# TECHNICAL SPECIFICATION

# IEC TS 62325-502

First edition
2005-02



## Framework for energy market communications –

## Part 502:
## Profile of ebXML

Reference number
IEC/TS 62325-502:2005(E)

## Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

## Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

## Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

# TECHNICAL SPECIFICATION IEC TS 62325-502

First edition
2005-02



## Framework for energy market communications –

## Part 502: Profile of ebXML



International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE U

*For price, see current catalogue*

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# FRAMEWORK FOR ENERGY MARKET COMMUNICATIONS –

# Part 502: Profile of ebXML

## FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards. [1]

IEC 62325-502, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.



[1] This would also include the specification of some options/parameters not yet specified in the profile, Annex A.

The IEC 62325 series cancels and replaces IEC 62195 (2000) and its amendment (2002). It constitutes a technical revision.

IEC 62195 (2000) dealt with deregulated energy market communications at an early stage. Its amendment 1 (2002) points out important technological advancements which make it possible to use modern internet technologies based on XML for e-business in energy markets as an alternative to traditional EDI with EDIFACT and X12. The new IEC 62325 framework series for energy market communications currently consisting of IEC 62325-101, IEC 62325-102, IEC 62325-501, and IEC 62325-502 follows this direction and replaces IEC 62195 together with its amendment.

The text of this technical specification is based on the following documents:

| Enquiry draft | Report on voting |
|---|---|
| 57/707/DTS | 57/724/RVC |

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IEC 62325 consists of the following parts, under the general title *Framework for energy market communications*:

Part 101: General guidelines
Part 102: Energy market model example
Part 201: Glossary [2]
Part 3XX: (Titles are still to be determined) [3]
Part 401: Abstract service model [4]
Part 501: General guidelines for use of ebXML
Part 502: Profile of ebXML
Part 503: Abstract service mapping to ebXML [4]
Part 601: General guidelines for use of web services [4]
Part 602: Profile of Web Services [4]
Part 603: Abstract service mapping to web services [4]



2 Under consideration. Because the technologies have an inherent own glossary within their standard definitions, this glossary is a placeholder for a glossary for future parts indicated with [2)] including energy market specific terms and definitions.

3 Under consideration. These parts for business content are mentioned for completeness only with a number space as placeholder. They extend the original scope and require an agreed new work item proposal for further work based on an overall strategy how to proceed.

4 Under consideration. These technical parts are mentioned for completeness with provisional title. They extend the original scope and require an agreed new work item proposal for further work.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual edition of this document may be issued at a later date.

# INTRODUCTION

With the transition of monopoly energy supply structures to deregulated energy markets, the function of the markets depends heavily on seamless e-business communication between market participants. Compared with global e-business, e-business in the energy market is only a small niche. Today EDIFACT or X12 messages, or propriety HTML and XML solutions based on Internet technologies are being used.

The 'electronic business Extensible Markup Language' (ebXML) specification and architecture stems from UN/CEFACT and OASIS and these are now partly standards within the ISO 15000 series being complemented in future to cover all aspects of ebXML. ebXML is a complete set of specifications and standards to enable secure electronic business using proven, open standards such as TCP/IP, HTTP, SOAP, XML, and SOAP signature and encryptation. ebXML is also evolutionary in nature, built on 25 years of EDI experience, designed to work with existing EDI solutions, or be used to develop an emerging class of internet based electronic business applications based on XML. This means that with ebXML existing EDI messages (EDIFACT, X.12) as well as XML messages can be exchanged.

Profiles of ebXML allow the re-use of proven core components and communication platforms across markets, thus saving cost and implementation time.

.

# FRAMEWORK FOR ENERGY MARKET COMMUNICATIONS –

# Part 502: Profile of ebXML

## 1 Scope

This part of IEC 62325 specifies an energy market specific messaging profile based on the ISO 15000 series. The profile is intended to provide the basis for system configuration.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/TS 15000-1:2004, *Electronic business eXtensible Markup Language (ebXML) – Part 1: Collaboration-protocol profile and agreement specification (ebCPP)*

ISO/TS 15000-2:2004, *Electronic business eXtensible Markup Language (ebXML) – Part 2: Message service specification (ebMS)*

UN/CEFACT, *ebXML Business Process Specification Schema*, v1.10 or higher

UN/CEFACT, *ebXML Technical Architecture Specification*, v1.04 or higher

In this part of IEC 62325, RFCs (Request for comments) from the Internet Engineering Task Force (IETF) and recommendations from other Organisations such as the Word Wide Web Consortium (W3C) and the Organization for the Advancement of Structured Information Standards (OASIS) are mentioned which are not included here because these documents are referenced in the references above.

## 3 Terms, definitions and abbreviations

### 3.1 Terms and definitions

None.

