AS4 Interoperability Profile for Four-Corner Networks Version 1.0

Committee Specification Draft 01

02 June 2021

This stage:
https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/csd01/bdx-as4-v1.0-csd01.docx (Authoritative)
https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/csd01/bdx-as4-v1.0-csd01.html
https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/csd01/bdx-as4-v1.0-csd01.pdf

Previous stage:
N/A

Latest stage:
https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/bdx-as4-v1.0.docx (Authoritative)
https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/bdx-as4-v1.0.html
https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/bdx-as4-v1.0.pdf

Technical Committee:
OASIS Business Document Exchange (BDXR) TC

Chair:
Kenneth Bengtsson (kbengtsson@efact.pe), Individual member

Editors:
Todd Albers (todd.albers@mpls.frb.org), Federal Reserve Bank of Minneapolis
Kenneth Bengtsson (kbengtsson@efact.pe), Individual member
Sander Fieten (sander@chasquis-consulting.com), Individual member
Philip Helger (philip@helger.com), Individual member
Dennis Weddig (dennis.weddig@mpls.frb.org), Federal Reserve Bank of Minneapolis

Related work:
This document is related to:

- Exchange Header Envelope (XHE) Version 1.0
- Service Metadata Publishing (SMP) Version 2.0
- Service Metadata Publishing (SMP) Version 1.0

Abstract:
This specification defines an interoperability profile of the AS4 Profile of ebMS 3.0 for use in four-corner networks.

Status:
This document was last revised or approved by the OASIS Business Document Exchange (BDXR) TC on the above date. The level of approval is also listed above. Check the "Latest stage" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=bdxr#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/bdxr/.

This specification is provided under the Non-Assertion Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/bdxr/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Key words:
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

Citation format:
When referencing this document, the following citation format should be used:

[BDX-AS4-v1.0]

AS4 Interoperability Profile for Four-Corner Networks Version 1.0. Edited by Todd Albers, Kenneth Bengtsson, Sander Fieten, Philip Helger, and Dennis Weddig. 02 June 2021. OASIS Committee Specification Draft 01. https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/csd01/bdx-as4-v1.0-csd01.html. Latest stage: https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/bdx-as4-v1.0.html.

Table of Contents

1 Introduction

1.1 Rationale and objectives

The AS4 Profile of ebMS 3.0 Version 1.0 (**[AS4]**) is a profile of the OASIS ebXML Messaging Services Version 3.0 (**[ebMS3Core]**) that defines a protocol for exchanging business documents and messages. AS4 defines three different conformance profiles, each designed to meet the requirements and capabilities of implementations of varied complexities: the AS4 ebHandler profile, the AS4 Light Client profile and the AS4 Minimal Client profile. AS4 defines both general usage and conformance of an implementation. It is designed to be flexible and can accommodate a wide range of use cases and scenarios, however, by doing so it requires further profiling for two implementations to be interoperable.

When using AS4 in a four-corner network, a network-wide profile needs to be agreed upon, defining not only the general use of AS4 but also defining a broad range of processing mode (P-Mode) parameters and configurations. This ensures all Access Points in the network are interoperable and capable of exchanging business messages without the need for any bilateral coordination between them.

The overall objective of this specification is to standardize AS4 P-Mode parameters and configuration options when used in a four-corner network. Any Access Point conformant with this specification will be able to successfully exchange AS4 messages with any other Access Point conformant with this specification, without the need for any further conventions or agreements. This facilitates the development of universal “develop once - use everywhere” software implementations that can be used in any conformant business document exchange network, ultimately lowering both complexity and costs as well as increasing quality and reducing risks for both implementing networks and communities as well as software developers.

Additionally, this specification describes the interrelationship between AS4 and the other supporting technologies in a four-corner network, Service Metadata Publishing (**[SMP-1.0]** and **[SMP-2.0]**) and the OPTIONAL Exchange Header Envelope (**[XHE-1.0]**).

The interoperability profile defined in this specification is a profile of the AS4 ebHandler profile.

1.2 Definitions of terms

Access Point: a network service that facilitates the sending and receiving of business documents on behalf of a network Participant.

Final Recipient or **Corner 4**: The Participant who is receiving a business document from Corner 1.

Original Sender or **Corner 1**: In a given business document exchange, Corner 1 is the Participant who wishes to *send* the business document.

Receiving Access Point or **Corner 3**: The Access Point receiving a business document on behalf of Corner 4.

Sending Access Point or **Corner 2**: The Access Point sending a business document on behalf of Corner 1.

Participant: The end-user of the network, using the network to exchange business documents with other Participants.

Service Metadata Publisher or **SMP**: A network service that exposes information about the technical capabilities about a network Participant, such as which business documents that can receive, where to locate their Access Point, and how to communicate with their Access Point.

