Remittance Delivery Assessment Report

An assessment of the feasibility of using exchange framework standards and technology to deliver electronic remittance information.

THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

BPC
Business Payments Coalition

Table of Contents

Glossary terms are colored green upon first use.
Please refer to Appendix 6.3.

1 Executive Summary

The U.S. payment system is undergoing vital modernization to meet the changing dynamics and demands of digital commerce. Modernizing business-to-business (B2B)[1] payments is essential for businesses to drive innovation, reduce resource-intensive manual processes and lower costs through increased automation and straight-through processing (STP) of invoices, payments and remittance information from start to finish.

At the heart of achieving straight-through processing is establishing the ability to exchange electronic documents between business accounting systems. While the U.S. payments industry previously struggled to identify a path forward, it has now made notable progress by establishing electronic document exchange frameworks. These exchange frameworks provide the infrastructure for businesses of all sizes to send and receive a wide variety of electronic documents with minimal changes to end-user systems. They also provide a platform for service providers,[2] financial institutions and software providers to expand their client services, including delivery of electronic remittance (e-remittance) information and automation of cash application.

As one example, the Business Payments Coalition (BPC)[3] has advanced its electronic invoice (e-invoice) exchange framework through its 2022 E-invoice Exchange Market Pilot ("E-invoice Market Pilot"), which provides a basis for broad adoption plans in 2023. Based on this industry progress, which addresses similar challenges with processing remittance information, the BPC, in collaboration with the Federal Reserve, launched the Remittance Delivery Assessment Work Group last year to determine the feasibility of applying this e-invoice exchange framework to deliver e-remittance information independent of the payment type. This effort leveraged talent and expertise from corporates, service providers, payment networks, financial institutions (FIs), industry and standards organizations and other industry stakeholders.

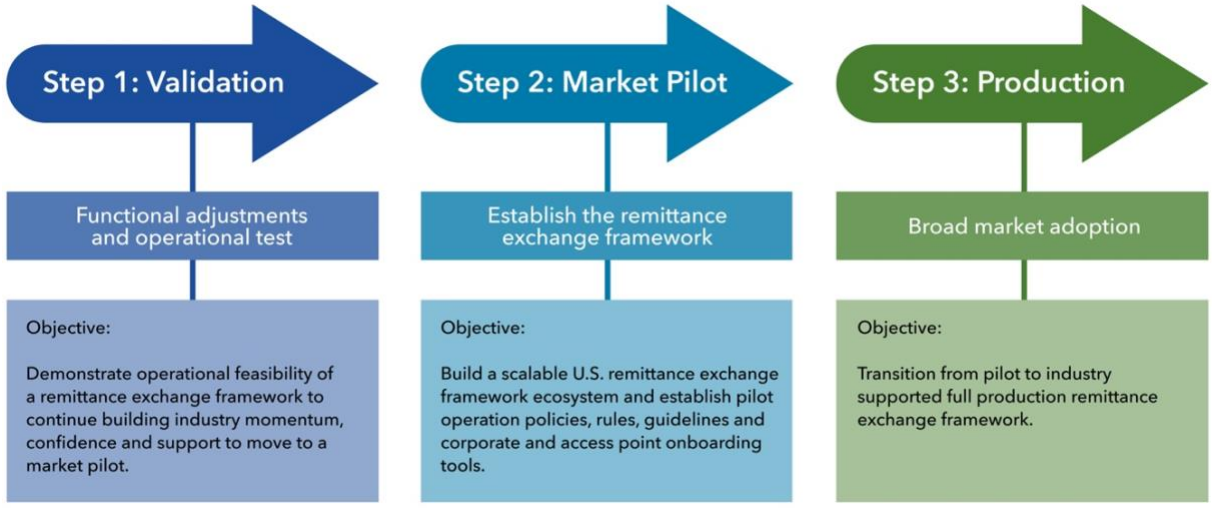
The work group assessed the core architectural components of the e-invoice exchange framework related to the requirements for delivering remittance information. This included: 1) the method of discovering the receiver's electronic address for sending remittance information, 2) the network communication standards for delivering the remittance information, 3) the data exchange standards, and 4) the concept of leveraging service providers as Access Points to facilitate the exchange with minimal changes to business accounting systems.

The assessment concluded that the e-invoice exchange framework provides a feasible solution to the challenges that have prevented effective electronic delivery and automated processing of remittance information. The work group further recommended the industry establish an exchange framework for remittance. To achieve this, the group endorsed a three-step approach that is similar to the way the BPC established its e-invoice exchange framework, as illustrated in the graphic below.

[1] Throughout this report, the term B2B should be interpreted expansively to include government entities and other organization types that interact for typical business functions.

[2] Glossary terms are colored green upon first use. Refer to Appendix 6.3.

[3] The BPC is a volunteer group of organizations and individuals working together to promote greater adoption of electronic B2B payments, remittance data and invoices. The BPC's wide-ranging goal is to make B2B electronic payments more efficient across the end-to-end process.



In the validation phase, participants will further define and operationalize framework adaptations for testing. These adaptations are primarily related to differences in data and security requirements, as well as business functions specific to remittance versus invoicing. The work group believes the framework can be readily adapted, but recommends further deliberation during the validation phase to determine the appropriate requirements.

Finally, the work group stressed the importance of maintaining momentum by rapidly transitioning to the validation phase in 2022. This first phase requires both collaboration among industry stakeholders and a strong understanding of proposed exchange framework fundamentals. Therefore, current work group members are ideal participants in the validation phase.

The industry momentum generated by the E-invoice Market Pilot makes now the ideal time to establish and advance market adoption of the framework for remittance exchange. Capitalizing on the core architectural components of the e-invoicing framework and leveraging the learnings from the e-invoicing market pilot could dramatically reduce the time to validate and establish a remittance exchange framework.

This report provides background on exchange frameworks and explains the Remittance Delivery Assessment Work Group's progress, conclusions and recommendations for establishing a remittance exchange framework.

2 Introduction

2.1 Audience

This Remittance Delivery Assessment Report is intended for U.S. business and technology stakeholders interested in advancing the electronic delivery of structured remittance information (not an emailed PDF) to facilitate process automation.

Business Stakeholders (Primary Audience)

- Individuals responsible for implementing and supporting accounting technology systems.
- Individuals responsible for identifying, defining and supporting business requirements for accounting technology systems that support accounts receivable (AR), accounts payable (AP) and electronic exchange of business documents.
- Individuals responsible for FI products and services that support remittance data for payments.

Technology Stakeholders (Secondary Audience)

- Individuals responsible for the design, implementation and support of accounting technology systems and solutions for electronic exchange of business documents.
- Individuals responsible for the design, integration and operational support of business applications that include AR, AP and electronic exchange of business documents.

2.2 Disclaimers, Copyright and Acknowledgments

Views expressed here are not necessarily those of, and should not be attributed to, the Federal Reserve System or any particular BPC participant or organization.

Readers are free to republish this report in whole or in part without further permission, as long as the work is attributed to the Business Payments Coalition and Federal Reserve, and in no way suggests the Federal Reserve System or 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 Federal Reserve and the BPC acknowledge the work of the Remittance Delivery Assessment Work Group and other contributors during the assessment process.

2.3 Background

Electronic delivery and automated processing of remittance information are essential to reducing payment application costs and improving overall electronic payment efficiency. Ideally, all remittance information would be sent within the payment message and passed on to the payee electronically. Unfortunately, there are many barriers to achieving that ideal state. Alternative approaches to enable electronic delivery outside the payment can facilitate automated processing.

Remittance information explains what the payment is for and any variances between the amount billed and amount paid. Historically, remittance information was included in a transmittal with the check for payment. Since the introduction of electronic payments, most remittance information is sent separately from the payment using emails or web portals. This requires manual processes to match remittance information with the payment.

The payments industry has struggled to find effective methods for businesses to send remittance information that facilitates automation and STP. To achieve effective system-to-system exchange for STP, an electronic delivery mechanism for the necessary data must reach the target business AR system in a structured format that can be ingested by the system for automated payment posting.

While e-remittance information can be included with some types of payments, such as by using ACH addenda, only a small percentage of B2B payments currently include structured remittance data that can be automatically processed. Simple remittance information (e.g., one invoice per payment, few adjustments) is suitable to flow within an electronic payment. Complex or voluminous remittance information (e.g., an extensive list of invoices paid, detailed exception information) generally cannot be accommodated by payment systems that limit the size of remittance information, so it needs to flow outside these payment systems. Additionally, independent of the complexity and volume of information, companies frequently have technical challenges that prevent sending remittance information with a payment.

These challenges can be solved with an exchange framework. This is an underlying infrastructure to exchange a wide variety of electronic documents for businesses of all sizes and types. The BPC has been working on an e-invoice exchange framework to address the widespread challenge of manual processes required when receiving invoices by paper, email and web portals. Likewise, a remittance exchange

framework could address similar challenges by facilitating delivery (including the receiver's electronic address), formatting requirements and reassociation of the payment with remittance information to achieve process automation. Additional benefits include standardizing remittance information across payment systems and addressing the need for business systems to generate and ingest remittance information.

A remittance exchange framework is not a payment system. It is intended to facilitate sending remittance information through a separate electronic delivery channel, not within an ACH or other payment message. Additionally, it is not intended to displace, replace or change solutions currently in place that already work well, such as B2B payment networks and electronic data interchange value-added networks (EDI VANs). However, it can complement and expand the reach of those solutions.

2.3.1 BPC E-invoicing Work

A 2019 BPC assessment of e-invoice exchange framework standards and technology concluded that a framework is feasible to exchange e-invoices in the U.S. market. Subsequent work in 2020 and 2021 further delved into existing semantic models, federated registry services and oversight requirements. This work confirmed that adaptations to the existing e-invoicing framework standards and ecosystems will accommodate U.S. requirements.

In 2022, the BPC formed the E-invoice Market Pilot Work Group to complete a pilot in preparation for full production in 2023. The market pilot will implement the U.S. market standards, technology and configuration, which will remain aligned with exchange frameworks in other regions of the world. More than 75 organizations are participating in the market pilot in various roles.

2.4 Objective and Scope

The Remittance Delivery Assessment Work Group was convened to assess the feasibility of applying the e-invoice exchange framework electronic delivery standards and architectural approach to delivering remittance information for all B2B electronic payment types. *Subsequent references to "exchange framework" throughout this report refer to the U.S. e-invoice exchange framework as documented in various BPC documents.*

The scope of the work included identifying and documenting:

- Gaps and adaptations required for the technical standards implemented within existing e-invoice exchange frameworks to support remittance delivery.
- Operational considerations required for establishing a remittance exchange framework.
- Recommended industry next steps.

Items out of scope included:

- Evaluating alternative solutions.
- Establishing detailed oversight requirements and approaches for a remittance exchange framework.
- Assessing the current International Organization for Standardization ISO® 20022 remittance data repository/data model for potential changes.
- Assessing approaches or developing plans to build broad market adoption.