### 3.2 Abbreviations

| | |
|---|---|
| A2A | Application-to-Application |
| AES | Advanced Encryption Standard |
| B2B | Business-to-Business |
| BDS | Business Document Specification (instance) |
| BDSS | Business Document Specification Schema |
| BIE | Business Information Entity |
| BOV | Business Operational View |
| BPMS | Business Process Management System |
| BPSS | Business Process Specification Schema (or instance) |
| BSI | Business Service Interface |

| | |
|---|---|
| CC | Core Component (based on BIE) |
| CIM | Common Information Model |
| CPA | Collaboration Protocol Agreement |
| CPP | Collaboration Protocol Profile |
| DSO | Distribution System Operator (of power system |
| DUNS | Data Universal Numbering System (North America) |
| EAN | European Article Number (Europe) |
| ebMS | ebXML Messaging Service |
| ebXML | electronic business XML |
| EDI | Electronic Data Exchange |
| EIA | Enterprise Application Integration |
| EMS | Energy Management Systems |
| ERP | Enterprise Resource Planning |
| FOV | Functional Service View |
| FTP | File Transfer Protocol |
| HTTP | Hypertext Transport Protocol |
| ICT | Information and Communication Technology |
| ISO | Independent System Operator |
| IT | Information Technology |
| MIME | Secure/Multipurpose Internet Mail Extensions |
| MIS | Market Identification Schema |
| MOM | Message-oriented middleware |
| MSH | Message Service Handler |
| PKI | Public Key Infrastructure |
| QoS | Quality of Service |
| RPC | Remote Procedure Call |
| RR | Registry / Repository |
| SAML | Security Assertion Mark-up Language |
| SCADA | Supervision, Control, and Data Acquisition |
| SMTP | Simple Mail Transfer Protocol |
| SO | System Operator (of power system) |
| SOAP | Simple Object Access Protocol |
| TLS | Transport Layer Security |
| TSO | Transmission System Operator (of power system) |
| UML | Unified Modelling Language |
| UMM | UN/CEFACT Modelling Methodology |
| VPN | Virtual Private Network |
| WS | Web Services |
| WSDL | Web Services Definition Language |
| XML | eXtensible Markup Language |
| XKMS | XML Key Management Specification |

# 4 Guideline of how to use the architecture

## 4.1 Profile of the architecture

Within the ebXML specification framework, two business partners agree on how to perform e-business using machine-readable Trading Partner Agreements based on XML syntax and named Collaboration Profile Agreements (CPA). In the general case of global e-business, the CPA is negotiated as the intersection of the Collaboration Protocol Profiles (CPP) of these two partners, who may have discovered each other using the registry partner-discovering feature.

Energy markets normally exist in a specific geographical area or geopolitical region with known business partners, agreed market rules and communication infrastructure. In this environment, a simplification may be possible where alternatively pre-negotiated CPA's of each business process are stored pre-defined in the registry/repository and can be downloaded for use.

Within each market, a profile or a limited set of profiles of the ebXML architecture should be used to harmonise and simplify e-business. Since the ebXML specification framework does not define any market specific profiles, the profile for energy markets has to be specified. In the following business process driven BPSS "security profiles", CPP/CPA "technical profiles" and "messaging profiles" are specified.

For better understanding of the profiles defined below 4.2 to 4.4, Figure 1 shows the configuration files used with its content structure.

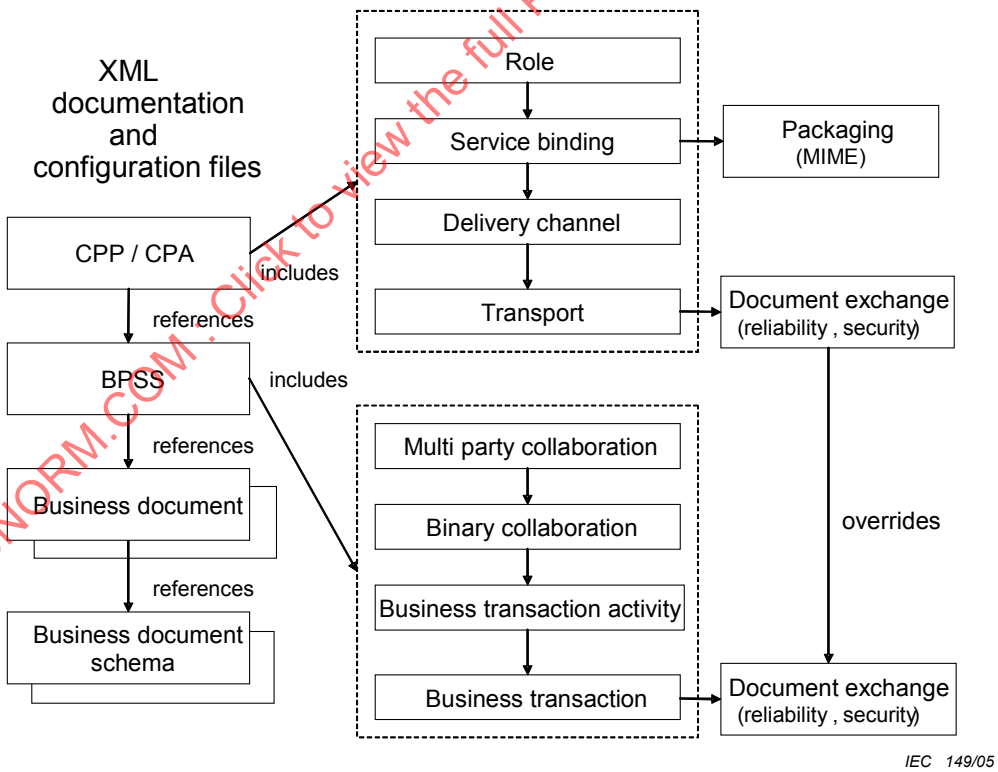


**Figure 1 – References and content of ebXML documents**

### 4.2 Security profile of the BPSS

The ebXML BPSS instance provides the possibility for a collaboration to specify message reliability and message security, including non-repudiation with legally binding at the business level.