2 Processing Mode Parameters

2.1 Introduction

This section contains a complete list of the Processing Mode (P-Mode) parameters used by this specification, as well as their use. A conformant Access Point in a four-corner network implementing this specification MUST comply with the P-Mode parameter values and configurations as specified in this section.

2.2 Parameters

2.2.1 PMode.Initiator.Role

Parameter	PMode.Initiator.Role
Type	Constant
Value	`http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator`
Description and usage	Specifies the role of the *sending* Access Point (Corner 2). MUST be set to the specified value.

2.2.2 PMode.Initiator.Party

Parameter	PMode.Initiator.Party
Type	Dynamic
Value	*The value of the Subject Common Name ("CN") field of the signing certificate used by the sending AP.*
Description and usage	The Party ID of the *sending* Access Point (Corner 2). This MUST be identical to the Subject CN field of the certificate used for signing the AS4 User Message. The *receiving* Access Point SHOULD validate that the Subject CN field of the signing certificate matches the PMode.Initiator.Party identifier, i.e. is equal to the `//eb:From/eb:PartyId` in the ebMS messaging header of the received message. When the validation of the Party ID fails, the *receiving* Access Point (Corner 3) SHOULD reject the message and respond with an ebMS EBMS:0103 (PolicyNonCompliance) Error.

2.2.3 PMode.Initiator.Party type

Parameter	PMode.Initiator.Party type
Type	Constant
Value	`http://docs.oasis-open.org/bdxr/AS4/1`
Description and usage	Specifies the type of Party ID of the *sending* Access Point (Corner 2). MUST be set to the specified value.

2.2.4 PMode.Responder.Role

Parameter	PMode.Responder.Role
Type	Constant
Value	`http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder`
Description and usage	Specifies the role of the *receiving* Access Point (Corner 3). MUST be set to the specified value.

2.2.5 PMode.Responder.Party

Parameter	PMode.Responder.Party
Type	Dynamic
Value	*The value of the Subject Common Name ("CN") field of the signing certificate used by the receiving Access Point (Corner 3), as specified in the SMP service response.*
Description and usage	The Party ID of the *receiving* Access Point (Corner 3). The sending Access Point (Corner 2) MUST retrieve this information from the Service Metadata Publishing (SMP) service of the final recipient (*Corner 4*). The *receiving* Access Point MUST set the PMode.Responder.Party ID to the Subject's Common Name ("CN") field of the certificate registered in the SMP. The *receiving* Access Point MUST sign the Receipt Signal Message with a certificate with an identical value for the Subject's CN field. The sending Access Point SHOULD verify that the value of the Subject CN field of the certificate used to sign the Receipt Signal Message is identical to the PMode.Responder.Party ID. When using with **[SMP-2.0]**: The Access Points MUST use the Subject CN of the certificate provided in the value of the `Endpoint/Certificate/ContentBinaryObject` field of the SMP response. The `Certificate/TypeCode` code(s) of the certificate(s) used for the **[AS4]** PMode.Responder.Party ID MUST be "bdxr-as4-signing" (case-sensitive). The listAgencyName attribute of the Certificate/TypeCode SHOULD be set to "OASIS BDXR TC" and the listVersion attribute SHOULD be set to "1.0". An implementing network or community may choose to allow several certificates to be associated with an Access Point in the SMP response as long as these don't conflict with any of the above uses (see also section 5.2). Endpoints included in the response of Corner 4's SMP service which use this specification MUST include one active certificate with the network's policy specified TypeCode. When using with **[SMP-1.0]**: The Access Points MUST use the Subject CN of the certificate provided in the value of the `Endpoint/Certificate` field of the SMP response.

	Endpoints included in the response of Corner 4's SMP service which use this specification MUST include a certificate.

2.2.6 PMode.Responder.Party type

Parameter	PMode.Responder.Party type
Type	Constant
Value	`http://docs.oasis-open.org/bdxr/AS4/1`
Description and usage	Specifies the type of Party ID of the *receiving* Access Point.

2.2.7 PMode.Agreement

Parameter	PMode.Agreement
Type	Constant
Value	*Defined by the network or community*
Description and usage	Uniquely identifies the network or community agreement that governs the sending of the message. This value MUST be a URI and MUST defined by the implementing network or community (see also section 5.3).

2.2.8 PMode.Agreement type

Parameter	PMode.Agreement type
Type	Not used
Value	
Description and usage	A sending Access Point MUST NOT use the `PMode.Agreement/@type` attribute.

2.2.9 PMode.MEP

Parameter	PMode.MEP
Type	Constant
Value	`http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay`
Description and usage	Specifies the Message Exchange Pattern (MEP). Only One-Way MEP is supported.

2.2.10 PMode.MEPbinding

Parameter	PMode.MEPbinding
Type	Constant
Value	`http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push`

Description and usage	Specifies the transport channel binding of the MEP. Only Push is supported.