2.5 Work Group Approach

The work group consisted of a diverse group of volunteer payments stakeholders, including FIs, service providers, standards development organizations, corporates, consulting firms and other interested parties. The work group took the following steps to complete its assessment:

- Education: Reviewed the basics of remittance information, e-invoicing framework architecture and standards to obtain a common understanding of exchange framework functions.
- Assessment: Identified and documented gaps and adaptations required for the framework to support remittance.
- Findings: Documented conclusions, resulting considerations and industry next steps to encourage U.S. market acceptance of the model.

The concept of an exchange framework, including the technology, standards and operational ecosystem, was new to most of the participants. Therefore, establishing a common understanding was the initial priority. This work group's first three meetings were dedicated to studying the architectural foundation, open-consensus standards and technology that enable the exchange framework ecosystem. Based on a shared understanding of these topics, sub-teams assessed each core component to determine its suitability for meeting the requirements to send remittance information. The core components consist of:

- Discovery: A methodology to facilitate dynamic discovery of where to send the remittance information.
- Delivery: The communication protocol and enveloping standards for sending the remittance information between two Access Points within the framework.
- Data: The data format used for exchanging remittance information between Access Points.
- Access Points: The exchange framework incorporates a four-corner network model, where service providers act as Access Points to facilitate translation and sending of the data between businesses to minimize or eliminate changes to business accounting systems.

The work group divided into two sub-teams to perform the assessments. Each performed deep-dive assessments of two of the core components, focusing on capabilities and limitations as they relate to requirements for sending remittance information. Each sub-team documented and voted on conclusions to assure consensus before presenting their findings to the full work group.

The assessment findings endorsed by the full work group are incorporated into this final report.

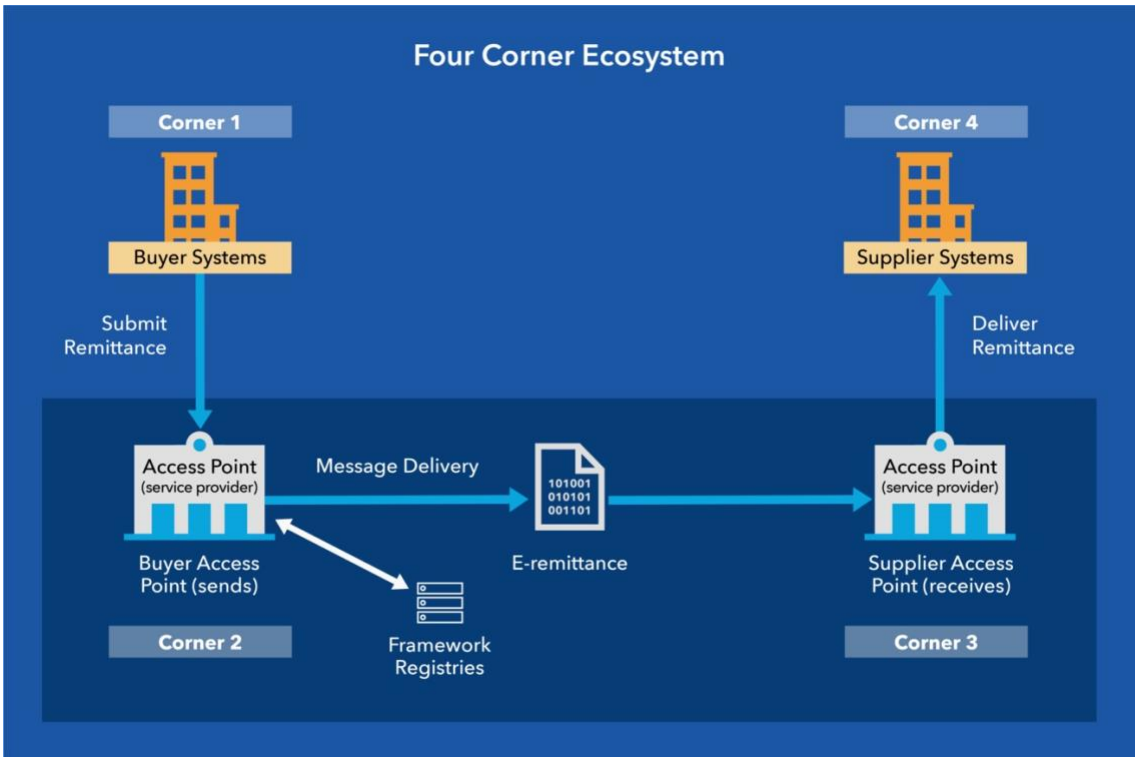
3 Exchange Framework Overview

This section provides an overview of remittance information delivery requirements and outlines how the exchange framework can contribute to efficient delivery of remittance information. For more information, see Appendix 6.1, Exchange Framework Details.

3.1 A Virtual Ecosystem

The exchange framework is modeled after the global email exchange service ecosystem and can be formed when industry stakeholders agree to a set of prescriptive open consensus standards, policies and guidelines for interoperability. To send and receive email, users sign up with an email provider – such as Gmail or a local internet provider. The email providers serve as Access Points into email exchanges to deliver emails between users over the internet using prescribed standards for interoperability.

Like email systems, the exchange framework enables businesses to connect once, then exchange information with any business on the virtual network, independent of the platform, system or applications used by individual participants. It is based on a four-corner ecosystem where service providers act as Access Points, send and receive electronic documents and perform the necessary data transformations to and from the data standard to minimize – or eliminate – the need for changes to business accounting systems. The network is considered virtual because it connects geographically and physically unrelated computers via the internet. Since it is independent of payment systems, it can deliver remittance information for all payment types. Service providers need to apply for, and receive, authentication certificates to become Access Points to send and receive electronic documents through the exchange framework.



3.1.1 Access Points as Enablers

Exchange frameworks consist of Access Points that operate under a collection of open-consensus standards addressing:

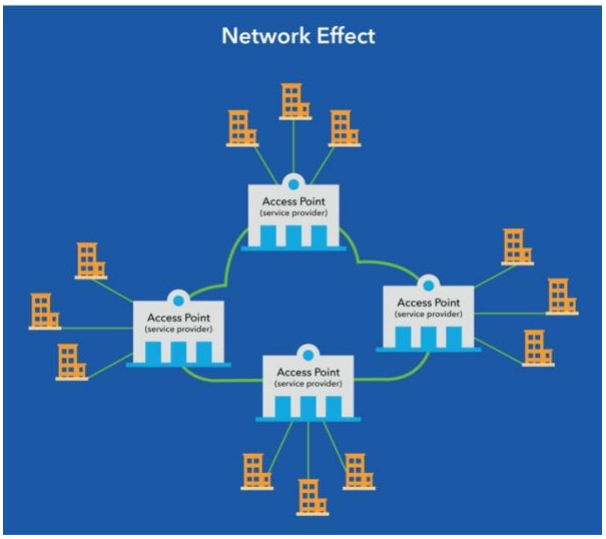
1. Discovery: how to identify where to send electronic documents.
2. Delivery: electronic delivery communication protocols.
3. Data: invoice or remittance data content.

Access points perform the “heavy lifting” for sending and receiving companies, including data transformations to and from the data standard and electronic delivery. Access points may be banks, AP providers, AR providers, B2B networks and individual businesses. They register clients into the network, map data to and from the exchange standard and deliver data using prescribed standards.

Because Access Points map and transform remittance information to and from the data standard (e.g., ISO 20022), there is minimal impact on businesses’ billing, AP and AR systems. In other words, those individual systems will require minor or no changes. Translation into structured data improves STP and reduces exceptions because all parties understand the data being sent and received.

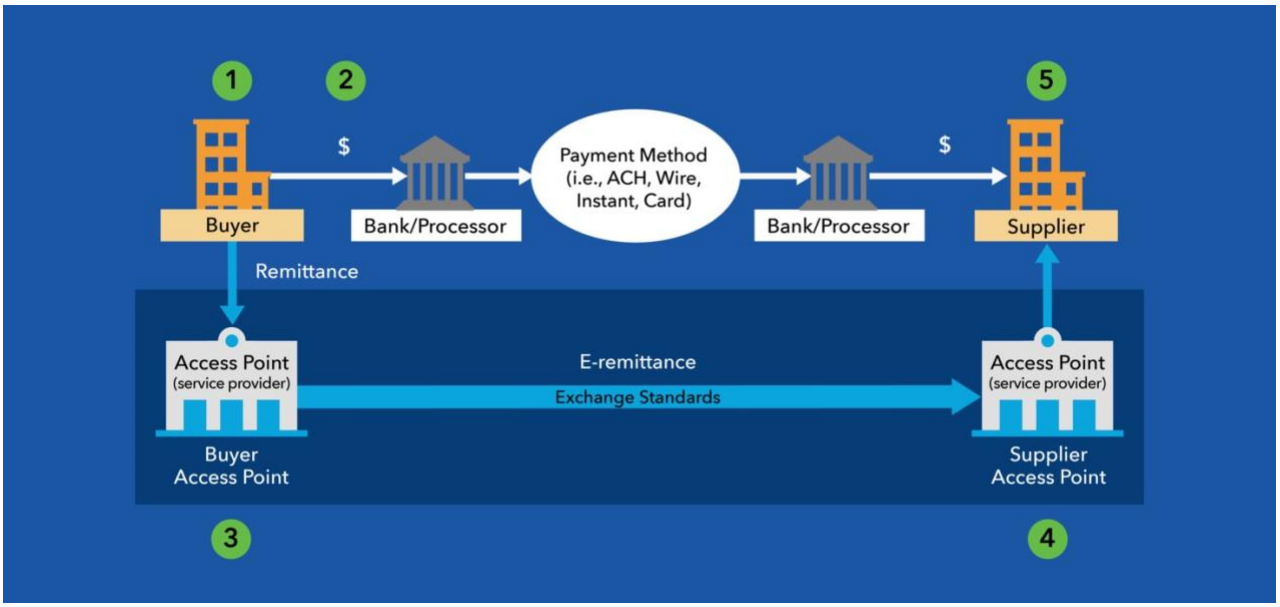
3.1.2 Network Effect

The value of an exchange framework ecosystem to any given participant increases in value when more organizations join – the classic "network effect." The framework expands the reach of existing solutions beyond their current ecosystem. Each time a new Access Point or business joins, a single connection enables sending and receiving electronic documents with all other registered Access Points and businesses. Maintaining fewer connections to and between providers also eases onboarding, implementation and development.



3.1.3 How the Exchange Framework Works

The diagram below illustrates that the exchange framework is independent of, and complementary to, existing payment systems.



First, the buyer (1) processes an invoice and pays through its preferred payment type (e.g., instant payment, ACH, card payment), as depicted in the top row (2). The payment system is not part of the framework. The buyer (1) also issues the remittance information and sends it to the Access Point in whatever format the buyer's system generates (3). The buyer's Access Point transforms the remittance information into the exchange standard format and delivers it to the supplier's Access Point (4). The supplier's Access Point converts the remittance information to the supplier's required format and sends it to the supplier (5). The supplier's system matches the remittance to the payment and applies the cash.