The BPSS is used for more than one collaboration between market participants. Note that the CPA for a specific collaboration may therefore override the reliability, non-repudiation and security attribute values of a BPSS.

Table 1 shows the *recommended profiles*. Reliability is included in all profiles. Profile #1 only provides reliability. Profile #2 adds *non-persistent* (transient) confidentiality and *non-persistent* (transient) authentication (on transport or network level, for example TLS, IPsec). Profile #3 adds *persistent* confidentiality, *persistent* authentication, and tamper-proof messages (signed messages with keyed digest). The latter is sometimes also called non-repudiation of origin. Profile #4 is for full *persistent* security including *persistent* non-repudiation and invoked authorisation. The profiles #3 and #4 should be preferred because only these profiles guarantee end-to-end persistent security and non-repudiation within a market with established relationships.

The table also includes the mapping of the BPSS profiles to the MSH profiles 0, 3, 16, and 21. The MSH profiles 16 and 21 can be optional, used with a *trusted* time stamp if this service is available and needed.

For the sake of compatibility within a project or market, choices have to be made about:

- the location of the persistent security services. *Persistent* end-to-end security should be implemented on application level by default. The optional use of MSH security services, if supported, is a project or market decision;
- a single BPSS profile for each process. Different processes can have different BPSS profiles, depending of the need for security.

In the following subclauses, the BBSS attribute options which have to be chosen according to the recommended profiles in Table 1 are shown. The signature should apply to the whole message, including the envelope where the Signature element is contained. The partial signing of XML documents should not be used for sake of simplicity, because there is no known requirement.

**Table 1 – BPSS profiles for reliability, non-repudiation, and security**

| Feature | Options | Profile #1 | Profile #2 | Profile #3 | Profile #4 |
|---|---|---|---|---|---|
| MSH profile | Supported Security Services | 0 | 3 | 16 | 21 |
| Persistence | *Persistent* Security and Non-repudiation | NA | NO | YES | YES |
| Reliability | | | | | |
| | Guaranteed Delivery (acknowledgement, retry) [1)] | X | X | X | X |
| | Intelligible Check (message validation with a schema) | X | X | X | X |
| Non-repudiation | | | | | |
| | Non-Repudiation (saved audit trail of documents) | | | | X [2)] |
| | Non-Repudiation of Receipt (signed receipt) [1)] | | | | X [2)] |
| | Legally Binding (legal document) | | | | X |
| Security | | | | | |
| | Authorization Required (validation of identity, e.g. SAML) | | | | X |
| | Tamper Proof (signed message and keyed digest) | | | X | X |
| | Confidential (encryption) | | X [1)] | X | X |
| | Authenticated (proof of identity) | | X [1)] | X | X |

1) Service of the MSH.
2) Alternatively.



### Message reliability

Messages are received, validated and accepted. This concept is based on acknowledgements on the messaging level and validation of received messages with schemas. Table 2 shows the reliability options and choices.

Within the reliability profile, all options should be true and all parameters should be filled in.

- Profile 1, 2, 3, 4: reliability with all attributes mandatory and true and parameters filled in.

**Table 2 – Message reliability**

| Element | Attribute | m/o | Options and choices or remark |
|---|---|---|---|
| BusinessTransaction/ | | m | |
| | isGuaranteedDeliveryRequired | m | “true” |
| RequestingBusinessActivity | | m | > 0, e.g. “P2H” |
| | isIntelligibleCheckRequired | m | “true” |
| | timeToAcknowledgeReceipt | m | > 0, e.g. “P2H” |
| | timeToAcknowledgeAcceptance | m | > 0, e.g. “P4H” |
| RespondingBusinessActivity | | | |
| | isIntelligibleCheckRequired | m | “true” |
| | timeToAcknowledgeReceipt | m | > 0, e.g. “P2H” |
| BusinessTransactionActivity | | | |
| | timeToPerform | m | > 0, e.g. “P1D” |

The column m/o means mandatory/optional.

### Non-repudiation and legally binding security

Messages are signed in order to provide message and sending party authentication, non-repudiation and to make them legally binding. Furthermore, authorisations can be configured. Table 3 shows non-repudiation and legally binding options and choices.

Within the non-repudiation profile, the following should be used:

- Profile 1, 2, 3: Non-repudiation with all attributes “false”, or
- Profile 4: Non-repudiation with the “isNonRepudiationRequired” or the “isNonRepudiationOfReceiptRequired” attribute “true”.