2.2.11 PMode[1].Protocol.Address

Parameter	PMode[1].Protocol.Address
Type	Dynamic
Value	*The technical endpoint URL of the receiving AP (Corner 3), as specified in the SMP service response.*
Description and usage	The technical endpoint URL where the *sending* Access Point (Corner 2) shall send the message. The sending Access Point MUST retrieve this information from the Service Metadata Publishing (SMP) service of the final recipient (Corner 4). When using with **[SMP-2.0]**: The sending Access Point MUST retrieve this value from the `Endpoint/AddressURI` element of the SMP response. The response of the Corner 4 SMP service MUST include this information as the value of the `Endpoint/AddressURI` element. When using with **[SMP-1.0]**: The sending Access Point MUST retrieve this value from the `Endpoint/EndpointURI` element of the SMP response.

2.2.12 PMode[1].Protocol.SOAPVersion

Parameter	PMode[1].Protocol.SOAPVersion
Type	Constant
Value	`1.2`
Description and usage	The SOAP version used for the message exchange. Only **[SOAP-1.2]** is supported.

2.2.13 PMode[1].BusinessInfo.Service

Parameter	PMode[1].BusinessInfo.Service
Type	Dynamic
Value	*Either a Process Identifier OR the fixed value* `bdx:noprocess`*.*
Description and usage	Holds information about the business process in which the business document is exchanged. When the business document is part of a business process then this value MUST be set to the Process Identifier. When the business document is not part of a business process then this value MUST be set to `bdx:noprocess`. MUST be identical to the Process Identifier in the SMP response. Corresponds to the `Process/ID` in **[SMP-2.0]** and to the `Process/ProcessIdentifier` in **[SMP-1.0]**.

2.2.14 PMode[1].BusinessInfo.Service type

Parameter	PMode[1].BusinessInfo.Service type
Type	Dynamic
Value	*The Process Scheme Identifier.*
Description and usage	When the Process Identifier is part of a defined scheme then this value MUST be set to the Scheme Identifier.

2.2.15 PMode[1].BusinessInfo.Action

Parameter	PMode[1].BusinessInfo.Action
Type	Dynamic
Value	*The Document type Identifier.*
Description and usage	Identifies the type of Document being exchanged. MUST be identical to the Service Identifier in the SMP response. Corresponds to the `ServiceMetadata/ID` in **[SMP-2.0]** and to the `ServiceMetadata/ServiceInformation/DocumentIdentifier` in **[SMP-1.0]**.

2.2.16 PMode[1].BusinessInfo.MPC

Parameter	PMode[1].BusinessInfo.MPC
Type	Constant
Value	`http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC`
Description and usage	The Message Partition Channel (MPC). The default MPC MUST be used.

2.2.17 PMode[1].BusinessInfo.Properties.EndpointParticipantIdentifier

Parameter	PMode[1].BusinessInfo.Properties.EndpointParticipantIdentifier
Type	Dynamic
Value	*A complete Participant Identifier registered to the* sending *Access Point.*
Description and usage	When the *receiving* Access Point (Corner 3) needs to be able to send a response document to the *sending* Access Point (Corner 2), such as application and validation responses as further explained in section 3, this property MUST contain Corner 2's complete Participant Identifier, as registered in the SMP, where such response messages are to be received. When sending the response message to Corner 2, Corner 3 MUST use this Participant Identifier to discover the endpoint where the response message is to be delivered. The Participant Identifier MUST be formatted as specified in section 3.6.2 of **[SMP-2.0]**, but MUST NOT use the URL percent encoding, i.e.: *[{identifier scheme}::]{participant ID}*

2.2.18 PMode[1].Security.WSSVersion

Parameter	PMode[1].Security.WSSVersion
Type	Constant
Value	`1.1.1`
Description and usage	The version of Web Services Security being used. Only **[WSS-SOAP-Message-Security-V1.1.1]** is supported.

2.2.19 PMode[1].Security.X509.Signature.Algorithm

Parameter	PMode[1].Security.X509.Signature.Algorithm
Type	Constant
Value	`http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`
Description and usage	The algorithm used for computing the digital signature of the AS4 message. Only RSA with SHA-256 is supported. The use of RSA with SHA-256 in XML signatures is specified in **[XMLDSIG]**.

2.2.20 PMode[1].Security.X509.Signature.HashFunction

Parameter	PMode[1].Security.X509.Signature.HashFunction
Type	Constant
Value	`http://www.w3.org/2001/04/xmlenc#sha256`
Description and usage	The algorithm used for computing the digest of the AS4 message. Only SHA-256 is supported. The use of SHA-256 in XML signatures is specified in **[XMLDSIG]**.

2.2.21 PMode[1].Security.X509.Signature.Certificate

Parameter	PMode[1].Security.X509.Signature.Certificate
Type	Dynamic
Value	*Public certificate of the signing Access Point*
Description and usage	The public certificate of the signing Access Point that is used for validating the signature of the AS4 message. The signing Access Point MUST include the public X509 certificate as a X509v3 binary security token as specified in **[WSS-X509-Certificate-Token-Profile-V1.1.1]**.