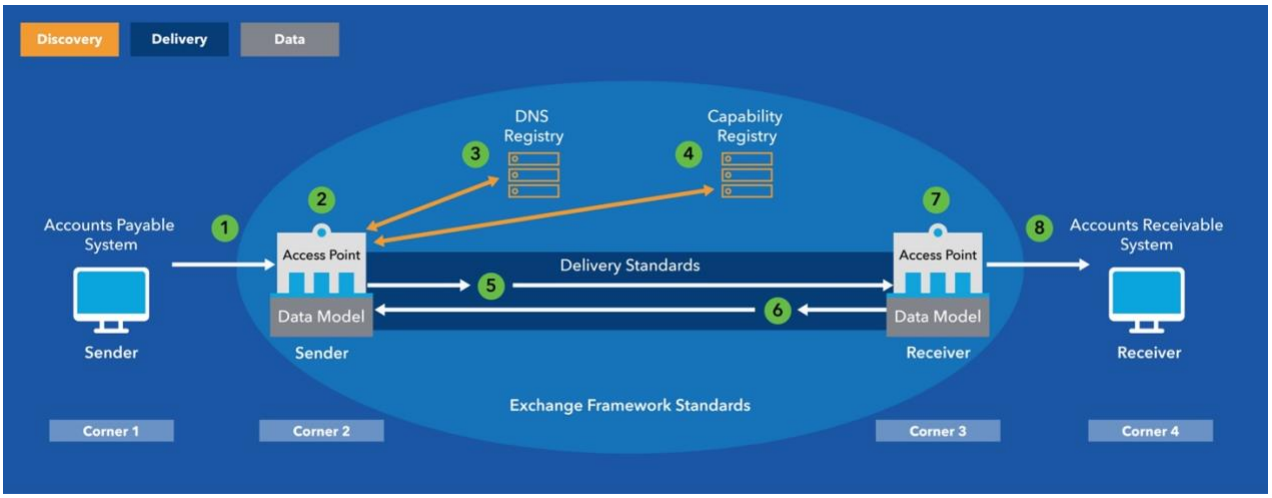
3.2 Core Operational Aspects

This section provides greater operational detail on how the exchange framework operates, showing delivery of remittance information as the document type. For more information, refer to Appendix 6.1, Exchange Framework Details.

Access Points tie various functions of the exchange framework together. This includes the ability to:

- Register their customers for sending and receiving.
- Leverage federated participant registries to dynamically **discover** the participants and delivery address.
- Map/transform remittance information to and from the **data** standard (e.g., ISO 20022) on behalf of clients.
- **Deliver** remittance information on behalf of payer and payee customers using framework delivery standards.

The following diagram illustrates the key aspects and steps involved in sending and receiving data.



Step 1: The AP system (corner 1) sends the remittance information to the Access Point.

Steps 2 – 5: The sender Access Point (corner 2):

2. Converts the remittance information to the data exchange standard.
3. Looks up the receiver (corner 4).
4. Looks up receiver's Access Point (corner 3) and capabilities.
5. Sends remittance to the receiving Access Point (corner 3) in the exchange standard format.

Steps 6 – 8: The receiver Access Point (corner 3):

6. Receives the remittance and sends confirmation of receipt to the sending Access Point (corner 2).
7. Converts the data to the format needed for the receiver's AR system.
8. Sends the data to the AR system (corner 4).

3.2.1 Discovery

Discovery provides the ability to dynamically (in real time) discover where to send a document to businesses served by other Access Points. The federated network of registries bridges individual registries so that businesses only need to register with one Access Point and are discoverable across the entire network.[4]

The exchange framework's discovery function was developed by the Organization for the Advancement of Structured Information Standards (OASIS) Business Document Exchange (BDXR) Technical Committee, which advances an open standards framework to support public e-procurement and e-invoicing. The discovery function was built to Business Document Exchange Location (BDXL) and OASIS Service Metadata Publisher specifications.[5] More specifically, the BDXL standard, generally referred to as Service Metadata Location (SML), specifies the access and use of the Domain Name System (DNS), and the OASIS Service Metadata Publisher (SMP) provides specifications for establishing a Capability registry. The terms DNS Registry and Capability registry used throughout this document refer to the SML and SMP functionality of those specifications. The combination of the DNS registry and the Capability Registry enable the search and discovery of Access Points and electronic delivery of a document.

Management of the registries can, but does not have to, be federated to avoid the need for a central operator. Federated management enables qualified providers to provide registry update services on a shared registry. The registries do not contain sensitive data. Rather, they have metadata to determine where to send electronic documents, Access Point capability information and corresponding end points. This metadata preserves the confidentiality of the customer-provider relationship and sensitive customer information.

The discovery process uses internet DNS technology and application programming interfaces (APIs) for queries. The DNS address in the registries map a company's identifier to a numeric internet routing address. The two registries in the exchange network accommodate a two-step discovery process as described below.

1. Query of business end point participants: The DNS registry enables look-up of a receiving end point participant to find the Access Point serving that entity. The query returns the Access Point's address in the Capability registry.
2. Query of Access Points: The Capability registry contains the capabilities of Access Points and business end points, as well as the DNS routing address of the receiving Access Point. Capabilities include data standards supported and the types of documents Access Points and end points can receive, such as invoices, remittance information and pass-through data.

To support security and privacy, business end users can restrict message delivery by setting permission levels for access as open, conditional or pre-authorized. Open discovery allows all transactions and document types from any sender. Conditional discovery allows receiving end points to limit the transaction and document types they accept. Pre-authorization allows receiving end points to set limits on the sending end points from which they will accept information.

[4] Businesses have the option to use multiple Access Points to support different business units or functions (for example, for invoices versus remittance information).

[5] See OASIS Business Document Exchange Location (BDXL) v1.0 and OASIS Service Metadata Publisher (SMP) v2.015]

3.2.2 Delivery

The exchange framework supports secure message delivery. The standards leverage a network infrastructure that is robust and secure, while ensuring end-to-end message delivery between the sending and receiving Access Points.

The network uses the Applicability Statement 4 (AS4) transmission protocol to create connections between end points to deliver the message payload, such as remittance data. Exchange Header Envelope (XHE) technology standards provide a secure technical container (a structured header) that contains the embedded message. The AS4 transmission protocol and XHE enveloping technology are specified by the OASIS AS4 Interoperability Profile for Four-Corner Networks Version 1.0.[6]

Access Points are authenticated using digital certificates. The standards support encryption for both documents and the delivery channel between Access Points. End-to-end message encryption is available for business end points.

The network is scalable to support a large number of connected parties and high-volume messaging throughput of exchange transactions and has the capability to support and transmit large multi-part business document messages with attachments.

3.2.3 Data

Data standards establish a common understanding (semantics) of the data exchanged between the Access Points. Businesses use many different accounting, AR and AP systems that have proprietary formats and data definitions. The standards provide the "semantic map" that allows Access Points to bridge between various formats and definitions used by the business sender and receiver.

Data standards currently used for remittance information include ISO 20022, EDI 820 and other industry-specific standards. ISO 20022 for payments is rapidly emerging as the global standard for payment systems, and includes a robust data model for remittance information. EDI 820 (Payment Order/Remittance Advice) has the electronic data interchange format and data for payment initiation and remittance advices. EDI 820 (and the shortened STP 820) are mature and commonly used for ACH remittance information. An industry-specific example is EDI 835 (Electronic Remittance Advice), which is well established for healthcare claim payments.

The ISO 20022 standard is recommended for the remittance exchange framework. The Access Points will translate AP, AR and other data formats into the required standard on behalf of end points. End points also have the option to pass through other industry-specific data standards by agreement between themselves without translation by Access Points.

[6] See AS4 Interoperability Profile for Four-Corner Networks Version 1.0

3.3 Use Cases and Benefits

A remittance exchange framework offers participants a variety of roles, use cases and benefits. Roles include providing Access Point services, partnering with other Access Point providers or simply sending and receiving remittance information to Access Point service providers. Several participant use case examples below illustrate the possible roles of enterprise resource planning (ERP) providers, FIs, financial institution technology providers, lockboxes and businesses.

Access Point providers: Service providers acting as an Access Point are the key facilitators of exchange frameworks. They can expand services for their business clients, including:

- Sending and receiving remittance data.
- Automating a cash application on behalf of clients.
- Adding new document types for existing clients – for example, sending and receiving remittance information for existing e-invoice customers.
- Extending their reach, and thus their value to their clients, by sending and receiving remittance data to and from any business in the virtual network.

Examples of providers that are good candidates to serve as Access Points include, but are not limited to, integrated receivables providers, lockboxes, integrated payables providers, B2B networks, EDI providers, FI technology providers and FIs.

FIs, ERPs and other providers: FIs, ERP systems, providers and other payments stakeholders can serve as Access Points or choose to partner with other Access Point providers. They already may have relationships with Access Point partners, such as FI technology providers and lockboxes.

Examples of additional services FIs can provide include integration of remittance delivery with existing products and/or offering a standalone service for treasury management clients and small to mid-size businesses that send and receive ACH payments. ERP providers can integrate remittance delivery into their AR and AP software as an additional service.

Businesses: Businesses may have an existing provider that offers Access Point services. The greatest value of the framework is for businesses to receive structured remittance data for an automated cash application. Access Points facilitate STP by transforming the data into the AR system format and sending it to the AR system. If a business uses an integrated receivables or lockbox provider that is an Access Point, the remittance information can be incorporated into existing data files. Business end users also can use the framework to send remittance data from their AP systems. A business would send a file of remittance advices (e.g., for generating emails) to its Access Point, which then transforms the information to the data standard and sends it over the network to the recipients.

Businesses can have a consistent remittance process regardless of payment type. They can exchange e-remittance data with a greater number of counterparties because they have access to all other businesses in the network, which can substantially reduce the number of portals a business needs to use to send or receive remittance information. Businesses also will have fewer payment exceptions because of better-quality data.

4 Exchange Framework Assessment for Remittance Delivery

This section summarizes the assessment of whether the primary components of the exchange framework (discovery, delivery, data and access model) can meet the needs for remittance information delivery.

The assessment consisted of identifying the extent to which each component of the exchange framework met the requirements for delivering remittance information and whether there were gaps or adaptations necessary. For each requirement assessed, the group applied one or more of the following result classifiers:

1. **Gap**: a gap in functionality was identified.
2. **Adaptation**: the capability is supported but implementation adjustments are required.
3. **Further testing needed**: a change or enhancement to the framework needs to be further tested to confirm the capability as it applies to remittance.
4. **Recommended next steps**: require further definition or consideration in future work.
5. **Meets requirements**: capability meets the requirement and is currently supported by the exchange framework.
6. **E-invoicing working on a solution**: current work in process by the BPC E-invoice Market Pilot can be leveraged in its entirety or provide a foundation for the remittance exchange.

4.1 Summary of Findings

The work group concluded that there are no capability gaps in the exchange framework that need to be addressed before the industry can establish a similar framework for remittance. The exchange framework specifications accommodate the exchange of any document type, including remittance documents. While some operational, security and oversight considerations need to be addressed, the work group believes these operational adaptations can be readily achieved using the existing exchange framework technology, standards and operational model. The adaptations and other considerations are primarily related to differences in data requirements and operational functions of remittance versus invoicing.

