UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE

United Nations Centre for Trade Facilitation and Electronic Business

UN/CEFACT
Exchange Header Envelope (XHE)
Technical Specification

Version 1.0

29 June 2020

Abstract

This specification defines a business-oriented artefact either referencing (as a header) or containing (as an envelope) a payload of one or more business documents or other artefacts with supplemental semantic information about the collection of payloads as a whole. This is distinct from any transport-layer infrastructure header or envelope that may be required to propagate documents from one system to another. An exchange header envelope describes contextual information important to the sender and receiver about the payloads, without having to modify the payloads in any fashion.

Contents   Page

List of Figures   Page

1   Introduction

1.1   Conveying information about payloads

1.1.1   Overview

File or document headers have long been used to describe the information about a set of payloads in an entity that is kept separate and arm's-length from the payloads themselves.

The metaphor of a paper envelope in which one places business documents for transport or management is apt to describe the role of an exchange header envelope in a container relationship to its payloads. Concepts of routing, authentication, non-repudiation and concealment all apply in both the metaphor and the electronic equivalent.

1.1.2   What is an Exchange Header Envelope?

The Exchange Header Envelope (XHE) specifies an XML vocabulary [See 1.3 Normative References] expressing in machine- processable syntax the semantics of describing either a header to or an envelope of a set of payloads of content with information about that content. This vocabulary is modeled using the UN/CEFACT Core Component Technical Specification Version 2.01 [See 1.3 Normative References].

XHE, a specification developed jointly by UN/CEFACT and OASIS, is the successor to the UN/CEFACT Standard Business Document Header (SBDH) version 1.3 [See 1.4 Informative Reference] and the OASIS Business Document Envelope (BDE) version 1.1 [See 1.4 Informative Reference].

Note regarding publications: the UN/CEFACT Exchange Header Envelope and the OASIS Exchange Header Envelope are the same specification developed in collaboration and published as standards by the two organizations
following the practices of each.

This specification enumerates the information components of a payload header envelope and formally describes the semantics of each component.

Normative markings: all clauses not marked as "informative" and also not a subclause of a clause marked as "informative" are to be considered normative. All notes and examples are informative.

The XHE is designed to be either a header as an integral part of a business document (e.g. either XML instance document or EDI interchange), an object associated with the business document itself, or as an envelope functioning as wrapper that contains one or more business documents.

1.1.3   How is it used in EDI and XML environments?

There exist several business document exchange architectures and approaches, some using EDI formats and approaches, some using XML document types, and yet others use different document formats or non-standardized approaches. The XHE is designed to work with any document format and business process, whether standardized or not, and as such supports both the EDI, the XML and any other e-business community. Including a XHE in each instance of the business document reduces the effort needed to route and process documents and permits trading partner organizations to use different implementation approaches.

When implementing EDI, the provision of an additional business document header may not always be necessary, since EDI interchanges already contain functionality for some of the information in the XHE. An example is the UN/EDIFACT UNB interchange header, the UNH message header, and

the 'function' part of the BGM. The XHE specification allows for this existing approach and provides an option to express additional functionality, such as service and correlation information.

1.1.4   The Scope of the Exchange Header Envelope

Many users, implementers and supporting industry standard bodies are in agreement on the need for an Exchange Header Envelope. In their business-to-business activities, the XHE facilitates several different business needs:

— The routing of business documents from one point to another. This refers not only to the transfer of information from an external originator to receiver, but also from one intermediate application to another. Information in the XHE can help ensure that a document gets to the correct recipient.

— Ensuring integrity and confidentiality of business documents when routed over multiple hops, intermediaries, routers or access points, such as in 4-corner networks and architectures.

— Simplifying the bundling of several business documents or support documents into one package for simplified exchange.

— Facilitating the exchange of location pointers and access credentials to externally located business documents, not suitable for sending through an e-business network. This is necessary when the sending party needs to keep the business document confidential until a specified date (such as in tendering processes), and when sending very large files.