The attribute “isLegallyBinding” is “true” by default. If true, the market participants agree that the business commitment of exchanged messages within a transaction can be enforced in court.

**Table 3 – Non-repudiation and legally binding**

| Element | Attribute | m/o | Options and choices or remark |
|---|---|---|---|
| BusinessTransaction/ | | m | |
| RequestingBusinessActivity | | | |
| | isNonRepudiationRequired | o | “false” or “true” (save an audit trail, message digest) |
| | isNonRepudiationOfReceiptRequired | o | “false” or “true” (signed receipt) |
| RespondingBusinessActivity | | | |
| | isNonRepudiationRequired | o | “false” or “true” (save an audit trail, message digest) |
| | isNonRepudiationOfReceiptRequired | o | “false” or “true” (signed receipt) |
| BusinessTransactionActivity | | | |
| | isLegallyBinding | o | Default “true”, “false” |
| The column m/o means mandatory/optional. | | | |

### Message security

Security provides authorisation, authentication and confidentiality. Table 4 shows the security options and attributes. The following should be used:

- Profile 1: no security with the isAuthorizationRequired attribute “false” and all other attributes “none”, or
- Profile 2: security with the “isConfidential” and “isAuthenticated” attribute “transient”, or
- Profile 3: security with the “isConfidential”, “isAuthenticated”, and “isTemperProof” attribute “persistent”, or
- Profile 4: security with the isAuthorizationRequired attribute “true” and all other attributes “persistent”.

**Table 4 – Authorisation, Authentication and confidentiality**

| Element | Attribute | m/o | Options and choices or remark |
|---|---|---|---|
| BusinessTransaction/ | | m | |
| RequestingBusinessActivity | | | |
| | isAuthorizationRequired | o | "false" or "true" |
| RequestingBusinessActivity/ DocumentEnvelope | | | |
| | isTamperProof | o | "none" or "persistent" (signed message) |
| | isConfidential | o | "none" or "transient", "persistent" |
| | isAuthenticated | o | "none" or "transient", "persistent" |
| RespondingBusinessActivity | | | |
| | isAuthorizationRequired | o | "false" or "true" |
| RequestingBusinessActivity/ DocumentEnvelope | | | |
| | isTamperProof | o | "none" or "persistent" (signed message) |
| | isConfidential | o | "none" or "transient", "persistent" |
| | isAuthenticated | o | "none" or "transient", "persistent" |
| The column m/o means mandatory/optional. | | | |

## 4.3 Profile of the CPP/A

The mandatory elements and possible choices and options of the CPP version 2.0 are shown in Table 5.

### Party identification and reference

Within the "PartyInfo" element, the sub element "PartyID" is used to unambiguously identify the market participant. It has a string content attribute and a type attribute with a string value. The string content provides the identifier based on a *Market Identification Schema* defined by the type attribute string value. There can be multiple PartyIDs if different market identification schemas identify a single organisation. The latter is also used for migration from several market identification schemas to a future agreed single one.

The "PartyRef" element is an Xlink simple link, which can store references to other (descriptive) information about the party. It typically would reference the organisation's website. It is *not* used in this framework.

### Document security (optional)

The "Characteristics" sub element of "DeliveryChannel" specifies *optional* document security and is normally empty, but can be used bilaterally to override the values specified in the BPSS. If document security is used, all attributes or only the confidentiality option should be set to "true" if not already done in the BPSS (4.3). In this case, within the element "DocExchange", the sub element "NonRepudiation" for digital signatures or "DigitalEnvelope" for encryption becomes mandatory and all shown parameters should be filled in.

### Transport security (optional)

The "Characteristics" sub element of "DeliveryChannel" specifies *optional* non-persistent transport security and is normally empty but can be used bilaterally to override the value specified in the BPSS. Secure transport depends on the security method and is chosen if secure transport is used. In this case, the sub element "TransportSecurity" element of Transport should be filled in.