A key adaptation relates to the exchange format for sending data, one of the three core sets of standards within an exchange framework. The ability to add support for sending new data models or electronic documents is an inherent capability and objective of the exchange framework architecture. The remittance exchange framework will need to implement a remittance-specific data model. The work group's recommendation to use ISO 20022 as the primary data exchange format can provide rich remittance data that meets AR needs, enables STP and reduces payment processing exceptions.

The assessment of the discovery and delivery components determined that the registry and delivery standards are based on well-accepted international standards that can meet the security requirements for sending remittance information. The assessment did not determine if the e-invoice delivery security settings selected would meet the requirements for remittance information. The work group recommends additional discussion to determine the appropriate security configuration and authentication requirements for Access Points (security trust model).

The assessment further identified several additional operational considerations, including whether the remittance exchange framework should share common registries with the e-invoicing exchange framework and how various types of payments will be linked to the remittance information delivered through the network.

Finally, the work group noted the need to define an oversight authority and oversight requirements, including security governance, participant credentialing and framework participation agreement details.

A summary of adaptations and future work is included in section 4.6, Adaptations and Future Work.

4.2 Discovery Assessment

Discovery refers to the addressing infrastructure which allows Access Points to locate end-point business receivers and discover their capabilities. In short, this involves the ability to use a query to identify where to send an electronic document within the exchange framework. The work group assessed whether the discovery technology and specifications of the exchange framework are directly applicable to a remittance exchange framework. In particular, the assessment focused on the design of the DNS and Capability registries, which contain metadata that enable identifying (discovering) the electronic delivery instructions for the remittance information's target recipient.

4.2.1 Overview of Findings

The work group did not specifically study the OASIS registry standards but rather, invited technical experts to describe how they were implemented in the e-invoice exchange framework. After these discussions, the work group concluded the following functions are suitable in their current form for a remittance exchange:

- **Remittance-related data in the DNS and Capability registries:** The DNS registry, method to identify participants on the exchange framework and method to identify information on the Capability registry support remittance data.
- **Discovery API registry queries:** The APIs can support remittance registry queries.
- **Organization identifiers in the registries**: Organization identifiers issued by pre-approved bodies, such as DUNS, are appropriate for remittance.

No capability gaps were identified within the discovery design architecture. However, the following areas need to be addressed within the implementation specifications, which are referred to as adaptations in this document:

- **Remittance-related data in the DNS and Capability registries:** Add a remittance document type identifier to indicate remittance data will be exchanged and include information about which data standards are supported by Access Points and end points.
- **Conditional discovery:** Review and further consider policies for how to implement conditional discovery (allowing end point companies to specify what types of documents they can receive and at their option, restrict senders).
- **Sharing registries with e-invoicing:** Consider the potential to share the DNS and Capability registries with the e-invoicing framework.

4.2.2 Discovery Assessment Details

Remittance-related data in the DNS and Capability registries

Classifications: Adaptation, further testing needed, recommended next steps

The DNS registry, which contains participant identifiers and Capability registry look-ups, does not require modification for remittance. However, several remittance-specific requirements will need to be implemented within the Capability registry, such as the remittance document type identifier to indicate remittance data will be exchanged and information about which data standards are supported by Access Points and end points.

Currently, OASIS specifications for exchange frameworks use Universal Business Language (UBL) for the data exchange syntax. The work group recommends ISO 20022 syntax rather than UBL be used for the remittance exchange syntax, as the former indicates the global direction for payment messaging standards. In addition, the work group recommends supporting two data exchange options: (1) transforming received remittance data into the ISO 20022 exchange format, and (2) sending remittance data using other key standards as a pass-though. The latter will enable support for EDI 820 and other

well-entrenched, widely used remittance standards. Providing this choice will require businesses to indicate a data standard that their systems already support. However, it is recommended that the pass-through functionality be discouraged in general – and supported only in cases where a specific industry vertical/segment has well-established, entrenched remittance data standards that are supported by a large percentage of the sending and receiving businesses.

For additional details on data recommendations and data model conclusions, refer to section 4.4, Data.

Discovery API registry queries

Classification(s): Meets requirements, further testing needed

The discovery APIs currently available can support remittance queries to both the DNS and Capability registries. However, testing of the additions to the Capability registry will be required to confirm their effective operation.

Conditional discovery

Classification(s): Meets requirements, recommended next steps

The exchange framework supports conditional discovery with optional rules in the Capability registry, allowing end users to add restrictions on information delivery by setting permission levels. As an alternative to conditional discovery rules in the registry, end points could direct their Access Point to reject remittance messages and include a business response message with the reason. While this alternative would reduce the amount of information required in the Capability registry, it would increase the number of business response messages.

The trade-off between open versus restricted discovery relates to end point control versus accessibility and adoption. The E-invoice Market Pilot started with an open approach to test discoverability. However, it will support restricted discovery in production. Conditional discovery is a potential requirement for remittance stakeholders that should be addressed in future governance discussions.

Organization identifiers in the registries

Classification(s): Meets requirements, recommended next steps

Organization identifiers in exchange framework registries are used to look up participating businesses. Each end point participant chooses an organization identifier, which their Access Points register and assign a routing address in the DNS registry. The registries also support corporate hierarchies – legal name and Doing Business As (DBAs) – by assigning unique identifiers to each entity within a hierarchy. Business participants also can have different identifiers for different business functions, such as remittance information versus invoicing. Participating businesses provide their identifiers to the appropriate trading partners.

The DNS registry accommodates the use of multiple organization identifiers, in part because no one global standard organization identifier has widespread adoption. While the exchange framework does not designate a preferred organizational identifier type, it limits identifiers to those issued by pre-approved organizations, such as Global Location Number (GLN), Legal Entity Identifier (LEI), Data Universal Numbering System (DUNS) and Employer Identification Number (EIN). Each issuing organization ensures the uniqueness of identifiers within its system and the identifier type is included to assure uniqueness within the exchange framework.

Organization identifiers allowed by the e-invoicing framework were deemed sufficient for a remittance exchange framework and should be used instead of proprietary identifiers. However, the work group agreed that EINs are not a best practice for remittance because they are specific to domestic companies

and publishing EINs can increase fraud risk. If necessary, exchange framework oversight could address any additional identifier requirements.

Sharing registries with e-invoicing

Classification(s): Recommended next steps

The DNS registry model is flexible and registry information requirements for remittance and invoicing are sufficiently aligned that the remittance and e-invoicing network could share registries. Benefits would include reduced duplication of infrastructure and increased efficiency for Access Points that support both domains.

The Capability registry contains technical information about data standards and documents supported by the receiving Access Point, such as the remittance standard(s) and e-invoicing document types. The OASIS SMP standards were designed to enable support for many document types within a single exchange framework. Accordingly, the Capability registry can support both invoicing and remittance requirements in a single structure.

The work group recommended that future initiatives address oversight and technical implications of sharing registries.

Discovery oversight

Classification(s): Recommended next steps, e-invoicing working on a solution

The work group identified the following discovery oversight considerations for the future:

- Access Points populate the DNS and Capability registries when onboarding new end points and make periodic updates as required. This function is built into the exchange framework oversight. A future work effort should determine if the requirements and process for maintaining the registries meet the requirements for a remittance exchange framework.
- Oversight of the e-invoice exchange framework should include policies for vetting and governance of registrars and Access Points. A future work effort should determine if the requirements and process are suitable for remittances.
- All registrars and Access Points in the exchange framework are required to execute a participation agreement. A future work effort will need to determine the appropriate language for a remittance exchange framework agreement.

4.2.3 Discovery Topics Out of Scope

The following item discussed by the work group was determined to be out of scope.

Agreements

Commercial agreements between business end points and their service providers are out of scope for the framework.

4.3 Delivery

The message transport protocol, or delivery specifications, of a business document exchange framework allows Access Points to exchange business documents using one or more transport protocols. In the exchange framework, electronic documents are delivered securely over the network by Access Points using the AS4 transmission protocol and XHE enveloping technology.

4.3.1 Overview of Findings

The work group concluded that current delivery technology and capabilities specified by the framework (the AS4 transmission protocol and XHE enveloping technology) meet the requirements for remittance information exchange.

No functional gaps or necessary adaptations were identified. The following functions are suitable for remittance in their current form:

- **Non-repudiation of message delivery:** The transport-level response is appropriate for remittance.
- **Validation of business end points:** Business end points for remittance data will be subject to Know Your Customer (KYC) vetting before they may participate in the network.
- **Authentication of participants:** All Access Points must be authenticated before network connections are allowed.

However, the following should be further defined and/or tested:

- **Network response messages:**
    1. Develop rules for and content of network message-level responses related to compliance with the data standard.
    2. Define best practices for business response messages, such as rejection of a remittance message by the receiving end point due to incorrect information.
- **Delivery standards and encryption:** Determine the level of security and encryption to be implemented within the delivery standards for remittance.
- **Risk-based policies for message acceptance:** Establish framework policy for Access Point connections based on the geographic location of senders and allow/disallow lists.
- **Access Point provisioning:** Determine remittance-specific policies for Access Point provisioning/credentialing.
- **Remittance message virus screening:** Determine framework policies for virus screening of additional payload attachments and links included in the payload message.

4.3.2 Delivery Assessment

Network response messages

Classification(s): Meets requirements, recommended next steps, e-invoicing working on a solution

1. The exchange framework includes several types of status and informational messages to support data exchange. One is a *message-level response*, which acknowledges that the message format is valid and in accordance with the data standard. The framework has options for the content of this response message and determining when it is mandatory. A future work effort should define these options specifically for remittance.
2. Another message is a *business response message,* which indicates if a message is accepted or rejected by the receiving end point and includes the rejection reason. This message is sent by the receiving business to the sending business. Reasons for remittance business responses include an unauthorized deduction or incorrect invoice number. Because remittance-specific

business response messages have not been defined, a future work effort could develop best practice guidance for common, consistent messages.

Non-repudiation of message delivery

Classification(s): Meets requirements

The non-repudiation of messages between sending and receiving Access Points is provided by a mandatory transport-level response that includes an AS4 hash function to show the message was received.

Validation of business end points

Classification(s): Meets requirements

Access Points are responsible for KYC vetting before registering businesses on the framework. Registration services include submitting the identifiers and capabilities required to be added to the registries.

Authentication of participants

Classification(s): Meets requirements

Authentication takes place when one Access Point connects to another. The exchange framework uses x.509 public key infrastructure (PKI) certificates issued by a designated certificate authority for the framework.

Delivery standards and encryption

Classification(s): Meets requirements, recommended next steps, e-invoicing working on a solution

The framework specifies security standards between Access Points. It does not establish security requirements for communication between sending or receiving businesses and their Access Point. The Access Points are responsible for establishing security protocols that meet the requirements of their end point customers.

The envelope technology used in the exchange framework supports a range of security levels and encryption within the AS4 and XHE standards that can meet security requirements for remittance. The final security policy and settings for the remittance exchange framework will need to be determined when the exchange framework oversight is established. All Access Points would be required to comply with the security policy.