— The simplified processing of documents. Processing refers to taking action on data, for example transforming it from one format into another. Information in the XHE can reduce the effort required to determine the correct processing actions.

— Associating a data message with its originator is important from a business and legal perspective. It is especially important when using intermediaries for data transfer, as information from the transport protocol, may be lost after the initial transmission. Because information in the XHE is retained, it can help ensure that a document's originator is correctly identified.

In addition to header functions provided by the XHE for routing and/or processing of business documents, there is the need for a completely separate technical communications transport layer. This deals with communications protocols and physical addresses which are outside the scope of this technical specification. Transport specifications including EDIINT-AS2 and ebXML Message Service (ebMS) are among a number of possible transport options that address technical communications needs by defining a separate technical header. The transport layer is completely outside the scope as it is a different layer of the stack.

1.1.5   Dual Semantic Identifiers

This specification accommodates both UN/CEFACT and OASIS naming conventions of all semantic identifiers by documenting the two values for every business information entity. In each table row in section 2 Header and envelope information the semantic identifiers are provided in two sub-rows, the upper one carrying the UN/CEFACT semantic identifier and the lower one carrying the OASIS semantic identifier.

1.1.6   Stakeholders and Audience

All organizations that manage infrastructure operations and business processes for various functional areas (e.g. ordering, invoicing, planning, or financial), all service provider organizations

and associations, as well as e-business networks and infrastructures, which create, route and process business documents can benefit from the use of the Exchange Header Envelope.

1.2   Terminology

1.2.1   Key words

The key words MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, OPTIONAL and SHOULD in this document are to be interpreted as described in [See 1.3 Normative Reference].

1.2.2   Symbols and Abbreviations

1.2.2.1
ABIE
Aggregate Business Information Entity

1.2.2.2
BBIE
Basic Business Information Entity

1.2.2.3
ASBIE
Association Business Information Entity

1.2.2.4
RFC
Request for comment

1.3   Normative References

CCTS 2.01 UN/CEFACT Core Components Technical Specification, Version 2.0115 November 2003
http://www.unece.org/fileadmin/DAM/cefact/codesfortrade/CCTS/CCTS_V2-01_Final.pdf

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>.

XML Extensible Markup Language (XML) 1.0 (Fifth Edition), Bray T. , Paoli J. , Sperberg-McQueen C. M. , Maler E. , Yergeau F. , Editors, W3C Recommendation, November 26, 2008, http://www.w3.org/TR/2008/REC-xml-20081126/. Latest version available at http://www.w3.org/TR/xml/.

XMLDSIG-CORE1 XML-Signature Syntax and Processing Version 1.1, Eastlake D. E. , Reagle J. , Solo D. , Hirsch F. , Nyström M. , Roessler T. , Yiu K. , Editors, W3C Recommendation, April 11, 2013, http://www.w3.org/TR/2013/REC-xmldsig-core1-20130411/. Latest version available at http://www.w3.org/TR/xmldsig-core1/.

1.4   Informative References

BDE Business Document Envelope Version 1.1 Edited by G. Ken Holman and Kenneth Bengtsson. 05 December 2016. OASIS Committee Specification 01. Latest version: http://docs.oasis-open.org/bdxr/bdx-bde/v1.1/bdx-bde-v1.1.html.

RFC5652 Housley R. , Cryptographic Message Syntax (CMS), STD 70, RFC 5652, DOI 10.17487/ RFC5652,September 2009, https://tools.ietf.org/html/rfc5652.

genericode Code List Representation (Genericode) Version 1.0. Edited by Anthony B. Coates. 28 December 2007. Committee Specification 01. http://docs.oasis-open.org/codelist/genericode/. Latest version: http://docs.oasis-open.org/codelist/genericode/doc/oasis-code-list-representation-genericode.html.