2.2.22 PMode[1].Security.SendReceipt

Parameter	PMode[1].Security.SendReceipt
Type	Constant
Value	`True`
Description and usage	A receiving Access Point MUST respond with a signed `eb:Receipt` message.

2.2.23 PMode[1].Security.SendReceipt.NonRepudiation

Parameter	PMode[1].Security.SendReceipt.NonRepudiation
Type	Constant
Value	`True`
Description and usage	An eb:Receipt message MUST contain nonrepudiation information as a single `ebbpsig:NonRepudiationInformation` element.

2.2.24 PMode[1].Security.SendReceipt.ReplyPattern

Parameter	PMode[1].Security.SendReceipt.ReplyPattern
Type	Constant
Value	`Response`
Description and usage	A receiving Access Point MUST provide the `eb:Receipt` message synchronously in the response to the sending Access Point.

2.2.25 PMode.ID

Parameter	PMode.ID
Type	Not used
Value	
Description and usage	A sending Access Point MUST NOT use the `PMode.ID` to reference a predefined P-Mode configuration. An `AgreementRef/@pmode` attribute MUST NOT be present in a conformant AS4 message.

2.2.26 PMode[1].ReceptionAwareness

Parameter	PMode[1].ReceptionAwareness
Type	Constant
Value	`True`
Description and usage	A sending Access Point MUST implement reception awareness.

2.2.27 PMode[1].ReceptionAwareness.Retry

Parameter	PMode[1].ReceptionAwareness.Retry
Type	Constant
Value	*Implementation or community specific*
Description and usage	A sending Access Point MUST follow network and community resend policies and requirements when such are defined (see section 5.4). If such policies and requirements are not defined by the network or community, the sending Access Point SHOULD attempt to retry sending messages in case of message sending failure.

2.2.28 PMode[1].ReceptionAwareness.Retry.Parameters

Parameter	PMode[1].ReceptionAwareness.Retry.Parameters
Type	Constant
Value	*Implementation or community specific*
Description and usage	A sending Access Point MUST implement and configure retry parameters according to network and community policies and requirements when such are defined (see section 5.4). If such policies and requirements are not defined by the network or community, the sending Access Point SHOULD implement and configure retry parameters in accordance with the recommendations in section 5.4 of this specification.

2.2.29 PMode[1].ReceptionAwareness.DuplicateDetection

Parameter	PMode[1].ReceptionAwareness.DuplicateDetection
Type	Constant
Value	`True`
Description and usage	A receiving Access Point MUST detect if a message has already been received.

2.2.30 PMode[1].ReceptionAwareness.DetectDuplicates.Parameters

Parameter	PMode[1].ReceptionAwareness.DetectDuplicates.Parameters
Type	Constant
Value	*Defined by the network or community*
Description and usage	A receiving Access Point MUST implement message retention policies in accordance with network and community policies and requirements as defined in section 5.4. A receiving Access Point MUST detect if a received message is a duplicate of a message already received within its message retention span. A receiving Access Point SHOULD eliminate duplicate messages.

2.2.31 PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer

Parameter	PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer
Type	Constant
Value	`True`
Description and usage	A sending Access Point SHOULD report any error to the calling application.

2.2.32 PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer

Parameter	PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer
Type	Constant

Value	`True`
Description and usage	A sending Access Point MUST notify the calling application in case of permanent message delivery failure, and, when such policies are defined, MUST handle message sending failures in accordance with network and community policies (see section 5.4).

2.2.33 PMode[1].ErrorHandling.Report.AsResponse

Parameter	PMode[1].ErrorHandling.Report.AsResponse
Type	Constant
Value	`True`
Description and usage	A receiving Access Point MUST provide the ebMS Error Message synchronously in the HTTP response to the sending Access Point.

2.2.34 PMode[1].ErrorHandling.Report.SenderErrorsTo

Parameter	PMode[1].ErrorHandling.Report.SenderErrorsTo
Type	Not used
Value	
Description and usage	The SenderErrorsTo parameter MUST NOT be used to configure asynchronous error signal messages. Instead, Access Points MUST follow network and community policies for handling message sending failures as specified in section 5.4.

2.2.35 PMode[1].Security.X509.Encryption.Encrypt

Parameter	PMode[1].Security.X509.Encryption.Encrypt
Type	Constant
Value	*`True` or `false`, depending on network or community policies*
Description and usage	A sending Access Point MUST encrypt business data in accordance with the policies of the implementing network or community when these exist (see section 5.5). If no policies are defined by the network or community, a sending Access Point MAY use AS4 encryption. When using of AS4 encryption, encryption MUST be implemented in accordance with this specification.

