method of securing participant entries to their specific SML Services provider.
3) Existing open-source tools supporting the implementation of e-Invoice exchange framework access points are lacking necessary instructions and best practices, are challenging to implement, and do not leverage current software development and deployment practices. The industry would benefit from enhanced common tools that significantly decrease the development time and cost for adoption as well as aid a future in-market pilot participation. The BPC technical work group will initiate an effort in 2021 to enhance the open-source tools to address these needs. (Section 4.4).
4) The work group identified the need for a common, standardized configuration of the processing mode (P-Mode)[9] parameters for a four-corner network. The P-Mode parameter configurations of the ebMS3/AS4 message transport protocol differ between existing exchange frameworks. It is essential for exchange frameworks to align at the message transport level to achieve interoperability. (Section 5.2)
5) A common approach to certificate management will need to be determined between the registration authorities. The POC validation exercise used a simple certificate management process for Private Key Infrastructure (PKI) support. A robust certificate management process will need to be determined for the network. The current e-Invoice frameworks utilize a central authority for issuing certificates. A central authority issuer may not be possible in a federated registry services model (Section 4.3)

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 or to join, visit the website at https://businesspaymentscoalition.org/

[7] *Business Document Metadata Service Location (BDXL) Version 1.0 OASIS standard, 01 August 2017* http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html,

[8] *Service Metadata Publishing (SMP) Version 2.0, OASIS Committee Specification 02, 16 January 2020.* https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/bdx-smp-v2.0.html

[9] Processing mode (P-Mode) is a structured set of parameters that determine how messages are exchanged. Aspects covered by the P-Mode include security, reliability, transmission mode, error handling and the use of AS4 advance features.

1.2 Audience

This 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.

1.3 Disclaimers, Copyright and Acknowledgments

Views expressed here are not necessarily those of, and should not be attributed to, any particular BPC 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.

This report is the work product of the BPC, and 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 expertise, dedication, and contributions of the e-Invoice Technical Assessment Work Group. Without their involvement, the validation exercise would not have been possible.

2 Background

For several years now[10], the BPC has facilitated discussions and collaboration with the industry to achieve widespread adoption of e-Invoicing for the U.S. This led the BPC to identify and assess several e-Invoice exchange frameworks from other parts of the world for potential options to address the significant inefficiencies that exist between businesses within the U.S. for exchanging electronic payment information, such as invoices and remittance data. In 2019, the BPC published several assessment papers, including an e-Invoice Interoperability Framework – e-Delivery Network Feasibility Assessment Report. The core recommendation from the report:

> The U.S. should proceed with establishing an e-Invoice exchange framework modeled after existing frameworks with one primary difference of leveraging a federated registry services model using the Domain Name System (DNS) to enable discovery across all participants within the e-Invoice exchange framework. The BPC concluded that a federated registry services approach addresses several challenges facing the market, including the lack of a central, federal or state governmental authority to establish and administer a framework or a mandate for Business-to-Business (B2B) or Business-to-Government (B2G)[11] e-invoicing.

[10] A complete list of the BPC and Federal Reserve e-invoice publications can be found in Appendix G.

[11] The Office of Management and Budget (OMB) of the Executive Branch of the U.S. Federal Government has issued several memorandums providing instructions to agencies that fall under the CFO Act of 1991 to support "e-Invoices". However, the memorandums fail to define what a "e-invoice" is.

The BPC Technical Work Group further recommended performing a POC validation test of federated registry services supporting network participants through the internet DNS addressing scheme. In collaboration with BPC members, the federated registry environment was established between ten entities creating the network, and exercises conducted in the fall of 2020.

2.1 The e-Invoice Exchange Framework

An e-Invoice exchange framework addresses the complexity and inefficiency associated with multiple connections through portals, point-to-point, and three-party networks. The exchange framework is modeled after CEF, OpenPeppol, and EESPA which have successfully addressed the connection issues through a set of interoperable exchange standards. The exchange framework approach significantly lowers the cost and technical barriers for businesses to connect to send and receive e-Invoices.

This exchange framework model helps increase broad e-Invoice support by simplifying the implementation, maximizing business endpoint reach through a single connection that allows connecting with many, and increasing affordability for small and medium-size businesses (SMBs).

The e-Invoice exchange framework is based on a four-corner network model that defines the technical, business, and legal requirements to achieve interoperability[12] between invoice senders and receivers using disparate service providers and 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 or network (as in a three-corner model network[13]), but many will be directed to other platforms used by other receivers. Under interoperability agreements, two service providers become access points and connect to each other and transmit or accept invoices on behalf of their customers. A four-corner network model is complimentary to existing connection models and will co-exist within the exchange framework.

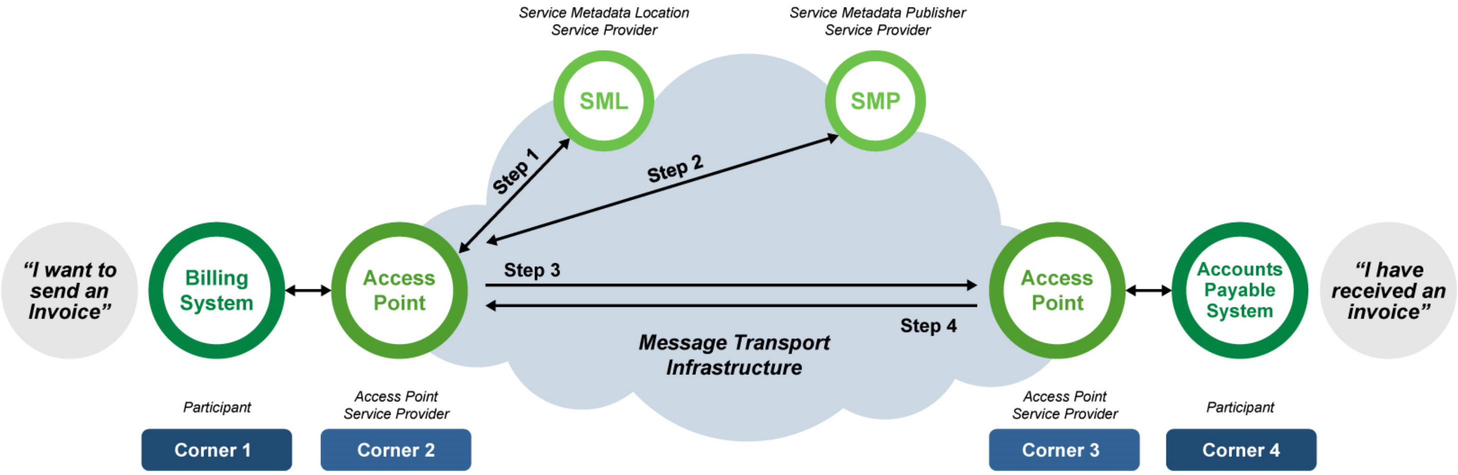
The four-corner network model depicted in Figure 1 delivers the essential exchange framework architecture for pervasive reach for all parties. Each corner in the model represents the following:

- Corner 1 (C1) = Sender
- Corner 2 (C2) = Sender’s access point
- Corner 3 (C3) = Receiver’s access point
- Corner 4 (C4) = Receiver

[12] For more information on the interoperability requirements can be found at Overview of an e-Invoice Interoperability Framework (PDF)

[13] 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.

Figure 1
The Four-Corner Model of an e-Delivery Network[14]


Service Metadata Location Service Provider
Service Metadata Publisher Service Provider
SML
SMP
Step 1
Step 2
"I want to send an Invoice"
Billing System
Access Point
Step 3
Access Point
Accounts Payable System
"I have received an invoice"
Step 4
Message Transport Infrastructure
Participant
Access Point Service Provider
Access Point Service Provider
Participant
Corner 1
Corner 2
Corner 3
Corner 4

The rules and interoperability requirements for a successful framework predominantly focus on the connections between access point providers in C2 and C3. The connections between trading parties and the access points (C1 to C2 and C3 to C4) are outside the scope of the framework and under the control of the access points and their C1 and C4 clients. This helps preserve existing relationships and facilitates access point service providers to deliver additional value-added services to their clients (C1 and C4). A detailed description of end-to-end e-Invoice exchange in a four-corner model can be found in section 5.2.[15]

2.2 2019 Proof of Concept (POC) for e-Delivery Network Technology Concept

During the 2019 technical feasibility assessment, the BPC created a simple, yet functional, representation of a typical e-Delivery network. The purpose was to explore the level of complexity associated with developing critical network components and to gain insight into concepts associated with:

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

Testing involved emulating an access point using registry location (SML service) and meta-data (SMP) service providers to register their C1 and C4 clients and the execution of basic discovery processes allowing for testing the flow of messages. The client integration layer between C1 and C2 or C3 and C4 were not extensively emulated. The test provided a necessary steppingstone for defining and proceeding with a POC validation exercise for extensive functionality and features associated with a federated registry services model.

[14] Adapted from the e-Invoice Interoperability Framework, Digital Business Council, Version 1.0, July 27, 2016.
[15] Additional e-Invoicing background information can be found in the BPC and Federal Reserve Bank publications in Appendix G.

2.3 Terms, Definitions and Standards

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

Access Point: An Access Point (AP) is a network service that facilitates the sending and receiving of business documents on behalf of a network participant. The AP of the participant initiating the exchange is referred to as the Corner 2, while the AP of the receiving Participant is referred to as the Corner 3 of the document exchange.

Access Point 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. In the e-Delivery network, they may provide Access Point or Service Metadata Publisher services.

AS4 Profile of ebMS 3.0: Applicability Statement 4 profile of ebXML Messaging Service (ebMS[16]) - Using ebMS 3.0 as a base, this profile is a subset of functionality defined along with implementation guidelines adopted based on basic design principles and AS2 functional requirements to trim down ebMS 3.0 into a more simplified and AS2-like specification for Web Services B2B messaging.

Business Document Exchange Location (BDXL): The OASIS Business Document Exchange (BDXR) Technical Committee[17] created the Business Document Metadata Service Location (BDXL) Version 1.0 specification[18] as a way to define a standardized implementation of an SML service.

Centralized Registry Management Model: A single registry service usually managed by a single authority.

Decentralized Registry Management Model: A network utilizing multiple registry services (e.g. federated registry services) managed by separate authorities.

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.

Participant Discovery: The process used to discover (i.e. look-up) the digital location and capabilities of a Participant, where and how to send an invoice and/or other message. This includes registry services and other decentralized discovery mechanisms.

Domain Name System (DNS): An interoperable, distributed, and accessible network technology used as the core method to discover resources on the internet.

e-Delivery Network: Refers to the components of the technical interoperability layer to deliver documents electronically across the Internet. e-Invoices are just one of the many documents for which the e-Delivery network can be used.

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

[16] *AS4 Profile of ebMS 3.0 Version 1.0, OASIS Standard, 23 January 2013.* http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html

[17] *OASIS Business Document Exchange (BDXR) TC.* https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=bdxr

[18] *Business Document Metadata Service Location (BDXL) Version 1.0 OASIS standard, 01 August 2017* http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html

Electronic Invoice (e-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.

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

Federated Registry Services: A structure that enables non-affiliated providers to independently administer participants who can then access a shared Registry.

Four-corner Network Model: An established networking model that connects four parties to deliver electronic documents and messages: the sender (C1), the sender's access point (C2), the receiver's access point (C3) and the receiver (C4).

Global Interoperability Framework (GIF): An approach created by Peppol, EESPA, ConnectOnce, and the BPC on a set of recommended practices, policies, and standards for the operation of any four-corner e-Invoice network model organized within a collaborative governance framework wishing to be GIF compliant[19].

ISO/IEC 19845 - OASIS UBL v2.x: Defines a generic interchange format for business documents that can be restricted or extended to meet the requirements of specific industries.

Message Acknowledgement:

Transport Layer Response (TLR): (protocol level) Formal acknowledgement of receipt of a message without validating the payload.

> **Application Layer Response (ALR) (aka: Data Layer Response (DLR), Message Layer Response (MLR))**: Technical acknowledgement from the data integrity check confirming that the message payload received conforms to the syntax, usually asynchronously initiated by the original receiver. It is defined by the semantic model and focuses on data validation and integrity of the received invoice specific to the semantic data model for that transaction type.
>
> **Business Layer Response (BLR)**: Response provided by C4 upon receipt of the invoice and may include payment, agreement to pay, pricing and other transaction specific issues; usually asynchronously initiated by the original receiver.

Message Envelope: A technical 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.

[19] Global Interoperability Framework (GIF), On route to Global Interoperability, The GIF Group. http://gifworks.io/

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.

OpenPeppol: A non-profit international association under Belgian law and consists of both public sector and private members. The association has assumed full responsibility for the development and maintenance of the Peppol specifications, building blocks and its services and implementation across Europe[20].