Other frameworks have published their security and encryption algorithms. Peppol uses the Advanced Encryption Standard AES-128 encryption algorithm with Galois/Counter Mode (GCM). The exchange framework uses AES-256 with GCM, which is recommended by the National Institute of Standards and Technology (NIST) and approved for military applications in the United States.

The work group recommends that the remittance exchange framework consider other broader security controls within the security policy, such as the Payment Card Industry (PCI) and NIST security guidance frameworks. The work group considers these broader controls outside the scope of the exchange framework. In general, the more controls, the higher the barrier for network adoption – and the fewer controls, the less secure the network. Considerations for a remittance framework include facility security, SOC certification and NIST 800 standards.[7]

[7] NIST's Special Publication (SP) 800 series covers guidelines, recommendations, technical specifications and annual reports of NIST's cybersecurity activities. The publications are developed to address and support the security and privacy needs of U.S. Federal Government information and information systems and may be voluntarily adopted by non-Federal entities.

Risk-based policies for message acceptance

Classification(s): Recommended next steps

The exchange framework does not enable individual Access Points to block the reception of e-invoices from other Access Points in the network. The Access Point KYC and vetting process before acceptance into the network is considered sufficient to address security concerns. Assessment participants raised a concern about the potential need to provide an option to block remittance messages from certain high risk geographic areas in a way that would not block legitimate senders. The policy could vary by market. For example, low-risk market connections could be accepted with one authentication step but higher-risk markets might require multiple steps.

A policy decision for consideration is allow/disallow lists of Access Points. If permitted by policy, an Access Point could have an allow/disallow list of other Access Points in accordance with its internal risk policies, so that each Access Point could choose to block connections from specific participants even if that participant has legitimate network certification. However, this type of policy would lessen the exchange framework's reach.

Access Point provisioning

Classification(s): Meets requirements, recommended next steps

All exchange framework participants require a certificate issued by the certificate authority in accordance with the framework's Access Point authorization criteria for joining the network. Framework policies determine to whom credentials are issued, and theoretically, an individual (private person) could become an Access Point. The remittance exchange framework will need to establish Access Point participation and registration policies and procedures that meet exchange remittance information security requirements.

Remittance message virus screening

Classification(s): Recommended next steps

Security controls to mitigate the inclusion of viruses, malware, spyware and other malicious code in messages were raised as a concern that should be further considered. Access Points also may need to verify message attachments and Uniform Resource Identifiers (URIs).[8] These requirements could be in scope within a remittance framework participation agreement and should be evaluated further.

4.3.3 Delivery Topics Out of Scope

The following items discussed by the work group were determined to be out of scope.

Additional validation of senders

A receiving Access Point may incorporate additional verification and gating of senders on behalf of an end point client. This is a business agreement between those entities and therefore, outside the scope of the framework.

Payment rejection

Since the remittance is delivered separately from the payment, rejection of a payment does not cause rejection of the related remittance. However, the remittance would not have a payment to match against. Handling payment rejections is a business process for end points and therefore, out of scope. Both the payment and remittance would be exception items for businesses to handle.

[8] Even if malicious content is not in the message itself, it could appear on the other end of the URI to be verified.

Theft of network credentials

Security procedures for addressing the potential theft of network credentials were not considered in scope of this technical feasibility assessment.

4.4 Data

Electronic document exchange frameworks are predicated on establishing a single exchange data model and syntax for each document exchanged within it. The OASIS electronic document exchange standards specify UBL syntax for sending data. The data model for each document type to be exchanged within the framework, which is unlimited, is defined by the stakeholder community intending to exchange the documents. For example, BPC stakeholders interested in establishing the U.S. e-invoice exchange framework defined the e-invoice data model.

4.4.1 Overview of Findings

Establishing a primary data remittance model is vitally important for the framework to optimize operational cost efficiency for Access Points and support future interoperability with other frameworks in other parts of the world. The work group assessed remittance requirements for data models and standards needed to support remittance information exchange and determined ISO 20022 would be the most appropriate for the U.S. payments industry to adopt as the exchange framework standard.

The following capabilities met the requirements for remittance in their current form:

- **Data translation to and from ERP data models:** ERP data formats can be translated into the framework data model.
- **Additional files in remittance message:** Additional binary files, such as PDFs and spreadsheets, can be sent within remittance messages.
- **Pass-through remittance data:** Pass-through of remittance data between end points without translation into the primary data standard is supported.
- **Encryption of messages by end points:** Messages can be encrypted from end-to-end between business end points.

The following items require further definition and testing:

- **Primary data model:** Establish the ISO 20022 syntax and remittance data model as the exchange framework standard.
- **Alternate data models:** Support the pass-through of select, widely used alternate data models, such as EDI 820.
- **Industry-specific data extensions:** Include support for industry-specific extensions of the data model to expand the adoption of the framework.
- **Data integrity – validation against the schema**: Implement a schema validation for the remittance data standard.
- **Absence of structured data in a remittance message:** Determine changes needed for messages sent without structured remittance data when binary files are permitted.
- **Linkage identifiers:** Test the ISO 20022 mechanism that links a payment to a separate remittance message and establish best practices for linking remittance messages to different payment types.
- **Updates to data standards and compliance with data models:** Determine policies for updates of the exchange data standard and restrictions on customization of the model(s).

4.4.2 Data Assessment

Primary data model

Classification(s): Adaptation, further testing needed

ISO 20022 will be the primary remittance data standard to be supported by all Access Points due to its widespread global adoption by the financial community. The data model has common core remittance data elements and is maintained outside the framework. The ISO 20022 syntax varies from the standard UBL syntax adopted in existing frameworks. However, the Business Document Exchange Standards can accommodate the use of other types of syntax within the XHE envelope. Access Points that deliver e-invoices or other documents will need to add support for the ISO 20022 syntax.

Alternate data models

Classification(s): Adaptation, recommended next steps

Support for additional data models will be considered to encourage broader initial adoption of the framework. Alternate data model standards should be limited to reduce network complexity and Access Point support requirements. However, the EDI 820 Remittance Advice is worth considering as an additional data model candidate because it is a well-established, mature standard widely used for remittance data. Adopting EDI 820 in addition to ISO 20022 would allow industry verticals and/or companies to leverage the framework's transport infrastructure and continue to use a standard widely supported by business end points. While support for this capability is recommended, broad use of alternative data models is discouraged because it could delay adoption of the primary standard and negate the primary benefit of the exchange framework. The policy for this capability should be further assessed by the remittance exchange oversight.

Industry-specific data extensions

Classification(s): Recommended next steps

The framework addresses industry-specific needs through data standard extensions. Extensions are data standards added to the base data model that Access Points can support. By mutual agreement, sending and receiving business end points can use industry-specific standards in pass-through data that is not translated by the sending and receiving Access Points. For example, the EDI 835 Electronic Remittance Advice is a widely used, mature standard in the healthcare industry.

Data translation to and from ERP data models

Classification(s): Meets requirements

Individual ERPs – for example, SAP and QuickBooks – have their own data models. Many ERPs and accounting systems are in wide use, and sending and receiving business end points are likely to use different systems. Access Points overcome variations in ERPs' data models by translating ERP data to and from the exchange standard, as needed. This data translation reduces many-to-many ERP mappings between Access Points and assures the exchange framework is ERP-agnostic.

ERP software vendors could provide valuable assistance to Access Points in mapping and testing.

Additional files in remittance messages

Classification(s): Meets requirements

Excel files, PDFs, images and other binary file types are common additional means to transmit remittance information and important to support small businesses. Binary files in the message payload are currently supported by the framework using XHE enveloping technology.

Data integrity – validation against the schema

Classification(s): Adaptation, further testing needed

Data should not be truncated or otherwise compromised. A schema ensures integrity of data according to the data model, such as Extensible Markup Language (XML) or EDI.[9] The sending and receiving Access Points are responsible for validating data integrity against the schema of the standard. The framework supports an "invalid message" response by the receiving Access Point when the message format is invalid. Schema validation for the remittance data model needs to be developed.

Absence of structured data in a remittance message

Classification(s): Adaptation, recommended next steps

The framework supports sharing of additional file types (Excel files, PDFs, images and other binary file types) in the message envelope along with the structured data. It assumes the structured data always is delivered even when other file types are included. Although ISO 20022 remittance data enables both structured and unstructured remittance data, the exchange framework assumes additional files are sent in conjunction with the primary structured messages. The requirement to support sending files without inclusion of the primary structured message is not currently supported and would require further definition in a future work effort.

Linkage identifiers

Classification(s): Further testing needed, recommended next steps

A linkage identifier is a data element included in both the payment and remittance data that links an electronic payment with a separate e-remittance message. A unique identifier is required for automation of matching payments with remittance information sent through a separate channel from the payment.[10] Different agreed-upon mechanisms in the framework can link the remittance message to the payment. The receiving end point uses a linkage identifier to link the payment to the remittance message delivered through the network. *This linking function resides outside the network*.[11]

Examples of current linking mechanisms include a unique ISO 20022 Remittance Identifier for ISO 20022 payments and a healthcare industry standards trace number that appears in an ACH payment addenda record and related EDI 835 remittance message. The ISO 20022 linking mechanism should be tested in future work efforts. As the linkage function occurs outside the network, testing would be the responsibility of end points and their Access Points.

Consistent remittance information can be delivered over the network for all payment types. A future work effort should develop best practices for populating linkage identifiers in different payment types, considering payment formats and available data elements. For example, ACH payments could link the remittance message by populating the unique ISO 20022 Remittance Identifier in the ACH addenda and separate remittance message.

---

[9] An XML schema defines elements in an XML file and a specific structure for XML data, which is important when sharing files between multiple systems.

[10] The payer populates the payment and remittance information with a linkage identifier that is a unique value available from its accounts payable system (e.g., an electronic payment number). The value is unique to that payer only. When receiving the linkage identifier, the payee uses the combination of payer and identifier to match the payment to the remittance information. Because linkage identifiers are unique for each payer, there is no need to specify the payment type in the remittance data.

[11] The *ISO 20022 Remittance Content Market Guide*, published by X9, contains a detailed explanation and proper usage of the linkage identifier.

Pass-through remittance data

Classification(s): Meets requirements

When two business end points agree to use a specific standard for remittance data, this data can pass straight through the Access Points without translation into the primary data standard of the exchange framework. For example, an EDI 835 healthcare message can flow from the sending end point to the receiving end point without translation by Access Points. When end points agree to exchange non-standard pass-through data through the framework, both end points need agreements with their respective Access Points to send and receive the specific type(s) of data. The receiving Access Point would include the ability to receive EDI 835 messages in the Capability registry. Based on this, the sending Access Point would send the message through without translation.

Data encrypted by the sending end point also would pass through without translation, as the Access Points would not have access to the data. Pass-through information is important for remittance processing, and this capability is currently supported by the framework.

Encryption of messages by end points

Classification(s): Meets requirements

End-to-end encryption is required for some remittance messages. The two end points must coordinate to determine encryption methodology and keys. Access Points have no ability to transform data in end-to-end encrypted messages to the exchange standard on behalf of their customers.