RFC4880 Callas J. , Donnerhacke L. , Finney H. , Shaw D. , and Thayer R. , OpenPGP Message Format, RFC4880, DOI 10.17487/RFC4880, November 2007, https://tools.ietf.org/html/rfc4880.

SBDH UN/CEFACT Standard Business Document Header https://www.gs1.org/sites/default/files/docs/ gs1_un-cefact_%20xml_%20profiles/CEFACT_SBDH_TS_version1.3.pdf

XAdES XML Advanced Electronic Signatures. ETSI TS 101 903 V1.4.1, June 2009 http://uri.etsi.org/ 01903/v1.4.1/ts_101903v010401p.pdf

XMLENC-CORE1 XML Encryption Syntax and Processing Version 1.1, Eastlake D. , Reagle J. , Hirsh F., Roessler T., W3C Recommendation April 22, 2013, http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/. Latest version available at http://www.w3.org/TR/xmlenc-core1/.

2 **Header and envelope information**

2.1 XHE entity diagrams

The information derived for XHE has been distilled into a suite of CCTS Aggregate Business Information Entities (ABIEs), each comprised of a set of Basic Business Information Entities (BBIEs) and/or Association Business Information Entities (ASBIEs).

Each entity is listed with its two semantic identifiers, one specified by UN/CEFACT members of the development team, and one specified by OASIS members of the development team. See section 1.1.5 Dual Semantic Identifiers for more information.

The relationships between these business information entities are depicted in this class diagram using the UN/CEFACT names:
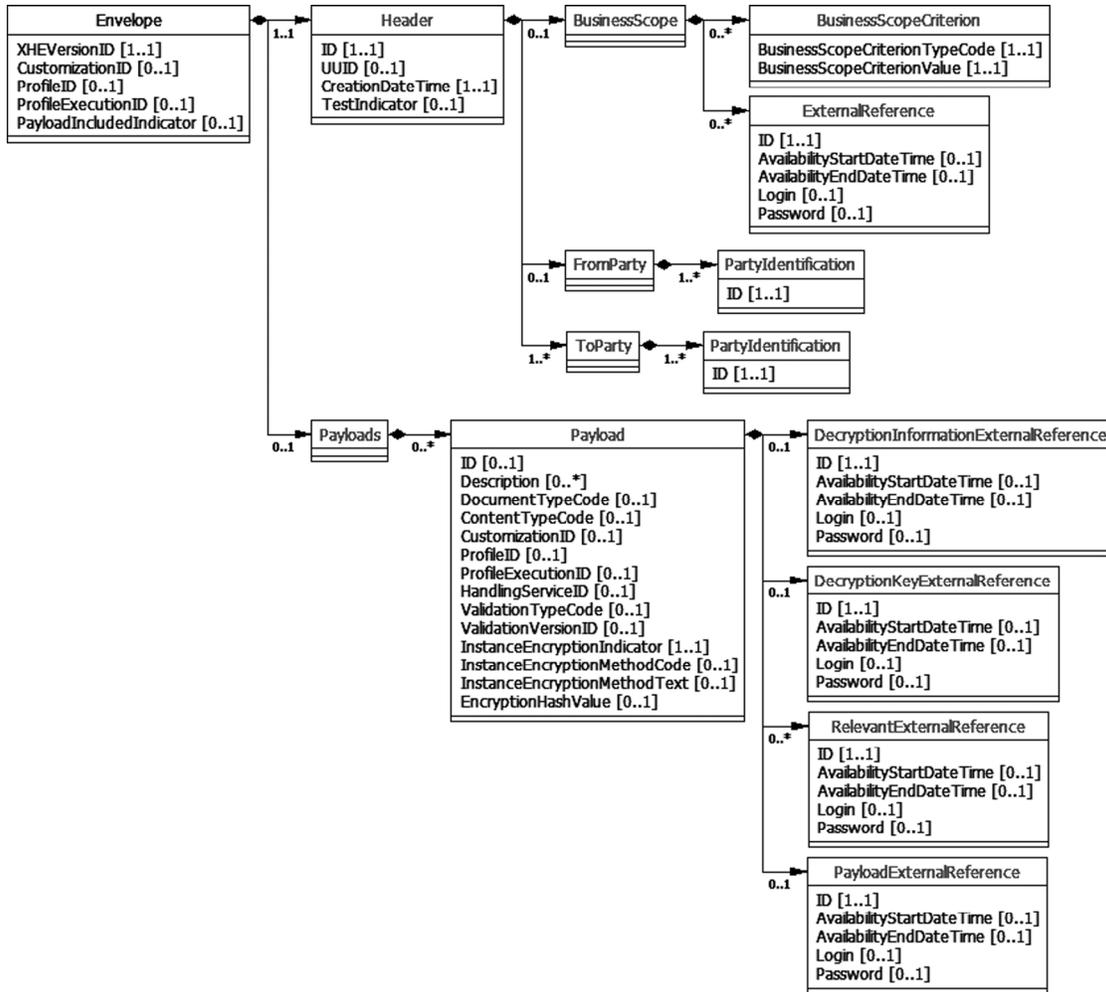
Figure 1 — Exchange Header Envelope entity diagram – UN/CEFACT names

