TECHNICAL REPORT

IEC TR 62325-101

First edition
2005-02

Framework for energy market communications –

Part 101: General guidelines

Reference number
IEC/TR 62325-101:2005(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 On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.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 REPORT

IEC TR 62325-101

First edition
2005-02

Framework for energy market communications –

Part 101: General guidelines

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 W

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FRAMEWORK FOR ENERGY MARKET COMMUNICATIONS –

Part 101: General guidelines

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. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62325-101, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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 report is based on the following documents:

Enquiry draft	Report on voting
57/704/DTR	57/721/RVC

Full information on the voting for the approval of this technical report 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 [1]

Part 3XX: (Titles are still to be determined) [2]

Part 401: Abstract service model [3]

Part 501: General guidelines for use of ebXML

Part 502: Profile of ebXML

Part 503: Abstract service mapping to ebXML [3]

Part 601: General guidelines for use of web services [3]

Part 602: Profile of Web Services [3]

Part 603: Abstract service mapping to web services [3]

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

1 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.

2 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.

3 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.

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, UN/EDIFACT or ANSI ASC X12 messages, or proprietary HTML and XML solutions based on Internet technologies are being used. With the advent of new e-business technologies such as ebXML by UN/CEFACT (United Nations / Centre for Trade and Electronic Business) together with OASIS (Organization for the Advancement of Structured Information Standards), and Web Services by W3C (World Wide Web Consortium) and OASIS based on Internet technologies, an energy market specific profile of these standards can be used for regional energy markets. These profiles allow the re-use of proven core components and communication platforms across markets, thus saving cost and implementation time. Because some of these technologies are still under development, other technologies or converged technologies are not excluded for the future.

The IEC 62325 series includes, besides general requirements and guidelines, the business operational view with profiles of technical e-business communication architectures together with migration scenarios. The process and information model as well the abstract service model is not included in the first edition of the IEC 62325 series but may be added in the future. It does not itself define standards and only references available standards.

It supports the communication aspects of all e-business applications in deregulated energy markets with emphasis on system operators. The business operational view includes the market communication aspects of system operator applications with interfaces to other market participants from trading over supply to balancing planned generation and consumption, change of supplier, market services and billing.

The ‘process’ real-time communication of energy systems is beyond the scope of the IEC 62325 series.

The IEC 62325 series is subject to legal and security aspects of e-business and energy market rules that may be different from country to country or region to region.

It is important to note that the IEC 62325 series specifies no “content” (market model with processes, collaborations, transactions, messages, core components) because energy markets still vary. The specific content modelling of regional markets is subject of regional projects and/or may be candidate for future standardisation extending the IEC 62325 series. But methods and tools of modelling are described and in part 102 non-normative examples of core models, processes and messages, which show how the IEC 62325 series might be used.

Note that work is in progress at UN/CEFACT regarding the “content” of business information exchange for example as Core Components (UN/CEFACT – Core Components Technical Specification), Core Component Library (CCL, accessible through an registry/repository), Catalogue of Core Components (including industry groups), Common Business Processes, UMM Business Library, XML message design rules (UN/CEFACT – XML Naming and Design Rules (Draft 2004)).

The energy market specific vocabulary can be derived from Core Components or/and a knowledge based energy market information model (for example the so called CIM market extension of the CIM Common Information Model (IEC 61970-301)).

Whereas IEC 62325-501 and IEC 62325-502 of the current IEC 62325 series edition are restricted to the use of the ebXML technology, the planned technical parts are intended to convert the framework into a more open framework taking into account also other e-business technologies besides ebXML, as Web Services with future IEC 62325-6XX. This may also include with future IEC 62325-401 an abstraction service model with mapping to the various e-business technologies (future IEC 62325-503, and future IEC 62325-603) to hide the e-business technology actually used from the application.

It is important to note that the definition of a full and detailed energy market model is beyond the scope of the IEC 62325 series, because energy markets are different. But what might be included in future with the future IEC 62325-3XX is an extensible and adaptable core set of information model definitions in UML which can be used as an vocabulary for the interface of utilities to the market together with XML schema design rules for the mapping from UML to XML, and market identification schemas. This would enable and support, but not restrict, parties of the energy market to define complete energy market models in detail.

FRAMEWORK FOR ENERGY MARKET COMMUNICATIONS –

Part 101: General guidelines

1 Scope

This part of IEC 62325 gives *technology independent* general guidelines applicable for e-business in energy markets based on Internet technologies providing:

- a description of the energy market specific environment;
- a description of the energy market specify requirements for e-business;
- an example of the energy market structure;
- an introduction to the modelling methodology;
- network configuration examples;
- a general assessment of communication security.

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.

2.1 Generic Open-edi standards

The IEC 62325 series is based on ISO/IEC 14662 and Internet technologies, notably on XML (Extensible Markup Language) of the W3C (Word Wide Web Consortium) with references to existing or emerging standards or de-facto standards for global e-business.

IEC 60870-6 (all parts), *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations*

IEC 61968 (all parts), *Application integration at electric utilities – System interfaces for distribution management*

IEC 61970 (all parts), *Energy management system application program interface (EMS-API)*

IEC 62210, *Power system control and associated communications – Data and communication security*

ISO/IEC 14662, *Information technology – Open-edi reference model*

ANSI ASC X12, Release 4040, December 2000

UN/EDIFACT, D.01A Directory, January 2001

UN/CEFACT *Modelling Methodology (UMM)*, NO90 R12 or higher

UN/CEFACT *Meta Model*, NO90 R10 or higher

UN/CEFACT *XML Naming and Design Rules*, draft 2004[4]

UN/CEFACT Core Components Technical Specification

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 referred to in the references above.

2.2 Sectorial Open-edi standards

Market modelling based on this implies to some extent sectorial standards. At the moment no references are given.

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)
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

[4] Under consideration.

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 Energy market requirements

4.1 Communication and data networks

Many market participants need to communicate with each other in the energy market. In the IEC 62325 series, it is assumed that e-business in energy markets makes use of Internet, which is public, unreliable and insecure in a reliable and secure manner (see Figure 1).

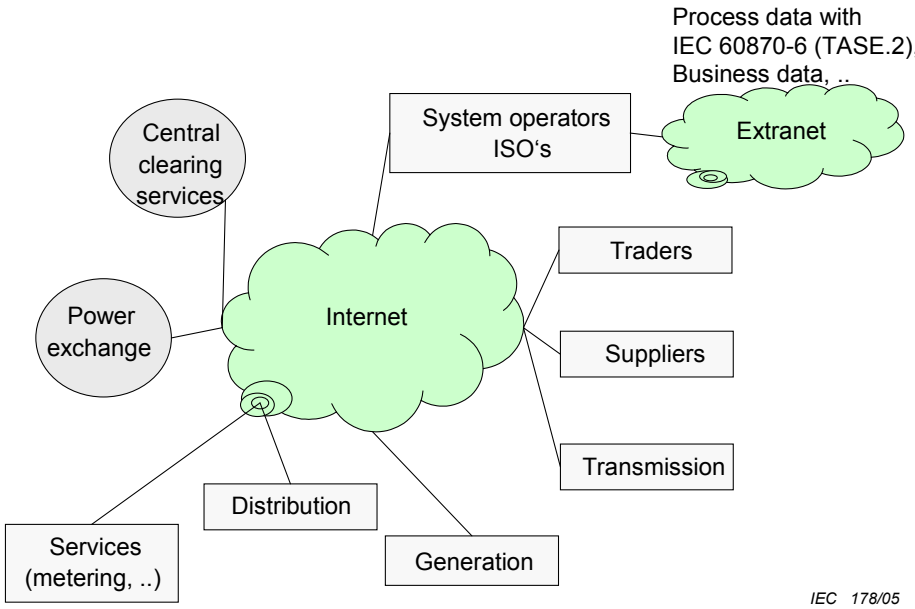


Figure 1 – Energy market communication over the Internet

Within the market, other types of networks besides the Internet also are possible by agreement, as shown by Table 1.

Table 1 – Type of data networks

Network	Features	Remark
Internet	Cheap, unreliable, insecure	Public
Virtual private network (VPN)	Secure logical network in the Internet	Uses the Internet in a closed user group for trusted partners
Extranet	Private physically separated network	For trusted partners

It is important to note that the relationship of market participants for communication purposes follows more the 'one-to-many' then the general 'any-to-any' pattern. For example transmission system operators and power exchanges have a 'one-to-many' relationship to traders. Clearing service providers, for example for change of suppliers, have a one-to-many relationship to distribution service providers and suppliers. Energy brokers providing trading information do not trade themselves and have a 'one-to-many' relationship with traders. From this point of view, it is natural that the communication hubs at the "one-to" end of the relationship are responsible in order to define the business communication interfaces for the corresponding market participants in a harmonised and standardized fashion, based on an agreed technology. Because e-business technologies are positioned for global e-business of any business, including discovery of *a priori* unknown business partners, the many options of this technologies should be reduced to a minimal profile that satisfies the requirements.