The delivery architecture of the exchange framework can support end-to-end encrypted messages.

Updates to data standards

Classification(s): Recommended next steps

Standards for individual ISO 20022 messages are updated by the respective ISO 20022 Standards Evaluation Groups during their annual maintenance cycles. Updates to remittance data standards, such as ISO 20022 and EDI 820, are not expected to be frequent, even when other sections of the standards are updated more often. Typically, the process of updating standards ensures backward compatibility. The exchange framework governance authority will need to determine the standards version(s) supported and timetables for implementing standards version updates.

Compliance with data models

Classification(s): Recommended next steps

Compliance with data model(s) is key to ensure exchange framework interoperability and efficiency for Access Points and end points. Future work should consider governance-related compliance and customization policies.

4.4.3 Data Topics Out of Scope

Supplemental file alert

An alert from the receiving Access Point to notify the receiving business end point of additional files is not handled by the framework because all interactions between the Access Points and their direct customers occur outside the exchange framework. The message envelope indicates the number of files in the message. Therefore, the framework has the information needed to create a notification, but an alert is not part of the framework specifications. A supplemental file alert process should be handled either by business agreements between those parties, or as a best-practice recommendation by the exchange framework oversight.

Data irregularities

The framework is not designed to test for data irregularities in message content that may indicate fraud. This functionality could be a value-added service provided by an Access Point at its own discretion.

Security of embedded files

Security concerns about embedded files and links sent within messages are the responsibility of the receiving business end point, which can decide whether to trust the sending party and accept them.

Data elements included in the remittance information

The Capability registry does not itemize data elements the receiving end point wants to receive, as this is a business process outside the framework.

4.5 Access Points

Access Points, referred to as corners 2 and 3 in our framework, play a critical role performing the data translation and electronic delivery of documents in a four-corner network model document exchange framework. This section addresses implementation and operational requirements for Access Points in a remittance exchange framework.

4.5.1 Overview of Findings

The work group identified several support requirements for Access Points, as described below.

- **Access Point offline message:** Test how the exchange framework handles messages when a message is sent, but the receiving Access Point is offline.
- **Onboarding toolkit for Access Points and a test environment:** Revise the exchange framework Access Point onboarding toolkit for remittance and establish an Access Point testing environment for implementation and ongoing operations.
- **Data security:** Determine policies for remittance data security.
- **Real-time remittance messages:** Determine the process for Access Point support of real-time remittance messages.

4.5.2 Access Point Assessment

Access Point offline message

Classification(s): Further testing needed, meets requirements

The framework sends a connection rejection message from the offline Access Point when another Access Point tries to make a connection.

As part of the framework policy but requiring future testing, the connecting Access Point will retry for a set period of time after receiving a connection rejection message, and receive a receipt acknowledgement when the connection is successful.

Onboarding toolkit for Access Points and a test environment

Classification(s): Meets requirements, recommended next steps, e-invoicing working on a solution

Setting up an Access Point involves configuring and testing specified framework standards and tools. The time required to set up a remittance exchange framework Access Point may be reduced by leveraging the e-invoice exchange framework onboarding toolkit developed and tested in the E-invoice Market Pilot.

Establishing a test environment to support Access Point development also can support broad adoption of a remittance exchange framework. A test environment should include “test Access Points” for both the sending and receiving functions and support testing of software updates and end point onboarding.

Data security

Classification(s): Meets requirements, recommended next steps, e-invoicing working on a solution

The exchange framework uses standard secure delivery protocols to provide data transport security. The framework participation agreement specifies other data security policies for operational topics, such as data loss and data breaches, along with related participant responsibilities and liabilities.

Policies for remittance data security will need to be determined in the future. Topics might include required actions in the event of a data breach, policies for third parties, required data security and cyber insurance. Framework policies for data compromise should be communicated to end point clients.

Exchange framework agreements and policies can facilitate establishment of remittance-specific participation agreements.

Real-time remittance messages

Classification(s): Adaptation, recommended next steps

The network delivers messages in real time, but Access Points choose the timing for message delivery. An operational requirement for real-time remittance concurrent with instant payments would be an adaptation, and a future work effort would need to determine how Access Points can accommodate this message timing. Although most reconciliation by end points does not occur in real time today, this may be required in the future to support instant payments.

4.5.3 Access Point Topics Out of Scope

Payment initiation

Access points may offer bundled services that include payment initiation with remittance delivery. This is an additional value-added service, usually associated with integrated receivables and payables offerings. FIs also could process both payment and remittance information. Payment initiation and processing is out of scope of the framework, as payments travel on different rails.

Data translation and mapping services

The data model is integral to the framework. Access Points provide data model mapping services for sending and receiving business end points. Both financial and non-financial providers offer mapping services for businesses. Some service providers are "middleware agents" that map data on behalf of end points for various business functions. These could be ERPs, accounting service providers or other third parties.

Providers of services to small businesses may not offer as much automation as those that serve large businesses. Large companies may have internal development teams to handle mapping.

The business arrangement for mapping services is out of scope for the exchange framework.

Timing of message delivery to end points

The timing of delivery of remittance information between end points and their Access Points falls outside the domain of the exchange framework and should be addressed within service-level agreements (SLAs) between an Access Point and end point.

4.6 Adaptations and Future Work

This section summarizes necessary discovery, delivery, data and Access Point adaptations, as well as future work identified during the work group's assessment.

The following chart outlines adaptations to the exchange framework to support requirements for exchanging remittance information. Six are listed, but only three are required to get an operational framework up and running. The "R/O" column in chart below represents Required or Optional.

Adaptation	R/O	Category
Determine if any changes are required to the structure and data stored within the Capability registry to meet the requirements for the exchange of remittance information. Changes may require revisions to registry queries that support the e-invoice exchange framework.	R	Discovery, section 4.2.2
Implement ISO 20022 remittance data elements as the primary data model.	R	Data, section 4.4.2
Develop and implement schema validation to ensure integrity of data according to the data model.	R	Data, section 4.4.2
Determine support for widely used alternate data models, such as EDI 820.	O	Data, section 4.4.2
Determine framework policy for sending remittance information without structured remittance data when binary files are sent.	O	Data, section 4.4.2
Determine support requirements for real-time remittance messages between Access Points.	O	Access Points, section 4.5.2

The following items, although not adaptations, require definition or consideration for further work.

Recommended next steps	Category
Assess potential to share registries with the e-invoicing framework. This is a key operational decision that also has governance/oversight considerations.	Discovery, section 4.2.2
Define methods for linking specific payment types to the remittance message; key to achieving benefits of the framework. Some market precedents can guide this work.	Data, section 4.4.2
Develop a remittance-specific Access Point onboarding toolkit and guide. This is an important foundation to encourage adoption by Access Points.	Access Points, section 4.5.2
Make recommendations for remittance-specific business response messages, such as rejection of a remittance message by the receiving end point due to incorrect information. While best-practice recommendations are not required for an operational framework, they will assist with messaging consistency.	Delivery, section 4.3.2
Develop data standard extensions to support industry verticals or other specific needs. This is optional, but extensions need to be defined before being implemented.	Data, section 4.4.2
Determine policy for implementing conditional (restricted) discovery, which allows end users to add restrictions on delivery by setting permission levels. As the framework currently supports conditional discovery, this policy decision is not required for an operational framework.	Discovery, section 4.2.2

The following items do not require definition but do require testing for remittance information.

Further testing needed	Category
Create an Access Point testing environment for implementation and ongoing operations. This is an important foundation to encourage adoption by Access Points.	Access Points, section 4.5.2
Test the ISO 20022 mechanism that links a payment to a separate ISO 20022 remittance message. This is key to business end point automation.	Data, section 4.4.2

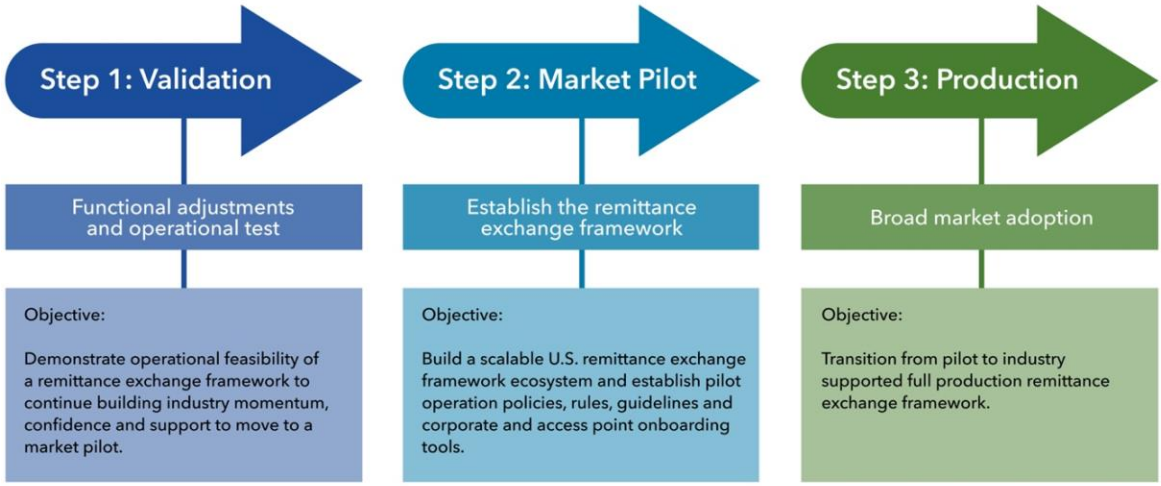
The following governance, oversight and/or policy items should be addressed. As most of these governance and policy topics also are relevant to the e-invoicing exchange framework, the work of the E-invoice Market Pilot can be leveraged to facilitate timely completion of the remittance work.

Requires future work for governance, oversight and/or policy considerations	Category
Develop remittance-specific governance and oversight of the framework, including policies on vetting, provisioning and credentialing Access Point participants.	Delivery, section 4.3.2
Determine the appropriate governance of registrars for the DNS and federated Capability registries.	Discovery, section 4.2.2
Develop the appropriate Access Point participation agreement for remittance.	All
Determine security levels and encryption to be implemented within the delivery standards for remittance.	Delivery, section 4.3.2
Determine policies and processes for updating DNS and Capability registries for remittance.	Discovery, section 4.2.2
Develop remittance message virus/malware screening policies.	Delivery, section 4.3.2
Develop rules for, and content of, network message-level responses for message compliance with the data standard.	Delivery, section 4.3.2
Develop policies for remittance data security and data compromises (Access Points).	Access Points, section 4.5.2
Confirm supported versions of the exchange data standard and the timetable for implementing standards version updates.	Data, section 4.4.2
Develop policies for compliance with data model(s).	Data, section 4.4.2

5 Conclusion and Recommended Next Steps

The work group found that an e-remittance exchange framework that is similar to the e-invoice exchange framework would be a feasible solution for delivering remittance information in support of straight-through processing. To succeed, the remittance exchange framework would need to incorporate rich structured remittance data using the ISO 20022 standard and provide a mechanism for data to travel to any payee connected to the network. The framework would need to offer service providers a secure way to deliver remittance information on behalf of their clients (end points). Access Points are key enablers, mapping and translating data to minimize changes to business AP and AR systems, which is vital for broad adoption by businesses of all sizes.