Participant (Business Participant): An entity, typically a business or government, which sends and/or receives invoices. In a four-corner model network Corner 1 (C1) and Corner 4 (C4) are both participants.

Participant 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.

Registrar: An official, or organization, responsible for keeping and managing participant registrations in a network.

Registry: The complete collection of participants registered in the e-Delivery network, identified by their participant identifiers.

Registry (Registration) Services: A service that enables the processes and mechanisms of enacting changes to the Registry.

Service Metadata Location (SML) Service: A registry service that facilitates the participant discovery by enabling Access Points to locate the Service Metadata Publisher (SMP) Service associated with a Participant in a four-corner e-Invoice network.

Service Metadata Location (SML): The Service Metadata Location (SML) facilitates the discovery of Participants in a network by providing a standardized interface for looking up the associated Service Metadata Publisher (SMP) of a given Participant. Using only an unambiguous identifier of the Participant, the SML resolves the network address of the Participant's associated SMP service. The SML service is therefore only required when a network comprises multiple SMP services where it is used in the first step of the network discovery process when sending a business document through the network.

Service Metadata Publisher (SMP) Service: A Service Metadata Publisher (SMP) service exposes metadata about the capabilities of a Participant in the network. Metadata includes information about business document types and formats that the Participant is capable of receiving, business processes supported or implemented by the Participant, what information the Participant expects to receive within a certain business document, as well as information about the technical endpoint(s) and transport protocol(s) where the Participant will receive business documents.

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. In the e-Delivery network, they may provide Access Point or Service Metadata Publisher services.

[20] OpenPEPPOL
https://peppol.eu/about-openpeppol

Single Top-Level Domain: Top level Domain scheme for all participants in certain Registry models that utilizes DNS. An example Federated Registry Services model would utilize this design through use of Dynamic DNS Updates (or similar capabilities) allowing multiple SML Services providers making changes on the same registry. Alternatively, a Central Registry Service model could use the Single Top-Level Domain without the need of technology allowing multiple providers making changes.

SOAP (Simple Object Access Protocol): A specific type of design model used as a programmatic interface with a defined request-response message system that relies on XML as well as uses HTTP/HTTPS as its transport layer.

Standards Oversight Body: The standards oversight body referred to in the paper is a proposed group or groups that will be responsible for oversight of e-Invoice exchange framework standards.

Universal Business Language (**UBL):** An open library of standard electronic XML business documents for procurement and transportation such as purchase order, invoices, transport logistics and waybills.

Exchange Header Envelope (XHE): The Exchange Header Envelope (XHE) is a 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 network model.

3 Approach

This section provides an overview of the guiding principles, scope and processes used for the 2020 validation exercise.

3.1 Guiding Principles

The following guiding principles were used to determine whether the technical specifications, tools, models, standards, and practices could be utilized to support management of a decentralized electronic invoicing Federated Registry Services model:

1) Involve a broad cross-section of industry stakeholders to validate the technical requirements and specifications through a functional network with several registry services managed in a decentralized manner.
2) Leverage readily available open-source software; transparent and open, non-proprietary technical specifications, and standards.
3) Use exchange framework components that meet current market capabilities, are successfully implemented in another country, and actively drive adoption.
4) Uses standards that are open, royalty-free and vendor-agnostic. The standards should not require a singular platform or solution for electronic business document exchange, but rather support a federated network of access points and service providers.

3.2 Scope

The scope of the POC included testing and gaining experience with available standards and open source software that is already used by existing exchange frameworks, as well as, to gauge the level of complexity to implement the Access Point, SMP, and federated registry service (i.e. SML services) components of the e-Delivery network.

Based on recommendations in the 2019 report and considering industry and standards developments since publication, the BPC identified the following POC objectives for the validation exercise:

- Determine an approach to federated registry services to support e-invoicing
- Review the current discovery process and determine the best path forward within the current standards used by existing exchange frameworks
- Ensure security is maintained with standard security practices and methodology
- Assess message enveloping technology and payload capabilities

3.3 Process

The BPC Technical Work Group conducted research and collaborated closely on requirements to prepare the test environment. The work group utilized various collaboration tools to facilitate dialogue, coordinate the development of the components for the framework, and to conduct and complete testing. Leveraging various collaboration tools significantly helped further the development of the necessary functional exchange framework components, including portions of access points, SMPs, and SML services to test the federated registry services concept.

4 Validation Exercise Set-up

To prepare for the validation exercise, the work group identified the initial critical configuration components for the environment. The research and discussion included analyzing different approaches to a federated registry services model, architecture, standards, and software. The following section details the research, selection criteria and determinations made to set-up the validation exercise.

4.1 Approaches to a Federated Registry Service

To meet the recommendation from the feasibility assessment, the BPC considered four approaches for creating a federated registry services model. The attributes evaluated against the guiding principles[21] for the different approaches included relative complexity, cost to implement, support from existing standards, maturity of the technology, support towards federated ownership, adherence to common standards, and risk of fraudulent updates and entries. The results of the evaluation are found in Table 2. Detailed diagrams of the other three registry approaches can be found in Appendix D.

[21] See 3.1 Guiding Principles

Table 1
Approaches to Federated Registry Services Model

Approaches	Description
Multiple domains	Each SML service provider, or registrar, utilizes their own Domain Name. SML service providers would either replicate their participant entries between each other's domain, or a new discovery model would be required. Similar to internet email, the email address contains the routing information (the "@domain.com") used for locating the email server of the intended receiver. This is not the case with business identifiers (e.g. GLN, DUNS, tax IDs), which only consist of a sequence of numbers and/or letters. To fully replicate the behavior of email, existing business identifier formats would have to be redefined.
Single top-level domain with sub-domains	Each SML service provider has a sub-domain underneath a single top-level domain. Replication is not used between registries. However, the discovery model may need to be adjusted to support this option. In one design of this model, which minimizes discovery changes, each SML service has jurisdiction over a group of participant identifiers. For example, participants using DUNS numbers would be registered in the Dun & Bradstreet SML service, participants using GLN numbers as identifiers would be registered in the GS1 SML service, etc. No known networks are currently using this model. However, at least one European network is contemplating this model to allow the registration authority in each participating country with jurisdiction over network participants.
Single top-level domain (decentralized)	Top level Domain scheme for all participants. SML services would utilize Dynamic DNS Update to provide changes initiated by decentralized custom software used by each SML as the management interface for registry. This enables federated registry services as defined earlier, that is, a service with the same technical information as a central registry but with separate registry services managed by multiple authorities in a decentralized manner. In this model, individual participants may choose which SML service provider to register with. Additionally, participant identifiers can be ported from one SML service to another allowing participants to switch to a different SML service while maintaining their original identity in the network which promotes competition between SML service providers. Similarly, a company or individual may buy a phone service with a phone number and later switch to a competing phone service while maintaining their phone number.
Blockchain	Some form of distributed ledger, or other blockchain type, (e.g. Ethereum) used as the registry of participants. Blockchain technology is currently used mostly to track changes and ownership of network assets. No known networks are using blockchain as a registry of network entities.

Table 2
Approach Considerations for Federated Registry Services POC

Approach Considerations	Multiple Domains	Single top-level with sub-domains	Single top-level domain decentralized	Blockchain
Implementation and validation exercise test complexity	○	◐	●	○
Supports existing discovery mechanisms	○	◐	●	○
Relative (to each other) implementation cost	◐	◐	●	○
Relative operating cost	◐	●	●	○
Relative complexity for participant to change registry service provider	○	○	◐	n/a
Maturity of technology	●	●	●	○
Relative complexity to prevent fraudulent registry updates	◐	◐	●	●
Support for federated ownership of registry	●	○	●	●
Adherence to common accepted standards	●	●	●	○
Relative scalability concerns	◐	●	●	○

LEGEND:

● Met the guiding principles ◐ Partially met the guiding principles ○ Did not meet the guiding principles

Source: Business Payments Coalition

Based on the assessment, the work group determined to proceed with the single top-level domain (decentralized) Figure 2 for testing federated registry services managed in a decentralized manner. This approach allowed for a straightforward implementation and low level of complexity for establishing the federated registry services. Additionally, this approach:

- Supports current out of the box discovery mechanisms supported by the OASIS BDXR standards
- Involves the least amount of complexity for participants to change registry service providers
- Supports a single top-level domain of federated registry services; a key approach consideration.

4.1.1 Rationale

When considering the four options for the POC, the sub-domain and multi-domain models would have required changes to the discovery standards in order to find participants in the network. As the number of registry (SML services) providers increases, the multi-domain model poses scalability concerns, and depending on the discovery model, it could add a significant amount of latency into the participant discovery process. Finally, these models also require the implementation of complex business rules to change SML service providers.

Blockchain natively supports federated control and ownership better than any of the other options. Most notably, a participant changing SML service providers becomes a non-issue, as each participant gets a record in the blockchain without reference to a specific owner other than the participant itself. However, significant challenges with industry maturity, potential impact to the discovery model, lack of established standards, along with scalability concerns, make it clear that Blockchain is not an option at this time. It has potential as a future solution for registry management and should be reevaluated as the technology matures.

Additionally, an independent test[22] of a federated approach to registration services was conducted using subdirectories with DNS Zone delegation as a method to 'federate' Registration Services in a single e-invoicing network. The test concluded that as long as each Registry Service Operator only updates the Registry that is delegated to them, then the solution is secure. However further work regarding security would need to take place to allow one Registry Service Operator to update records in a Registry operated by another Registry Service Operator.

[22] Intech Solutions performed the test using a proprietary registry software tool. www.intechsolutions.com.au

4.2 POC Architecture and Standards

The following table outlines the baseline architecture and standards used to conduct the POC. Included are the e-Delivery network components and corresponding recommendations from the 2019 Technical Feasibility Assessment report, along with the approach taken for the validation exercise and rationale for use of the selected architecture and standards.

Table 3
Architecture and Standards

Component	Technical Feasibility Assessment Recommendation	Validation Exercise Approach	Rationale
Overall Architecture	Base the overall architecture of the e-Invoice exchange framework on a four-corner network model.	The assessment implemented the recommended four-corner network.	The four-corner network model supports an open framework. Three party networks are proprietary and do not provide the opportunity for ubiquitous access and scale that a four-corner model enables. In addition, three and four corner network models can co-exist in a complementary manner.
Message Transport Protocols	Support both the AS2 and AS4 message transport protocol models for access points.	AS4[23] was the default message transport protocol of the software used for validation testing.	AS4 provides additional logging, metadata, and header capabilities. Access Point providers using AS4 can also support AS2 and will likely need to support both protocols for backward compatibility for some timeframe for their clients.
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.	An XHE[24] formed document was included in the testing.	XHE is the most current envelope standard and is designed to hold or contain a digitally signed or encrypted payload fit within AS4. XHE supersedes SBDH and is currently the only envelope technology standard available that provides end-to-end envelope technology to support a four-corner network model.
Envelope Payload	Use a single semantic model (under development in the Semantic Model Work Group) and the ISO/IEC 19845 - OASIS UBL v2.x	A well-formed XML schema was implemented that meets minimum requirements of OASIS	The actual payload was not tested; therefore, only the minimum OASIS UBL standard was necessary.

[23] *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
[24] *OASIS Exchange Header Envelope (XHE) Version 1.0, Committee Specification 03, 13 December 2020* https://docs.oasis-open.org/bdxr/xhe/v1.0/xhe-v1.0-oasis.html

Component	Technical Feasibility Assessment Recommendation	Validation Exercise Approach	Rationale
	syntax for payload messages.	UBL[25] syntax. Payload requirements were not defined for the validation exercise thus making them agnostic to the envelope content.	
Message Acknowledgements	Adopt message responses compatible with those under development in Europe.	The validation exercise tested only transport layer responses (non-repudiation) to confirm message receipt.	Transport Layer Response was utilized to provide verification for sending of messages. Validity of the payload (i.e. invoice) was not within scope of the POC test.
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.	The discovery model implemented the BDXL 1.0[26] and SMP Standard 2.0[27] while working within federated registry services.	OASIS standards are the most universal in the electronic document exchange space and widely incorporated in e-procurement systems globally. BDXL is an established standard for the four-corner network model. While SMP 2.0 is relatively new, it provides several advantages over SMP 1.0[28].
Identifiers	The identifier system should have three distinct levels: 1. Entity (and sub-entity) Identifier, 2. Electronic Address Identifier, and 3. Electronic Routing Address	The OASIS ebCore Party Id Type Technical Specification Version 1.0[29] was implemented.	• The EbCore Party Id Type is an OASIS standard and is the standard recommended by CEF. Also, it has been identified as the standard to be used by EESPA and recommended in the GIF as the Party ID Type. • The electronic address identifier approach is used by CEF.