4.2 Business areas and processes

In the energy market, energy is generated (electricity) or produced (gas), traded (wholesale) and supplied (retail) to the customer (consumption). At every moment, generation and supply should be in balance and the security of the energy network should be granted. Producers and customer have non-discriminatory access to the energy network and customers can chose their supplier in a deregulated market. The commercial use of energy networks for transmission and distribution is transparent to the market participants regardless of the physical structure (voltage level, hierarchy, control areas involved). The market also needs services to support the core functions such as registration of market participants and network access, change of supplier, relocation of customers, metering and collection of metering data, settlement of accounts, and billing.

Figure 2 shows a high-level presentation of the supply chain of energy with basically three main phases: In the *trading planning phase,* energy consumption is forecast and trading is planned. In the *trading operational phase,* energy is traded to meet the forecast, and respective generation resources are allocated. The implementation of the physical energy path from generation over the transmission and distribution network to consumption affords co-ordinated planning of balanced schedules in the *system operation planning phase* for generation, import/export and consumption. In the *system operation operational phase,* energy flows directly from the producer to the customer over the transmission and distribution network. System operation guarantees that in this phase, generation meets consumption in real-time (balancing) and that the system is reliable. Many services are needed to support the core processes. In the *settlement phase,* for example, the settlement service provides the means to bill consumption and imbalances. Any imbalance of operation (difference between schedules and metered generation and consumption) is in the financial responsibility of the Balance-Responsible Parties (traders and others).

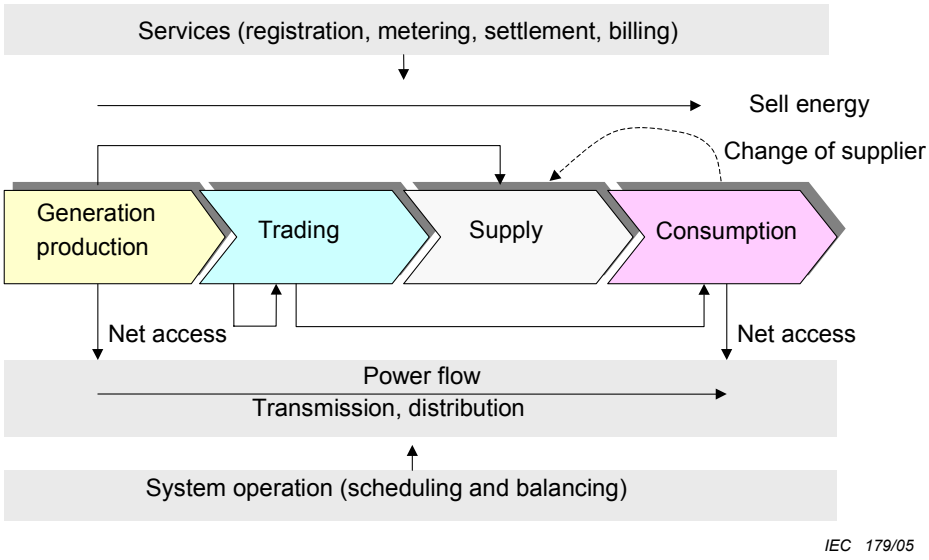


Figure 2 – Energy supply chain

Table 2 identifies the business areas, processes within the areas and the involved roles of market participants. For an informative *simplified market model* which serves only for the purpose of giving a specific context to e-business in energy markets refer to IEC 62325-102. The nomenclature may change from market to market. Some business processes are identified as energy services to indicate that these processes could be outsourced to service providers. In addition to suppliers, sub-suppliers also exist as aggregators (aggregation of consumption), but are not included.

It is important to note that where reference is made to ‘market participants’, this should be understood to mean ‘market participant roles’ rather than market participants in the sense of companies. This is because a market participant can take on many roles. For example, a distribution utility can take on the roles of distribution system operator (network control), distribution service provider (network planning, construction and maintenance), supplier (buying and selling energy to end consumers), energy service provider (registration, change of supplier, metering, settlement of accounts, billing), within the constraints of a particular regulatory system.

Table 2 – Business areas, processes and market participants

Business area	Business process	Roles of involved market participants
Generation		
	Generation planning	Generator
Trading		
	Bilateral trading	Trader, central matching service provider (confirmation)
	Brokering	Trader, Broker
	Bidding at power exchange	Trader, Power exchange
	Financial clearing	Trader, clearing responsible parties
	Auxiliary services trading	Trader, transmission system operator
	Cross boarder auctioning	Trader, transmission system operator
Supply		
	Selling energy to end consumers	Supplier
Transmission		
	Registration, network access and transmission	Transmission system operator, transmission service provider, generators, customers
Distribution		
	Registration, network access and distribution	Distribution system operator, distribution service provider, generators, customers
System operation		
	Scheduling consumption and generation	Transmission system operator, balance responsible parties (trader, supplier, generator)
	Scheduling import/export	Transmission system operator, balance responsible parties (trader)
	Operation (Balancing)	Transmission System operator, generators (auxiliary services)
Energy services		Service provider, etc. many market participants
	Metering (meter readings)	Customer, distribution service provider, metering service provider
	Access to collected metering data	Supplier, trader, metering service provider
	Settlement of accounts of consumption and generation	Service provider, supplier, generator, etc.
	Settlement of accounts of imbalance	Transmission system operator, balance responsible parties (trader, supplier, generators), service provider
	Billing	Service provider, etc.
	Change of supplier	Customer, supplier, distribution service provider
	Relocation of customer	Customer, supplier, distribution service provider
	Exchange of market metadata	Customer, supplier, distribution service provider

4.3 Performance

Table 3 shows generic performance requirements in terms of duration of a message interaction between market participants for a business process to end within a certain period. The duration is the *maximum* end-to-end time for the transport of the messages without application processing time. These requirements may change from market to market. They should be defined in a project.

Table 3 – Performance requirements

Business area	Business process	Process period	Maximum duration of interaction
Generation			
	Generation planning	Next hour, day, month	< 1 min
Trading			
	Bilateral trading	Next day, next month, next year, next years	< 5 s
	Brokering	Next day, next month, next year, next years	< 5 s
	Bidding at power exchange	Intra day, next day	< 5 s
	Financial Clearing	Intra day, next day, next week, next month, next year, next years	< 1 h
Supply			
	Selling energy to end consumers	Month	< 1 day
Transmission			
	Network access, contract	Month	< 1 day
Distribution			
	Network access, contract	Month	< 1 day
System operation			
	Planning (scheduling)	Next hour, next day	< 1 min
	Auxiliary services	Next day	< 2 min to 4 h
Energy services			
	Metering (readings)	Week, month	< 1 day
	Access to collected metering data	Day, week, month	< 1 h
	Settlement of accounts of consumption and generation	Month	< 1 day
	Settlement of accounts of imbalance	Month	< 1 day
	Billing	Month	< 1 day
	Clearing of change of supplier	Month (week, day)	< 1 day
	Change of supplier	Week, month	< 1 day
	Relocation of customer	Month	< 1 day
	Exchange of market metadata	Week, month	< 1 day

For B2B peer-to-peer network configurations over the Internet (HTTP) these requirements should not be a problem with message transfer times typically less than 5 s. In portal network configurations (hubs with push-pull) with intermediate message storage, the duration of message transport depends on requesting stored messages. The same is true for dial-up lines (SMTP). In portal network configurations with routing, the duration of message transport depends on the throughput at peak load.

4.4 Quality of service

4.4.1 General

Quality of service (QoS) deals with reliable and secure messaging transfer and is dealt with in the following paragraphs. The service parameters should be configurable so that within an energy market, a specific profile can be used. This profile depends on the used network and business processes.

4.4.2 Reliability

Messages transmitted over a network can get lost, corrupted, duplicated, be out of sequence, not be accepted by the recipient or simply not reach its intended destination. Furthermore systems can fail and messaging services can become interrupted by network failures. Without counter measures and with best efforts, the network will provide only an unreliable service. Table 4 shows the reliability risks and counter measures. Counter measures also include persistent storage of messages to protect against system failure or interruption and messaging error notification to the application.

Table 4 – Reliability

Reliability risk	Counter measures
Lost	Acknowledgement with re-transmission after time out
Corrupted	Acknowledgement with re-transmission after time out
Duplicated	Filtering
Out of sequence	Sequence control with sequence number
Not accepted	Unsigned or signed delivery receipt

A reliable messaging service should provide measures to guarantee a reliable service, especially using the unreliable Internet. A “reliable messaging service” should provide a reliable service taking into account the risks stated in Table 4. This service is a mandatory requirement over the Internet for certain business processes.

4.4.3 Security

In common with all other e-businesses, the energy market depends on security measures, especially when using the insecure Internet and operating within a legal framework. Since e-business in energy markets form only a small niche of global e-business, all enterprises have to deal with the fact that there are no specific requirements for energy markets. Table 5 shows the possible security risks and counter measures.

The Annex B covers the appropriate areas of security that impact the implementation and use of e-business technologies in the context of the IEC 62210 with regard to computerized supervision, control, metering, and protection systems in electrically utilities.

Table 5 – Security

Security risk	Counter measures
Non-repudiation of origin and receipt	Audit trails, logging of messages
- of origin	Digital signed messages
- of receipt	Digital signed acknowledgements and receipts
Loss of integrity of messages	Message digest and digital signatures of messages
Loss of confidentiality	Encryption of messages
Wrong identity	Authentication of origin with digital signatures and credentials
Unauthorized access and fraud	Authorisation with access control lists based on digital signatures
Forged date and time	Authentication of date and time within a message

A secure messaging service should provide a secure service taken into account the risks stated in Table 5.