As next steps, the work group recommends quick transition to a validation phase to leverage momentum and potential synergies with the BPC's E-invoice Market Pilot. Swift testing of the concept can help build industry confidence and support for a remittance exchange framework market pilot. The work group suggests a three-step approach, illustrated below, to lead to a production-ready remittance exchange framework.



This approach is based on the success of the e-invoice exchange framework, which has provided valuable insight on how to achieve critical milestones and considerations for each step. The timing of these steps can enable the remittance work to leverage infrastructure components of the E-invoice Market Pilot, accelerating validation testing.

The primary technical objectives for the validation phase will include, but are not limited to:

- Establishing multiple Access Points.
- Integrating and testing remittance requirements into business discovery registries.
- Sending remittance information through the exchange framework from end to end.
- Integrating the ISO 20022 based remittance exchange data format.
- Testing payment linkages to remittance messages.
- Assessing other possible requirements and adaptations to determine other critical features, functions and capabilities that need validation before the Step 2 Market Pilot phase.

Validation phase results will be published with recommendations for a market pilot.

In summary, industry momentum generated by the E-invoice Market Pilot indicates this is the ideal time to advance remittance exchange framework market adoption. Leveraging core e-invoicing framework architectural components and learnings from the E-invoice Market Pilot could dramatically reduce the time to validate and establish a remittance exchange framework.

6 Appendices

6.1 Exchange Framework Details

Section 3 of this report contains an overview of the exchange framework. This appendix provides additional detail about exchange frameworks and the standards used. For further discussion of the standards and technical details, see the BPC e-invoicing reports:

e-Invoice Interoperability Framework – e-Delivery Network Feasibility Assessment Report

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

6.1.1 Description of the Payment and Remittance Flow

These diagrams illustrate the flow of remittance information sent separately from a payment. **One key difference of the exchange framework from the current state is that structured data is sent electronically so that it can be automatedly processed by all parties**.

Diagram on how remittance information currently is sent separate from a payment:

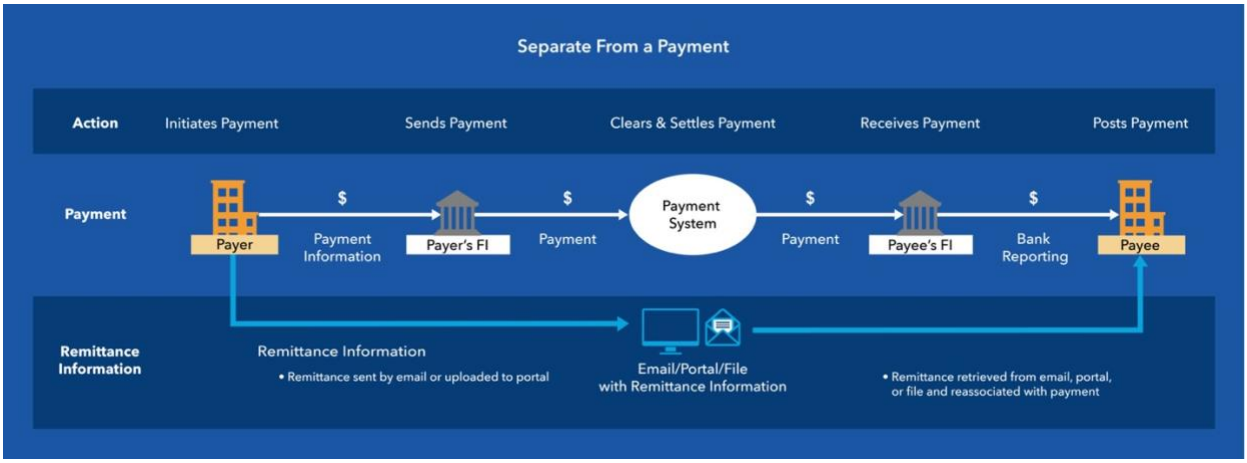
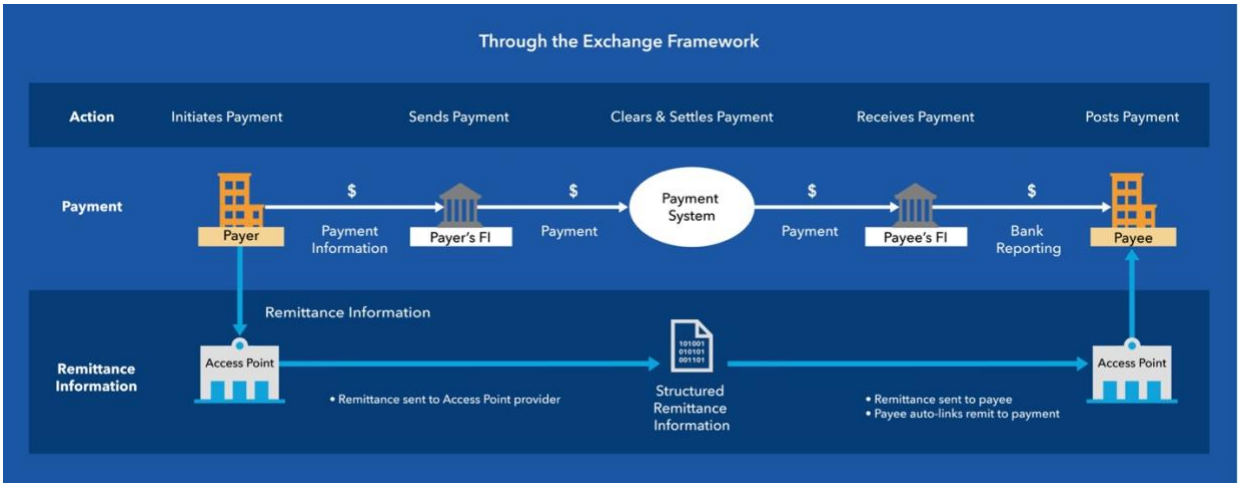


Diagram on how ISO 20022 remittance information is sent through the exchange framework:



6.1.2 The Discovery Function: Registries

Registries determine where to send data. Their important features include:

- Dynamic (real-time) discovery of all businesses in the network and the types of documents the business can receive.
- Confidentiality of business end point details.
- Permission levels for access. End users can set access as open, conditional (similar to call blocking on a phone) or pre-authorized (similar to call screening on a phone).
- Identifiers must support business entity hierarchies.

Discovery allows two registries to dynamically discover where to send a document for businesses served by other Access Points.

- The DNS registry contains all participants in the network. It is used to look up end points and find their entries in the Capability registry.
- The Capability registry contains the routing address of the Access Point to send the remittance data and the remittance data receipt capabilities of the Access Point and end point.

Registries are not databases or directories. Directories contain specific information about entities and enable all information from one source, while registries contain metadata or identifiers of end points and internet addresses of service providers.

- The identifier of a business must be known to look it up in the Capability registry.
- Metadata promotes confidentiality of business (end user) information and alleviates competitive concerns.
- Only the Access Point service provider has end point information and interacts with the end point.

The framework supports conditional (restricted) discovery, enabling end-user rules to be applied when receiving or sending transactions.

- Open: The receiving party is open to receive all classes of transactions and documents supported by the network and accepted by the recipient, from any trading party with a business relationship or any Access Point with access capabilities. This is analogous to a public phone number that accepts all calls. Open discovery can promote accessibility and adoption. However, business end points may have privacy and security concerns.
- Conditional: Open to any trading party with limitations on supported transactions, document types and processes. A receiver that only accepts remittance data is analogous to call blocking on a phone.
- Pre-authorized: Pre-authorization is required by the receiving end user and communicated directly or through its Access Point. This is analogous to call screening on a phone.

Federated: Registries are federated and may be hosted by Access Points or other registry providers. Individual Access Points register their clients as end points for sending and receiving data in the network. Federation bridges individual registries so businesses need to register with only one Access Point to be discoverable across the entire network. The federated nature helps keep data up to date and accurate because each registrar maintains information for its registrants.

DNS Registry: The DNS registry contains unique entity identifiers to locate business end users. Each entity and sub-entity has an identifier in the registry, such as an LEI, DUNS, Tax ID or Global Locator Number (GLN). No single identifier specifically is dedicated to use in the DNS registry.

Capability Registry: The Capability registry has two identifiers and capabilities of Access Points and end points:

- Electronic Address Identifier: address for document and message routing.
- Electronic Routing Address: service provider or receiving technical platform address.
- Capabilities: remittance standard(s) supported by Access Points and business end points.

Registry prescribed standards: The registries use well-established standards for registries.

- Domain Name System (DNS) standards.
- OASIS BDXR business document exchange standards for the DNS and Capability Registries, which support global interoperability and are most widely used for this type of exchange by procurement systems.
    - Open, non-proprietary standards for a registry.
    - The only prevailing international standard that exists for a real-time discovery process.
    - OASIS Business Document Metadata Service Location 1.0 (SML) and OASIS Service Metadata Publishing 2.0 (SMP) specifications.

Technology: Registries leverage internet DNS technology, similar to how emails are routed: the sender's email provider looks up where to send the email based on the email address.

- The DNS Registry is enabled by standard, mature DNS technology.
- Access Points use APIs to query the registries.

6.1.3 The Delivery Function

Access Points send and receive information on behalf of their end point clients, similar to the way email exchange service providers deliver email messages. The prescribed standards provide secure message delivery between Access Points.

The sending Access Point:

1. Integrates with the sending business end point's AP system to receive remittance information. The sending end point provides data "as is" from the AP system.
2. Uses standard discovery APIs to look up the receiving end point's Access Point identity, location and types of electronic documents the receiving end point can receive (e.g., e-remittance).
3. Maps/transforms the data into the remittance standard (e.g., ISO 20022).
4. Packages and delivers the e-remittance message in a secure envelope to the receiving Access Point. The envelope and delivery comply with prescribed standards for secure transmission.

The receiving Access Point:

1. Receives the message from the sending Access Point.
2. Checks the message's integrity against the data standard.
3. Maps/transforms data into the appropriate format for the receiving business end point's AR system.
4. Sends the remittance data to the receiving business end point. The receiver gets data in its current AR system data format.

Network delivery features include:

- Provides delivery assurance regardless of whether the receiving gateway is available at the time of delivery.
- Prevents duplication of messages and assures non-repudiation.
- Supports encryption for both documents and the delivery channel between Access Points.
- Supports encrypted end-to-end messages between businesses for remittance data and associated structured and unstructured documents and attachments.
- Includes trusted authentication procedures for Access Points using digital certificates.
- Is scalable to support large numbers of connected parties and high-volume messaging throughput of exchange transactions.
- Has the capability to support and transmit large multi-part business document messages (up to 50 MB or as otherwise agreed).
- Supports a range of response, status and servicing messages to permit a dynamic flow of information and asynchronous interactions.
- Preserves the confidentiality of customer information with data privacy protections.

Delivery Standards: Prescribed delivery standards consist of the AS4 transmission protocol and XHE enveloping technology.