[25] *OASIS Universal Business Language (UBL) TC.* https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl

[26] *OASIS Business Document Metadata Service Location Version 1.0, OASIS Standard, 01 August 2017.* https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl

[27] *Service Metadata Publishing (SMP) Version 2.0, OASIS Committee Specification 02, 16 January 2020.* https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/bdx-smp-v2.0.html. Advantages of SMP 2.0 include: The previous static XML data model has been refactored to be more flexible and modular, so as to support a wider range of business scenarios. In the refactoring of the data model we have introduced new features, such as the inclusion of participant roles and the support of multiple certificates; the XML data model is now building on the UN/CEFACT Core Component Technical Specification ([CCTS]) to align with other XML implementations and to make implementation easier by reusing existing building blocks; the extension model has been improved to align with other OASIS work products.

[28] *Service Metadata Publishing (SMP) Version 1.0, OASIS Standard, 01 August 2017.* http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html

[29] *OASIS ebCore Party Id Type Technical Specification Version 1.0, Committee Specification 01, 28 September 2010.* http://docs.oasis-open.org/ebcore/PartyIdType/v1.0/CS01/PartyIdType-1.0.html

Component	Technical Feasibility Assessment Recommendation	Validation Exercise Approach	Rationale
Registry Approaches	Use federated registry services using the Domain Name System (DNS) to enable discovery across all access points and participants that choose to use the service.	Two SML services were developed using OASIS BDXL specification to provide edits to records in a single registry utilizing 'DNS Update" (nsupdate) to manage the changes to DNS.	• Provides a participant lookup mechanism. • Adds a level of security by obfuscation with non-reversible hashing of participant ids. • Provided the ability to maintain current discovery mechanisms used by access points. • DNS is a mature known scalable technology and an accepted standard used for many applications.
Discovery Conditions	Support conditional permission levels for trading party access.	This was not in scope.	This is not a network requirement and didn't fit into the validation exercise at this time.
Registry standards	Use the OASIS BDXL and SMP specifications for the registry infrastructure.	The test incorporated the Business Document Metadata Service Location (BDXL) Version 1.0, Service Metadata Publishing (SMP) v 2.0, OASIS ebCore Party Id Type Technical Specification Version 1.0	These are the most current versions of accepted industry standards designed specifically to support a four-corner network model.
Security	Support a variety of security options within a defined set of minimum technical requirements that meet current industry security standards. A standards oversight body 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.	The test incorporated the security measures outlined in Table 4.	A minimum security standard required for the exchange framework was incorporated into the test and did not include message encryption.

4.3 Security

The following table outlines the security measures implemented to support the DNS architecture, discovery and message transport for the validation exercise which conformed to the minimum-security requirements to conduct the test. The work group did not attempt to adhere to production-level security requirements. The security requirements between C2 and C3 within the four-corner network should be further defined as a next step.

Table 4
Security Overview

Component	Security Approach	Observations
DNS Architecture	SML services DNSUPDATEs used Tsig Shared Secret, rfc 2845[30]	● rfc2845 was used because testing DNS security was not a primary objective for the validation exercise**.** This specification offers a shared secret methodology of securing dynamic DNS updates, called Tsig, which is used to sign and authorize updates. It supports use of multiple keygen techniques including the common standard of hmac-sha256. ● Alternatively, rfc 2137[31] outlines a method to secure Dynamic DNS Updates using public key cryptography. However, it was not used given that it is computationally expensive and complex to setup, especially across multiple providers. ● Either implementation will work for a production environment, with rfc 2137 being more secure than 2845, but at a cost of greater complexity. Both should be reviewed to weigh pros and cons. ● Additionally, 2137 and 2845 address security preventing outside entities from making changes to the registry. However, these do not prevent registry service providers from accidental/unauthorized changes to the DNS registry. See 6.1 Recommendations, #18.

[30] *Internet Engineering Task Force (ITEF), Secret Key Transaction Authentication for DNS (TSIG), May 2000.* https://tools.ietf.org/html/rfc2845
[31] *Internet Engineering Task Force (ITEF), Secure Domain Name System Dynamic Update, April 1997.* https://tools.ietf.org/html/rfc2137

Discovery/Message	XMLDsig used for signing the SMP XML files	• This method stems from a W3C Recommendation[32] that provides a standard set of XML syntax to support signing of XML documents using public/private key pairs. There are no real options outside of moving away from XML based syntax which would then not meet SMP standards.
Message	SSL/TLS used for communication between APs and SMPs	• Secure communications between two points across any network is a staple of standard communications, even more so across the internet. SSL/TLS is accepted standard methodology for use with a wide range of options and standards to meet most requirements.
	Enabled and used non-repudiation	• Non-repudiation is a functionality of the AS4 protocol and is a common requirement for business transactions to acknowledge that documents have been received.
	Enabled AS4 signing of messages	• Built in AS4 message signing functionality was used to ensure compatibility with other AS4 implementations that follow standards.
	Central Certificate Authority (CA)	• A central CA was used only for purposes of reducing complexity of the validation exercise. For production implementations, it is recommended that options for multiple CAs be reviewed to ensure there is no single authority controlling certificate issuance.
	Implemented private Public Key Infrastructure (PKI) for creating and issuing certificates	• A simple method of utilizing scripts and a central repository on a local file system, along with OPENSLL, was used as the PKI for issuing certificates from the CA. In a production framework, choosing a PKI is dependent on the requirements of the overall CA implementation.

[32] *XML Signature Syntax and Processing Version 1.1, W3C Recommendation 11 April 2013.* http://www.w3.org/TR/xmldsig-core/

4.4 Software

The following table outlines available software and tools that were evaluated and/or used for each of the components for the POC validation exercise, most of which are open-sourced, and freely available for use. Below is the software considered, observations and recommendations from the validation exercise.

Table 5
Software used for the validation exercise

Component	Software Considered	Observations	Recommendation
BDXL/SML – DNS	AWS Route 53	- Does not support Dynamic DNS Update.	Choose software that supports Dynamic DNS Updates.
	Microsoft DNS	- Experienced compatibility issues with Dynamic DNS Update during initial testing.	
	Bind v9	- Is an open source tool. - Supports Dynamic DNS Update for federated management and yielded positive testing results.	
	Custom Java	- Java based BIND functionality was used following DNS standards as both a secondary Domain Name server and as a mechanism for making Dynamic DNS Updates to the Primary Domain Name server.	
BDXL/SML – Software Interface	CEF Digital "SML" software	- Open source software. - Attempts to make it work with signed certificate-based communications failed due to hardcoded certificate details.	Interface for editing and managing the registry should be user-friendly and work with signed certificate-based communications.
	Custom Interface written by work group member	- Allowed for editing/managing the registry (i.e. BDXL/SML) utilizing a user-friendly web-based interface.	
SMP	CEF SMP	- Open source software. - Experienced compatibility issues with non-CEF/Peppol certificates.	Software for managing participants should be SMP v2.0 compliant and compatible with non-CEF/Peppol certificates.
	PHOSS SMP	- Open source software. - Fully functional SMP, however was only SMP v1.0 compliant.	

Component	Software Considered	Observations	Recommendation
	Two custom services created by work group members	• SMP v2.0 compliant XML based web service (no user interface) to manage participants. • SMP V2.0 compliant XML based web service with a user-friendly interface to manage participants.	
Access Point	Domibus	• Open source tool includes built in discovery mechanism. • Very complex to setup – Java based with instructions limited to only a very basic install with minimal security configurations. • P-Mode configuration requirements were significantly more extensive than what was minimally needed for the POC. • Unable to configure for interoperability with Holodeck in context of the POC.	Software used for an access point platform should have a built-in discovery mechanism, an intuitive GUI for managing the application, automated methodology for sending messages, straightforward P-Mode configuration requirements and simple to set up with detailed instructions allowing for more complex and secure configurations based on needs.
	Holodeck B2B	• Open source tool. • Simple to setup. • P-Mode configuration straight forward and minimally compliant with standard specification. • Did NOT have discovery capability built in (had modules but required development effort to integrate).	
	AS4 client built by work group member using PHASE 4 libraries	• Open source software. • A GUI front end provided for sending messages. • Followed BDXL 1.0 and SMP 2.0 standards. • Participants were able to continue to use their Holodeck implementations as receive only APs. • Designed as a send only AP that provided the discovery mechanisms to properly test the federated registry services.	

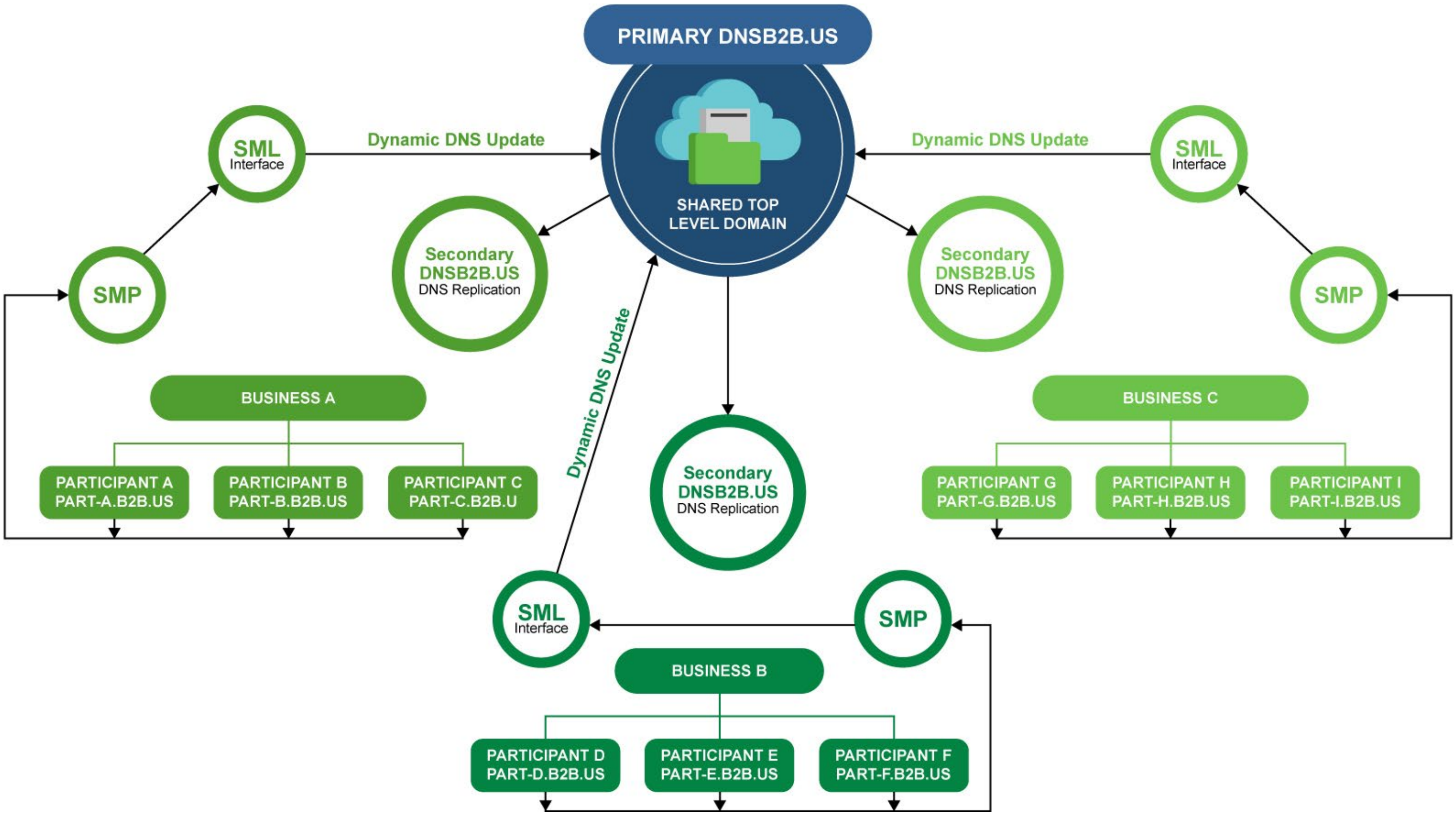
5 Federated Registry Services Model Concepts

This section provides an overview of the federated registry services model and the end-to-end invoice exchange workflow within a four-corner network model.

5.1 Federated Registry Services Model

This section provides an overview of the technical architecture for an e-Delivery network in a shared top-level domain model.