The need and level of security should be a part of a model of a business process, and is beyond the scope of this part of IEC 62325. For these, security profiles (see relevant parts of the IEC 62325 series) should be used.

5 Application of the Open-edi reference model

5.1 The Open-edi reference model

The e-business architecture and the IEC 62325 series follow the Open-edi reference model ISO/IEC 14662 (see Figure 3). Fundamental to the model is the division of the business transactions into the Business Operational View (BOV) and the Functional Service (FSV) with mapping of services between to ensure independence of the communication technology used.

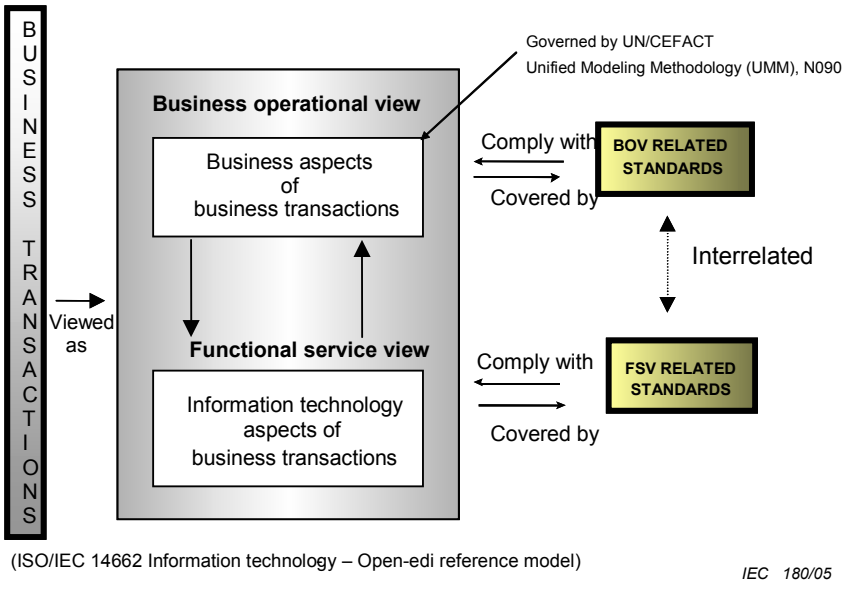


Figure 3 – The Open-edi reference model

5.2 Market structure and business views

The IEC 62325 series assumes that the energy market consists of business areas, which use the same e-business communication infrastructure. It is further assumed that besides specific market models within each business area (specific BOV), the overlapping and interaction of business areas also leads to common market models (common BOV). Figure 4 shows the market structure and views.

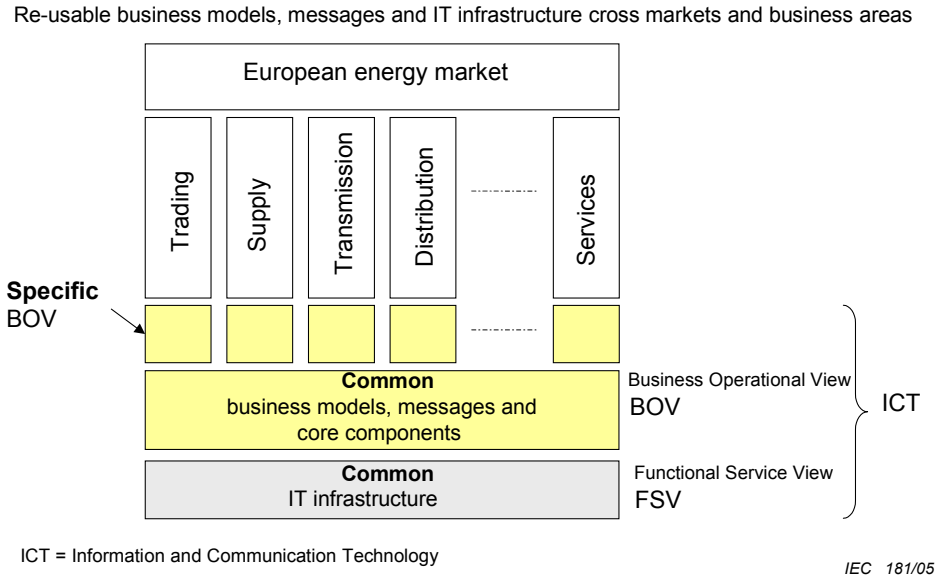


Figure 4 – Energy market structure and views

6 The Open-edi architecture for deregulated energy markets

6.1 Delimitation: market versus process

In deregulated energy markets, market participants decide 'who' produces 'how' much energy 'where' and 'when'. They also decide about the choices in the whole supply chain where customers have the choice of supplier (retail), suppliers have the choice of traders (wholesale), and traders have the choice of generators. Only the energy network is a natural monopoly. The market deals with the economic choice and delivery of products and energy related services within a time frame down to hours or less. It depends on reliable and secure system operation of the technical process.

The technical process (generation, transmission and distribution) supports the market transactions and guarantees reliable and secure system operation including energy exchanges and real-time balancing of generation and load within a time frame down to seconds (load-frequency control, telecontrol) and milliseconds (local protection).

The business-oriented market and the technical process are the two sides of the commercial/technical system with close dependencies and relationships. For example, planned schedules of market participants for generation and load have indirect impact on the process. On the other hand, the market for example has to adapt to notified congestion and outages in the process. So a part of e-business in energy markets deals with the interface between the market and the process. This interface is part of the market.

In the context of market communications, a series of standards on the process side deal with control centres and are to some degree, closely interrelated with market transactions:

The IEC 60870-6 series (TASE.2) deals with inter control centre communication of process data including energy exchange schedules. The latter is also possible using the e-business technologies described in the IEC 62325 series over a process Extranet. In this case the same communication technology is used for the interface between the market and the process and between control centres.

The IEC 61970 series facilitate integration of applications within a control centre, including the interactions with external operations in distribution as well as other external sources/sinks of information needed for real-time operations. The IEC 61968 series develops interfaces for distributed management systems for information exchange with other IT systems. Both series of standards deal with the Integration Bus (IB) and the Common Information Model (CIM). The CIM model may also include parts that are influenced by the market, for example scheduling for energy exchange, reservation, and financial.

6.2 Conventions

6.2.1 Modelling methodology

In common with other markets, the energy market has specific legal, commercial and technical requirements. Although a convergence of market structures and market rules can be observed with liberalisation, requirements may still be different from market to market and within one market and even from one region to the other. Some requirements are generic and apply to all markets and some are specific to the market or region. Before e-business can be introduced in an energy market, it is necessary to have a common shared understanding amongst all market participants about the justification, requirements, business rules and business processes. The description of business processes includes the identification and definition of roles of market participants, business areas, business processes within areas, business collaborations (logically coupled multiple transactions) and transactions (multi-party and binary), business information to be exchanged and the required e-business services. This common understanding is captured in a business market model using a formalised e-business modelling methodology that is or should be independent of the actual e-business communication technology used. This will allow mapping the model onto different e-business communication technologies now and in the future. In this way, the model can be expected to retain a long-lasting value.

It is recommended to use the UN/CEFACT Modelling Methodology (UMM) to describe the Business Operational View (BOV) of the ISO/IEC 14662 Open-edi reference model standard. E-business modelling methodologies other than UMM are not excluded, but UMM should be used with the ebXML e-business technology. UMM is a modified subset of a specialisation of the Unified Software Development Process named Rational Unified Process (RUP). It uses the Unified Modeling Language (UML) of the Open Management Group (OMG) including extensions of the UML meta model through business domain specific stereotyping to support business process and information definition, resulting objects and interface-specific object behaviour descriptions.

Additional worksheets with predefined structure to capture textual information may be used. Tools are available for UML and these can be specialised for e-business by using stereotypes.

Table 6 gives a simplified overview of the UMM workflow, its focus and artefacts.

Table 6 – UMM workflow

Workflow	Main focus for e-business	View	UML and XML artefacts
Business modelling	Business context, business area, process area	BOM (Business Operations Map)	Use case diagrams, scenario descriptions
Requirements	Business processes and collaborations	BRV (Business Requirements View)	Detailed use case diagrams, Activity diagrams
Analysis	Transactions, identification of business documents	BTV (Business Transaction View)	Sequence diagrams, collaboration diagrams
Design	Business documents, Business service interface	BSV (Business Service View)	Class diagrams, XML-messages, interaction parameters

Typical examples of business areas in energy markets are: generation, trading, supply, system operation (scheduling and balancing, settlement of imbalances), energy services (change of supplier, metering, settlement of account and billing), transmission and distribution.

Table 7 shows an example workflow with 'drill-down' from business modelling to analysis for change of supplier (exchange of market metadata).

Table 7 – Example workflow with drill down

Work flow	Focus	Example
Business modelling		
	Business domain	Electricity market
	Business area	Supply
	Process area	Change of supplier
Requirements		
	Business processes and collaborations	
		Network access registration, etc.
Analysis		
	Transaction	Request of contract data of new customer
	Identification of documents	Contract data request document, etc.