The relationships between these business information entities are depicted in this class diagram using the OASIS names:
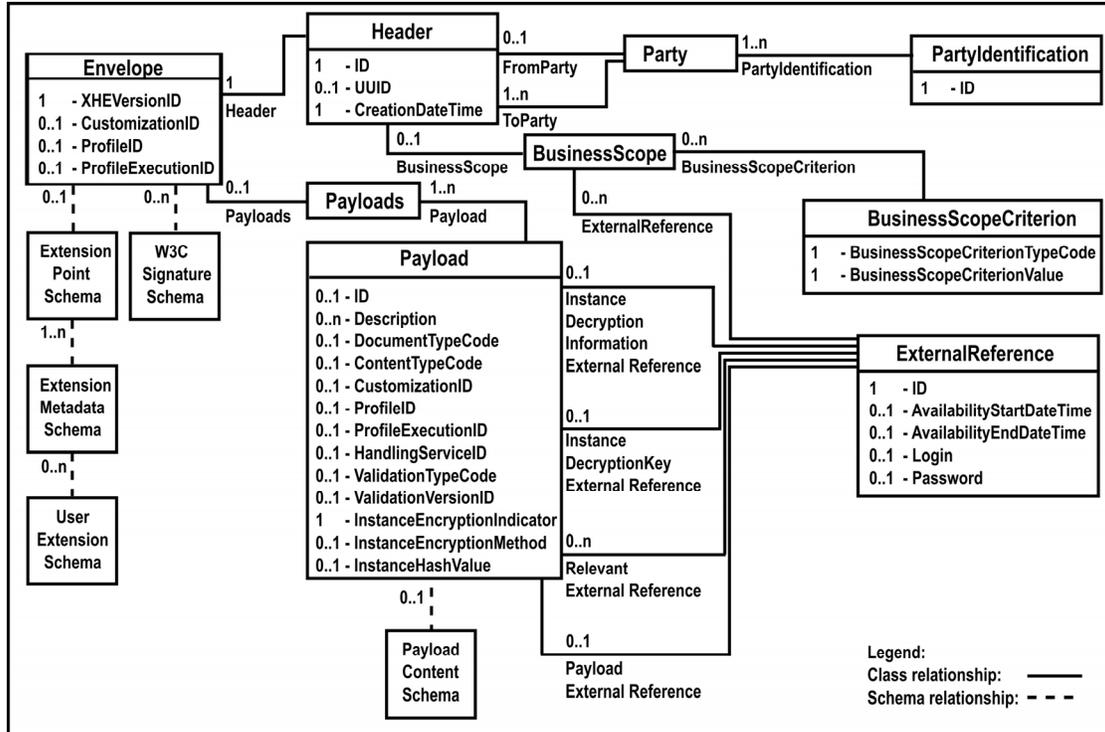
Figure 2 — Exchange Header Envelope entity diagram - OASIS names

