Specification

Acronym: PEPPOL

Grant Agreement number:

Title: Pan-European Public Procurement Online

PEPPOL Transport Infrastructure
AS2

Version: 1.00

Authors:

Edmund Gray IT Sligo Ireland

Project co-funded by the European Commission within the ICT Policy Support Programme		
Dissemination Level		
P	Public	
C	Confidential, only for members of the consortium and the Commission Services	X

Revision History

Version	Date	Author	Organisation	Description
0.01	20120701	Edmund Gray	IT Sligo	Draft

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. However as it is an alternative to the ICT-Transport-START_Service_Specification document, published by PEPPOL, then its structure and wording is related. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Contributors

Organisations

DIFI (Direktoratet for forvaltning og IKT)[1], Norway, www.difi.no
NITA (IT- og Telestyrelsen)[2], Denmark, www.itst.dk
IT Sligo, Ireland, www.itsligo.ie

Persons

Klaus Vilstrup Pedersen, DIFI
Sven Rasmussen
Edmund Gray
Padraig Harte

[1] English: Agency for Public Management and eGovernment

[2] English: National IT- and Telecom Agency

Table of Content

1 Introduction

1.1 Objective

This document describes an alternative BUSDOX specification to be used to exchange business messages between Access Points (AP) as part of the PEPPOL infrastructure. This alternative uses the AS2 specification as specified in RFC4130 HTTP Applicability Statement 2 (AS2). AS2 was chosen because of its popularity among existing EDI Service Providers and the fact that it has already undergone extensive interoperability testing. This specification therefore focusses on leveraging these existing AS2 systems to become part of the PEPPOL network of Access Points. This specification will show how these systems can be enhanced by using the BUSDOX Service Metadata to dynamically exchange Digital Certificates and Endpoint URLs and therefore automate the inclusion of new or modified APs.

The PEPPOL AS2 Specification will use security settings which are equivalent to the Secure Trusted Asynchronous Reliable Transport (START) security settings, as specified in the ICT-Transport-START_Service_Specification document. AS2 uses an S/MIME-based profile which provides security using Digital Certificates in much the same way as START. Therefore the same Certificates can be used for both protocols. It also uses URLs to identify the Endpoint addresses therefore the Service Metadata obtained from existing SMPs can be reused for AS2 Endpoints.

AS2 provides a Transport infrastructure for exchanging structured business data securely using the HTTP transfer protocol. This exchange is normally XML but can also exchange other Electronic Data Interchange (EDI) formats such as the UN Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT) format. The data is packaged using standard MIME structures. Authentication and data confidentiality are obtained by using Cryptographic Message Syntax (CMS) with S/MIME security body parts. Authenticated acknowledgements make use of multipart/signed Message Disposition Notification (MDN) responses to the original HTTP message. This provides a non-repudiation of receipt[1] for the exchange of an electronic business message and therefore assures the sender their responsibility has been executed.

The PEPPOL AS2 Transport Specification defines a secure, reliable profile using a set of well-known standards and specifications for BUSDOX Access Points data exchange:

- BUSDOX Metadata Lookup and publishing specifications and services
- RFC4130 HTTP Applicability Statement 2 – AS2
  - RFC 2616 Hyper Text Transfer Protocol
  - RFC 1767 EDI Content Type
  - RFC 3023 XML Media Types
  - RFC 1847 Security Multiparts for MIME
  - RFC 3462 Multipart/Report
  - RFC 2045 to 2049 MIME RFCs
  - RFC 3798 Message Disposition Notification
  - RFC 3851, 3852 S/MIME v3.1 Specification
  - RFC 5652, Cryptographic Message Syntax (CMS)

[1] The term non-repudiation of receipt (NRR) is often used in combination with receipts. NRR refers to a legal event that occurs only when the original sender of an interchange has verified the signed receipt coming back from recipient of the message, and has verified that the returned MIC value inside the MDN matches the previously recorded value for the original message