It is important to note that the modelling methodology is not an exact science and is more based on good business practice. Therefore, no general concept of how to use UMM can be recommended. The UML workflows may not directly correspond to phases of an e-business project. There is also no clear boundary between the UML workflows because the workflows drill down to more detail from workflow to workflow.

The UMM defines analysis patterns of business transactions. Patterns are common transactions that can be re-used in any business collaboration. UMM defines six patterns using activity diagrams: (1) Commercial Transaction, (2) Request/Confirm, (3) Query/Response, (4) Request/Response, (5), Notification, (6) Information Distribution. The Commercial Transaction is used to model the "offer and acceptance" business transaction process that results in a residual obligation between both parties to fulfil the terms of the contract with economic commitment.

The transaction patterns are associated with seven predefined property values (interaction parameters) for the requesting and responding business activity: (1) time to acknowledge receipt, (2) time to acknowledge acceptance, (3) time to perform, (4) authorisation required (true or false), (5) non-repudiation of origin and content (true or false), (6) non-repudiation of receipt (true or false), (7) recurrence (number of re-transmissions). Of course, the property values can also be set individually within a specific agreed business transaction.

The UMM defines also the following five business service interactions for business transactions and business collaboration agreements based on UML sequence diagrams: (1) Service-Service, (3) Agent-Service-Service, (4) Service-Service-Agent, (5) Service-Agent-Service, (6) Agent-Service-Agent.

6.2.2 Business documents language and schemas

Business documents are defined in XML (Extensible Markup Language), a subset of the SGML (Standard Generalised Markup Language) language. XML is not a language as the name implies but a meta language to define application languages with the help of DTD (document type definitions) and XML Schemas.

Where XML documents are the preferred payload, documents of arbitrary syntax are also allowed (for example EDIFACT, X12) and will be used for migration.

6.2.3 Re-use of information entities and processes

Industry groups or organisations using information entities based on re-usable core components standardized by UN/CEFACT define domain specific XML business documents. Domain independent business documents of general interest are standardized by UN/CEFACT. The same applies to core processes. Both core components and core processes will be made available in business libraries within registries/repositories.

Before standardization is finished, it is possible to define one’s own market specific messages, core components and core processes and later switch to standardized ones.

6.3 Business and information model

6.3.1 General

The identified generic market processes in 4.2 are described IEC 62325-102 for information only to establish a context for energy market e-business communication. It shows as an example, a simplified market model in UMM.

The deliveries of market modelling should enable the market participants to have a detailed understanding of the market including the dynamic behaviour and should enable the vendors to implement systems for a given e-business technology. They should be understood as the *result* of modelling and not as the phases of the iterative and incremental modelling process. The deliveries include two parts, the market user guide, and the formal UMM Market Model for system implementation.

6.3.2 Market user guide

The *market user guide* is a human readable description of the market model including text, tables, pictures and graphics. It should also include the description of the legal and regulatory environment.

6.3.3 Market model

The *market model* is the formal, precise and detailed description of the whole market using for example the e-business UN/CEFACT modelling methodology UMM based on the UML modelling language for the four workflows business modelling, requirements, analysis, and design. Note that for the documentation of the market model, only the *result* of the modelling is of interest and not the iterations and intermediary versions of artefacts in the course of workflows.

The *workflows* business modelling, requirements, and analysis should be as far as possible independent of the e-business technology used. The organisation of these workflows with the *Business Operations Map* (BOM) is based on the functional decomposition of the whole market into business areas, process areas, and supporting business processes and furthermore of the market participants in roles (in UML called actors) to minimise the size of the model parts and the information flow and interfaces in the model.

The BOM *model management diagram* uses UML packages to organise and analyse the high level architecture of the e-business system by understanding the subsystems (business areas, business process areas, and business processes) and their dependencies. A package can contain any other model elements, including classes, use cases, activity diagrams, or other packages. At a conceptual stage, the packages show the names of the classes that are included.

UML *use cases* document the interactions between the roles (actors) of market participants and subsets of system functionality as business areas, business processes, business collaborations and business transactions without showing how these interactions are implemented. *Use case diagrams* capture a model of how several use cases depend on each other and how one or more actors interact with those use cases. UMM forms capture structured textual information about use cases and are supplemented by plain text descriptions.

Variations of use-cases from a base use-case are modelled with use-case extensions (associations to this with the stereotype extension). Use-cases can be split into smaller parts using dependency relationships, stereotyped as includes.

UML *activity diagrams* are realisations of use cases showing the business process workflow and have two purposes: The first purpose is to give an overview of the business dynamics of the whole market (business domain) or parts (business areas) of it. In this case activity diagrams are created in parallel with the use cases and can span several or all use cases of a market or business area. A swim lane represents each business area or business process. The second purpose is the visual documentation of a business workflow *within* a use case representing a business process, business collaboration or business transaction with one start state and multiple end states. Each role (actor) of a market participant is represented by a swim lane.

UML *sequence diagrams* model the interaction among roles (actors) of market participants by emphasising the time-ordering sequence of business messages (documents) and are especially suited for the modelling of business transactions.

UML *class diagrams* are used to model business processes, business collaborations, business transactions, and exchanged business documents. Business documents are created using business information entities derived from standardized core components. UML core components visually represent the elements, relationships, and constrains of the e-business energy market vocabulary.

The design workflow depends on the e-business technology used and includes technology specific configuration details in machine-readable XML format.

NOTE 1 A big and inhomogeneous market may be split in a homogenous core part (for example federal or international regulated wholesale market) and regional inhomogeneous market parts (for example regional or national regulated retail and supply). There may also be the possibility of process alternatives. In inhomogeneous markets a Market Reference Model may be useful for the future harmonisation of market processes.

NOTE 2 Market areas are not isolated and may have interfaces to each other (for example trading and system operation for scheduling). Therefore common modelling design guidelines may be necessary to allow different organisations responsible of specific market areas to model in a harmonised and extensible fashion.

NOTE 3 For some business areas of the energy market a common cross-domain solution is desirable. This is especially true for traders trading electricity as well as gas.

Table 8 shows the UMM model deliveries regarding forms, definitions, and artefacts. As a general guideline within the 'drill down' of modelling, the business modelling workflow is focused on the organisation of modelling and the identification of business areas. The business requirement workflow is focused on requirements (use cases) and business processes whereas the analysis workflow deals mainly with business collaborations within business processes. The design workflow is focused on business transactions within business collaborations including XML messages, XML documentation, and XML configuration documents for the implementation of e-business systems.

Table 8 – UMM model deliveries

Workflow	Forms and definitions	Artefacts (UML and XML)
Business modelling		
	FORMS: Describe business reference model, Describe business area, Describe process area, Identification of business process.	UML model management diagram (BOM) UML Packages, conceptual use cases, conceptual activity diagrams.
Business requirement		
	FORMS: Describe business process use case, Describe business collaboration, Business collaboration protocol table. DEFINITIONS: Market terms, roles of market participants, Market references. Glossary.	UML Use cases of business collaborations, transactions, Use case identification of business processes, Activity diagrams of business collaborations. UML Activity diagram of the whole market with functional decomposition.
Analysis		
	FORMS: Describe business transaction, Business transaction property values, Business transaction transition table. DEFINITIONS: Market identification schema, code definitions, core components or references to it, elements of messages.	UML Business collaboration protocol [Activity Diagram], Business transactions [Activity Diagram], Business documents [Class Diagram].
Design		
	DEFINITIONS: Profile for secure and reliable messaging, transport, Technical references. Glossary.	UML Service Collaboration [Object Collaboration], Network Component [Class Diagram], Business Service [Class Diagram], Service Transactions [Sequence Diagram], Business Documents (detail) [Class Diagram]. E-business technology dependent artefacts.

The following definitions and references are part of the model:

Market identification schemas

The market identification schema is the basis to identify market participants, market areas, metering points. See also 6.4.

Role definition of market participants

The role model is part of the market model and defines for each business area, the roles of market participants (actors in the UML sense). This is necessary to allow legal entities to play one or more roles for a given business area.

Code definitions

The code definitions define short codes used in messages for example roles, products, auction type, measurement unit (dimension), messages, processes, and coding schemas.

Core components

The core components define or reference the core components used in messages including its context of use. A name and an identifier identify each core component.

Definitions

A list of definitions defining all used market specific terms to facilitate a clear understanding of the market.

Glossary

A list of technical or market specific words explaining their meanings.

References

The references include all necessary references.

6.4 Market identification schema

E-business in energy markets provides a common Market Identification Schema (MIS). The primary objects that need to be identified are:

- Market participant: traders, generators, suppliers, system operators, big consumers, power exchanges, transmission network providers, distribution network providers, agents and service providers (brokers, metering providers, clearing providers).
- Area: distribution networks, transmission networks, balance areas (control areas) consisting of a number of networks, market areas, etc.
- Metering point: for generation units, cross border connections, consumers, etc.

The MIS requires that the allocated codes do not change over time: For enterprises, one code or one code for each market role should be provided. The code should only change if the enterprise changes its legal status. If the enterprise merely changes its name, its code will be the same. Network area codes should only change if the network areas change (combination, division). Metering point codes should not change even if the meter is changed or the network service provider in the role of metering provider or the metering provider changes.

The MIS also requires services such as correct allocation of codes, management of the code lists (deletion and modification), information about the meaning of codes, contact details about the designated organisations and communication parameters (e-mail, WWW, network address, etc.).