Figure 2
Single top-level domain (decentralized)


PRIMARY DNSB2B.US
SHARED TOP LEVEL DOMAIN
Dynamic DNS Update
Dynamic DNS Update
Dynamic DNS Update
SML Interface
SML Interface
SML Interface
SMP
SMP
SMP
Secondary DNSB2B.US DNS Replication
Secondary DNSB2B.US DNS Replication
Secondary DNSB2B.US DNS Replication
BUSINESS A
PARTICIPANT A PART-A.B2B.US
PARTICIPANT B PART-B.B2B.US
PARTICIPANT C PART-C.B2B.U
BUSINESS C
PARTICIPANT G PART-G.B2B.US
PARTICIPANT H PART-H.B2B.US
PARTICIPANT I PART-I.B2B.US
BUSINESS B
PARTICIPANT D PART-D.B2B.US
PARTICIPANT E PART-E.B2B.US
PARTICIPANT F PART-F.B2B.US

Source: Business Payments Coalition

In the federated registry services model above, a top level (primary) domain name (i.e. B2B.US) is used to register all participants. SML service providers host secondary DNS servers for local DNS resolution. Dynamic DNS Update is utilized by SML service providers to make changes to the primary Domain Name Server (directly) which then propagate to the Secondary Domain servers with DNS replication.

This differs from existing centralized registry models by allowing multiple SML service providers to make changes to the registry. Dynamic DNS Update provides security mechanisms to help prevent unauthorized changes by outside network sources.

5.2 End-to-End e-Invoice Exchange in a Four-Corner Network Model

The exchange framework defines the prescriptive standards enabling end to end exchange of electronic invoices between separate systems, networks, and platforms. The POC focused on building the connections for the message transport infrastructure including the discovery and delivery components to establish connectivity within the e-Delivery network. While the overall network architecture is based on a four-corner network model, the validation exercise focused specifically on the interactions between C2 and C3. Figure 3 provides the detailed steps required for successful message exchange between C2 and C3. Processes between C2 and C3, and C3 and C4 were simulated during the validation exercise.

For the purposes of the diagram on the next page, sender and receiver references are as follows:

- C1 = Original Sender
- C2 = Access Point Service Provider for C1
- C4 = Final Recipient
- C3 = Access Point Service Provider for C4

The invoice exchange process begins when C1 sends an invoice to C2 and C2 processes the invoice based on business rules defined between C1 and C2 (Steps A and B). Because the validation exercise focused on interactions between C2 and C3, the steps between C1 and C2 were only emulated during testing.

After semantic processing is complete, C2 compiles the data needed to discover the recipient's endpoint based on the ebCorePartyID Type Specification, including the original sender, final recipient, process type and schema and service type and schema (Step C), using the formatting below:

- Core Identifier: urn:oasis:names:tc:ebcore:partyid-type:
- Party ID Type and Schema: urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060
- Full identifier: urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060::1824375643

The full identifier is then used to create the query for finding the participant record in the registry. It is formulated as such:

- Electronic Address Identifier: base32(sha256(lowercase(full identifier)))[33]
- Electronic Routing Address: eletronicaddressidentifier.toplevel.com

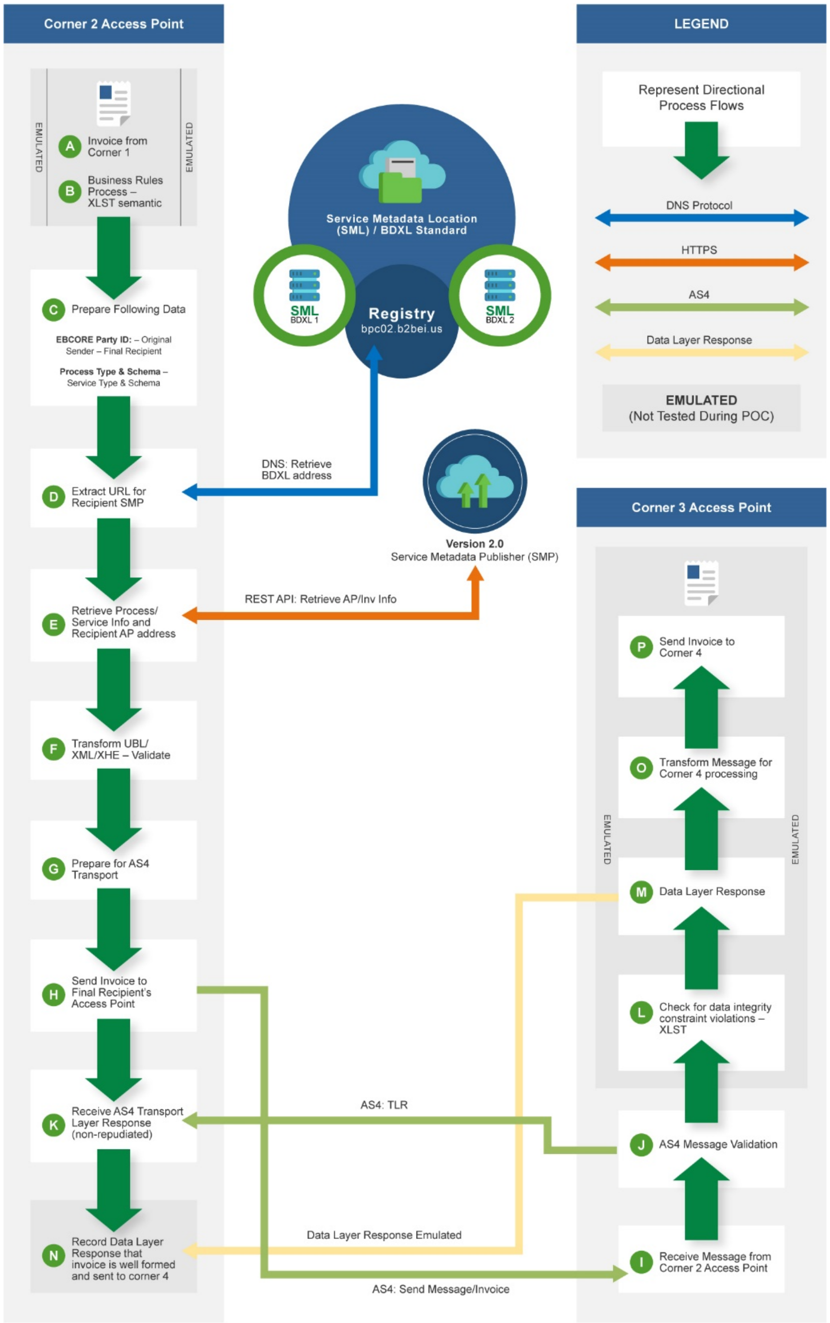
Using the Final Recipient identifier, C2 sends a DNS query to the registry to retrieve the SMP URL address of the final recipient's Access Point (Step D). Next, C2 sends a request to the SMP to retrieve the endpoint recipient access point address and capabilities (Step E) using the SMP 2.0 REST API specifications.

After receipt of the endpoint's access point address and capabilities, C2 transforms the message into an XML file that complies with UBL 2.x and XHE standards (Step F) and

[33] SHA256 is a subset of the SHA-2 set of cryptographic functions. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: **SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256**. SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively.

assembles the transport components (XML, message payload, message envelope) into a well-formatted AS4 message using P-Mode parameters in preparation for transport (Step G).

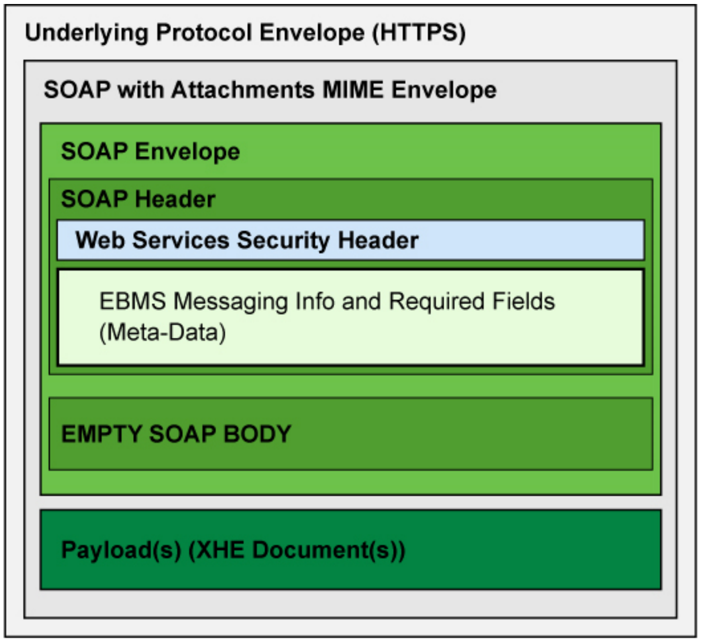
Figure 3
Detailed Workflow within a Four Corner Network Model


Corner 2 Access Point
EMULATED
A Invoice from Corner 1
B Business Rules Process – XLST semantic
EMULATED
C Prepare Following Data
EBCORE Party ID: – Original Sender – Final Recipient
Process Type & Schema – Service Type & Schema
D Extract URL for Recipient SMP
E Retrieve Process/ Service Info and Recipient AP address
F Transform UBL/ XML/XHE – Validate
G Prepare for AS4 Transport
H Send Invoice to Final Recipient's Access Point
K Receive AS4 Transport Layer Response (non-repudiated)
N Record Data Layer Response that invoice is well formed and sent to corner 4
Service Metadata Location (SML) / BDXL Standard
SML BDXL 1
Registry bpc02.b2bei.us
SML BDXL 2
DNS: Retrieve BDXL address
Version 2.0 Service Metadata Publisher (SMP)
REST API: Retrieve AP/Inv Info
AS4: TLR
Data Layer Response Emulated
AS4: Send Message/Invoice
LEGEND
Represent Directional Process Flows
DNS Protocol
HTTPS
AS4
Data Layer Response
EMULATED (Not Tested During POC)
Corner 3 Access Point
EMULATED
P Send Invoice to Corner 4
O Transform Message for Corner 4 processing
M Data Layer Response
L Check for data integrity constraint violations – XLST
EMULATED
J AS4 Message Validation
I Receive Message from Corner 2 Access Point

Source: Business Payments Coalition

Figure 4 provides a high-level view of the message envelope contents. The envelope structure is payload agnostic and adds flexibility to the framework by allowing the exchange of multiple payload types. A detailed envelope diagram can be found in Appendix F Message Packaging Details.

Figure 4
Message Packaging[34]


Underlying Protocol Envelope (HTTPS)
SOAP with Attachments MIME Envelope
SOAP Envelope
SOAP Header
Web Services Security Header
EBMS Messaging Info and Required Fields (Meta-Data)
EMPTY SOAP BODY
Payload(s) (XHE Document(s))

C2 sends the AS4 message to the access point of the final recipient (C3), who after receiving the message, sends an AS4 transport receipt back to C2 for purposes of non-repudiation (Steps H-K). The transport receipt serves only as confirmation that C3 received the outgoing message and does not indicate that the invoice met the data content and format required for the target business (C4) to accept and effectively process the invoice.

C3 evaluates the semantics of the invoice against the data integrity constraints and any business rules specific to standards oversight requirements. Based on the results, C3 sends an Application Layer Response (ALR) to C2 containing the status of the invoice (Steps L-M). C2 records the ALR and depending on previously established business rules, may forward the response to C1, the original sender (Step N).

After sending the ALR to C2, C3 processes and transforms the invoice based on unique requirements and custom configuration of C4's ERP system and sends the final invoice to C4, the final recipient (Steps O-P).

For a text version of the diagram steps, see Appendix C Detailed Workflow within a Four Corner Model (steps).

[34] Adapted from eDelivery AS4 – 1.14 CEF Digital https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.14

5.3 Results and Findings

Below are additional findings from the validation exercise that led the BPC to the recommendations in Table 7.

Table 6
Additional Findings

Category	Finding
Discovery	No changes are necessary to current OASIS BDXR discovery standards to achieve endpoint dynamic discovery across a framework utilizing a federated registry services model. This was tested and proved that it is ***technically*** feasible to establish a decentralized registry management model in the framework. The validation test was performed through configuration settings within the context of current standards without significant complexity.
Registry Management	It's possible to manage (in a federated registry services model) multiple SML services and make changes to the registry (without business controls) under a single DNS.
Security	Security is inherently complex and increases in complexity depending on the desired level of encryption. The standards oversight entity should further define security requirements. The architecture validated as part of this exercise will not limit the strength of security or increase the complexity required to implement it.
	Security keys only allowed the SML services within the network to make changes to DNS name, preventing unauthorized updates from outside sources.
	A registry maintenance and security need was identified with multiple SML Services. While security measures on the Dynamic DNS Update processes can prevent outside framework interference, it does not prevent accidental/unauthorized changes from other authorized registry service providers.
Messaging	The implementation of AS4 specifications did not require any changes to the message response for the federated registry services model that was tested.
Identifiers	It is critical to configure the service IDs and scheme IDs so they are in alignment with standards and specifications to ensure successful message transmission and interoperability.
	ebCore party specifications reduced complexity of interoperability within the network; guaranteed unique IDs while allowing participants to use IDs of their choice.
Software	Although not tested, each AP would need to set up individual business rules by business ID. The standards oversight body should make this part of the AP requirements.
	The primary DNS for a federated registry service is dependent on using the Dynamic DNS Update function. For the POC, Bind v9 and custom Java were used for the Dynamic DNS Update. It is presumed that any software that supports secure Dynamic DNS Updates can be configured to work for a federated registry service. Use of AWS Route 53 may cause issues with maintaining DNS due to the lack of support for Dynamic DNS Update.
Open Source Tools	The open source Access Point tools explored include Domibus, Holodeck and Phase-4. Discovery mechanisms are not always included in a standard Access Point offering. For example, Holodeck doesn’t include discovery, but has an add on that can be developed. Phase-4 is an open source java library that provides discovery functionality using the BDXL and SMP standards. It is available to use for integration into existing java based AS4 message transport applications.