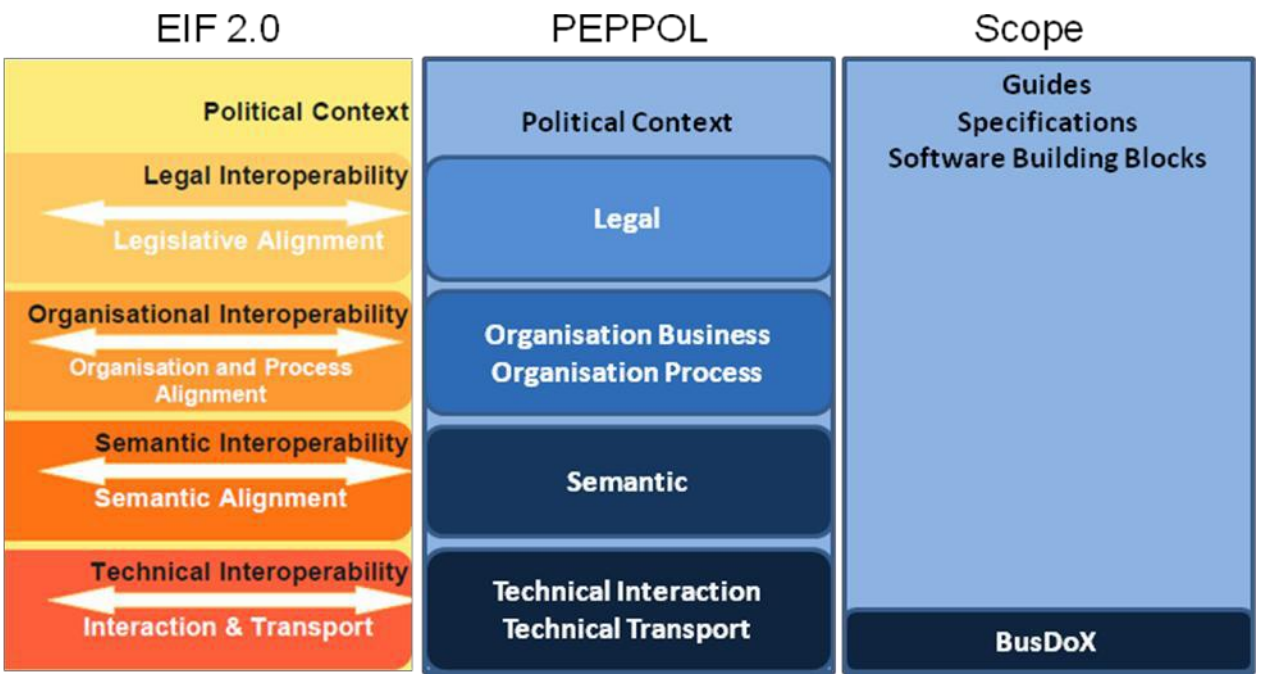
BUSDOX Access Points communicate in a peer-to-peer model across the internet to form the BUSDOX infrastructure. Each Access Point derives the endpoint addresses of other BUSDOX Access Points through the BUSDOX Service Metadata Publishing Infrastructure.

In order to instantiate a working network, certain profile information is expected. For example, an instance of BUSDOX is the PEPPOL infrastructure, which includes governance models, certificate rules, identifier formats, and other profiling. This specification therefore excludes such profiling information.

This specification profile describes the usage of these standards to support the requirements of BUSDOX. In particular the usage of these standards is restricted to certain patterns to enable interoperability to be achieved.

1.2 Scope

This specification relates to the Technical Transport Layer i.e. BusDox specifications. The BusDox specifications can be used in many interoperability settings. In the PEPPOL context, it provides transport for e-procurement messages for both pre and post award scenarios as specified in the PEPPOL Profiles.