2.2.36 PMode[1].Security.X509.Encryption.Certificate

Parameter	PMode[1].Security.X509.Encryption.Certificate
Type	Dynamic
Value	*Public certificate of the receiving Access Point*
Description and usage	When a sending Access Point uses AS4 encryption, the message MUST be encrypted using the public certificate of the receiving Access Point as published in the SMP. The sending Access Point MUST include the X.509

	certificate as a X509v3 binary security token as specified in **[WSS-X509-Certificate-Token-Profile-V1.1.1]**. When using with **[SMP-2.0]**: The sending Access Point MUST retrieve the certificate from the `Endpoint/Certificate/ContentBinaryObject` element of the SMP response. Endpoints included in the response of Corner 4's SMP service which use this specification MUST include one active certificate with the TypeCode "bdxr-as4-encryption". TODO: add CCTS attributes. TODO: only one active with this type code. When using with **[SMP-1.0]**: The sending Access Point MUST retrieve the certificate from the `Endpoint/Certificate` element of the SMP response.

2.2.37 PMode[1].Security.X509.Encryption.Algorithm

Parameter	PMode[1].Security.X509.Encryption.Algorithm
Type	Constant

Value	MUST be either
	`http://www.w3.org/2009/xmlenc11#aes128-gcm`
	or
	`http://www.w3.org/2009/xmlenc11#aes256-gcm`

Description and usage	A sending Access Point using AS4 encryption MUST use either AES-128 with GCM mode or AES-256 with GCM mode. A receiving Access Point MUST be able to decrypt a received message using both algorithms. An implementing network or community may require that only one and not the other algorithm is used within the network, as explained in section 5.5.

2.2.38 PMode[1].Security.X509.Encryption.MinimumStrength

Parameter	PMode[1].Security.X509.Encryption.MinimumStrength
Type	Not used
Value	
Description and usage	The MinimumStrength parameter MUST NOT be used. Instead, Access Points MUST use one of the encryption algorithms defined in this specification when using AS4 encryption.

3 Response Messages

In a four-corner network Participants use one or more Access Points to implement the information exchange with their trading partners. It's the Access Points' responsibility that the document exchange conforms to the network policies. Therefore, it is sometimes necessary for a *receiving* Access Point (Corner 3) to send a Response Message to the *sending* Access Point (Corner 2). For example, when a business document received from Corner 2 does not conform to agreed technical and/or business validation rules, the network or community MAY define the use of an application response that Corner 3 can automatically generate and send back to Corner 2 to signal nonconformance and that the business document will not be delivered to its final recipient. Like other business message, such Response messages are sent asynchronously after the original business document has been sent to Corner 3 since they typically entail processing and validation of the business document that can only happen after it has been received.

Since Response Messages are sent asynchronously and independently from the original business document exchange, they are essentially a new business document exchange with reversed roles where the Corner 3 Access Point sends a business document to Corner 2. To facilitate this process, Corner 2 MUST operate a conformant Access Point for *receiving* Response Messages. Conversely, Corner 3 MUST operate a conformant Access Point for *sending* Response Messages.

Furthermore, Corner 2 MUST signal how and where they want to receive Response Messages. This is done by including a complete Participant Identifier in the `PMode[1].BusinessInfo.Properties.EndpointParticipantIdentifier` P-Mode parameter, as specified in section 2.2.17. This Participant Identifier MUST be registered and discoverable in the network.

To send a Response Message back to Corner 2, Corner 3 MUST use the Participant Identifier provided by Corner 2 to perform a full network discovery to find the endpoint address and properties of the Access Point that will receive the Response Message, as shown in the following diagram:

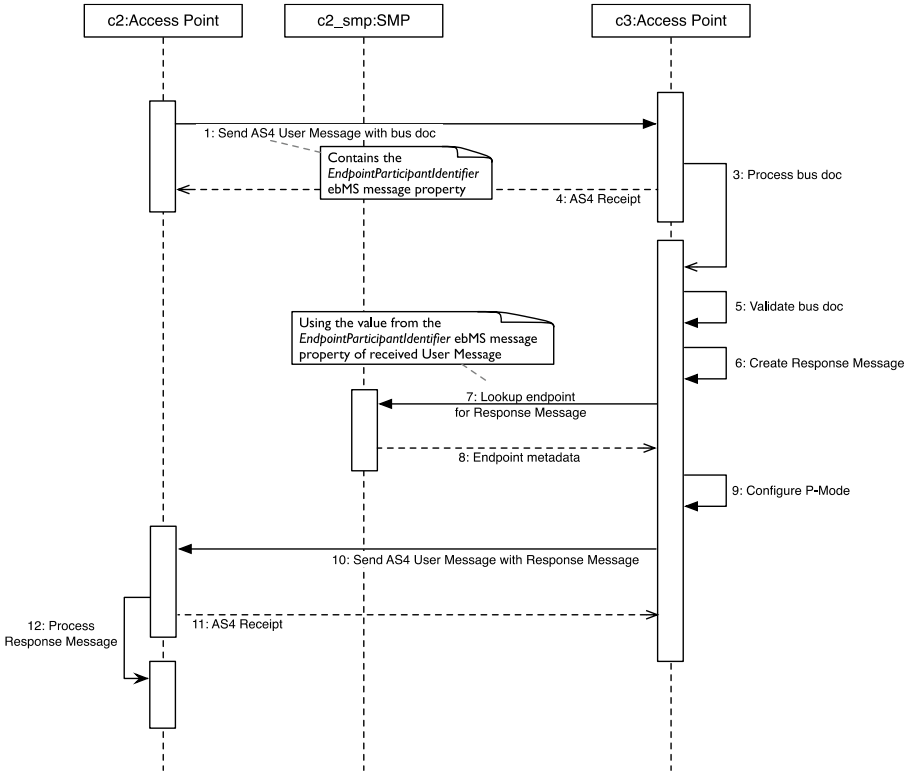

Figure 1: Network discovery process

Note that these response messages MUST NOT be used as a nonrepudiation device to evidence that a business document has been received by Corner 3. Nonrepudiation is already defined in **[AS4]** and uses a `ebbpsig:NonRepudiationInformation` element within an `eb:Receipt` to signal nonrepudiation of message received. See also sections 2.2.23 (PMode[1].Security.SendReceipt.NonRepudiation) and 2.2.24 (PMode[1].Security.SendReceipt.ReplyPattern).

4 Exchange Header Envelope

4.1 General use

In a four-corner network, Access Points (Corners 2 and 3) are used as intermediary gateways to relay business documents between an original sender (Corner 1) and a final recipient (Corner 4). The **[AS4]** specification is designed as a point-to-point protocol and defines parameters for sending a message from Corner 2 to Corner 3 but does not in itself define metadata or other information about Corners 1 and 4. Consequently, the Corner 3 Access Point relies entirely on the business document in the AS4 payload to determine further processing and routing of a received message.

While most standards describing structured business document formats do specify how to express the sending and receiving parties of a business document, this is done very different from one standard to another. It also cannot be assumed that the business document is always in a structured format. Thus, the need for a standardized document header or envelope such as the **[XHE-1.0]**, where routing and processing information can be transmitted along with the business document itself, in a manner that is structured and universally understood. This allows Access Points to understand how to process and route the business document without having to understand its syntax and semantics.

At the same time, four-corner networks are designed to be modular so that it is possible to replace individual components of the network without impacting other network components or without impacting network operability in general. For example, a four-corner network can replace the communications protocol with another communications protocol without impacting the discovery process, replace components of the discovery process without impacting the communications protocol, and even have several communications protocols enabled in parallel. It is therefore desirable to separate metadata concerning Corners 1 and 4 from the communications layer that is used between Corners 2 and 3.

To achieve this, an implementing network or community MAY mandate that Access Points apply the Exchange Header Envelope (**[XHE-1.0]**) (XHE) specification as an envelope technology when exchanging business documents. If defined by the policies of the implementing network or community, a Corner 2 Access Point MUST always embed a business document as a payload in an XHE envelope before sending to Corner 3. A conformant Corner 3 Access Point in a network or community applying the XHE MUST always be able to receive an XHE from a sending Access Point. The only exception is when exchanging Response Messages as defined in section 3, which are only designed to be relayed between Corners 2 and 3, and not between Corners 1 and 4.

An XHE MAY also be used to exchange several business documents in a single transaction by including multiple documents as individual payloads within a single XHE, as explained in the **[XHE-1.0]** specification.

4.2 Specifying the original sender and the final recipient

When using the **[XHE-1.0]** with this specification, the Participant ID of the *original sender* (Corner 1) MUST be included in the `xha:Header/xha:FromParty/xha:PartyIdentification/xhb:ID` element of the XHE and the Participant ID of the *final recipient* (Corner 4) MUST be included in the `xha:Header/xha:ToParty/xha:PartyIdentification/xhb:ID` element of the XHE.

When receiving a message with an XHE, a Corner 3 (receiving) Access Point MUST validate that they can receive messages on behalf of the *final recipient* party specified in the XHE. The possible response to this validation, such as Corner 3's refusal to accept the message, is not specified in AS4 and is therefore outside of the scope of this specification. Implementing networks and communities MUST define requirements for a Response Message to be send back to Corner 2 when Corner 3 refuses to accept the message (see section 3).

4.3 Specifying payloads

A business document embedded in an XHE SHOULD be properly marked for identification by relaying information about the business document in the Payload metadata of the XHE. Wherever applicable,

- the ID of the business document (for example, the invoice number, order number, etc.) SHOULD be included in the `xhb:ID` element of its XHE Payload container,
- the Customization ID of the business document SHOULD be included in the `xhb:CustomizationID` element of its Payload container, and
- The Profile ID of the business document SHOULD be included in the `xhb:ProfileID` element of its Payload container.