**Table 5 – CPP/CPA options and choices**

| Element | Sub element or attribute | Sub element or attribute | n | m/o | Options and choices or remark |
|---|---|---|---|---|---|
| PartyInfo | | | 1 | m | |
| | PartyID | | | m | |
| | PartyRef | | | o | Not used. |
| | Certificate | | | o | For public key-based security |
| CollaborationRole | | | 1 | m | |
| | ProcessSpecification | | | m | Identifies BBSS |
| | Role | | | m | Initiating or responding role of partner within BPSS |
| | ServiceBinding | | | m | Binds channel, packaging |
| | | - channelID | | m | |
| | | - packageID | | m | |
| | | - Service (…) | n | m | Only 1 |
| | | Override | | o | |
| DeliveryChannel | | | 1 | m | |
| | - channelID | | | m | Ref by ServiceBinding |
| | - transportID | | | m | References Transport |
| | - docExchangeID | | | m | References DocExchange |
| | Characteristics | (overrides BPSS!) | | m | Normally empty |
| | Document level security | - synchReplyMode | | o | Default “none” |
| | | - nonrepudiationOfOrigin | | o | Empty or “true” or “false” |
| | | - nonrepudiationOfReceipt | | o | Empty or “true” or “false” |
| | | - secureTransport | | o | Default “false” |
| | | - confidentiality | | o | Empty or “true” or “false” |
| | | - authenticated | | o | Empty or “true” or “false” |
| | | - authorized | | o | Empty or “true” or “false” |
| Packaging | | | n | m | Only 1. MIME. |
| | - id | | | m | Ref by ServiceBinding |
| | ProcessingCapabilities | | | | |
| | | - parse | | m | “true” |
| | | - generate | | m | “true” |
| | SimplePart | | n | | |
| | | - id | | m | |
| | | - mimetype | | m | |
| | | - mimeparameters | | o | |
| | | NamespaceSupported | | o | |
| | CompositeList | | 1 | | |
| | | Composite (id, mimetype) | n | m | |
| Transport | | | n | m | |
| Protocols and Transport level security | - transportID | | | | |
| | SendingProtocol | | 1 | | |
| | | - version | | m | Version of transport protocol |
| | | protocol (HTTP or SMTP, …) | | m | “HTTP” or “SMTP” |
| | ReceivingProtocol | | 1 | | |
| | | - version | | m | Version of transport protocol |
| | | - protocol (HTTP or SMTP, ..) | | m | “HTTP” or “SMTP” |
| | TransportSecurity | | 1 | o | For transport level security |
| | if no message level security is defined | Protocol (version, type) | | o | e.g. version 3, “SSL” or “TLS” |
| | | CertificateRef (certID) | | o | |
| DocExchange | | | n | | |

| | | | | | |
|---|---|---|---|---|---|
| Message level security (replaces transport level security) | - docExchangeID | | | m | |
| | ebXMLBinding | | | m | |
| | - version | | | m | Version of ebXML, e.g. “2.0” |
| | - ReliableMessaging | | | m | Used |
| | | idempotency | | m | “true” (check of duplicates) |
| | | deliverySemantics | | m | “OnceAndOnlyOnce” |
| | | messageOrderSemantics | | m | Guaranteed |
| | | Retries (…) | | m | Any Number |
| | | RetryInterval (…) | | m | Any number of Seconds |
| | | PersistentDuration (…) | | m | e.g. “P40D” for 40 days |
| | - NonRepudiation | | | o | See profile of BPSS |
| | | Protocol | | m | “application/signature+xml” |
| | | HashFunction | | m | “SHA-1” |
| | | SignatureAlgorithm | | m | “DH” (Diffie-Hellman, ANSI X9.42) with DSS |
| | | CertificateRef | | m | Reference to the certificate which binds the public key |
| | - DigitalEnvelope | | | o | See profile of BPSS |
| | | Protocol | | m | “application/encryption+xml” |
| | | EncryptionAlgorithm | | m | “AES-128” with CBC |
| | | CertificateRef | | m | Reference to the certificate which binds the public key |
| | - NamespaceSupported | | | o | Used |
| | | Location | | m | |
| | | Version | | m | |
| The column m/o means mandatory/optional. | | | | | |

In Tables 6 and 7, two alternative profiles of persistent security features and parameters are shown that depend on the encryption technology used. These profiles apply if no transport level security such as SSL or TLS is used. In the energy market, the default XML encryption should be AES-128 (Advanced Encryption Standard with Cipher Block Chaining and 128 bit key) or one of the alternatives below if XML Encryption is not available for any reason.

Table 6 shows the parameters for S/MIME v3.

The packaging mime type is “multipart/signed” and “mime/application-pkcs7”.

**Table 6 – S/MIME v3 security parameters**

| **DocExchange** | | | **n** | **m/o** | |
|---|---|---|---|---|---|
| | DigitalEnvelope | | | o | Used |
| | | Protocol | | m | S/MIME v3 |
| | | EncryptionAlgorithm | | m | TripleDES (DES EDE3 CBC) |
| | | CertificateRef | | m | Reference to the certificate which binds the public key |
| | NamespaceSupported | | | o | Used |
| | | location | | m | |
| | | version | | m | |
| The column m/o means mandatory/optional. | | | | | |

Table 7 shows the parameters for OpenPGP/MIME.

The packaging mime type is “multipart/signed” and “multipart/encrypted”.

**Table 7 – OpenPGP/MIME security parameters**

| DocExchange | | | n | m/o | |
|---|---|---|---|---|---|
| | DigitalEnvelope | | | o | Used |
| | | Protocol | | m | |
| | | EncryptionAlgorithm | | m | TripleDES (DES EDE3 Eccentric CFB) |
| | | CertificateRef | | m | Reference to the certificate which binds the public key |
| | NamespaceSupported | | | o | Used |
| | | location | | m | |
| | | version | | m | |
| The column m/o means mandatory/optional. | | | | | |

### 4.4 Messaging service profile

The ebXML Message Service (MS) has many options and alternatives. Annex A describes the profile of the ebXML MS implementation with the OASIS ebXML messaging service deployment template for the ebXML Message Service Specification 2.0.

## 5 Implementation level

The implementation of ebXML can follow a stepwise approach from level to level or can have a certain level just from the beginning. Annex B shows possible implementation levels of ebXML based on the above defined profiles.