6 Recommendations and Next Steps

6.1 Recommendations

The table below summarizes the recommendations provided in this report. In 2021, the BPC will develop open source tools to help in the orchestration of a 2022 in-market pilot.

Table 7
Summary Recommendations

Component	#	Recommendations	Related Section(s)
Overall Architecture	1	It is our assumption and recommendation that the overall architecture of the e-Invoice exchange framework be based on a four-corner network model.	2.1, 4.2
	2	Service providers should develop their Access Points to dynamically adjust Product and Service Type information based on what is found in the SMP.	
Registry Approach	3	A single domain approach is recommended for a U.S. framework given that it allows multiple registries to use a single lookup, its straightforward implementation and low level of complexity for establishing the federated registry service (e.g. DNSB2B.US)	4.1, 4.2, 5.1
	4	A separate analysis should be completed for global interoperability, taking into consideration technical, legal, security and yet to be discovered considerations. The U.S. e-Invoice framework should continue coordination with existing frameworks to work toward global interoperability.[35]	
	5	Continue to coordinate efforts with OASIS BDXR in researching and evaluating options for providing participant record ownership of registry entries, tied to specific SML Services Providers, in order to prevent accidental/unauthorized changes to the registry from federated SML services members. Base approach on specification currently being discussed by OASIS BDXR committee.	
Registry Standards	6	Continue use of Business Document Metadata Service Location (BDXL) Version 1.0 and Service Metadata Publishing (SMP) v 2.0 standards, as well as the next revision of the standards that are currently in committee.[36]	4.1, 4.2, 5.1
Business Discovery Process	7	Use BDXL 1.x and SMP 2.0 standards.	4.2, 5.2

[35] For example, using ebCore party ID would support interoperability, but the standards oversight entity group will need to determine strategies/collaboration efforts to support standardization across frameworks (Peppol, EESPA, GIF).

[36] OASIS BDXR group is updating the current BDXL specification; updates may provide a standardized approach to:

1) How to prevent accidental/unauthorized changes to entries that participant does not have access to
2) Rest API specification to allow for business rules to be applied and provide a standard method of remote management

Component	#	Recommendations	Related Section(s)
Identifiers	8	Move forward with ebCore party ID specification. Follow the BDXR specifications as they are released.	4.2,5.2
Message Transport Protocols	9	Access Points should use AS4 in a four-corner network model.	4.2, 5.2
	10	Implement the AS4 profile based on the forthcoming OASIS BDXR Committee Specification[37,38].	4.2, 5.2
Message Envelope Standards	12	XHE should be considered the default envelope standard.	4.2, 5.2
Envelope Payload	13	Use OASIS UBL 2.3[39] due to its common data dictionary and use of a single syntax.	4.2, 5.2
Message Response	14	To ensure interoperability with other frameworks using the BDXR standards, some level of ALR standardization (e.g. expected responses) is needed. The BPC Technical Work Group should define and test a UBL application layer response standard prior to the in-market pilot. The BPC should continue collaborating with OASIS on a set of standards for application layer responses.	4.2, 5.2
	15	The BPC Semantic Model Work Group should define business processes and appropriate business layer responses.	
Security	16	Require AS4 message encryption as defined in recommendation 10.	4.2, 4.3
	17	Enable optional XHE envelope encryption for end to end processing.	
	18	Use multiple PKIs to control and maintain trust across federated membership. A standards oversight organization should define requirements and finalize trust network policies based on those requirements.	
	19	Recommend that SML service providers act as the issuing Certificate Authorities to simplify certificate management as part of overall trust model. Additionally, processes should be determined for authentication and efficient methods for updating the public keys (similar to how the card industry updates the PKI for the industry).	
Software	20	BDXL/SML Services software should support using Dynamic DNS Updates.	4.2, 4.4
	21	The Interface for editing and managing the registry should be user-friendly and work for signed certificate-based communications.	
	22	Software for managing participants should be SMP v2.0 compliant.	

[37] The OASIS Technical Committee is working on a committee specification based on the AS4 profile that would be implemented across frameworks to ensure interoperability.

[38] OASIS BDXR Committee Specification using AES-128 with Galois/Counter (GCM) mode and X.509 for digital certificate encryption and signing.

[39] 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.

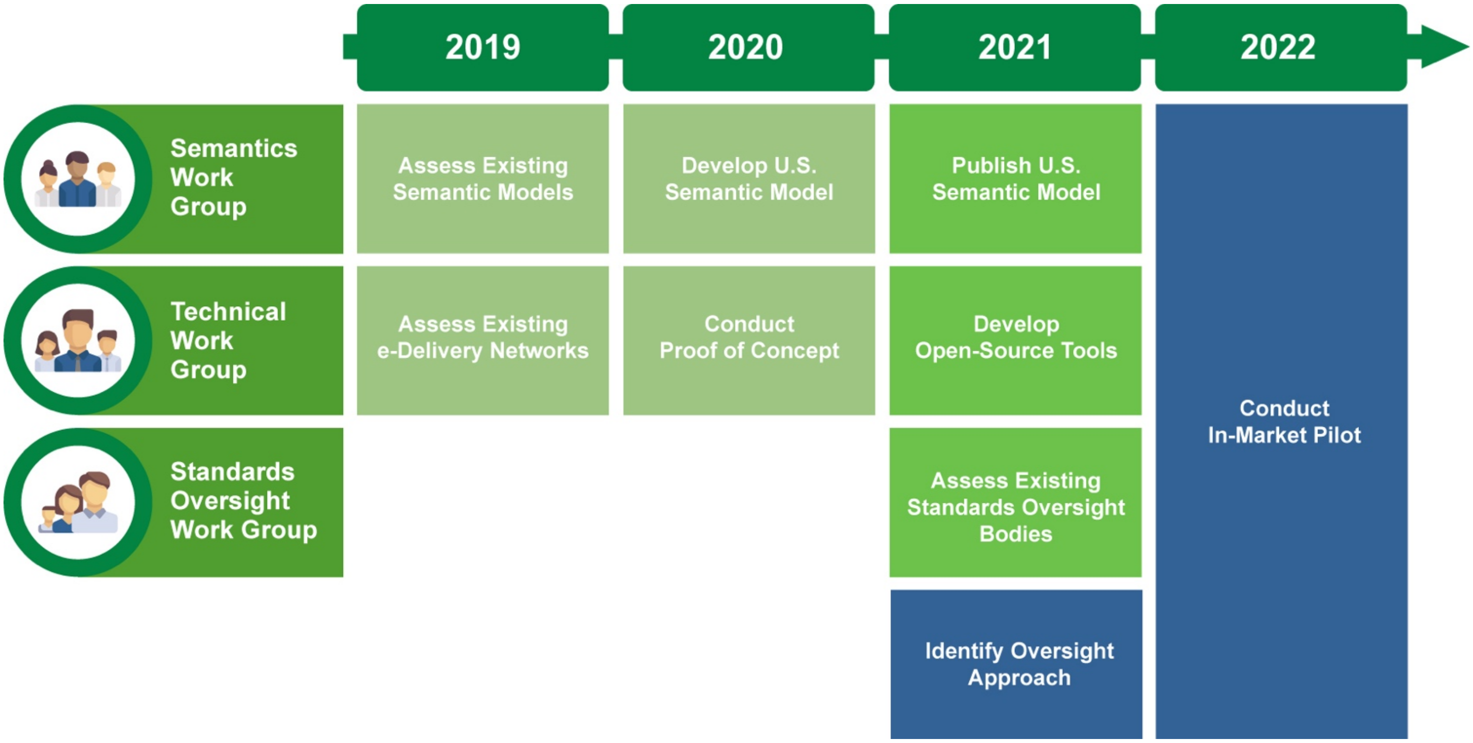
6.2 Next Steps

The BPC e-Invoice Technical Work Group will coordinate active industry involvement in the following activities:

1) Requirements gathering, development and testing of open source tools focused on Access Point components.
2) Creation of an onboarding toolkit illustrating how to build and deploy an access point. The onboarding toolkit will help participants understand the standards, best practices, and steps for implementation.
3) Continue work group assessment of the standards oversight requirements for the exchange framework. Recommendations and findings from this report will be shared with the Technical Work Group regarding oversight requirements for federated registry services.
4) Complete and publish the e-Invoice Semantic Model Specifications for the e-Invoice exchange framework, a critical component for an in-market pilot program.

The next steps identified above are critical for establishing and conducting an in-market pilot, where we will invite industry involvement to utilize the open source tools and onboarding toolkit in support of establishing the exchange framework.

Figure 5
Exchange Framework Initiative Work Group Timelines



	2019	2020	2021	2022
Semantics Work Group	Assess Existing Semantic Models	Develop U.S. Semantic Model	Publish U.S. Semantic Model	Conduct In-Market Pilot
Technical Work Group	Assess Existing e-Delivery Networks	Conduct Proof of Concept	Develop Open-Source Tools	
Standards Oversight Work Group			Assess Existing Standards Oversight Bodies	
			Identify Oversight Approach	