4.4 Additional use of the XHE

An implementing network or community MAY define additional use, properties, and elements of the XHE, such as encryption and signing, as long as these don't violate the constraints specified in sections 4.2, 4.3 and 5 of this specification.

5 Implementing networks and communities

5.1 Introduction

While many AS4 Processing Mode Parameters define explicit technical properties and requirements for Access Point implementations, there are also parameters that are configurable and must be implemented according to the policies and specifications of an implementing network or community. Additionally, an implementing network or community may choose to limit options for Access Point configuration, for example by defining explicit requirements for encryption and encryption algorithms.

This section defines the explicit requirements for network and community policies when implementing this specification for AS4 messaging in a network.

5.2 The use of multiple Access Point certificates with SMP 2.0

Section 2.2.5 (PMode.Responder.Party) specifies the use of certificates associated with a receiving Access Point in the response of an SMP 2.0 service, and how this information is used by the sending Access Point to validate the Receipt Signal Message. SMP 2.0 allows for associating several certificates with an Access Point in the SMP response, and although describing use cases for multiple certificate scenarios is outside of the scope of this specification, an implementing network or community MAY choose to allow several certificates to be associated with an Access Point in the SMP response. Notwithstanding, any policy or specification that defines or allows the use of multiple Access Point certificates in the SMP response MUST NOT conflict with the use or functionality described in section 2.2.5.

5.3 Network agreement identifiers

The exchange of business documents in a network or community is governed by its policies and agreements. As specified in section 2.2.7 (PMode.Agreement), a sending Access Point must include information that unambiguously identifies the agreement governing the transaction when initiating communication with a receiving Access Point. Consequently, an implementing network or community MUST define a unique identifier that unambiguously references the policies and agreements that governs the exchange of information between Access Points in the network. This identifier MUST be a URI.

5.4 Message delivery, retention, and error handling policies

To ensure that requirements for message delivery are properly aligned, including assuring that no Access Point fails to deliver a message if communication fails in the first attempt as well as assuring that no Access Point generates excessive network traffic by continuously trying to resend a message that can't be delivered, an implementing network or community SHOULD require that Access Points resend messages (see also section 2.2.27).

When an implementing network or community requires that Access Points resend messages, policies, and requirements for retry parameters MUST be specified. It is RECOMMENDED that `max retries` be set as no less than 2 and no more than 5, and that the `retry period` be set to no less than 5000 milliseconds. It is furthermore RECOMMENDED that sending Access Points are required to increment the retry period after every retry (see also section 2.2.28).

To avoid duplicate messages such as may resulting from accidental resends, receiving Access Points are required to detect if a received message is a duplicate of a message already received within its message retention span (see section 2.2.30). Consequently, to ensure standardized duplicate detection, an implementing network or community MUST specify message retention policies and requirements for Access Points. It is NOT RECOMMENDED that implementers or implementing networks and communities specify a maximum log size for duplicate detection.

An implementing network or community SHOULD define a policy for handling permanent message delivery failures, such as agreed protocols for contacting involved parties and Access Points, and for case escalation (see also sections 2.2.32 and 2.2.34).

5.5 Message encryption

It is RECOMMENDED that implementing networks and communities define a policy for encrypting business data. The use of AS4 encryption as such is OPTIONAL and the policy MAY dictate the use of **[XHE-1.0]** or other mechanism to encrypt data in the exchange between Access Points. It is NOT RECOMMENDED to allow Access Points to exchange business data without encryption.

When using AS4 encryption, an implementing network or community MAY define that either AES-128 with GCM mode or AES-256 with GCM mode be used, or that Access Points may freely choose between the two. The implementing network or community MUST NOT require that any other encryption algorithms be used for AS4 encryption.

See also sections 2.2.35 and 2.2.37.

6 Conformance

6.1 Access Point conformance

An implementing Access Point is conformant with this specification when:

1) The Access Point has implemented and configured all Processing Mode (P-Mode) parameters as specified in section 2.2; and
2) The Access Point has not implemented or configured any additional P-Mode parameters that could impede the interoperability with a conformant Access Point; and
3) The Access Point has implemented discovery, sending, and receiving of Response Messages as specified in section 3.

As a consequence of section 3 (Response Messages), all conformant Access Points MUST effectively be able to both send and receive messages. All Access Points MUST therefore be compliant with all the above statements to claim conformance with this specification, regardless of their role in the network.

6.2 Network and community conformance

An implementing network or community is conformant with this specification when:

1) The network or community has implemented all policies and requirements as specified in sections 3, 4 and 5; and
2) The network or community does not implement any policies or other requirements that could impede interoperability between conformant Access Points.

6.3 Access Point with Exchange Header Envelope (XHE) conformance

When an implementing network or community requires the application of an Exchange Header Envelope (XHE) to convey metadata about the original sender (Corner 1) and final recipient (Corner 4) as specified in section 4.1, an Access Point is conformant with this specification when able to generate, send, receive and process an XHE as specified in sections 4.2 and 4.3, and when conformant with all the mandatory conformance clauses in section 6.1.