For the identification in the energy market, market specific schemas as for example EIC (ETSO (European Transmission System Operators) Identification Code), or international schemas as for example EAN or DUNS should be used. In case of EAN, an example of MIS is:

- Market participant: Number of 13 digits including a check digit called the Global Location Number (GLN).
- Network area: Number of 13 digits (GLN).
- Metering point: Number of 18 digits including a check digit called the Global Service Related Number (GSRN). The number is allocated in large series, so existing numbers can normally be used "surrounded" by a long prefix and a check digit as suffix.

7 Security

Security has a scope far beyond an e-business communication infrastructure and may be a challenge. Besides the legal framework, technologies and standards, it depends also on organisational means. Security for e-business in energy markets is based on legal frameworks. Some countries or regions accept the legal binding of electronic commercial transactions with electronic signatures as being legally equivalent to hand-written signatures.

Security is treated here only from the communication point of view. For full XML end-to-end persistent security, including the application, more complete frameworks are needed. These are in progress with the Security Assertion Mark-up Language (SAML) and the XML Access Control Mark-up Language (XACML, based on access limitations ACL (with access control lists)) of the OASIS initiative and the XML Key Management Specification (XKMS) of W3C. The latter is shortly described below.

The countermeasures to security risks are based on three fundamental technologies: encryption, digital signatures and trusted certification of public key pairs within a public key infrastructure (PKI, see below). Encryption provides privacy. Digital signatures provide both message integrity and requester authentication and are used as well for access authorisation based on the requester's identity.

Public key encryption schemas use considerable computing resources. This is the reason why with most technologies and standards, the public key encryption is combined with the secret key encryption where the secret key is used for encryption only on a session basis and is exchanged with public key encryption.

In the energy market with established relations between market participants only "persistent" and "message or application layer" security with XML Digital Signature (W3C) and as a default XML Encryption (W3C) should be used. "Persistent" means that the security configuration has a duration much longer than a session. "Message or application layer" means that the security is end-to-end (sender/recipient) in contrast to only site-to-site as with transport and network security. The XML digital signature provides message and sender/recipient integrity and authentication and can be used as well for authorisation. If both signatures and encryption are used normally, the message is first signed and then encrypted. The XML digital signature should be applied to the whole ebXML message, the message envelope where the signature element is contained and the message payload.

Table 9 shows the security technologies available for energy markets. XML Encryption is the recommended default encryption and optionally S/MIME and OpenPGP/MIME can also be used, but S/MIME should be preferred over OpenPGP/MIME. Non-persistent transport layer and network layer encryption (TLS, IPSec) should be used alternatively only by agreement.

Table 9 – Security technologies

Technology	From	Used on layer	Persistent	Energy market
XML Digital Signature /MIME	W3C	application or message	yes	Should be used if needed
XML Encryption /MIME				Default encryption if needed
S/MIME v3	IETF			Optional encryption [1)]
OpenPGP/MIME				
TLS (SSL v3 only for backward compatibility)	IETF	transport	no	Optional encryption
IPSec (for VPN)	IETF	network		Optional encryption
[1)] only if XML Encryption /MIME is not available				

HTTP/S is a combination of HTTP and TLS or SSL.

Annex A provides background information.

Whereas user authentication is based on signatures on application level, system authentication and possibly encryption takes place on transport or network level preferably in the DMZ ("demilitarised zone") between firewalls.

XKMS

The XML Key Management Specification (XKMS) W3C recommendation draft deals with the management of security information related to public key pairs within, but not limited to Public Key Infrastructures (PKI), based on trusted certificates such as X.509 v3, SPKI, or within PKI-less environments, for example, as with OpenPGP. XKMS is an API-like protocol using the Simple Object Access Protocol (SOAP), Web Services Language (WSDL) and XML Schema. The idea is to relieve the application from the task of key management by an enterprise trust service. This service provides registration, access, revocation and recovery of security information based on identifier information bound to public keys. Whereas the XKMS trust service is independent of public key schemas such as W3C XML Digital Signature and XML Encryption, it is aimed to complement these standards and hide the complexity of PKI to the application. Figure 5 shows the XKMS concept with relation to XML messaging.

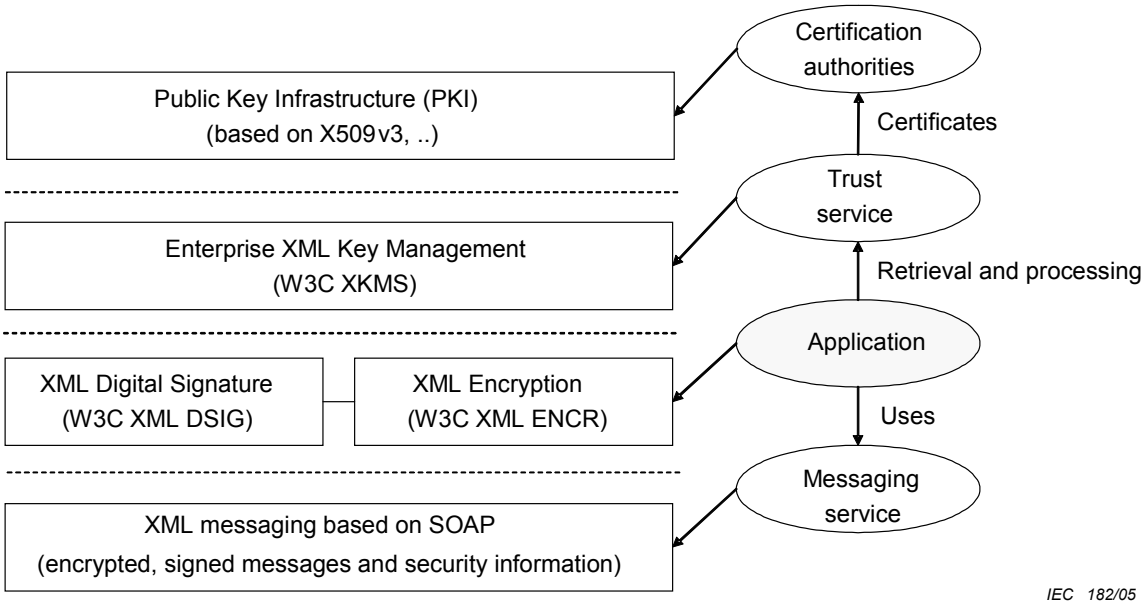


Figure 5 – Example of use of XKMS within a public key infrastructure (PKI)

PKI-profile

Regional energy markets should define, or better chose, an already existing PKI-profile if security is a requirement and needed for energy market communications. This profile in most cases will cover a wide range of applications far beyond energy market communications (for example e-Government, general e-business, ..). The PKI-profile is based on X.509 v3 and relevant RFC's and describes data formats and communication protocols to be employed in interoperable PKI-based applications. The profile focuses on security services for authentication (including user identification and data integrity), confidentiality and non-repudiation. It concentrates on interoperability aspects, embracing different on-line services of certification service providers (CSPs), such as certification service, directory service and time-stamp service, as well as client applications accessing and relying on those services. A typical set-up of PKI components is depicted in Figure 6. Note that the presented components and respectively their partitioning into sub-modules are only an example. Market participants can act themselves as CSP's or relay on a third party CSP providers. In the first case, market participants have the option to cross-certificate themselves.