2.2   Header envelope information

Metadata information about the header envelope itself, independent of the information it contains, includes the following:

Semantic identifier	Card.	Definition
XHE_ Envelope. Details	N/A	The Exchange Header Envelope
XHE. Details		
XHE_ Envelope. Version. Identifier	1	The version of the specific envelope model in use.
XHE. XHE Version Identifier. Identifier		
XHE_ Envelope. Customization. Identifier	0..1	The identification of a customization or use of the envelope model.
XHE. Customization Identifier. Identifier		
XHE_ Envelope. Profile. Identifier	0..1	The identification of a specific profile found within the customization.
XHE. Profile Identifier. Identifier		
XHE_ Envelope. Profile Execution. Identifier	0..1	The identification of a particular instance of using the given profile.
XHE. Profile Execution Identifier. Identifier		
XHE_ Envelope. Metadata. XHE_ Document	1	Information relevant to the handling of the envelope.
XHE. Header		
XHE_ Envelope. Included. XHE_ Payload	0..1	The set of payloads
XHE. Payloads		

The information for a header envelope ends with an additional optional and repeatable number of digital signatures that are neither a BBIE nor an ASBIE and so are not modeled using CCTS. Rather, these signatures are a schema artefact published by the W3C. See section 3.1 Signing the exchange header envelope for more information.

2.3 Header information

Metadata information about the header envelope itself, independent of the information it contains or references, includes the following:

Semantic identifier	Card.	Definition
XHE_ Document. Identification. Identifier	1	Unique ID of the envelope for tracking purposes.
Header. Identifier		
XHE_ Document. UUID. Identifier	0..1	An additional identifier of the envelope.
Header. UUID		
XHE_ Document. Creation. Date Time	1	Date and time when the envelope was created.
Header. Creation Date Time. Date Time		
XHE_ Document. Scope. XHE_ Context	0..1	Documentation of the scope of business or other contextual details useful to understand the purpose of the envelope and its contents. For examples: Europe vs Asia, Direct-to-Consumer vs Replenishment, or Prepaid vs Credit.
Header. Business Scope		
XHE_ Document. Sender. XHE_ Party	0..1	Information about the party that originated the envelope.
Header. From_ Party. Party		
XHE_ Document. Recipient. XHE_ Party	1..n	Information about the parties to receive the envelope.
Header. To_ Party. Party		

2.4 Party information

The information about a party includes the following:

Semantic identifier	Card.	Definition
XHE_ Party. Specified. XHE_ Identity	1..n	Unambiguous identifications of a party.
Party. Party Identification		

2.5 Party identification information

The information about a party's identification includes the following:

Semantic identifier	Card.	Definition
XHE_ Party. Specified. XHE_ Identity	1	An unambiguous identification of a party.
Party Identification. Identifier		

2.6 Business scope information

Documentation of the scope of business or other contextual details useful to understand the purpose of the envelope and its contents includes the following:

Semantic identifier	Card.	Definition
XHE_ Context. Specified. XHE_ Parameter	0..n	Internal specification of the scope and/or context of business.
Business Scope. Business Scope Criterion		
XHE_ Context. Scope. XHE_ Reference	0..n	External documentation of the scope and/or context of business.
Business Scope. External Reference		

2.7   Business scope criterion information

Documentation of one criterion of the scope of business or other contextual detail useful to understand the purpose of the envelope and its contents includes the following:

Semantic identifier	Card.	Definition
XHE_ Parameter. Type. Code	1	Identifies the property of the scope by a code.
Business Scope Criterion. Business Scope Criterion Type. Code		
XHE_ Parameter. Value. Text	1	Specifies the value of the given property.
Business Scope Criterion. Business Scope Criterion Value. Text		