Appendix A. References

This appendix contains the normative and informative references that are used in this document. Normative references are specific (identified by date of publication and/or edition number or Version number) and Informative references are either specific or non-specific.

While any hyperlinks included in this appendix were valid at the time of publication, OASIS cannot guarantee their long term validity.

A.1 Normative References

The following documents are referenced in such a way that some or all of their content constitutes requirements of this document.

[AS4]

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

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC8174]

Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

[SMP-1.0]

Service Metadata Publishing (SMP) Version 1.0. Edited by Jens Aabol, Kenneth Bengtsson, Erlend Klakegg Bergheim, Sander Fieten, and Sven Rasmussen. 01 August 2017. OASIS Standard. http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/os/bdx-smp-v1.0-os.html. Latest version: http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html.

[SMP-2.0]

Service Metadata Publishing (SMP) Version 2.0. Edited by Kenneth Bengtsson, Erlend Klakegg Bergheim, Sander Fieten, and G. Ken Holman. 14 February 2021. OASIS Standard. https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/os/bdx-smp-v2.0-os.html. Latest stage: https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/bdx-smp-v2.0.html.

[SOAP-1.2]

SOAP Version 1.2 Part 1: Messaging Framework, M. Gudgin, M. Hadley, N. Mendelsohn, J. Moreau, H. Frystyk Nielsen, Editors, W3C Recommendation, June 24, 2003, http://www.w3.org/TR/2003/REC-soap12-part1-20030624/.

[WSS-X509-Certificate-Token-Profile-V1.1.1]

Web Services Security X.509 Certificate Token Profile Version 1.1.1. 18 May 2012. OASIS Standard. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html.

[WSS-SOAP-Message-Security-V1.1.1]

Web Services Security: SOAP Message Security Version 1.1.1. 18 May 2012. OASIS Standard. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html.

[XHE-1.0]

Exchange Header Envelope (XHE) Version 1.0. Edited by G. Ken Holman. 25 April 2021. OASIS Standard. https://docs.oasis-open.org/bdxr/xhe/v1.0/os/xhe-v1.0-os-oasis.html. Latest version: https://docs.oasis-open.org/bdxr/xhe/v1.0/xhe-v1.0-oasis.html.

[XMLDSIG]

XML Signature Syntax and Processing (Second Edition), D. Eastlake, J. Reagle, D. Solo, F. Hirsch, T. Roessler, Editors, W3C Recommendation, June 10, 2008, http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

[XMLENC]

XML Encryption Syntax and Processing, D. Eastlake, J. Reagle, Editors, W3C Recommendation, December 10, 2002, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

A.2 Informative References

The following referenced documents are not required for the application of this document but may assist the reader with regard to a particular subject area.

[ebMS3Core]

OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features, 1 October 2007, OASIS Standard. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.html.

Appendix B. Acknowledgments

B.1 Participants

The following individuals were members of this Technical Committee during the creation of this document and their contributions are gratefully acknowledged:

Jens Aabol, Norwegian Digitalisation Agency

Todd Albers, Federal Reserve Bank of Minneapolis

Rui Barros, Individual

Oriol Bausa Peris, Individual

Kenneth Bengtsson, Individual

Erlend Klakegg Bergheim, Norwegian Digitalisation Agency

Mikkel Brun, Tradeshift Network Ltd.

Ger Clancy, IBM

Kees Duvekot, RFS Holland Holding B.V.

Pim van der Eijk, Sonnenglanz Consulting

Sander Fieten, Individual

Martin Forsberg, Swedish Association of Local Authorities & Regions

Philip Helger, Individual

David Hixon, IBM

Ken Holman, Crane Softwrights Ltd.

Levine Naidoo, IBM

Matt Vickers, Xero

Dennis Weddig, Federal Reserve Bank of Minneapolis

Appendix C. Revision History

Revisions made since the initial stage of this numbered Version of this document may be tracked here.

Revision	Date	Editor	Changes Made
CSD01	11 May 2021	Todd Albers, Kenneth Bengtsson, Sander Fieten, Philip Helger, Dennis Weddig	Initial Committee Specification Draft

Appendix D. Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website: [https://www.oasis-open.org/policies-guidelines/ipr].

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OASIS AND ITS MEMBERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR ANY PART THEREOF.

As stated in the OASIS IPR Policy, the following three paragraphs in brackets apply to OASIS Standards Final Deliverable documents (Committee Specifications, OASIS Standards, or Approved Errata).

[OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this deliverable.]

[OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this OASIS Standards Final Deliverable. OASIS may include such claims on its website, but disclaims any obligation to do so.]

[OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this OASIS Standards Final Deliverable or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Standards Final Deliverable, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.]

The name "OASIS" is a trademark of OASIS, the owner and developer of this document, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, documents, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.