1.3 Goals and non-goals

The goal of this profile is to support a high level of assurance and proof-of-delivery across the BUSDOX Infrastructure. The profile is designed to:

- facilitate implementers to leverage existing systems and therefore gain access to PEPPOL, without the need to make significant changes to existing systems.
- Clearly state the transport level requirements in a single document.
- Identify the additional steps required to update an existing AS2 system so it complies with the requirements and can therefore participate as a BUSDOX compliant Access Point (AP).
- Define a simple, interoperable, reliable and safe communications pattern that APs can use to communicate.
- Define the message exchange formats and patterns clearly.
- Ensure that messages are reliably delivered between APs, including providing the prerequisites for logging and proof-of-delivery for messages at the transport level
- Ensure confidentiality during the exchange by using message-level encryption using the Triple DES specification.
- Ensure integrity and authenticity of received messages is maintained by using the Cryptographic Message Syntax (CMS), which is used to digitally sign, digest, authenticate and encrypt the electronic message.
- Establish a common format for representing authentication and authorisation events in BUSDOX using PEPPOL provided Digital Certificates.
- Recipients can assume that senders are trusted by the trust chain of the PEPPOL issued certificates and the Governance documents already signed by members.

The Profile does NOT address:

- The verification of certificates, format of participant identifiers, and other details required to create a full instantiation of BUSDOX.
- Communication with BUSDOX Service Metadata services.

1.4 Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.
For common terms used in these specifications, please see [BDEN-CDEF].

Notational conventions
For notational conventions, see [BDEN-CDEF].

Normative references
[BDEN-CDEF] Business Document Exchange Network - Common Definitions, CommonDefinitions.pdf

Moberg D. “MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)” RFC4130 July 2005

Hansen T. Message Disposition Notification RFC 3798 May 2004

Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

Vaudreuil, G., "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages", RFC 3462, January 2003.

Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling", RFC 3850, July 2004.

Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

2 Overview

The BUSDOX AS2 specification provides a secure reliable approach for messages exchange from one PEPPOL Access Point (AP) to another. The key factor here is utilising the SMP lookup in an efficient way so that existing APs can use the downloaded metadata to automatically initiate the exchange. The AS2 and the START specifications have similarities as they are both peer-to-peer models designed to deliver a business message in a safe and reliable manner. This ensures AS2 can be a direct replacement for START. The key common metadata elements provided by the SMP are the Public Certificate and a service based URL.

A typical workflow between APs AP1 to AP2 might be:

- An electronic message is received by AP1 from Company C1. The method used to receive the message is outside the scope of this document but the recipient MUST assure the authenticity and integrity of the message.

  .
- The message received by Access Point AP1, includes information required such as:
  - Recipient Identifier and identifier type
  - Sender Identifier and identifier type
  - Document identifier and process identifier
- AP1 identifies the appropriate recipient Access Point (AP2) endpoint from cached SMP data. The cache is updated by regular calls to the SMP - the BUSDOX Metadata Lookup and publishing specifications and services.
- AP1 gets Private Key X509 certificate for signing from own stores and Public Key X509 Certificate of AP2 for encryption from the downloaded SMP data.
- AP1 MUST ensure the correct headers containing recipient, sender and document type information are included with the message.
- AP1 signs and encrypts the message using PEPPOL Certificates.
- AP1 uses HTTP to send message to AP2 using the URL as downloaded in the SMP Metadata.
- AP2 responds with a signed proof-of-delivery message to AP1 using the Message Delivery Notification (MDN) specification.
- Finally AP1 archives the MDN as a signed proof-of-delivery of the message

In this model, AP1 is acting as a Source Access Point (SrcAP) and AP2 is acting as a Destination Access Point (DestAP). The expectation is that most Access Points will act as both SrcAP and DestAP, however this is not required by the specifications.

3 Specification Profile Details

The following requirements apply to the BUSDOX AS2 Profile.

3.1 Use of Digital Certificates

In this specification the use of PKI ensures security of transmission by using PEPPOL supplied certificates for both signing and encryption, while the use of a signed MDN provides a non-repudiatable transaction. The sender does this by verifying the signed MDN with the receiving partner's public key, and by verifying that the returned MIC (Message Integrity Check) value in the MDN is the same as the MIC for the original message.

3.2 BUSDOX defined headers

Please see [BDEN-CDEF].

3.3 Message Exchange

This profile uses HTTP for transport and S/MIME for content to send any electronic business message from one Access Point to another. The transmission should be idempotent so that the SrcAP can resend to DestAP without issue of duplication.