2.8   External reference information

A reference to a business case, document or other issues which are relevant to the handling of the envelope includes the following:

Semantic identifier	Card.	Definition
XHE_ Reference. Identification. Identifier	1	Identifies the referenced object by some identifier or URI.
External Reference. Identifier		
XHE_ Reference. Start_ Availability. Date Time	0..1	The start date and time when the information is available
External Reference. Availability Start Date Time. Date Time		
XHE_ Reference. End_ Availability. Date Time	0..1	The end date and time when the information is available
External Reference. Availability End Date Time. Date Time		
XHE_ Reference. Login. Text	0..1	Text describing any login details to access the information.
External Reference. Login. Text		
XHE_ Reference. Password. Text	0..1	A password needed to access the information.
External Reference. Password. Text		

2.9   Payload information

2.9.1   Payload set information

Information about the complete set of payloads includes the following:

Semantic identifier	Card.	Definition
XHE_ Payload. Included. XHE_ Payload Instance	1..n	The actual payload instance, such as a single invoice, conveyed within the envelope.
Payloads. Payload		

2.9.2   Payload item information

Information about an individual payload within the set of payloads includes the following:

Semantic identifier	Card.	Definition
XHE_ Payload Instance. Identification. Identifier	0..1	A unique identification of this payload instance contained within the envelope.
Payload. Identifier		
XHE_ Payload Instance. Description. Text	0..n	Text description of the payload instance.
Payload. Description. Text		
XHE_ Payload Instance. Document_ Type. Code	0..1	Identifies the abstract archetype of the payload instance.
Payload. Document Type Code. Code		
XHE_ Payload Instance. Content_ Type. Code	0..1	Identifies the file format or octet representation of the payload instance.
Payload. Content Type Code. Code		
XHE_ Payload Instance. Customization. Identifier	0..1	Identifies the customization that applies to the payload instance.
Payload. Customization Identifier. Identifier		
XHE_ Payload Instance. Profile. Identifier	0..1	Identifies the profile that the payload instance is part of.
Payload. Profile Identifier. Identifier		
XHE_ Payload Instance. Profile Execution. Identifier	0..1	Identifies the particular instance of an executing profile that the payload instance is part of.
Payload. Profile Execution Identifier. Identifier		
XHE_ Payload Instance. Handling Service. Identifier	0..1	Identifies the service that should process the payload instance.
Payload. Handling Service Identifier. Identifier		
XHE_ Payload Instance. Validation_ Type. Code	0..1	The validation type of the payload, used for the task of verifying that the grammar of a payload is valid.
Payload. Validation Type. Code		
XHE_ Payload Instance. Validation Version. Identifier	0..1	Descriptor containing version information of the validation type.
Payload. Validation Version Identifier. Identifier		
XHE_ Payload Instance. Encrypted. Indicator	1	Indicator to state whether the payload instance is encrypted or not.
Payload. Instance Encryption Indicator. Indicator		
XHE_ Payload Instance. Encryption Method. Text	0..1	Method used to encrypt the payload instance.
Payload. Instance Encryption Method. Text		

Semantic identifier	Card.	Definition
XHE_ Payload Instance. Encryption Hash Value. Text	0..1	SHA-256 hash total of the unencrypted payload instance.
Payload. Instance Hash Value. Text		
XHE_ Payload Instance. Decryption. XHE_ Reference	0..1	Decryption information that is available external to the envelope.
Payload. Instance Decryption Information_ External Reference. External Reference		
XHE_ Payload Instance. Decryption Key. XHE_ Reference	0..1	Decryption key data that is available external to the envelope.
Payload. Instance Decryption Key_ External Reference. External Reference		
XHE_ Payload Instance. Relevant. XHE_ Reference	0..n	A reference to a business case, document or other issues which are relevant to the handling of the payload.
Payload. Relevant_ External Reference. External Reference		
XHE_ Payload Instance. Payload. XHE_ Reference	0..1	The reference to the payload when it is not included within the envelope.
Payload. Payload_ External Reference. External Reference		

The information for an individual payload ends with an additional optional payload content item that is neither a BBIE nor an ASBIE and so is not modeled using CCTS. Rather, this content item is a schema artefact. This content item has the cardinality 0..1. This content item can have as its child either text only (no elements) or a single element, but not a combination of both nor more than one element.