Source: Business Payments Coalition

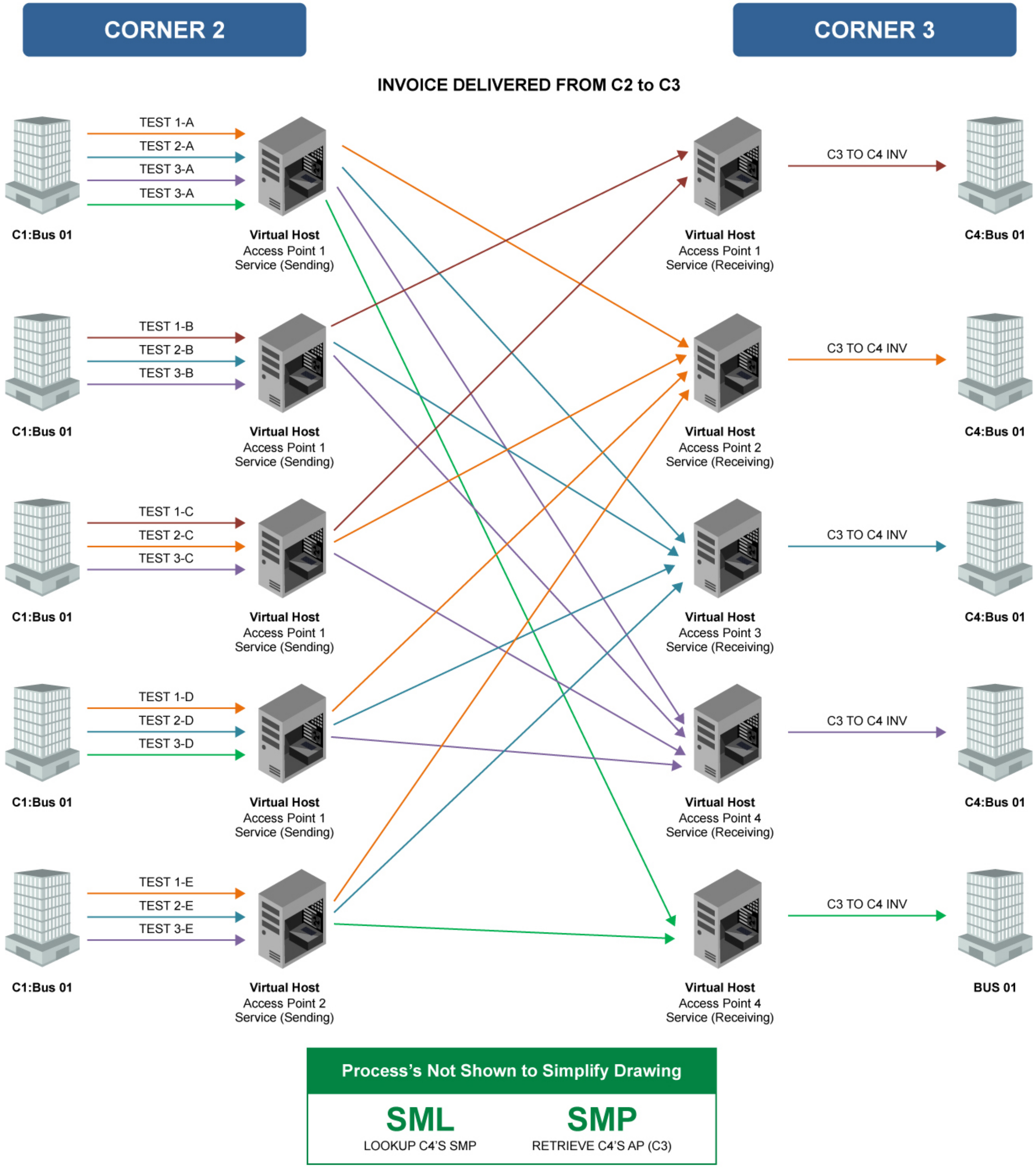
7 Appendices

7.1 Appendix A – Work Group Members

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

Name	Organization
Ahti Allikas	Opus Capita
Alberto Toledo	ATEB Servicios SA de CVa
Anna Tujunen	Dooap, Inc
Daniel Isaacs	Intech Solutions
Daniel Sanchez	Indicium Solutions
Evelina Erikkson	Pagero
G. Ken Holman	CraneSoftwrights Ltd
Ger Clancy	IBM
Janos Toberling	Partner Hub
Jason Elliston	Serrala
Jesus Pastran	ATEB Servicios SA de CV
Jesus Romulado	ATEB Servicios SA de CV
Jose Luis Ortiz	Indicium Solutions
Kenneth Bengtsson	Efact
Katalin Kauzli	Partner Hub
Lauri Holtta	Dooap, Inc
Omar Martinez	Factura Facilmente de Mexico SA de CV
Omar Valencia	Ekomercio
Philip Helger	Consultant
Sarika Sharma	Serrala
Sander Fieten	Chasquis
Steven Wasserman	Vments INC
Shane Samuel	Canada Revenue Agency
Terry Goodman	Intech Solutions
Timo Mäntynen	Dooap, Inc
Todd Albers (Convener)	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
Ethan Lamont	Federal Reserve Bank of Minneapolis

7.2 Appendix B – Validation Exercise Testing Matrix



Source: Business Payments Coalition

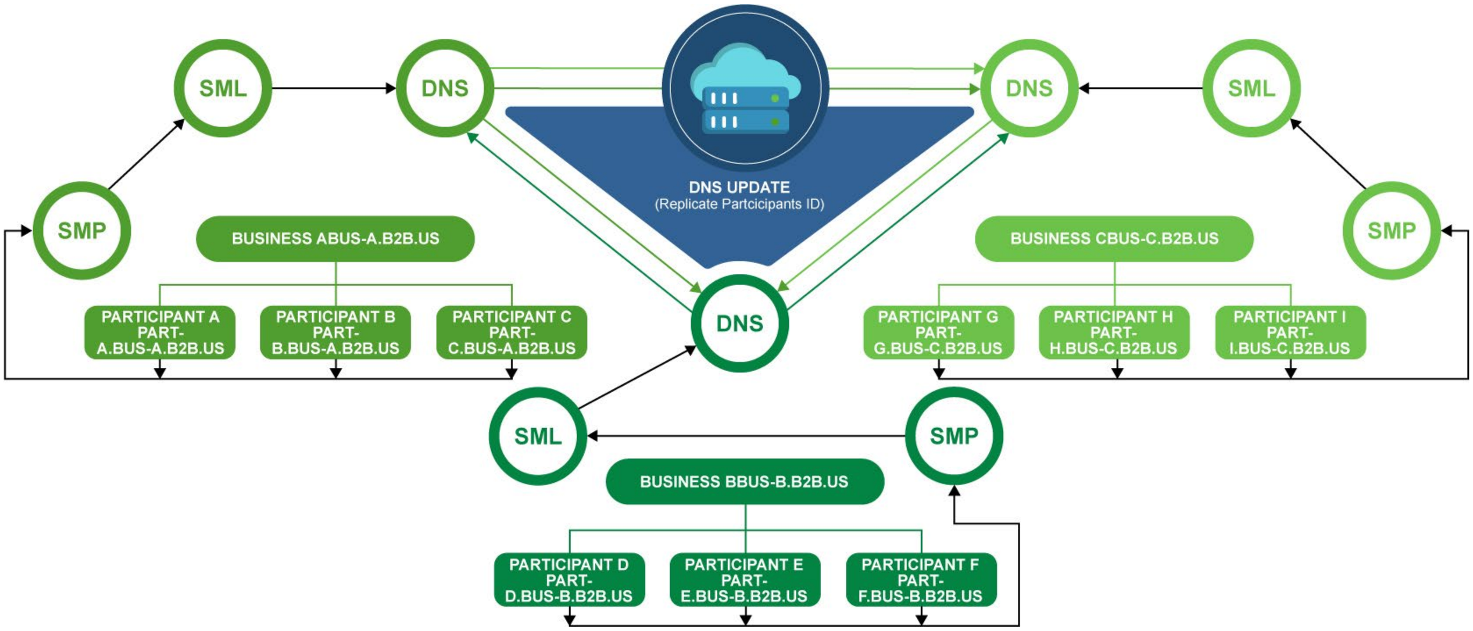
7.3 Appendix C – Detailed Workflow within a Four Corner Network Model (Steps)

Step	Description
A	*(emulated)* Process begins by sending an invoice from C1 to C2
B	Semantic processing occurs during this step (processing) by utilizing business rules defined between C1 (customer) and C2 (service provider). This process was not emulated for the validation exercise.
C	Preparing relevant data needed • Original Sender (C1) ○ Not required by standard; maintained at an envelope level • Final Recipient (C4) ○ Not required by standard; maintained at an envelope level • Process Type and Schema ○ Required by standard • Services Type and Schema ○ Required by standard
D	Using the Final Recipient, send a DNS query to the registry to get the SMP URL address of the Access Point where the final recipient is registered.
E	Send a request to the SMP to retrieve endpoint recipient access point address (electronic address identifier) and capabilities.
F	Transform the message into an XML file that complies with UBL 2.x and XHE standards.
G	Prepare for AS4 transport is a logical step that represents assembling the transport components (XML, message payload, message envelope) into a well-formatted AS4 message.
H	Send AS4 message to the Access Point of the final recipient.
I	C3 receives the message.
J	C3 sends AS4 transport receipt to C2.
K	C2 receives AS4 transport receipt for purposes of non-repudiation. This is confirmation that C3 received the outgoing message and does not indicate that the invoice was accepted.
L	C3 evaluates the semantics of the invoice against what the final recipient has established with their service provider. There may also be business rules specific to requirements from the standards oversight body. The outcome of this process is the Data Layer Response.
M	The Data Layer Response that is provided to C2 regarding the status of what was processed in previous step (L).
N	C2 records the Application Layer Response and depending on the business rules with their customer (C1) they may forward the response to the original sender.
O	This is a logical representation of what C3 does with an invoice prior to sending to their customer (C4.) The rules for processing/transforming are unique based on the requirements of the ERP system, and its custom configuration, that C4 uses.
P	The actual sending of the message (i.e. invoice) to C4 (Final Recipient.)

7.4 Appendix D - Federated Registry Approach Options

Option 1: Federated Registry services using Unique Domain scheme for each registry

Details: Use nsupdate to maintain participant ID replication between registrar's registries.


SML
DNS
DNS UPDATE
(Replicate Partcicipants ID)
DNS
SML
SMP
BUSINESS ABUS-A.B2B.US
PARTICIPANT A PART-A.BUS-A.B2B.US
PARTICIPANT B PART-B.BUS-A.B2B.US
PARTICIPANT C PART-C.BUS-A.B2B.US
DNS
BUSINESS CBUS-C.B2B.US
SMP
PARTICIPANT G PART-G.BUS-C.B2B.US
PARTICIPANT H PART-H.BUS-C.B2B.US
PARTICIPANT I PART-I.BUS-C.B2B.US
SML
SMP
BUSINESS BBUS-B.B2B.US
PARTICIPANT D PART-D.BUS-B.B2B.US
PARTICIPANT E PART-E.BUS-B.B2B.US
PARTICIPANT F PART-F.BUS-B.B2B.US

Source: Business Payments Coalition

Advantages:

1) Allows for true federated registries.
2) Technology exists today without modification.
3) Technology is well known, well understood and robust, with established mechanisms for management.
4) Could prove this concept with current work group resources.
5) No change to existing discovery model.

Disadvantages:

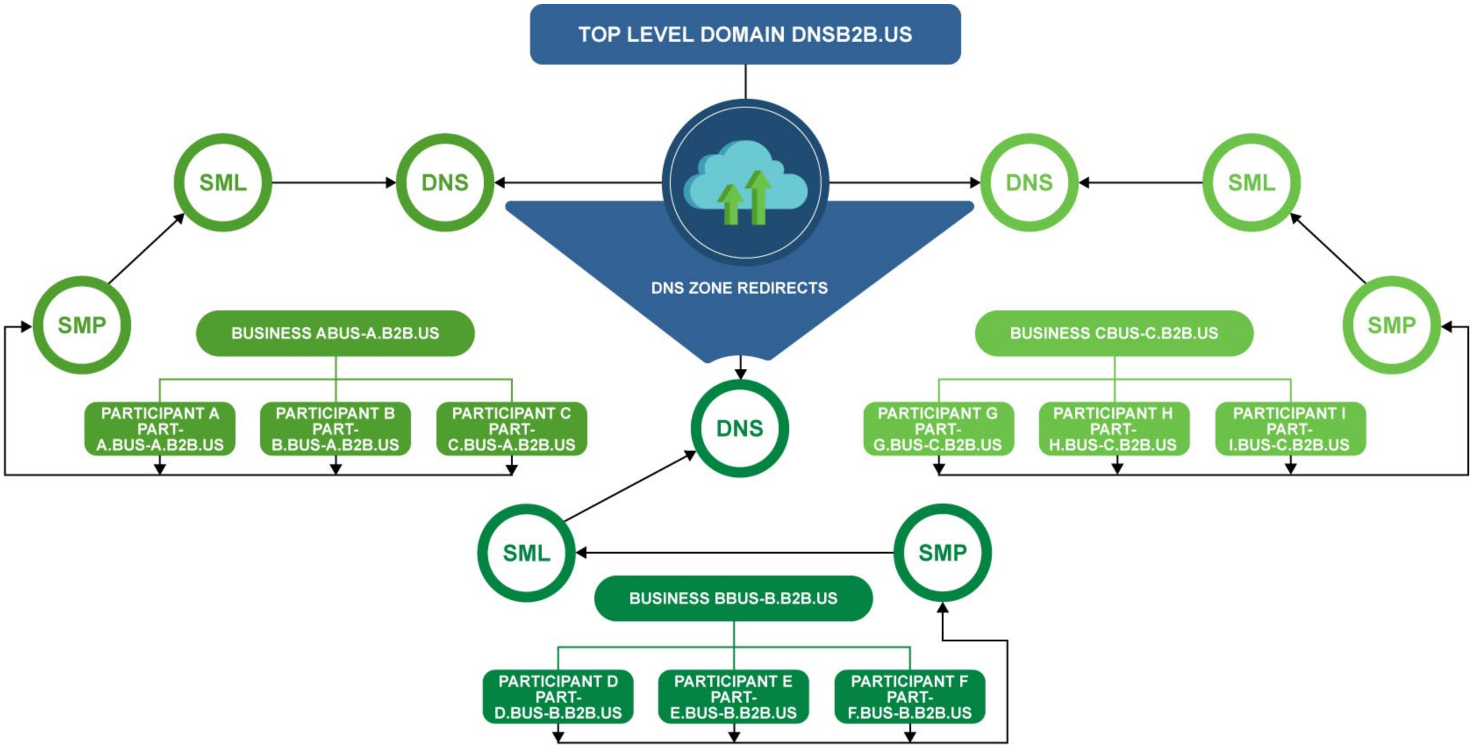
1) Potential scalability concerns with a star configuration of replication and NSUPDATE commands.
2) Every participant ID is replicated to every registry, which could cause participant information to be out of sync.
3) Moving to a different SML service can be difficult and complex – needs both SML service providers to cooperate fully.
4) DNS poses potential issue with latency when propagating around the world.

Organization notes:

- Fully federated standards oversight is supported.
- Should have third party auditing, or cross business auditing, to ensure business, technical and security requirements are met.

Option 2: Federated Registry services using a shared top-level Domain scheme

Details: Each registry has a sub-domain underneath. Replication is not used between registries.