Prerequisites for communication

Before an Access Point can deliver a message to another Access Point, the SrcAP MUST have the following information, which it MAY find in the BUSDOX Service Metadata Publishing document:

- The WS-Addressing EndpointReference for the *Destination Message Channel (DestMC)* of the DestAP.

Destination Message Channel

In order for a SrcAP to send a message to a DestAP, the DestAP MUST expose a Destination Message Channel (DestMC). The DestMC is an AS2 compliant endpoint that supports the specification as defined in this document. The Endpoint Reference of this channel is available in a BUSDOX Service Metadata Publishing document.

Delivery of BUSDOX messages

The SrcAP will consider the message to be delivered when it receives an MDN signifying that the message has been successfully processed and no error is received . Each message has a unique Id and the SrcAP should have a means of verifying which messages have yet to be receipted.

The transmission must include the following Service Metadata:

- RecipientIdentifier
  - Determined from the message contents.
  - /ns3:SignedServiceMetadata/ns3:ServiceMetadata/ns3:ServiceInformation/ParticipantIdentifier
- SenderIdentifier
  - Determined from the message contents
- DocumentIdentifier
  - /ns3:SignedServiceMetadata/ns3:ServiceMetadata/ns3:ServiceInformation/DocumentIdentifier
- ProcessIdentifier
  - /ns3:SignedServiceMetadata/ns3:ServiceMetadata/ns3:ServiceInformation/ns3:ProcessList/ns3:Process/ProcessIdentifier
- MessageIdentifier
  - Provided in the AS2 message Header - Message-Id:

The AS2 specification currently does not provide for these metadata elements. However the metadata MUST be sent as part of the transmission in such a way as the DestAP can easily associate the metadata with the appropriate documents. This could be done by enclosing the metadata file as a

separate document in a compressed file along with the associated document; the metadata file SHOULD have the same name (except the extension should be .metadata.xml). However when using UBL documents, then the required metadata is already included in the document and a separate document is not necessary.
The following UBL fields are mapped to the metadata requirements;

- /cbc:CustomizationID = DocumentIdentifier
- /cbc:ProfileID = ProcessIdentifier
- /cac:AccountingSupplierParty/cac:Party/cac:PartyIdentification/cbc:ID = SenderIdentifier
- /cac:AccountingCustomerParty/cac:Party/cac:PartyIdentification/cbc:ID = RecipientIdentifier

Faults/Errors returned;

Typically all AS2 errors from DestAP are returned using the MDN and the error reported in the "disposition-field". The DestAP has several integrity checks all of which may return errors. If the disposition-field states "MDN-sent-automatically; processed" then the transmission was successful. When errors occur in processing the received message (other than content), the "disposition-field" MUST be set to the "processed" value for disposition-type and the "error" value for disposition-modifier. Otherwise the SrcAP MUST determine the cause of the error and resend with the issue corrected. Other errors would be considered normal socket or HTTP errors and are outside the scope of this document. The MDN errors are;

Failure/Error	Possible cause
Failure: unsupported format	
Failure: unsupported MIC-algorithms	
Error: decryption-failed	the receiver could not decrypt the message contents.
Error: authentication-failed	the receiver could not authenticate the sender.
Error: integrity-check-failed	the receiver could not verify content integrity.
Error: unexpected-processing-error	a catch-all for any additional processing errors.
Error decoding certificate	AS2 system cannot decode partner's certificate.

3.4 Use of HTTP

Please see Common Definitions document

3.9 Security

AS2 APs MUST provide an equivalent level of security as the START Protocol. This means that PEPPOL supplied Certificates should be used for message signing and Triple DES encryption and the returned MDN must be signed. The MDN validation process ensures a non-repudiatable transaction. The sender does this by verifying the signed MDN with the receiving partner's public key, and by verifying that the returned MIC (Message Integrity Check) value in the MDN is the same as the MIC for the original message.

Message Authentication and Integrity

Authentication and integrity of messages is established by means of digital signatures applied to the S/MIME message. The authentication algorithm performs the following (source: RFC 4130):

- The message integrity check (MIC or Message Digest), is decrypted using the sender's public key.
- A MIC on the signed contents (the MIME header and encoded EDI object, as per RFC 1767) in the message received is calculated using the same one-way hash function that the sender used.
- The MIC extracted from the message that was sent and the MIC calculated using the same one-way hash function that the sending trading partner used are compared for equality.