3   XHE digital signatures

3.1   Signing the exchange header envelope

Using the IETF/W3C XML Digital Signature specification [XMLDSIG-CORE1] one can add multiple "non-final" signatures or a single "final" signature to the exchange header envelope as the last children of the document element, that is, after the last BIE of the document element. A non-final signature digitally signs all content other than any of the other sibling signature elements that may exist in the document. A final signature digitally signs all content including the other sibling signature elements that may exist in the document.

4   Conformance

In this conformance clause, the following abbreviated references to semantic identifiers are used for readability:

— payload information item

  — (UN/CEFACT) XHE_ Payload. Included. XHE_ Payload Instance

  — (OASIS) Payloads. Payload

— payload external reference information item

— (UN/CEFACT) XHE_ Payload Instance. Payload. XHE_ Reference

— (OASIS) Payload. Payload_ External Reference. External Reference

An Exchange Header Envelope instance exhibits conformance when complying with all of the following semantic criteria:

1) All semantic components defined by this specification, that is all information that is not found inside payload content or extension content, SHALL NOT have no value (that is, it SHALL NOT be empty).

2) When the XHE is embedded in a bounding document as a header, the properties of the first of all payload information items, if any are present, SHALL apply to the bounding document and SHALL NOT have either payload content nor the payload external reference information item child. Subsequent payload information items, if any are present, SHALL have one or the other of payload content or the payload external reference information item child (that is, it SHALL NOT have both and SHALL NOT have neither).

3) When the XHE is standalone in its own document as an envelope, all payload information items SHALL have one or the other of payload content or the payload external reference information item child (that is, it SHALL NOT have both and SHALL NOT have neither).

4) Each payload content SHALL NOT have a combination of text and an XML element (that is, it SHALL either be a non-empty string of text or be a single XML element).

Annex A
(informative)

Package structure

The base directory has the following files:

— **xhe-v1.0-cs02-cefact.pdf**

    — This document.

The document model is expressed in four ways, found in four files of the model subdirectory:

— **mod**

    — **XHE-Model-1.0.ods**

        — model information expressed in an OpenOffice spreadsheet

    — **XHE-Model-1.0.xls**

        — model information expressed in an Excel spreadsheet

    — **XHE-Model-1.0.gc**

        — model information expressed in a genericode [genericode] file

    — **XHE-Model-1.0.html**

        — model information expressed in hyperlinked human-readable tables as HTML

Annex B
(informative)

Revision History

B.1 Major version XHE 1.0

XHE version 1.0 establishes the initial suite of semantic components as a basis for all subsequent minor revisions of the Exchange Header Envelope.

Annex C
(informative)

Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Kenneth Bengtsson (co-chair)
Michel Bormans
Gait Boxman
Anders Grangard (co-chair)
G. Ken Holman (editor)

Annex D
(informative)

Encrypting payloads to multiple recipients

The XHE supports sending business documents to multiple recipients using a single envelope, which is obtained by adding multiple instances of the ToParty element to the XHE envelope.

When encrypting payloads of envelopes with multiple recipients, users SHOULD make use of encryption technologies that support multiple recipients so that an encrypted payload to multiple recipients can be contained in a single instance of an XHE envelope's PayloadContent. Examples of encryption technologies supporting multiple recipients are [RFC5652], [RFC4880] and [XMLENC-CORE1].

The workings of individual encryption technologies and methodologies are beyond the scope of this specification.