TOP LEVEL DOMAIN DNSB2B.US
DNS ZONE REDIRECTS
SML
DNS
SMP
BUSINESS ABUS-A.B2B.US
PARTICIPANT A PART-A.BUS-A.B2B.US
PARTICIPANT B PART-B.BUS-A.B2B.US
PARTICIPANT C PART-C.BUS-A.B2B.US
DNS
DNS
SML
SMP
BUSINESS CBUS-C.B2B.US
PARTICIPANT G PART-G.BUS-C.B2B.US
PARTICIPANT H PART-H.BUS-C.B2B.US
PARTICIPANT I PART-I.BUS-C.B2B.US
SML
SMP
BUSINESS BBUS-B.B2B.US
PARTICIPANT D PART-D.BUS-B.B2B.US
PARTICIPANT E PART-E.BUS-B.B2B.US
PARTICIPANT F PART-F.BUS-B.B2B.US

Source: Business Payments Coalition

Advantages:

1) Eliminates complex nsupdate methodologies for keeping participant IDs in sync.
2) Sub domain zone hosting can be moved back to registrars completely to give each registrar complete control over their registry.
3) Participant IDs only exist in one registry (no replication), reducing scalability concerns with option 1.
4) Could prove this concept with current work group resources.
5) Technology exists today to support this model.
6) Technology is well known, well understood and robust, with established mechanisms for management.
7) No change to existing discovery model.

Disadvantages:

1) Additional costs required to support top level domain; central ownership of the top-level domain can be contracted out using a registrar fee-based system to pay for costs.
2) Participant ID searching can impact performance as the network scales out. (Though may be manageable.)
3) Changing SML Service Providers has significant complexity that may be unmanageable.

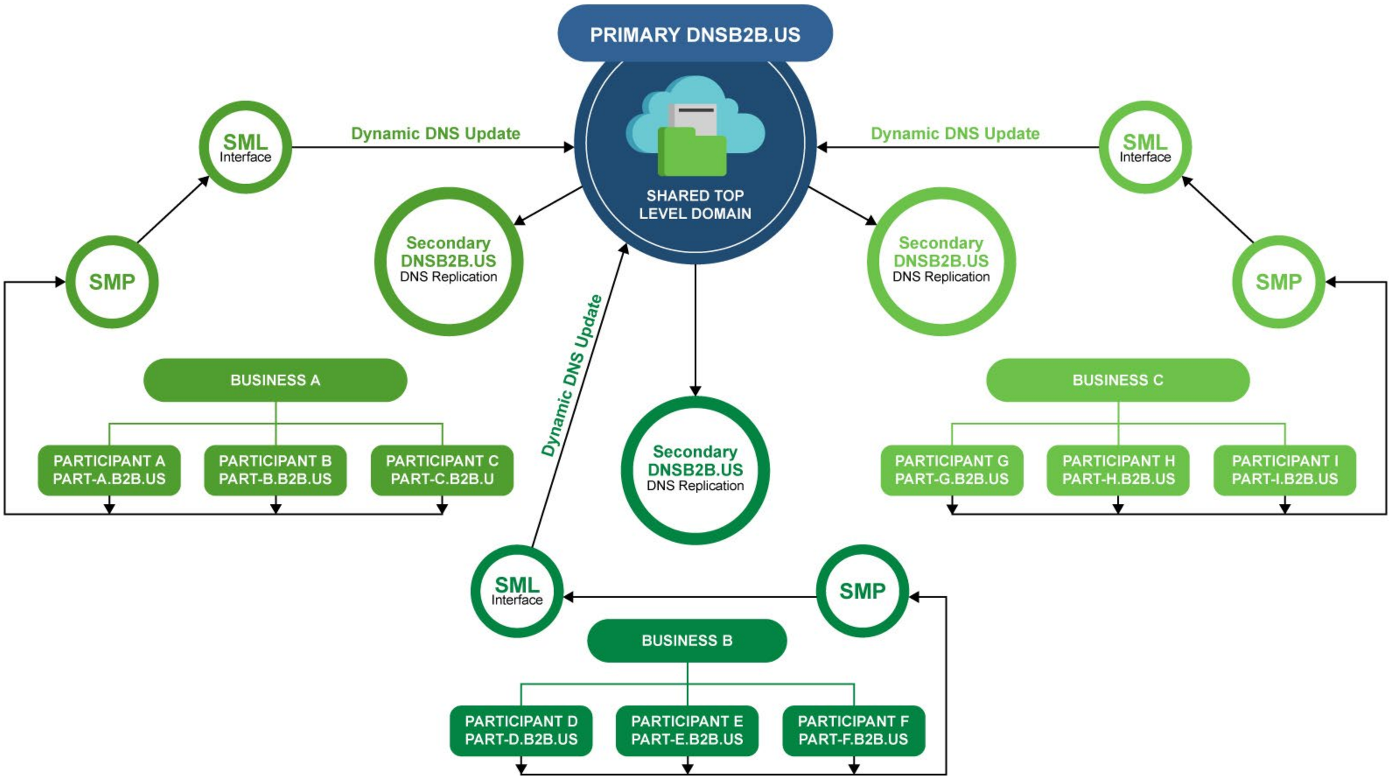
4) DNS poses potential issue with latency when propagating around the world.
5) Can we effectively provide a technical solution that supports a business process for modifications/updates to the registry (e.g. business rules are enforced through a technical solution, not through business process alone)?

Organization notes:

- Can still maintain completely federated ownership of the network. With the top-level domain only being managed without any input to the overall organizational rules/by-laws. There can be varying degrees to this. Responsibilities for domain manager include giving out new zones.
- Should have third party auditing or have top level domain manager do audits.

Option 3: Hybrid of 1 and 2 - Federated Registry services using a top-level Domain scheme and secondary DNS servers

Details: Top level domain scheme for all participants; SML service providers host secondary DNS servers that use NSUPDATE to provide changes.


PRIMARY DNSB2B.US
SHARED TOP LEVEL DOMAIN
Dynamic DNS Update
SML Interface
Dynamic DNS Update
SML Interface
SMP
Secondary DNSB2B.US DNS Replication
Secondary DNSB2B.US DNS Replication
SMP
BUSINESS A
PARTICIPANT A PART-A.B2B.US
PARTICIPANT B PART-B.B2B.US
PARTICIPANT C PART-C.B2B.U
Dynamic DNS Update
Secondary DNSB2B.US DNS Replication
BUSINESS C
PARTICIPANT G PART-G.B2B.US
PARTICIPANT H PART-H.B2B.US
PARTICIPANT I PART-I.B2B.US
SML Interface
SMP
BUSINESS B
PARTICIPANT D PART-D.B2B.US
PARTICIPANT E PART-E.B2B.US
PARTICIPANT F PART-F.B2B.US

Source: Business Payments Coalition

Advantages:

1) Reduces complexity with nsupdate methodologies that replicate only to top level domain, not each other.
2) Essentially only one registry, but with multiple owners, reduces complex searching for participants.
3) Could prove this concept with current work group resources.
4) No change to existing discovery model.
5) Fairly low additional costs (compared to option 1) for top level domain management (only a primary DNS management is needed.)
6) Changing SML service providers has low complexity/barriers.
7) Technology exists today to support this model.
8) Technology is well known, well understood and robust, with established mechanisms for management.
9) Supports reduction of fraud.

Disadvantages:

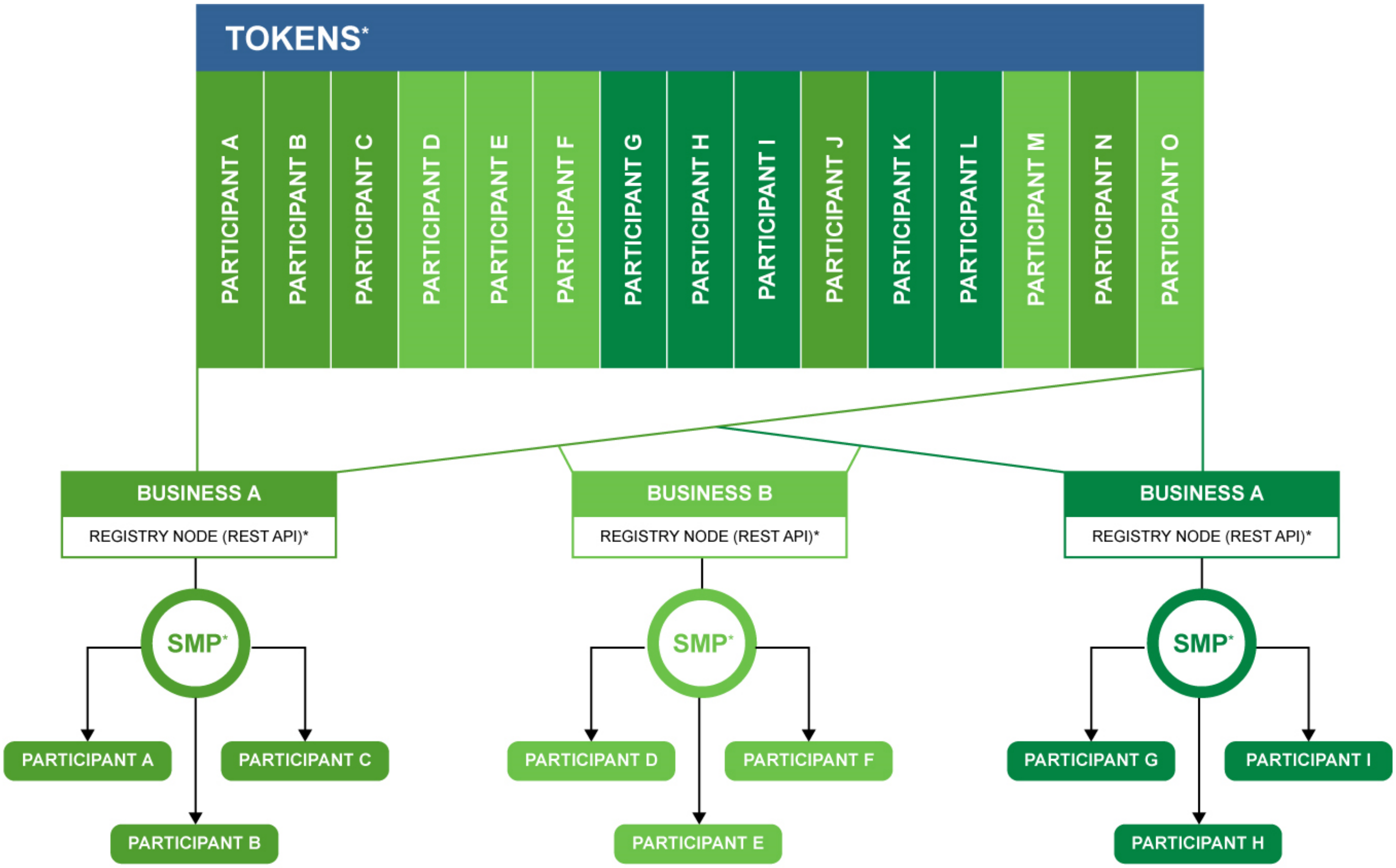
1) Additional costs required to support top level domain primary DNS controller.
2) Very clearly defined rules on updates to registry must be defined and followed, could create legal complexity.
3) DNS poses potential issue with latency when propagating around the world.
4) Can we effectively provide a technical solution that enforces a business process for modifications/updates to the registry (e.g. business rules are enforced through a technical solution, not through business process alone)?

Organization notes:

- Can still maintain completely federated ownership of the network. With the top-level primary domain servers being managed by third party.
- Should have third party auditing or have top level domain manager do audits.
- Ensure ability to accommodate third party identity validation.

Option 4: Blockchain registry for all participants

Details: Updated through a participant’s registrar.



*Blockchain – tokens represent each participant in the chatin.
** Registry Node is the interface into the blockchain – for managing and controlling connections to the blockchain
*** SMP updated standard to support connecting to the Registry Node

Source: Business Payments Coalition

Advantages:

1) Opens options to re-architect SML/SMP model.
   i. Could eliminate the existing SML/SMP model by having all the registration and meta-data in the Blockchain, thereby allowing the Access Point to connect directly into the blockchain.
2) Only the registrars need to be familiar with blockchain.
3) Can enforce business processes through technical functions.

Disadvantages:

1) New technology without widespread adoption.
2) Higher latency requirement than DNS.
3) Lookup volumes haven't been field tested yet.
4) Single blockchain registry could be vulnerable to denial of service or other attacks (more vulnerable than DNS).
5) Requires organization to manage the code base for the blockchain.
6) Interoperability is challenging with existing systems and B2B and B2G frameworks, as all transport mechanisms are changed from the top down.
7) Most likely highest federated member cost.
8) Need outside resources to prove this concept.
9) Requires a change the standards essentially replacing the SML services functionality with a standard that supports writing and retrieving registration information from a blockchain.
10) Requires a change to discovery process, either through the Access Points talking directly to the blockchain, or access points using a central DNS name to connect to a RestAPI on a node that connects to the blockchain on the AP's behalf.