# Annex A
(normative)

# Message service profile

## A.1 General

The ebXML Message Service (MS) has many options and alternatives. This annex describes the profile of the ebXML MS implementation with the OASIS ebXML messaging service deployment template for the ebXML Message Service Specification 2.0.

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 items that are not relevant, "Not Applicable" is specified. Likewise, "No Recommendation Given" will indicate that there is no modification or preference for an item notated as such. The Deployment Guide may also note "Recommendation Pending" for items that are likely to be specified in future versions of this profile.

Numbers before titles refer to chapters in the ebXML Message Service Specification 2.0.

## A.2 Business-level requirements

The items in this section are intended to be answered by a business process designer, and are either specific to the use cases and Business Processes being deployed, or are a matter of general policy.

### 3.1.1.1 PartyId Element

| Specification | Value |
|---|---|
| Is a specific standard used for party identification? Provide details. | No recommendation made. See IEC 62325-101 of this series for examples. |

### 3.1.2 CPA Access

| Specification | Value |
|---|---|
| Is a specific registry for storing CPAs required? If so, provide details. | No recommendation made. |
| Is there a set of predefined CPA templates that can be used to create given Parties' CPAs? | Predefined CPA templates SHOULD be used where possible. |

### 3.1.4 Service Element

| Specification | Value |
|---|---|
| Are Services (related groups of Actions) defined for each party of each business process? List them, or provide a reference to the source of these values. | No recommendation made. |

#### 3.1.5 Action Element

| Specification | Value |
|---|---|
| Are Actions defined for each party to each business process? List them, or provide a reference to the source of these values. | No recommendation made. |

#### 3.1.1.2 Role Element

| Specification | Value |
|---|---|
| Are Roles defined for each party of each business process? List them, or provide a reference to the source of these values. [Per-process; may reference Role values in BPSS definitions] | No recommendation made. Depends on business and information model. |

### Appendix C Supported Security Services

| Specification | Value |
|---|---|
| Which security profile(s) are used, and under what circumstances (for which Business Processes)? [Refer to Appendix C of Message Service Specification. May be partially captured by BPSS isConfidential, isTamperproof, isAuthenticated definitions.] | This depends on the security requirements of business processes.<br><br>See BPSS profiles in 4.3. For high security, it is it is RECOMMENDED to adopt persistent security at the application level, including persistent digital signature, persistent signed receipt, persistent confidentiality, persistent authentication. |
| Are any specific third-party security packages approved or required? | No recommendation made. |

#### 4.1.2 Security and Management

| Specification | Value |
|---|---|
| What security and management policies and practices are recommended? | No recommendation made. |

### 6.6 Reliable Messaging Combinations

| Specification | Value |
|---|---|
| Which Reliable Messaging feature combinations are required? | The CPA profile in 4.4 SHALL be used. |

## A.3 Technical-level requirements

This clause requires an in-depth knowledge of the ebXML message service and all its constituent standards and technologies, and their application to the specific use cases and Business Processes of the user community being addressed.

### 2 ebXML with SOAP

### 2.1 Packaging Specification

#### 2.1.3 Header Container

#### 2.1.3.2 charset attribute

| Specification | Value |
|---|---|
| Is the "charset" parameter of Content-Type header necessary?<br><br>If so, what is the (sub)set of allowed values? | No recommendation made. |

#### 2.1.4 Payload Container

| Specification | Value |
|---|---|
| How many Payload Containers must be present?<br>What is the structure and content of each container? [List MIME Content-Types and other process-specific requirements.]<br>How is each container distinguished from the others? [By a fixed ordering of containers, a fixed Manifest ordering, or specific Content-ID values.] | No recommendation made. |

### 2.3 ebXML SOAP Envelope extensions

#### 2.3.6 #wildcard Element Content

| Specification | Value |
|---|---|
| Are additional namespace-qualified extension elements required? If so, specify. | No recommendation made. |

#### 2.3.7 id attribute

| Specification | Value |
|---|---|
| Is a unique “id” attribute required for each (or any) ebXML SOAP extension elements, for the purpose of referencing it alone in a digital signature? | No recommendation made. |

#### 2.3.8 version attribute

| Specification | Value |
|---|---|
| Is a version other than "2.0" allowed or required for any extension elements? | No recommendation made. |

## A.4 Core extension elements

### 3.1 MessageHeader Element

#### 3.1.1 From and To Elements

##### 3.1.1.1 PartyId Element

| Specification | Value |
|---|---|
| Should multiple PartyId elements be present in From and To elements? | No recommendation made. |
| Is the type attribute needed for each PartyId, and if so, what must it contain? | The value of the type attribute SHOULD be URI. |

#### 3.1.2 CPAId Element

| Specification | Value |
|---|---|
| What identification scheme is used for the CPAId, and what form should it take? [If a URI, how is it constructed? Does it reference a real CPA, or is it just a symbolic identifier? | The value of the CPAId SHOULD be a concatenation of the Sender and Receiver Identifications followed by a four digit serial number. |