Applicability Statement 4 (AS4) is a transmission protocol used to create network connections between end points to deliver a message payload, such as an invoice, remittance information or other business document. It brings together many existing standards for electronic data packaging, security and transport into a single specification. AS4 is becoming prevalent around the world for e-invoicing exchange frameworks.

XHE is a message envelope standard that assures message integrity and confidentiality. It includes the ability to send multiple documents in one message, attachments and response messages.

6.1.4 Data Standards

Data models establish a common understanding of the data exchanged between the Access Points. Established standards have a data model and prescribed format and syntax. The prescribed envelope is flexible to support different standards as the message payload.

The standard is used by the Access Points to deliver data between themselves. Business end points do not have to implement the data standard in their systems. Instead, Access Points transform, package and deliver remittance data to and from end point AP and AR systems into the required exchange format.

For remittance, the proposed preferred standard is ISO 20022, which is emerging as the international standard for new payment systems. If needed, the framework can support alternatives, such as EDI 820/STP 820, and industry-specific standards, e.g., healthcare, transportation or real estate.

ISO 20022 has a robust remittance data model and supports remittance messages with the following data categories and data elements to fully explain the payment.

Category Description	Details
Payment-level data (data in payment, not remit)	Payer and payee name and identifiers
Document type	Code for type, issuer
Document number	E.g., invoice number
Document date	E.g., invoice date
Amount due	
Discount	Type and amount
Credit note	Amount
Tax amount	Type and amount
Adjustment	Amount, reason, additional info
Remitted amount	
Creditor reference	Type, reference
Invoicer name	
Invoicer address	Standard address structure
Invoicer organization ID	E.g., LEI or other ID
Invoicer person details	Details of a person (vs. organization)
Invoicee name	
Invoicee address	Standard address structure
Invoicee organization ID	E.g., LEI or other ID
Invoicee person details	Details of a person (versus organization)
Document line-item details	Type, number, description, amount, discount, adjustment, credit note, tax, reasons, etc.
Additional remit info	Unstructured
Remittance identifier	For reassociation of separate remittance in remt.001

ISO 20022 remittance information sent separately from a payment uses the standalone remittance message, remt.001. The remittance message includes a unique linkage identifier to automate the process of linking a payment to a remittance message sent through the framework.

The payer populates both the payment and remittance information with a remittance linkage identifier that is a unique value available from its AP or other accounting system (e.g., an electronic payment number). When receiving the linkage identifier, the payee uses the combination of payer and the identifier to match the payment to the remittance information.

6.2 Next Steps: Validation Phase

6.2.1 Validation Phase Work

The validation phase objective is to establish a rapidly demonstrable remittance exchange framework to build industry momentum, confidence and support for broad adoption. The work group recommends the following be completed during the validation phase. (See section 4.6, Adaptations and Future Work.)

- Determine changes to the Capability registry or identify another mechanism to include information for remittance data standards supported by Access Points and end points.
- Implement ISO 20022 remittance message data elements as the primary data model.
- Develop and implement schema validation to ensure data integrity according to the data model.
- Test payment linkage to the remittance message.
- Assess potential to share registries with the e-invoicing framework.
- Revise registry queries if needed.
- Create an Access Point testing environment.

The work group noted the validation phase may be able to leverage the E-invoicing Market Pilot infrastructure to avoid duplicating infrastructure and expedite testing. Feasibility of this idea should be explored further with the e-invoicing work groups.

6.2.2 Validation Phase Guiding Principles and Guardrails

The work group recommends validation phase guiding principles and guardrails for staying within scope of the work to ensure consistency with this assessment and compatibility with exchange framework standards and technology.

Validation Phase Guiding Principles

1. Framework adaptations should use standards and technology that are open, royalty-free, vendor and service provider-agnostic and do not require a single platform or solution.
2. Current standards specified by the exchange framework for discovery and delivery will be used.
3. Framework adaptations primarily are focused on facilitating remittance exchange independent of the payment method.
4. Ensuring ease of adoption and maintaining momentum are a high priority.
5. Remittance-specific components incorporated in the framework meet current U.S. market capabilities and drive adoption.
6. Remittance-specific adjustments should focus on facilitating corporate end user adoption for all types of businesses, service provider segments and sizes (e.g., including smaller businesses, banks and service providers).
7. Framework adaptations for industry-specific needs are out of scope for the validation phase.

Validation Phase Guardrails

1. Advocating for changes to the exchange framework's architectural and operational approach, other than those required specifically for remittance needs.
2. Advocating for, or debating, the standards used within the framework for discovery and delivery that were already addressed in the feasibility assessment and would materially change the exchange framework's operational ecosystem and principles.
3. Advocating for any proprietary data standard (e.g., unique to specific software or products) to be included as a core data exchange standard.
4. Discussing topics that fall within anti-trust restrictions.

6.2.3 Market Pilot and Production

Step 2, a market pilot, will incorporate learnings and recommendations from the validation phase. Step 3, production, will be shaped by market pilot learnings. Each step's work will be determined at inception. Any items in section 4.6, Adaptations and Future Work, that are not included in the validation phase would be incorporated into subsequent phases. The market pilot and production steps can leverage progress made in developing the e-invoicing exchange framework.

6.3 Glossary

Access Point: A network service that facilitates the sending and receiving of business documents on behalf of a network participant. The Access Point of the participant initiating the exchange is referred to as Corner 2 in a four-corner network model, while the Access Point of the receiving participant is referred to as Corner 3.

AS4 (Applicability Statement 4): A message protocol based on web services to securely exchange B2B messages between trading partners. It is an open OASIS standard for secure, payload-agnostic exchanges using web services.

Business Document Exchange Location (BDXL): The OASIS Business Document Exchange (BDXR) Technical Committee created the Business Document Metadata Service Location (BDXL) Version 1.0 standard to define a standardized implementation of an DNS registry.

Capability Registry: The Capability registry provides metadata about a participant's capabilities in the network. Metadata includes information about business document types and formats the participant can receive, business processes supported or implemented by the participant, information the participant expects to receive within a certain business document and information about the technical end point(s) and transport protocol(s) where the participant will receive business documents. This registry is referred to as the Service Metadata Publisher (SMP) service in the e-invoicing framework.

Data model: An abstract model that organizes elements of data and standardizes how data elements relate to one another. In this context, a data model defines data elements within a standard, such as ISO 20022, and explicitly determines the data structure.

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

DNS Registry: The DNS registry facilitates the discovery of a participant in an exchange network using only a participant's identifier. This registry is referred to as the Service Metadata Location (SML) service.

Domain Name System (DNS): An interoperable, distributed and accessible network technology used as the core method to discover resources on the internet. It is the hierarchical and decentralized naming system used to identify computers, services and other resources reachable through the Internet or other Internet Protocol (IP) networks.

E-delivery Network: Refers to components of the technical interoperability layer that deliver documents electronically across the Internet. Remittance information is one of many document types for e-delivery.

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

Electronic Invoice (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 Identifier in a service provider platform that routes digital documents and messages on behalf of a trading party.

End Point Participant: An entity, typically a business or government, which sends and/or receives remittance information. In a four-corner network model, the sending end point is corner 1 and the receiving end point is corner 4.

Entity Identifier: The unique digital identifier of a business, legal or fiscal entity or individual.

Exchange Header Envelope (XHE): The Exchange Header Envelope (XHE) is a joint OASIS and UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) specification, which supports both a header and an envelope and supersedes the two prevailing header/envelope standards – OASIS Business Document Envelope (BDE) and Standard Business Document Header (SBDH). XHE is currently the only envelope technology standard that provides end-to-end envelope to support a four-corner network model.

Federated Registry Services: A structure that enables non-affiliated providers to independently administer 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).

ISO 20022 Remittance Data Repository: ISO 20022 is a single standardization approach (methodology, process, repository) used by financial standards initiatives. Remittance data elements included in various ISO 20022 payment messages are documented in the *ISO 20022 Remittance Content Market Guide*, published by X9.

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

Message Payload: The information content and machine-readable syntax of a business message or document.

Message Transport Protocols: Technical transmission protocols used to create network connections between end points to deliver the message payload, such as remittance information and other documents.

Metadata: Data that provides information about other data, but not the actual content of the other data. For example, the author and creation date metadata stored in a Microsoft Word document contain a few details about the document, not the contents.

Non-repudiation: Assurance that the sender of information receives proof of delivery and the recipient obtains proof of the sender's identity, so neither can later deny having processed the information.

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

Peppol: A set of artifacts and specifications enabling interoperable cross-border electronic procurement. Peppol enables trading partners to exchange standards-based electronic documents over the Peppol network based on a four-corner network model. The use of Peppol is governed by a multilateral agreement structure which is owned and maintained by OpenPeppol.

Receiving Access Point: An organization that typically provides its customers with services for the receipt and processing of remittance and other business information and supporting software and services.

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

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

Registry: Centralized information about participants registered in the network and their participant identifiers.

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

Sending Access Point: An organization that provides its customers with services for the delivery and processing of remittance and other business information and supporting software and services.

Service Provider: An organization that provides its customers with services for the creation, delivery and processing of remittance information and other related e-business transactions, as well as supporting software and services. In the e-delivery network, it may provide Access Point or Capability registry services.

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

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

6.4 Work Group Members

Name	Company
Chris Adams	Versapay
Vijay Anand	Mastercard
Sahil Aggarwal	Centime
Kasivalliappan Annamalai	Finzly
Pawel Brataniec	Fluency
Steve Buzzard	Bill360
Michael Carbone	Visa International
Chris Clausen	Deluxe Corporation
Jonathan Cooper	Versapay
Carol Cox	Texas Health Resources
Jennifer Deam	The Commercial & Savings Bank
Richard Duvall	Nacha
Sharisse Fulton	CIT
Santhosh Gajula	Centime Inc
Andrew Goodman	Fifth Third Bank
Will Grace	Autobooks
Todd Harbison	Repay
Robert Hudecek	Jack Henry & Associates
David Jackson	Marketcy
Kamil Jamroz	Fluency
Jennifer Jones	U.S Bank
Jared King	Invoiced, Inc.

Name	Company
Charles Kopko	The NoCheck Group
Howard Lemons	Ameris Bank
Daniel Leshowitz	Workday, Inc.
Mark Majeske	FIS
Kurt Mangold	Deluxe
Diane Maurice	US Treasury
Erin McCune	Glenbrook Partners
Sarah Mille	UMB Bank
Sri Mudigere	Workday
Inga Mullins	Fluency
Jesus Pastran	ATEB
Isak Penttila	Payments Canada
Eric Probst	Teutopolis State Bank
Jose Quevedo	Wells Fargo
Nasreen Quibria	ICBA
Uwe Reimer	Workday
Mary Schaeffer	AP Now
Nitin Singh	Autobooks
Nils Strachanowski	Serrala Group
Mick Talley	University Bancorp
Jim Taylor	MarineNet
Anshul Tripathi	Payments Canada
Ritwik Unhale	Finzly Inc
Steven Wasserman	Vments Inc
Ashley Westcott	Fifth Third Bank
Kendra Wyatt	New Birth Company