Organization notes:

- Federated membership would be supported.
- Requires an association/group that manages blockchain codebase.
- Legal agreements will need to include very detailed business rules to properly support blockchain processing. Standards oversight body would need some knowledge of blockchain processes.

7.5 Appendix E – BPC Trial Federated Registration Service SML & DLS

Source: Intech Solutions

As part of the BPC Proof of Concept trials conducted during 2020, the BPC sought to test various configurations that enables a federated approach to Registration Services.

This section outlines the configuration, testing and findings of a federated approach to Registration Service (also known as SML) using Party-ID Schemas as subdirectories with DNS Zone delegation as a method to 'federate' Registration Services in a single electronic invoicing network.

The following aspects were configured and tested:

1) Multiple Registration Services established.
2) Each Registration Service conforming to:
   i. Common interfaces for its registration service.
   ii. Common and standards compliant recording of records in DNS.
3) Open-source discovery processes that can discover a Business Participant in the e-invoicing network irrespective of the Registration Service used to Register the Business Participant.
4) A single Party-ID Schema (i.e. urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060) Configured Solution.

The three distinct parts of the solution are:

1) **Libraries for registration and discovery** – open-source libraries were developed and tested for the purpose of being used by Service Providers (Access Points and SMPs) to develop and operate their applications. These libraries handle the SMPs Registration process and the Access Points Discovery process. They abstract the client application from the details of the Registration Service protocol and DNS record structure for ease of use.
2) **Registration Services** – two software services were configured running side by side performing Registrations. These were CEFs SML (used by Peppol) and Intech's DLS (initially developed to the specification of the Australian Digital Business Councils and then commercialised by Intech).
3) **DNS Registries** – a single root (participant.b2bei.us) was used, and Party-ID Schema specific DNS Zones were created and delegated for management by the applicable Registration Service Operator (RSO). The concept of this model is for each Schema's data to be stored in its own Registry, enabling security controls of each Registry to be assigned to a RSO rather than necessitate a centralised Registry across the e-invoicing network. The RSO will then have full control over the Schema's Registry and can allow (or deny) other RSOs from writing records in the Schema's Registry which it controls.

7.5.1 Libraries for registration and discovery

The following components were deployed and tested during the trial:

1) Open-source libraries and a test harness console application – a Java and C#.Net versions of these were created.
2) Web front end Graphical User Interface (GUI).

7.5.2 Registration Services

Two registration services were deployed:

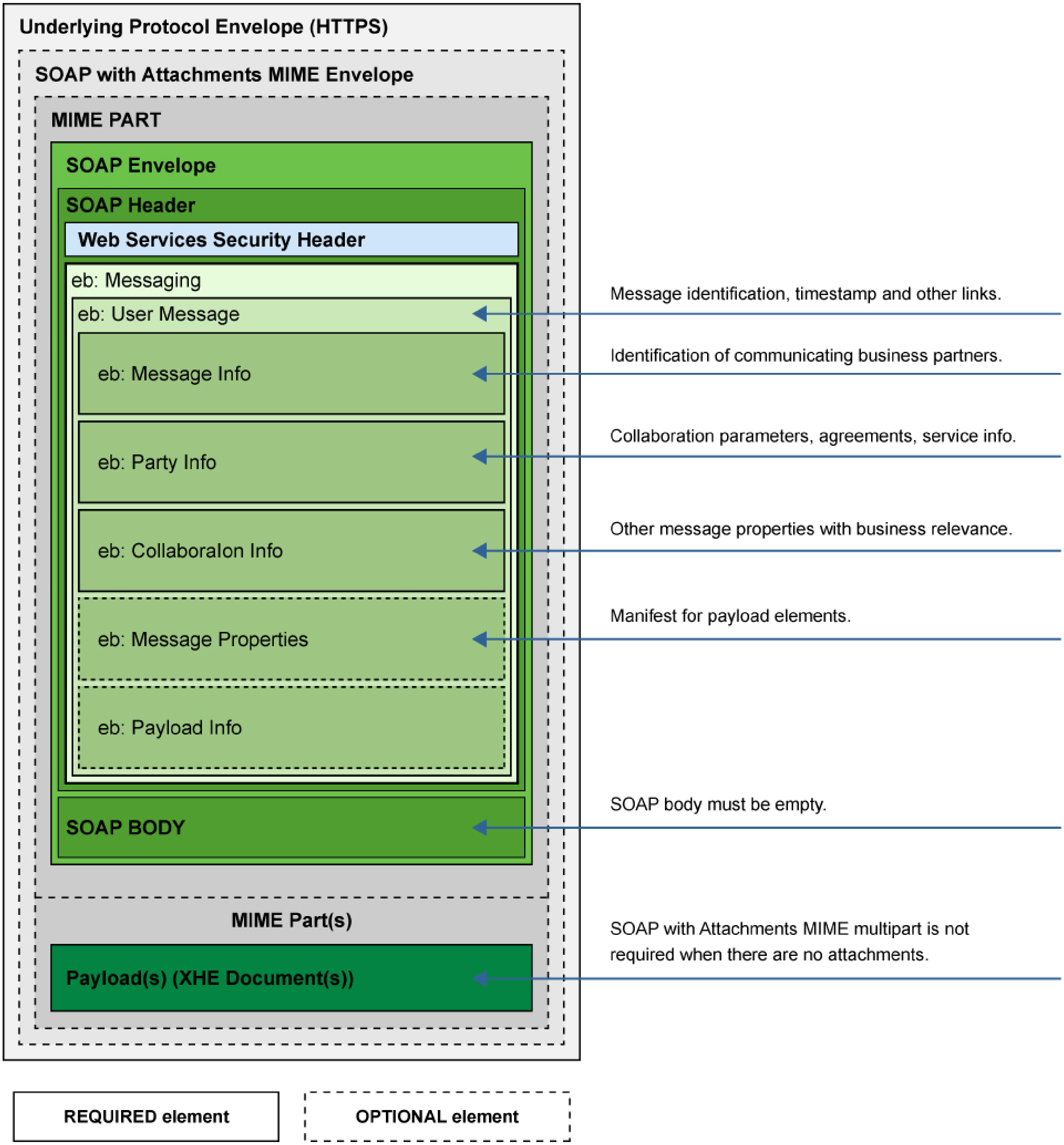
1) CEFs SML (Developed by CEF for Peppol) - this is an implementation of Connecting Europe Facilities (CEF) Java based SML, which implements an SML specification that is part of the Peppol eDelivery network (https://peppol.eu/what-is-peppol/peppol-transport-infrastructure/). This has been modified to work outside of the CEF BlueCoat environment. It contains the following interface:
    i. SML SOAP Web Service API (As per current Peppol specification)
2) Digital Locator Service (DLS) which is an implementation of Intech Solutions Digital Location Server which implements the Australian Digital Business Councils Digital Capability Locator service http://digitalbusinesscouncil.com.au/digital-capability-locator/. It contains the following Interfaces:
    i. SML SOAP Web Service API (As per current Peppol specification) – this is created specifically to allow client-side compatibility with the CEF SML interface.
    ii. DLS REST Web Service API Interface
    iii. Operator Management GUI

7.5.3 Findings

- The registration services method described in this appendix is viable, however it ties Registry Services Operators to specific Party-ID Schemas.
- Tying the Party-ID Schemas to an RSO makes migrating from one RSO provider to another all but virtually impossible as there is only one RSO servicing the registry any given participant ID can use. This can be arbitrated by separating the RSO from the SML functionality and having participants work with an SML provider rather than an RSO provider.
- The DNS server selection needs to be done carefully as not all DNS Servers support the required functionality. In this trial, the following DNS software was used:
    - BIND – initially used with CEF SML, but proved problematic when CEF SML functionality was modified.
    - PowerDNS – used successfully, initially with DLS only, and then with DLS (via PowerDNS proprietary API) and then with CEF SML using NSUpdate.

If each Registry Service Operator solely updates the Registry that is delegated to it, the solution is secure. Notably, further work regarding security would need to take place to allow one Registry Service Operator to update records in a Registry operated by another Registry Service Operator.

7.6 Appendix F - Message Packaging Details[40]



Message identification, timestamp and other links.

Identification of communicating business partners.

Collaboration parameters, agreements, service info.

Other message properties with business relevance.

Manifest for payload elements.

SOAP body must be empty.

SOAP with Attachments MIME multipart is not required when there are no attachments.

[40] Adapted from eDelivery AS4 – 1.14 CEF Digital https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.14

7.7 Appendix G – BPC and Federal Reserve System Publications

The following BPC and Federal Reserve Bank e-Invoicing publications are available on the BPC website[41]:

- Overview of an e-Invoice Interoperability Framework (PDF) (2019)
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.
- e-Invoice Interoperability Framework – e-Delivery Network Feasibility Assessment Report (PDF) (2019)
Provides business and technology stakeholders with an understanding of the high-level requirements and standards required to establish an open, federated network of access points for the U.S. market.
- e-Invoice Interoperability Framework: Semantic Model Assessment (PDF) (2019)
Provides a comprehensive analysis of existing semantic data models to determine the feasibility, high-level requirements, and recommendations for the U.S. market.
- e-Invoice Interoperability Framework Assessment Report (PDF) (2018)
Report of the findings of a preliminary e-Invoicing Interoperability Framework assessment with an overview of the goals and approach used for the preliminary assessment along with key themes that emerged. The report includes recommendations and considerations for future BPC e-Invoicing efforts.
- Catalog of Electronic Invoice Technical Standards in the U.S. (PDF) (2017)
The Catalog documents the large number of electronic invoice technical standards that exist in the U.S. market, resulting in a fragmented market and interoperability challenges among the standards.
- U.S. Adoption of Electronic Invoicing: Challenges and Opportunities (Off-site) (2016)
U.S. corporations lag behind the rest of the world in adopting electronic invoicing solutions. This white paper by the Payments, Standards, and Outreach Group of the Federal Reserve Bank of Minneapolis highlights opportunities for businesses to gain efficiencies and reduce costs by more broadly adopting e-Invoicing.

[41] Documents cited here are available at businesspaymentscoalition.org, under e-Invoicing, Resources.

7.8 Appendix H – Resources Links

Business Payments Coalition
https://businesspaymentscoalition.org

ConnectONCE
https://connect-once.com

EESPA
https://eespa.eu/

Global Interoperability Framework (GIF), On route to Global Interoperability, The GIF Group
http://gifworks.io/

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

OpenPeppol
https://peppol.eu/about-openpeppol

7.9 Appendix I – References

AS4 Profile of ebMS 3.0 Version 1.0, OASIS Standard, 23 January 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 (BDXL) Version 1.0, OASIS Standard, 01 August 2017.
http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html

CEF Digital AS4.NET.
https://ec.europa.eu/cefdigital/code/projects/EDELIVERY/repos/eessi-as4.net/browse

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

CEF Digital eDelivery AS4 – 1.14 CEF Digital
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.14

Domain Name System.
https://en.wikipedia.org/wiki/Domain_Name_System

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

Holodeck B2B, BDXR Common.
http://holodeck-b2b.org/download/other-tools/

I*nternet Engineering Task Force (ITEF), RFC 2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000.*
https://tools.ietf.org/html/rfc2845

Internet Engineering Task Force (ITEF), RFC 2137, Secure Domain Name System Dynamic Update, April 1997.
https://tools.ietf.org/html/rfc2137

Internet Engineering Task Force (ITEF) – The MDS Message-Digest Algorithm, April 1992.
https://tools.ietf.org/html/rfc1321.

The Naming Authority Pointer (NAPTR) DNS Resource Record, September 2000.
https://tools.ietf.org/html/rfc2915

OASIS Business Document Exchange (BDXR) TC.
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=bdxr

OASIS ebCore Party Id Type Technical Specification Version 1.0, Committee Specification 01, 28 September 2010.
http://docs.oasis-open.org/ebcore/PartyIdType/v1.0/CS01/PartyIdType-1.0.html

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

OASIS Exchange Header Envelope (XHE) Version 1.0, Committee Specification 03, 13 December 2020.
https://docs.oasis-open.org/bdxr/xhe/v1.0/xhe-v1.0-oasis.html

OASIS Universal Business Language (UBL) TC.
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl

Service Metadata Publishing (SMP) Version 1.0, OASIS Standard, 01 August 2017.
http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html

Service Metadata Publishing (SMP) Version 2.0, OASIS Committee Specification 02, 16 January 2020.
https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/bdx-smp-v2.0.html

XML Signature Syntax and Processing Version 1.1, W3C Recommendation 11 April 2013.
http://www.w3.org/TR/xmldsig-core/