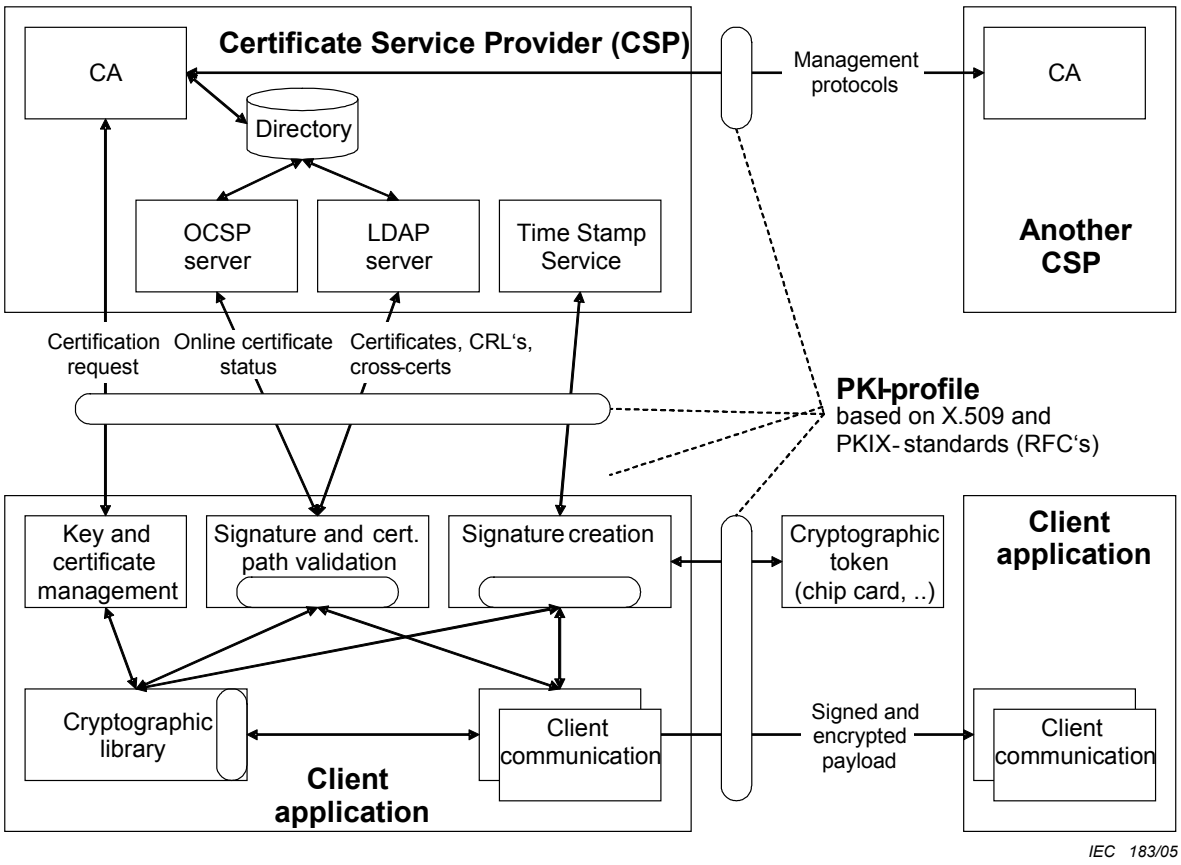


Figure 6 – PKI-profile for interfaces between PKI components (example)

8 Typical network configurations

The following subclauses describe various network configurations for e-business (see Figure 7).

8.1 Peer-to-peer

Within the peer-to-peer configuration, any market participant can directly communicate with any other participant over the Internet using a B2B gateway. This configuration needs a strong management within one market with compliance to common technology dependent artefacts essential for conducting e-business. A registry/repository managed and operated by

only *one* organisation according to market business rules *and* common specifications is recommended to support this.

The peer-to-peer configuration over HTTP requires that all market participants be always online. This means that dial-up lines cannot be used in this environment. Mailboxes can be provided using SMTP.

8.2 Portal

A portal (often called hub-and-spoke) is an alternative to peer-to-peer communication and should be managed and operated by *one* organisation for *all* market participants using the hub. These organisations are often “natural communication hubs” like regional system operators or ISO’s, or power exchanges. One important advantage is that all market participants *should* comply with the portal interface thus avoiding the proliferation of messages and interface configurations.

Simple portals only provide a path (routing) for messages with little added value such as for example message validation, certification, logging and test services.

Portals with more value-added services offer the service of format conversion. The portal can also act as a mailbox where one party sends a message, which is stored in the portal so that the receiving party can request the messages later (a method often called push-pull). More sophisticated portals would also be able to forward a request message from one market participant to many other addressed market participants and generate a response message which depends on the responses of all addressed market participants.

A portal may be of advantage in complex multi-party collaborations where many market participants share the same market metadata, for example for change of supplier, or where more than one party should agree to an overall collaboration, for example in energy exchange transactions.

Geographically widespread energy markets would be divided into regions with each region having its own portal networked with its neighbouring portals. The portal configuration permits dial-up lines for SME’s (small and medium enterprises) because the portal can act as a mailbox.

Portal configurations are centralised and should therefore deal with performance issues regarding the throughput. A priority schema for the message routing in the portal may therefore be appropriate, depending on the length of the messages.

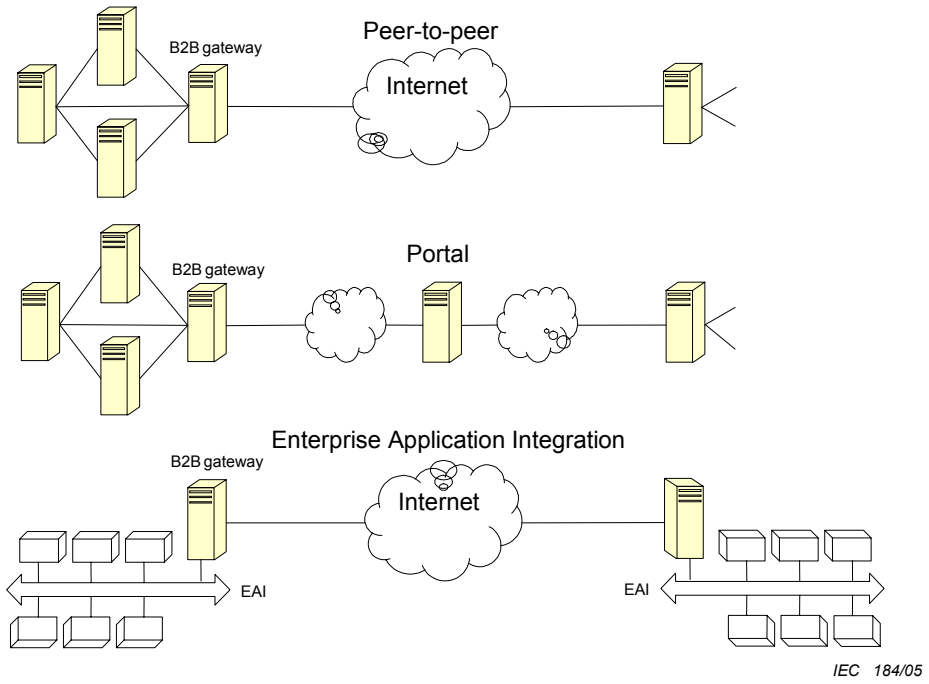


Figure 7 – Network configurations

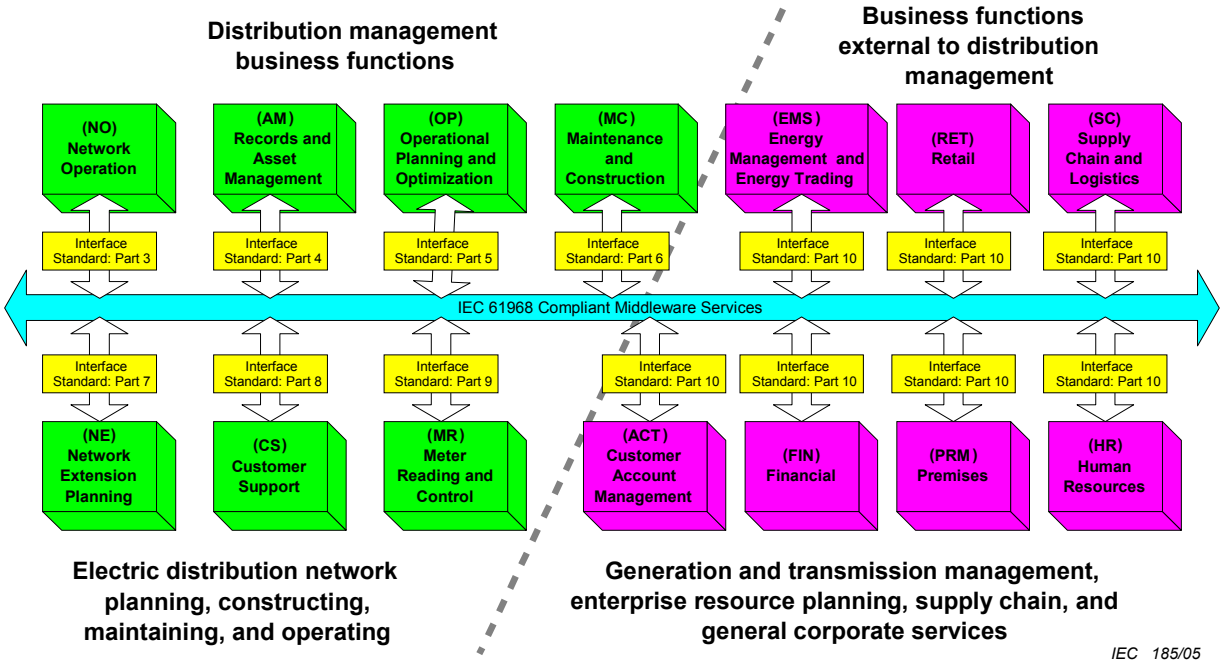
8.3 Enterprise Application Integration (EAI)

Middleware is a technological framework that allows diverse and distributed applications and systems of an organisation to communicate and interact with each other seamlessly. A well-designed middleware framework should:

- allow information to flow quickly and seamlessly to and from each application;
- enable new applications to be easily integrated into the enterprise “federation” of member applications and systems;
- provide a standard communication protocol to enable communication between all types of applications (mission-critical back-end systems, front-end customer interfaces, B2B gateway applications), regardless of whether they are from different vendors with different protocols;
- enable workflow management and automation of business processes across multiple applications;
- allow transformation of data between member applications with different data models and world-views;
- ideally use an event-driven model that employs a publish/subscribe approach to messaging that minimises network traffic, instead of the traditional request/reply model.
- contain a common repository for storing metadata definitions of each application’s data model.

In the utility world, the IEC 61970 series and IEC 61968 series specify an open standardized Enterprise Application Integration framework for A2A Integration with an abstraction layer hiding the underlying communication protocols from the application using generic services which can be mapped to any protocol. An example of this can be seen for distribution management in Figure 8, which is taken from IEC 61968-1. The EAI framework uses the CIM (Common Information Model, IEC 61970-301) metadata model to describe the power system and other operational domains of utility SCADA/EMS business to enable a common understanding between applications. ERP (Enterprise Resource Planning) systems following the OAG (Open Application Group) recommendations or others can also be integrated.