### 3.1.4 Service Element

| Specification | Value |
|---|---|
| Is there a defined "type" for Service elements? If so, what value must the type attribute contain? | The value of the type attribute MUST be "URI". |
| If not provided in Business-Level Requirements above, what is the set of possible values for the Service element? Is there a URI format scheme for this element? | [See reference in Business Requirements section.] |

### 3.1.6 MessageData Element

#### 3.1.6.2 Timestamp Element

| Specification | Value |
|---|---|
| Must Timestamp include the 'Z' (UTC) identifier? | No recommendation made. |

### 3.1.8 Description Element

| Specification | Value |
|---|---|
| Are one or more Message Header Description elements required? In what language(s)? Is there a convention for its contents? | No recommendation made. |

## 3.2 Manifest Element

### 3.2.2 Manifest Validation

| Specification | Value |
|---|---|
| How many Manifest elements must be present, and what must they reference? | No recommendation made. |
| Must a URI that cannot be resolved be reported as an error? | No recommendation made. |

### 3.2.1 Reference Element

| Specification | Value |
|---|---|
| Is the xlink:role attribute required? What is its value? | No recommendation made. |
| Are any other namespace-qualified attributes required? | No recommendation made. |

#### 3.2.1.1 Schema Element

| Specification | Value |
|---|---|
| Are any Schema elements required? If so, what are their location and version attributes? | No recommendation made. |

#### 3.2.1.2 Description Element

| Specification | Value |
|---|---|
| Are any Description elements required? If so, what are their contents? | No recommendation made. |

### 4.1 Security Module

#### 4.1.5 Security Considerations

| Specification | Value |
|---|---|
| Are any recommendations given, with respect to protection or proper handling of MIME headers within an ebXML Message? | Pending. |

#### 4.1.4.1 Persistent Digital Signature

| Specification | Value |
|---|---|
| Must messages be digitally signed? | Profile depends on requirements. See BPSS profiles in 4.3. |

#### 4.1.1 Signature Element

| Specification | Value |
|---|---|
| Are additional Signature elements required, by whom, and what should they reference? | Only one signature element SHOULD be used in normal case. |

#### 4.1.3 Signature Generation

| Specification | Value |
|---|---|
| What canonicalization method(s) must be applied to the data to be signed? [Recommended method is "http://www.w3.org/TR/2001/REC-xml-c14n-20010315".] | Pending. |
| What canonicalization method(s) must be applied to each payload object, if different from above? | Pending. |
| What signature method(s) must be applied? | The CPA profile in 4.4 SHALL be used. |
| What Certificate Authorities (issuers) are allowed or required for signing certificates? | No recommendation made. |
| Are direct-trusted (or self-signed) signing certificates allowed? | No recommendation made. |
| What certificate verification policies and procedures must be followed? | No recommendation made. |

#### 4.1.4.2 Persistent Signed Receipt

| Specification | Value |
|---|---|
| Is a digitally signed Acknowledgment message required? | This depends on requirements. See BPSS profiles in 4.3. |
| If so, what is the Acknowledgment or Receipt schema? | Pending. |

#### 4.1.4.3 Non-persistent Authentication

| Specification | Value |
|---|---|
| Are communication channel authentication methods required?<br><br>Which methods are allowed or required? | This depends on requirements. See BPSS profiles in 4.3.<br>Yes for using TLS transport layer non-persistent security. |

#### 4.1.4.4 Non-persistent Integrity

| Specification | Value |
|---|---|
| Are communication channel integrity methods required?<br>Which methods are allowed or required? | This depends on requirements. See BPSS profiles in 4.3.<br>Yes for using TLS transport layer non-persistent security. |

#### 4.1.4.5 Persistent Confidentiality

| Specification | Value |
|---|---|
| Is selective confidentiality of elements within an ebXML Message SOAP Header required? If so, how is this to be accomplished? | Normally not recommended. This depends on requirements. |
| Is payload confidentiality (encryption) required?<br>Which methods are allowed or required? | This depends on requirements. See BPSS profiles in 4.3.<br>Yes for using TLS transport layer non-persistent security. |

#### 4.1.4.6 Non-persistent Confidentiality

| Specification | Value |
|---|---|
| Are communication channel confidentiality methods required?<br>Which methods are allowed or required? | This depends on requirements. See BPSS profiles in 4.3.<br>Yes for using TLS transport layer non-persistent security. |

#### 4.1.4.7 Persistent Authorization

| Specification | Value |
|---|---|
| Are persistent authorization methods required?<br>Which methods are allowed or required? | Recommended.<br>No recommendation regarding the method. |

#### 4.1.4.8 Non-persistent Authorization

| Specification | Value |
|---|---|
| Are communication channel authorization methods required?<br>Which methods are allowed or required? | Pending. |

#### 4.1.4.9 Trusted Timestamp

| Specification | Value |
|---|---|
| Is a trusted timestamp required?<br>If so, provide details regarding its usage. | Pending. |

### Error Handling Module

#### 4.2.3 ErrorList Element

#### 4.2.3.2 Error Element

##### 4.2.3.2.2 codeContext attribute

| Specification | Value |
|---|---|
| Is an alternative codeContext used? If so, specify. | No recommendation made. |

#### 4.2.3.2.3 errorCode attribute

| Specification | Value |
|---|---|
| If an alternative codeContext is used, what is its errorCode list? | No recommendation made. |
| When errors should be reported to the sending application, how should this notification be performed (e.g. using a logging mechanism or a proactive callback)? | No recommendation made. |

### 4.2.4 Implementing Error Reporting and Handling

#### 4.2.4.2 Identifying the Error Reporting Location

| Specification | Value |
|---|---|
| Should errors be reported to a URI that is different from that identified within the From element? What are the requirements for the error reporting URI and the policy for defining it? | No recommendation made. |
| What is the policy for error reporting? | No recommendation made. |

### 4.3 SyncReply Module

| Specification | Value |
|---|---|
| Is SyncReply mode allowed, disallowed, or required, and under what circumstances? [May be process-specific.] | No recommendation made. |
| If SyncReply mode is used, are MSH signals, business messages or both expected synchronously? | No recommendation made. |

## A.5 Reliable messaging module

### 6.2 Methods of Implementing Reliable Messaging

| Specification | Value |
|---|---|
| If reliable messaging is required, by which method(s) may it be implemented? [The ebXML Reliable Messaging protocol, or an alternative reliable messaging or transfer protocol.] | The ebXML Reliable Messaging protocol SHALL be used. |

### 6.3 Reliable Messaging SOAP Header Extensions

#### 6.3.1 AckRequested Element

#### 6.3.1.1 SOAP actor attribute

| Specification | Value |
|---|---|
| Are point-to-point (nextMSH) MSH Acknowledgments to be requested? | No recommendation made. |
| Are end-to-end (toParty) MSH Acknowledgments to be requested? | End-to-end (toParty) MSH Acknowledgments SHOULD be requested. |

#### 6.3.1.2 signed attribute

| Specification | Value |
|---|---|
| Must MSH Acknowledgments be (requested to be) signed? | Profile depends on requirements. See BPSS profiles in 4.3. Yes for using TLS transport layer non-persistent security. |

## 6.4 Reliable Messaging Parameters

### 6.4.1 DuplicateElimination

| Specification | Value |
|---|---|
| Is elimination of duplicate messages required? | Recommended. |
| What is the expected scope in time of duplicate elimination? In other words, how long should messages or message Ids be kept in persistent storage for this purpose? | No recommendation made. |

### 6.4.3 Retries

| Specification | Value |
|---|---|
| If reliable messaging is used, how many times must an MSH attempt to redeliver an unacknowledged message? | No recommendation made. |

### 6.4.4 RetryInterval

| Specification | Value |
|---|---|
| What is the minimum time a Sending MSH should wait between retries of an unacknowledged message? | No recommendation made. |

### 6.4.6 PersistDuration

| Specification | Value |
|---|---|
| How long must data from a reliably sent message be kept in persistent storage by a receiving MSH, for the purpose of retransmission? | No recommendation made. |

## 6.5 ebXML Reliable Messaging Protocol

### 6.5.3 Generating an Acknowledgment Message

| Specification | Value |
|---|---|
| Must a response to a received message be included with the acknowledgment of the received message, are they to be separate, or are both forms allowed? | Response and acknowledgement SHOULD be separated. |

### 6.5.7 Failed Message Delivery

| Specification | Value |
|---|---|
| If a DeliveryFailure error message cannot be delivered successfully, how must the error message's destination party be informed of the problem? | No recommendation made. |

## 7 Message Status Service

| Specification | Value |
|---|---|
| Is the Message Status Service required for reliable and/or best-effort messaging? | No recommendation made. |

### 7.1 Message Status Messages

#### 7.1.1 Message Status Request Message

| Specification | Value |
|---|---|
| If used, must Message Status Request Messages be digitally signed? | No recommendation made. |

#### 7.1.2 Message Status Response Message

| Specification | Value |
|---|---|
| If used, must Message Status Response Messages be digitally signed? | No recommendation made. |

#### 7.1.3 Security Considerations

| Specification | Value |
|---|---|
| Must unauthorized Message Status Request messages be ignored, rather than responded to, due to security concerns? | No recommendation made. |

## A.6 Message service handler ping service

| Specification | Value |
|---|---|
| Is the Ping Service required? | No recommendation made. |

### 8.1 Message Service Handler Ping Message

| Specification | Value |
|---|---|
| **If used, must** Ping Messages be digitally signed? | No recommendation made. |

### 8.2 Message Service Handler Pong Message

| Specification | Value |
|---|---|
| If used, must Pong Messages be digitally signed? | No recommendation made. |
| Under what circumstances must a Pong Message not be sent? | No recommendation made. |

### 8.3 Security Considerations

| Specification | Value |
|---|---|
| If not supported or unauthorized, must the MSH receiving a Ping respond with an error message, or ignore it due to security concerns? | No recommendation made. |

## A.7 MessageOrder module

| Specification | Value |
|---|---|
| Is message ordering (within a Conversation) required? | The CPA profile in 4.4 SHALL be used. |