Responses

The signed MDN, when received by the sender of the EDI Interchange, can be used by the sender as follows (Source RFC 4130):

- As an acknowledgement that the EDI Interchange sent was delivered and acknowledged by the receiving trading partner. The receiver does this by returning the original-message-id of the sent message in the MDN portion of the signed receipt.
- As an acknowledgement that the integrity of the EDI Interchange was verified by the receiving trading partner. The receiver does this by returning the calculated MIC of the received EC Interchange (and 1767 MIME headers) in the "Received-content-MIC" field of the signed MDN.
- As an acknowledgement that the receiving trading partner has authenticated the sender of the EDI Interchange.
- As a non-repudiation of receipt when the signed MDN is successfully verified by the sender with the receiving trading partner's public key and the returned MIC value inside the MDN is the same as the digest of the original message.

Validation

The receiver of either request or response messages MUST validate the message signature (PEPPOL issued X.509 certificates) including issuer signature, test of validity period and Certificate trust chain through PEPPOL provided root and intermediate certificates. Depending on local policy, the receiver SHOULD check revocation status of any certificates used to sign and encrypt the message.

The SrcAP SHOULD validate that the Subject Unique Identifier of the certificate used to sign the response messages matches the Subject Unique Identifier published in the Service Metadata Publishing.

When validating a signed response message, the sender Access Point SHOULD check that the certificate in the response matches the metadata received from the Service Metadata Publisher. This is done by comparing the subject common name in the certificate to the value stated in the metadata. This check ensures that only the legitimate Access Point stated in the service metadata will be able to produce correct responses.

Use of HTTPS

Messages MAY be encrypted using one-way TLS. However as the Message MUST be encrypted and authentication and authorization are assured without TLS then use of HTTPS is not required.

Reliable exchange behaviour

The Request-URI[2] identifies a process for unpacking and handling the message data and for generating a reply for the client that contains a signed message disposition acknowledgement (MDN). The MDN is returned in the HTTP response message body. This request/reply transactional interchange provides secure, reliable, and authenticated exchange using HTTP as a transfer protocol.

The following requirements ensure that the reliable messaging framework effectively delivers messages from SrcAP to DestAP, or leaves the Access Points with a clear status of the transmitted messages.

- The SrcAP MUST assume unacknowledged messages are not delivered or accepted and SHOULD resend within a reasonable time span.
- The SrcAP MUST assume that only messages which have been receipted without error or failure have been successfully delivered.
- If the SrcAP is sending a transmission, then the DestAP closes the connection after 5 to 15 seconds to allow the channel to be reused and/or ensure SrcAP has received the signed acknowledgement response.
- The SrcAP SHOULD keep a persistent log of these signed acknowledgements for a reasonable length of time.

[2] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

4 Appendix A

4.1 XML Schema for message headers

For an XML Schema for the header identifiers, see [BDEN-CDEF].

4.2 XML Example Failures/Errors

(Source RFC 4130)The following set of examples represents allowable constructions of the Disposition field that combine the historic constructions above with optional RFC 3798 error, warning, and failure fields. AS2 implementations MAY produce these constructions. However, AS2 servers are not required to recognize or process optional error, warning, or failure fields at this time. Note that the use of the multiple error fields in the second example below provides for the indication of multiple error conditions.

Disposition: automatic-action/MDN-sent-automatically; processed

Disposition: automatic-action/MDN-sent-automatically;
processed/error: decryption-failed
Error: The signature did not decrypt into a valid PKCS#1 Type-2 block.
Error: The length of the decrypted key does not equal the octet length of the modulus.

Disposition: automatic-action/MDN-sent-automatically;
processed/warning: duplicate-document
Warning: An identical message already exists at the
destination server.

Disposition: automatic-action/MDN-sent-automatically;
failed/failure: sender-equals-receiver
Failure: The AS2-To name is identical to the AS2-From name.