Within the context of the IEC 62325 series, a B2B gateway would be connected to the EAI-Bus to provide access to the Internet. The middleware would bind the technology dependent XML description of the configuration to take full advantage of the descriptive nature of e-business collaborations.



NOTE The 'Parts' referred to are the parts of the IEC 61968 series.

Figure 8 – IEC 61968 compliant middleware services for distribution management

8.4 Business Process Management Systems (BPMS)

Because each application function may have its own business logic, it is difficult to manage the business processes where many applications communicate with each other (A2A) and with many applications of systems in different enterprises (B2B). In this environment, the idea behind the Business Process Management System (BPMS) is to separate the business logic from the application as already done for the presentation layer in order to make the business processes better manageable. The business process definition specification is based on a BPMS business process meta model including internal processes of the enterprise as well as external exposed processes used in B2B activities with other enterprises.

Business processes are described as a sequence of activities, which may invoke operations to communicate with internal applications and external applications over the Business Service Interface (BSI). The BSI provides access to a B2B gateway hiding the technology of the messaging service used.

The BPMS process meta model and notation is subject to current standardization. The BPMS business process model is an activity model viewed from the perspective of *one* enterprise which manages the model whereas the e-business collaboration model represents the shared-view of two enterprises regarding the message interchange between two business transaction activities.

Annex A
(informative)

Security

The following text is mainly based on the relevant RFC's and recommendations and provides general background of the base technologies.

A.1 XML digital signature and encryption

The W3C XML digital signature and XML encryption recommendations enable signing and encryption of arbitrary content (including EDIFACT or X12) as well as providing advanced support for XML content. This includes the ability to sign or encrypt portions of XML, reference multiple objects in a signature and include meta data information with signed or encrypted content. XML signatures support multiple signatures, useful when content is routed for approvals. Both XML Signatures and Encryption support inclusion of the signature or encrypted content in the original XML document, creating a close binding. Signatures may also be separate from the signed content, especially useful when the content is large or binary and would interfere with XML processing of the signature. Likewise, encrypted cipher data may be included in an XML encrypted element or managed separately.

RFC 1847 defines a general mechanism for security multiparts in MIME (Secure/Multipurpose Internet Mail Extensions), defining the Multipart/Signed and Multipart/Encrypted types. Multipart/Signed enables the first MIME part to contain arbitrary MIME content and the second to contain a signature over that content. Multipart/Encrypted uses the first part to contain encryption control information, and the second part for encrypted content. An alternative to Multipart/Encrypted is to pass a single MIME part containing encrypted content.

An Internet-Draft is in preparation to define how XML Digital Signatures and XML Encryption may be used with Multipart MIME security to provide MIME integrity and confidentiality. It extends RFC 1847 by defining application/signature+xml and application/encryption+xml protocols for the Multipart/Signed and Multipart/Encrypted MIME types. Although non-XML content may be signed or encrypted based on XML signing and encryption, additional capabilities are available for XML MIME content.

Signature

Multipart/Signed content consists of two parts by default, the content part and the signature part. The first part may be any type of content, encoded in MIME canonical format (for example base64 encoded), and should include MIME headers defining the content type. The second part is a signature over the entire first part, including the MIME headers. The second part should be labelled with the content type of "application/signature+xml". With transforms it is possible to sign only parts of the MIME part or the XML or only to use only one MIME part for both the content and the signature.

Encryption

Multipart/Encrypted content consists of two parts, a control part and the encrypted content part. The control part should be the same type as the protocol parameter, in this case "application/xml-encrypted". For XML encryption, the control part should contain the XML encryption content, XML containing one or more encrypted data elements. The encrypted content part of the MIME message may be empty if the cipher text is contained in the XML encrypted data elements. If the cipher data is not included in the XML encrypted data elements it may be placed in the second encrypted data MIME part, base64 encoded.

Table A.1 shows the main mandatory features.

Table A.1 – Mandatory features of XML signature and XML encryption with MIME

Main mandatory features	XML digital signature and XML encryption/MIME
Message format	base64
Certificate format	Binary, based on X.509v3
Symmetric encryption algorithm	TripleDES ANSI X.952 (DES EDE3 CBC) or AES-128, AES-256 (CBC)
Signature algorithm	DH (Diffie-Hellman, ANSI X9.42) with DSS
Hash algorithm	SHA-1
MIME encapsulation of signed data	multipart/signed or CMS format
MIME encapsulation of encrypted data	multipart/encrypted

A.2 S/MIME version 3

S/MIME version 3 (Secure/Multipurpose Internet Mail Extensions) is based on MIME and provides a consistent way to send and receive secure MIME data. It is based on 7-bit character encoding and converts 8-bit character encoding or binary data into a 7-bit character stream. It provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP. S/MIME v3 consists of four RFC parts: Cryptographic Message Syntax (RFC 2630), S/MIME Version 3 Message Specification (RFC 2633), S/MIME Version 3 Certificate Handling (RFC 2632), and Diffie-Hellman Key Agreement Method (RFC 2631).

S/MIME v3 is a W3C recommendation and free of patent issues. Its certificate structure is based on IETF's PKIX. S/MIME v2 is not recommended because it is only a RCF draft and depends on patents (RCA). An additional protocol, Enhanced Security Services for S/MIME (RFC 2634), is a set of extensions to S/MIME to allow signed receipts, security labels, and secure mailing lists.

Table A.2 shows the main mandatory features.

Table A.2 – Mandatory features of S/MIME v3

Main mandatory features	S/MIME v3
Message format	Binary, based on CMS
Certificate format	Binary, based on X.509v3
Symmetric encryption algorithm	TripleDES ANSI X.952 (DES EDE3 CBC)
Signature algorithm	DH (Diffie-Hellman, ANSI X9.42) with DSS
Hash algorithm	SHA-1
MIME encapsulation of signed data	Choice of multipart/signed or CMS format
MIME encapsulation of encrypted data	application/pkcs7-mime

A.3 OpenPGP/MIME

The OpenPGP protocol is also free of patent issues and described in the OpenPGP Message Format, draft RFC 2440. The MIME wrapping for OpenPGP is described in MIME Security with Pretty Good Privacy, RFC 3156. Whereas normally, PGP users do not use a PKI and mutually sign trusted users certificates if they know them personally, a PKI could also be used with OpenPGP.

Table A.3 shows the main mandatory features.

Table A.3 – Mandatory features of XML signature and encryption with MIME

Main mandatory features	OpenPGP/MIME
Message format	Binary, based on previous PGP
Certificate format	Binary, based on previous PGP
Symmetric encryption algorithm	TripleDES (DES EDE3 Eccentric CFB)
Signature algorithm	ElGamal with DSS
Hash algorithm	SHA-1
MIME encapsulation of signed data	multipart/signed with ASCII armour
MIME encapsulation of encrypted data	multipart/encrypted

A.4 Transport layer security with TLS

TLS is for transport layer security, not for end-end security on application level. It provides data integrity, confidentiality, authentication, and non-repudiation between client and server. Non-repudiation is done using digital signatures and public key certificates. Servers are authenticated, clients can be authenticated optionally.

TLS has the following features:

- The connection is private: symmetric cryptography is used for data encryption (for example, DES [DES], RC4 [RC4], etc.) The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption.
- The connection is reliable: message transport includes a message integrity check using a keyed MAC. Secure hash functions (for example, SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.
- The peer's identity can be authenticated using asymmetric, or public key, cryptography (for example, RSA [RSA], DSS [DSS], etc.). This authentication can be made optional, but is generally required for at least one of the peers (mostly the server).
- The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection, the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.
- The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.

Annex B
(informative)

IEC TR 62210 security

B.1 General

This annex covers the appropriate areas of security that impact the implementation and use of e-business technologies in the context of the IEC 62210. It is informative and offers the end users only recommendations.

IEC 62210 applies to computerized supervision, control, metering, and protection systems in electrical utilities. It deals with security aspects related to communication protocols used within and between such systems, the access to, and use of the systems. The main focus is on end-to-end communication security on application and system level. The recommendations are neutral in regard to the methodologies and technologies used and have no direct impact on the corporate security policy.

Figure B.1 shows the security aspects of energy market communications with relevance to power system security (in short, “process security”). IEC 62210 lists the following utility business areas to be secured: generation of power, transmission of power, distribution of power, measurement of trading and supply, asset management, energy conservation, and securing of power quality. From the perspective of process security, there are two areas of security concern with energy market communications: (1) Business-to-process communication (B2P) between market participants and utility business areas at the “interface point” to utility control functions, and (2) process-to-process communication (P2P) within utility business areas or between those of different utilities.

It is important to note that the same e-business technology can be used for both areas. An example for the second case between utility business areas and as an alternative to TASE.2 for inter control centre communication is scheduling of energy transactions, reservation of transmission capacity, exchange of metering readings of tie lines, exchange of power system model data and planning data.

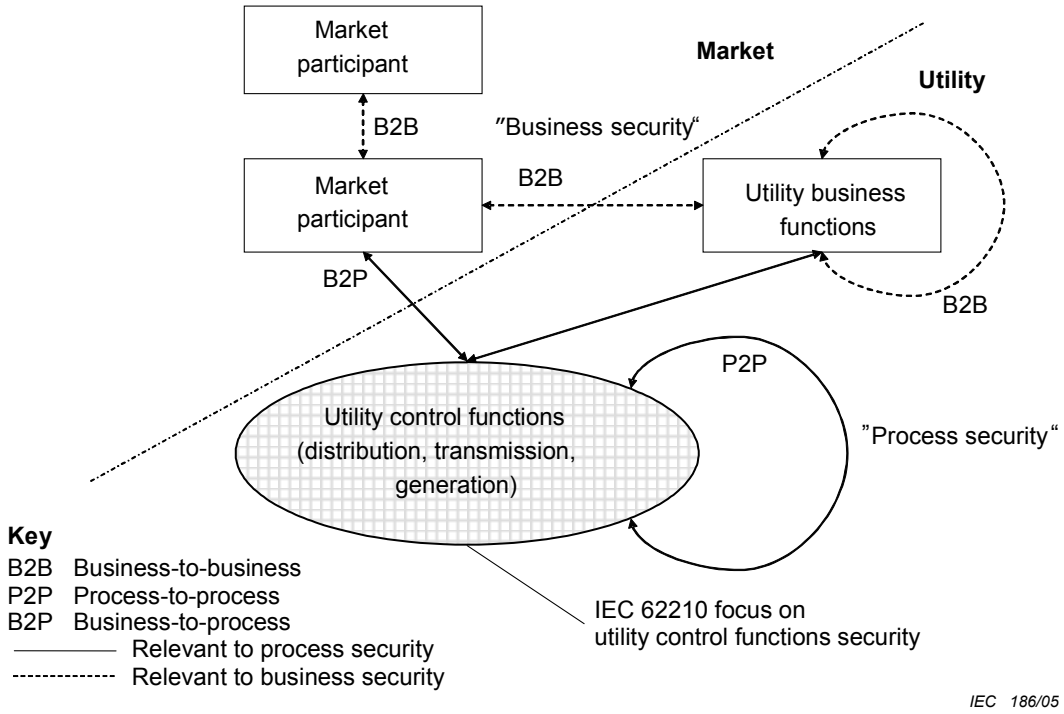


Figure B.1 – Security aspects of energy market communications

IEC 62210 recommends a security analysis based on the ISO 15408-1 methodology. This includes *protection profiles (PPs)* that state assumptions about the *Target Of Evaluation (TOE)*, identification of *threats and attacks* to *Security Targets (ST),* definition of *security objectives* to counter this threats, and finally identifying *security functions* to satisfy the security objectives.

The security objectives are: confidentiality, data-authentication, data-integrity, source-authentication including non-repudiation, availability (includes authorisation), and transaction-integrity.

Under the assumption that the stakeholders of energy market communications define the protection profiles this annex shows which *security functions* satisfying the *security objectives* can be chosen to avoid the risk of security issues (threats and attacks). This approach is *independent* of the e-business technology and architecture used because the technical solutions apply to all e-business technologies and architectures of this series.

In the context of IEC 62210, the following deals with P2P and B2P energy market communication having impact on utility control functions, see above. For the B2P energy market communication, it is recommended to avoid security attacks on the utility control functions by using fire walls and isolating the intranet for utility control functions from the external network (for example Internet) physically. This means that the hand-over of energy market information used for power system control is fully under the control of the utility. Nevertheless, the communication has to be secured in the same way as P2P because some of the market information has physical impact on utility control functions (for example scheduling of energy transactions).

B.2 Definitions

For the purposes of this annex, the definitions of security issues given in Table B.1 apply.

Table B.1 – Definitions of security issues

Security issues	Definitions
Authorisation Violation	An entity authorised to use a system for one purpose that uses it for another unauthorised purpose.
Availability	Information exchange is possible.
Bypassing Controls	System flaws or security weaknesses are intentionally attacked.
Denial of Service	Authorised communication flow/exchange is impeded.
Eavesdropping	Information is revealed to an unauthorised person via monitoring of communication traffic.
Illegitimate Use	An individual authorised for one action performs an action, control, or information retrieval, but an action is completed for which the individual is not authorised.
Indiscretion	An authorised person discloses restricted information to a non-authorised entity.
Information Leakage	An unauthorised entity acquires restricted information. Typically, this term is for non-eavesdropping acquisition of the information (for example, through other means of disclosure).
Integrity Violation	Information is created or modified by an unauthorised entity.
Intercept/Alter	A communication packet is intercepted, modified, and then forwarded as if the modified packet were the original. This is a typical man-in-the-middle scenario.
Masquerade	An unauthorised entity attempts to assume the identity of an authorised entity.
Replay	A communication packet is recorded and then retransmitted at an inopportune time.
Repudiation	An exchange of information occurs and one of the two parties in the exchange later denies that the exchange took place.
Spoof	This attack is a combination of one of the following threats: Eavesdropping; Information Leakage; Integrity Violation; or Intercept/Alter and Masquerade.

B.3 Recommended security objectives

Table B.2 shows the recommended security objectives to counter the security threats and attacks. Note that market communication issues only refer to “communication” on transport and application level and not to overall system security and administration of security.

Table B.2 – Recommended security objectives

Communication issue	Security issues	Recommended security objectives
Yes	Bypassing Controls	Strong security functions based on the security objectives.
Yes	Integrity Violation	O.DATA-INTEGRITY
No	Authorisation Violation	O.AVAILABILITY
No	Indiscretion	No recommendation.

Communication issue	Security issues	Recommended security objectives
Yes	Intercept/Alter	O.SOURCE-AUTHENTICATION, O.DATA-AUTHENTICATION
No	Illegitimate Use	No recommendation.
No	Information Leakage	No recommendation.
Yes	Spoof	O.CONFIDENTIALITY, O.DATA-INTEGRITY, O.DATA-AUTHENTICATION, O.SOURCE-AUTHENTICATION
Yes	Repudiation	O.NON-REPUDIATION
Yes	Masquerade	O.SOURCE-AUTHENTICATION, O.DATA-AUTHENTICATION
Yes	Availability (for example Denial of Service)	O.AVAILABILITY
Yes	Eavesdropping	O.CONFIDENTIALITY

B.4 Recommended security functions

Detailed technical security profiles based on the recommended security functions in Tables B.3 and B.4 are defined in the technology dependent parts of the IEC 62325 series. This profiles allow the adoption to specific security requirements.

Table B.3 shows the recommended security functions of communication to satisfy transport security objectives. The implementation depends on the chosen profile.

Table B.3 – Mapping of security objectives to transport security functions

Security objectives	Recommended security function
O.CONFIDENTIALITY	Implementation of TLS (IETF) on transport layer with proper security policies is recommended.
O.DATA-AUTHENTICATION	Implementation of TLS (IETF) on transport layer with proper security policies is recommended.
O.DATA-INTEGRITY	Implementation of TLS (IETF) on transport layer with proper security policies is recommended.
O.SOURCE-AUTHENTICATION	Implementation of TLS (IETF) on transport layer with proper security policies is recommended.
O.AVAILABILITY	No recommendation. This requires on application level authorisation, certificate/key management, and means against denial-of-service threats.
O.TANSACTION-INTEGRITY	No recommendation. This depends on the technology used.

Table B.4 shows the recommended security functions of communication to satisfy alternatively application security objectives. The implementation depends on the chosen profile.

Table B.4 – Mapping of maximum security objectives to application security functions

Security objectives	Recommended security function
O.CONFIDENTIALITY	Implementation of XML Encryption (W3C) on application layer with proper security policies is recommended.
O.DATA-AUTHENTICATION	Implementation of XML Digital Signature (W3C) and message digest on application layer with proper security policies is recommended.
O.DATA-INTEGRITY	Implementation of XML Signature (W3C) and message digest on application layer with proper security policies is recommended.
O.SOURCE-AUTHENTICATION	Implementation of XML Digital Signature (W3C) on application layer with proper security policies is recommended.

Security objectives	Recommended security function
O.NON-REPUDIATION	Implementation of XML Signature (W3C) and persistent logging of transactions.
O.AVAILABILITY	No recommendation. This requires an application level authorisation, certificate/key management, and means against denial-of-service threats.
O.TANSACTION-INTEGRITY	No recommendation. This depends on the technology used.

B.5 Security management

This annex does not specify a security policy or a specific digital certificate/key managing and maintaining processes. This is left as another “local implementation issue.”

The following areas need to be addressed by the user’s requirements:

- Know, on an association-by-association basis, which links are operating in a secure or non-secure mode.
- Allow simultaneous inter-operability with existing non-secure associations and new secure associations on an association-by-association basis.
- Allow or prevent, by prior mutual agreement, an association to be unilaterally taken out of (or returned to) secure mode for debug purposes on an association-by-association basis.
- Allow new associations to be commissioned in secure or non-secure mode without requiring a complete restart of the application.
- Allow certificate negotiation rates to be set on an association-by-association basis.
- Multiple digital certificates should be supported.

B.6 Network profiles

For network profiles, see the technology dependent parts of the IEC 62325 series.

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

ISBN 2-8318-7845-4

ICS 33.200

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND