DD CEN/TS 15523:2011

BSI Standards Publication

Postal Services — Statement of mailing submission

National foreword

This Draft for Development is the UK implementation of CEN/TS 15523:2011. It supersedes DD CEN/TS 15523:2006 which is withdrawn.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion to an international standard. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards.*

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee SVS/4, Postal services.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 73766 4

ICS 03.240

Compliance with a British Standard cannot confer immunity from legal obligations.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 30 September 2011.

Amendments issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15523

September 2011

ICS 03.240

Supersedes CEN/TS 15523:2006

English Version

Postal Services - Statement of mailing submission

Services postaux - Déclaration de dépôt du courrier

Postalische Dienstleistungen - Übertragung von Daten für Briefanlieferungen

This Technical Specification (CEN/TS) was approved by CEN on 4 June 2011 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (CEN/TS 15523:2011) has been prepared by Technical Committee CEN/TC 331 “Postal Services”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes CEN/TS 15523:2006.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

NOTE This document has been prepared by experts coming from the Technical Committee CEN/TC 331 “Postal Services” and UPU, under the frame of the Memorandum of Understanding between UPU and CEN.

The UPU’s contribution to the specification was made, by the UPU Standards Board[1] and its subgroups, in accordance with the rules given in Part V of the "General information on UPU standards".

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

[1] The UPU's Standards Board develops and maintains a growing number of standards to improve the exchange of postal-related information between posts, and promotes the compatibility of UPU and international postal initiatives. It works closely with posts, customers, suppliers and other partners, including various international organizations. The Standards Board ensures that coherent standards are developed in areas such as electronic data interchange (EDI), mail encoding, postal forms and meters. UPU standards are published in accordance with the rules given in Part VII of the General information on UPU standards, which can be freely downloaded from the UPU world-wide web site (www.upu.int).

Introduction

Widespread proliferation of electronic, internet-based data communications provides a cost-effective platform for integrating a global mail communication system. The essence of such integration is an automated exchange of computerised information between mailer's, postal and recipient's domains. Within each of these domains there is a wealth of information that has been or could be collected, computerised and subsequently communicated to other domains to enhance the overall mail system. This information is typically information *about* mail units and it allows for effective control and management of the entire mail distribution network.

Most commercial-purpose mail is created and finished with the help or under control of computer-driven equipment. Mail-descriptive computerised data is a by-product of the mail creation/finishing process and it has significant value for both postal operators and their agents and frequently for mail recipients. Specifically, when a plurality of mail items (designated as a *mailing submission*) are prepared for induction into a postal distribution network by a mailer, it is only natural that the mailing submission should be accompanied by an electronic document (or computer file) that is commonly referred to as a *statement of mailing submission*. The main goal of the statement of mailing submission (SMS) is to provide support information for mission-critical applications in the mail communication system, and specifically for applications in the postal domain. The most important applications in the postal domain come from operations (mail entry/induction, processing/sorting, transportation and delivery), postal marketing (maintenance of existing products and services, design of new postal products and services, customer relationship management and management of quality of service), and finance (revenue management including collection and protection of revenue).

The main purpose of the present technical specification is to define basic concepts associated with the statement of mailing submission (framed using methodology of an entity-relationship model), and then to define the content, message structure and protocol that can be used by mailers or their agents to communicate to posts information supporting major postal applications, and also to provide a detailed analysis of application-level security.

The following section describes information requirements supporting major postal processes.

Postal operations information requirements

Mail entry/induction process is a controlled acceptance process that is designed to enable transfer of typically medium or large size mailings (e.g. mailings containing more than several hundred mail items) from mailers or their agents to postal operators. *Mail entry* process involves verification of mail make-up (i.e. check of the information present on mail units for its postal process friendliness) and verification of payment. The process is based on comparison of information created or otherwise known to postal acceptance personnel against information supplied by mailer. Critical data elements supporting mailing submission entry are:

— Mailing submission composition such as number of mail units of various kind contained in the submission;

— Type and identities of mail units included into submission;

— Gross and net weight of mail units included into submission and gross and net weight of the submission itself;

— Worksharing information if mailing submission has been pre-sorted or contains mail pre-barcoded by mailer or its agents. This information includes geographic distribution (number and type of mail units for each postal code), postal codes assigned to and marked on each mail unit as well as information concerning quantity, location and markings for all non-qualified (or residual) entities;

— Payment information including accounting information and postage information for various categories of postal products included in the mailing and totals for each category;

- Identity of the SMS associated with the mailing submission;
- Security information such as key certificates as described in the present specification (Annex D).

Mail processing information requirements support cost-effective mail sorting. In addition to the information identified above, the mail sort-supporting electronic information may include identities of all mail units included in the submission linked with their associated address information including postal codes.

Mail transportation information requirements support cost-effective transportation of mail units and aggregates between postal processing and delivery offices. Thus, in addition to the information identified in the previous sections, mail transportation-supporting information may include (if they are known during mail preparation process) identities and scheduling data for various transportation vehicles (trucks, railroad cars, aircrafts and boats) that will be used for transporting mailing submission.

Mail delivery process information requirements support cost-effective delivery of mail. In addition to the information described above mail delivery-supporting information may include number, identity and type of mail units that require special delivery or handling (e.g. proof of delivery or return receipt).

Postal marketing information requirements

Marketing information is mainly concerned with a detailed description of a mailer’s use of various postal products and services offered by a postal operator. These may include:

- Number of first class mail items included in the submission;
- Number of second class mail items included in the submission;
- Number of special rate mail items (e.g. overweight or oversize);
- Number of mail items that require special delivery (e.g. registered, certified, time-specific delivery etc.);
- Number of items that require forwarding services or address correction;
- Preferred delivery instructions, redirection and address services (e.g. address hygiene).

Postal finance information requirements

Postal financial applications require an effective payment mechanism for the services by mailers or their agents. These include automatic generation of all required accounting and funds transfer data and its supporting documentation for billing and remittance processing. Finance information should include as a minimum data elements that allow to:

- Create, delete and update customer accounts (e.g. unique account IDs);
- Identify products and services used by the mailer together with their current tariffs;
- Identify mail attributes (e.g. item count, weight, volume) for specific postal products and services;
- Support payment for Business Reply and other recipient-paid services;
- Automate the receipt and processing of payments (e.g. by using Electronic Funds Transfer);
- Automate the processing of all legitimate refunds to mailers;
- All required management and control supporting reports.

Methodology

The methodology adopted for the organisation of SMS begins with a data structure describing all practical knowable information about mailing submission. This data structure containing all-inclusive information is a sort of a “super” file or “super” message. The specification describes how to collapse (or cluster) this super message into new data structures suitable for particular postal applications. This is done by eliminating the non-essential information depending on the informational needs and requirements of postal applications.

Selection (or adaptation) of data elements, their formats and communication protocols for various specific applications and environments for the SMS from the ones described in the present specification are left to postal operators and their customers. It was felt that no group of experts would have sufficiently detailed knowledge of a broad variety of existing and future postal applications and technical environments in order to accommodate even the most common ones. For this reason, it was decided that providing a definition of a super, all-inclusive and adaptable message and the methodology of collapsing it into application-specific messages (statements) would be the best choice. Similarly, timing considerations for various possible messages that could be exchanged between mailer and postal domains are outside of the scope of the present specification. Messages that are defined and described here can be arranged to be created by mailers and communicated to postal operators *before, during or after* the actual induction process takes place, depending on the value and the intended use of the communicated information. The specification leaves the choice of timing considerations to postal operators and their customers.

1 Scope

This Technical Specification specifies a methodology that allows postal operators to define specific statements of mailing submission customised according to their environment and applications.

The document defines information requirements for existing generic postal information processing applications related to major postal functions, namely operations, finance and marketing by specifically identifying the information that could be collected within the mailer's domain and transmitted to the postal domain.

In addition, this document defines the organisation of data into messages by describing data content, format and communication protocol suitable for communication of data originating in the mailer's domain.

The specification also provides a detailed analysis and recommendations for implementing application-level security threats and countermeasures particularly relevant for postal revenue protection in controlled mail entry settings.

Finally, this document provides several examples of concrete statements of mailing submissions and an example of a secure communication protocol recommended for transmission of such statements.

NOTE The SMS describes letter mail or flats that are submitted for distribution and would not deal explicitly with content of letters or flats whether it concerns customs or any other party that could in principle be interested in knowing the content of these mail units.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, or references to a version number, only the edition cited applies. For undated references and where there is no reference to a version number, the latest edition of the referenced document (including any amendments) applies.

EN 14615:2005, *Postal services – Digital postage marks – Applications, security and design*

ISO 10126-2:1991, *Banking – Procedures for message encipherment (wholesale) – Part 2: DEA algorithm*

ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*

ISO/IEC 15418, *Information technology – Automatic identification and data capture techniques – GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance*

ISO/IEC 15434, *Information technology – Automatic identification and data capture techniques – Syntax for high-capacity ADC media*

ISO/IEC 15459-1, *Information technology – Unique identifiers – Part 1: Unique identifiers for transport units*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
address list selection
process of selecting a mailing address for the intended recipient of the message

3.2
agent
entity involved in any part of the provision of postal services in respect of a mail unit

3.3
agent attribute
characteristic of the agent which is or can be represented by a data value

3.4
communication domain
set of parties, agents, and processes that together play a specific functional role (such as sender, channel or recipient) in a mail communication system

3.5
consolidator
party that is responsible for assembling mail units from a given creator together with mail units from other creators

3.6
containerisation
process of assembling together and putting mail units into receptacles for transportation

3.7
controlled acceptance/entry mail (CAM/CEM)
mail unit or mail aggregate that is examined by postal personnel before being accepted for processing for the purpose of compliance with postal regulations concerning proper payment (accounting) and mail make up

3.8
mail creator
party that is responsible for production (creation) of a mail item, a mail unit or an aggregate

3.9
electronic sortation
process of sorting a list of mailing addresses into groups having common characteristics (such as identical postal codes)

3.10
electronically exchanged message
EEM
electronic message sent or received by a mailer or postal operator during the process of mail creation, preparation, submission, acceptance, processing and delivery

3.11
expectation
set of mail unit attribute name-value pairs predicted, derived or assumed for a given date or a date range

3.12
finishing
process of direct printing of information on (or applying labels containing information to) assembled mail units, said information concerning payment evidence and endorsements required for the entry of finished mail units into the postal distribution network

3.13
insertion
process of folding printed message(s), assembling the content (that includes the message and optional additional enclosures) and inserting the entire content into a mailing envelope

3.14
list preparation (address cleansing)
process of comparing between mailing (postal) addresses in the selected address list and a standardised list containing corrected and up-to-date postal addresses for the purpose of finding and correcting erroneous entries in the selected list

3.15
mail unit
mail item or collection of mail items which are constrained to form a physical unit

3.16
mail unit attribute
characteristic of a mail unit which is or can be represented by a data value

3.17
mail induction/entry
process whereby mail units are handed over to a postal operator and which results in either the postal operator taking responsibility for the mail units concerned or rejecting all or some of the mail units presented for hand over

3.18
mail item
item
mailpiece
postal item
indivisible mailable entity in respect of which a mail service contractor accepts an obligation to provide postal services

3.19
mail receptacle
physical device which may be used to contain or carry mail so as to assist in its handling, transportation, storage or delivery as a unit

EXAMPLE Mailbags, trays, recipient mailbox, wheeled containers (roller cages), pallet and pallet-based containers and airfreight containers (ULDs).

NOTE Receptacles may contain mail which is housed in other (lower level) receptacles. For example, a roller cage may contain trays and/or bags of mail as well as individual (loose loaded) mail items and bundles. Some types of postal receptacle (e.g. roller cages and ULDs) have a residual value; others need not (e.g. disposable trays).

3.20
mail receptacle attribute
characteristic of a mail receptacle which is or can be represented by a data value

3.21
mail aggregate
aggregate
set of mail units that satisfy specific criteria defined in the context of a particular application

3.22
aggregate attribute
characteristic of an aggregate which is or can be represented by a data value

3.23
aggregate catalogue
collection of attribute names for mail units included in an aggregate

3.24
mailing submission
mail aggregate which has a unique identification and is presented or handed over for processing, by a postal operator, as part of a single induction unit

3.25
message preparation
process of preparing data that is designed to be sent as a message (content of a mail item) to the intended recipient

3.26
observation
set of mail unit attribute name-value pairs captured at a given date

3.27
observation attribute
set of name-value pairs related to or characterising the observation process

3.28
originator
party that controls a mail unit's content (i.e. the message to the recipient) and the mail unit's destination address and has the overall legal control and responsibility for the mail unit

3.29
party
legal entity involved in a mail communication process

3.30
party attribute
characteristic of the party which is or can be represented by a data value

3.31
payer
party responsible for payment of postal/carrier charges for services rendered by mail services contractor in respect of a mail unit

3.32
physical sortation
process of sorting mail units into groups having common characteristics (such as identical postal codes)

3.33
postal product/service
agreed-upon set of rules operating on the values of mail unit attributes governing both actions to be taken on the mail unit and communication of observations to all authorised parties

3.34
postal product/service attribute
characteristic of a postal product which is or can be represented by a data value

3.35
post/carrier domain
domain of the mail unit collection, acceptance, processing, transportation and delivery that includes all parties, agents, processes and their relationships that are involved in these activities

3.36
process in the mailer domain
series of sequential functional activities (or sub-processes) within the mailer domain resulting in finished mail units and aggregates being ready for entry into a postal/carrier distribution network

3.37
process in the postal domain
series of sequential functional activities (or sub-processes) within the postal domain including collection, facility entry, acceptance, processing (culling, facing, sorting), containerisation and transportation resulting in a mail unit being delivered to a recipient, discarded or returned to the mail originator (or a party authorised by the mail originator)

3.38
recipient domain
domain of the mail unit receipt and after receipt processing including activities when the mail unit has been received by a party or an agent other than the party specifically indicated by the sender as a recipient. It includes all parties, agents, processes and their relationships that are involved in these activities

3.39
sender/mailer domain
domain of the mail unit creation, finishing and submission for delivery that includes all parties, agents, processes and their relationships that are involved in these activities

3.40
statement of aggregate
collection of attribute name-value pairs for an aggregate assembled for the purpose of a specific application in the context of which the mail units comprising the aggregate form a logical unit

3.41
statement of mailing submission
collection of attribute name-value pairs which specifies a mailing submission and its content

3.42
submission group
aggregate consisting of a collection of mailing submissions that share an explicitly specified common attribute or attributes

3.43
submitter
party responsible for submitting (inducting) a mail unit or an aggregate into postal/carrier distribution network

4 Symbols and Abbreviations

CAM	controlled acceptance mail
CEM	controlled entry mail
DPM	digital postage mark
EEM	electronically exchanged message
ID	(identifier for) identity

MU	mail unit
MS	mailing submission
MS-ID	mailing submission identifier
PSD	postal security device.

NOTE Throughout this document, the following notation is used: entity.attribute. For example, the mail unit identifier is designated as "mailunit.ID".

5 General Concepts

This clause provides a detailed explanation for the basic concepts defined in the previous clause and the motivation behind introducing these concepts and their definitions.

This clause provides the background, motivation and an explanation for all concepts and objects defined in Clause 3.

General concepts are described referring to a mail communication system diagram presented in Figure 1.

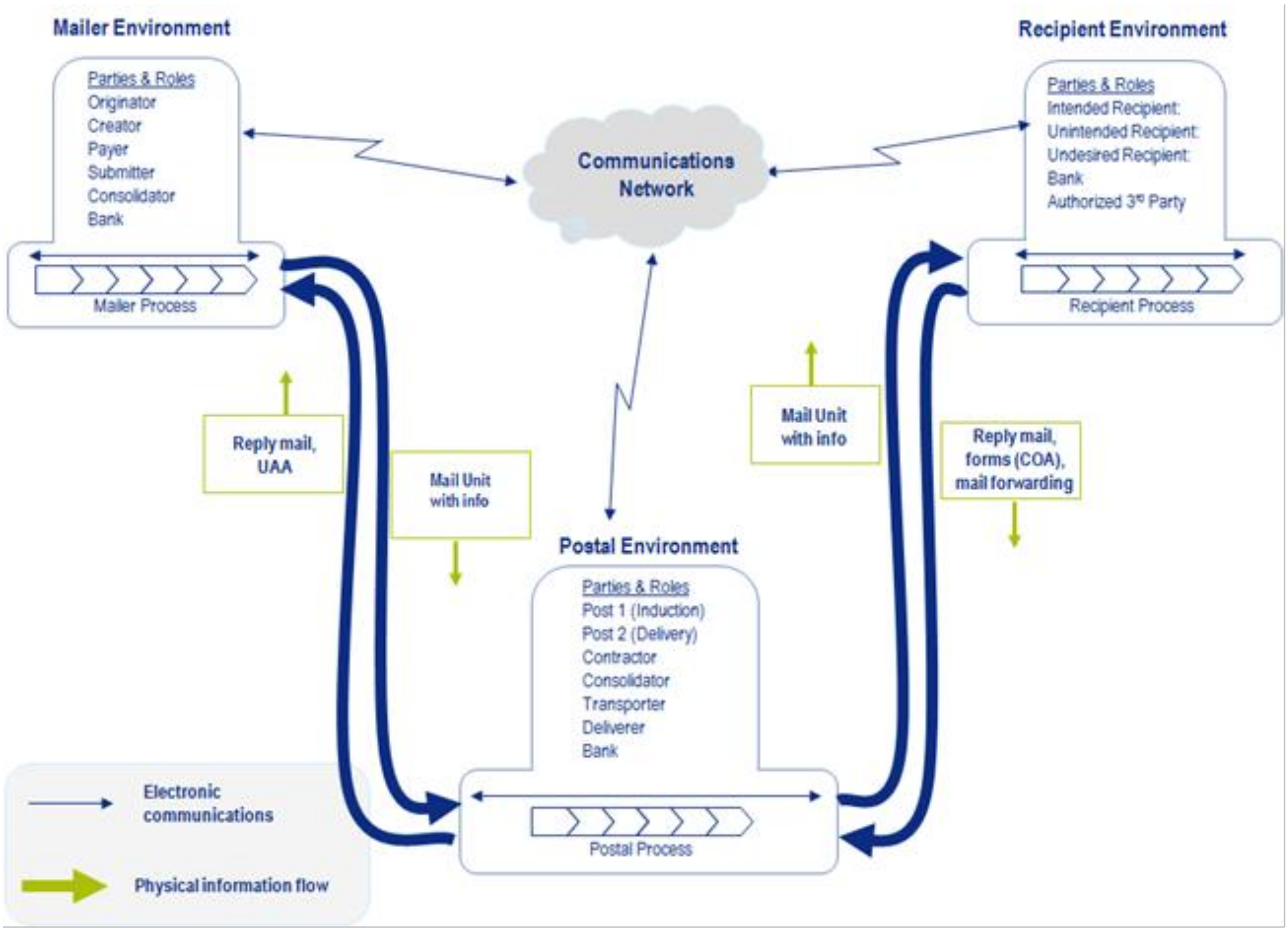


Figure 1 – Mail communication system diagram

5.1 Mail communication system domains

The communication system is a system that enables a *sender* to send (communicate) a *message* to a *recipient* using a *communication channel*. A mail communication system has three basic domains, namely the domain of the message sender, the domain of the message carrier (the communication channel) and the domain of the message recipient. In the context of a mail communication system, a *message* constitutes a *physical entity* (defined in the present document as the mail unit) and as such, it is understood to constitute a single physical object (mail item) or to include a broad variety of physical objects such as post cards, letters, flats, parcels or packages constrained to form a physical unit. Specific to the mail communication system is the notion that messages frequently have value other than informational value, for example monetary, legal or social value.

There are three commonly considered domains, namely Sender/Mailer, Post/Carrier and Recipient. Each domain can be described in terms of parties, agents, processes and their relationships. In the mail communication system, parties involved in each domain are usually independent legal entities that are nevertheless dependent on each other in the overall system process that involves creation and exchange of material (*mail units*) and informational objects (*mail unit attributes, observations, expectations and their attributes*) between domains.

5.2 Parties, agents and their roles

Parties involved in mail unit creation, finishing and submission for delivery are:

- Originator;
- Creator;
- Payer;
- Submitter;
- Consolidator;
- Bank (or other financial service institution involved in payment for mail unit creation, finishing and distribution).

The originator is understood as the party that needs to use the mail communication system to send mail units to (a list of) addresses that are chosen by the originator. The originator is also the primary beneficiary of communication. In the context of business applications involving mail communications, the originator also controls these applications, for example invoicing or product advertising.

The creator is understood as the party that controls physical process of mail unit creation, typically under a contract with the mail originator (for example when the mail creator and originators are different legal entities).

The payer is defined as the party that pays for postal products and services; frequently the originator and payer are the same legal entity.

The submitter performs the technical role of submitting mail units for induction into the mail distribution network, while a consolidator combines mail units from multiple mail creators, in order to achieve certain desirable characteristics for the resulting mail unit or aggregate. The most frequent reason and purpose for consolidation is the value added by presorting or other worksharing activities. In the vast majority of cases the consolidator also assumes the role of the submitter.

Finally the bank (which is used here synonymously with a financial institution) is capable of providing necessary credit and funds transfer functions.

Modern mail communication systems involve computer-controlled electro-mechanical machinery (e.g. sorting machines), transportation (e.g. delivery vehicles) and computer equipment (e.g. IT systems) and human participants (e.g. post office clerks). Mail processing machines, equipment and human participants are designated as agents. Agents involved in mail unit creation, finishing and submission for delivery are various automated, semi-automated and manual systems and their operators such as inserters (mail assembly machines), mailing machines, franking devices, mail sorters, containerisation systems, computerised accounting devices (also known as postal security devices or PSDs), scanning devices and the like. For example, mail sorting machines typically organise letters or flats into groups of mail items having identical postal codes by using information present on mail items, such as a destination address block. Important technology used by a vast majority mail sorting machines are either Optical Character Recognition or bar code reading.

Frequently, post and carriers employ several subcontractors or trusted agents in the complex process of mail acceptance, sortating, transportation and distribution. Parties involved in mail unit acceptance, induction, processing, transportation and delivery are:

- Originating postal operator (or a private carrier);
- Destination postal operator (or a private carrier);
- Consolidation contractor;
- Transportation contractor;
- Delivery contractor;
- Bank (or other financial service institution involved in payment for mail unit acceptance, induction, processing, transportation and delivery functions).

The originating postal operator or carrier may be the only party that is involved in mail unit/aggregate processing, transportation and delivery. Such is the case when the mail unit destination address is within the geographical boundaries of a country or territory where the originating postal operator is authorised to provide mail communication services and when the originating postal operator does not employ any other legal entities to perform such services. Alternatively, there could be several other legal entities involved in the provision of mail communication services such as contractors and other postal operators or private carriers. There also could be several intermediate carriers and contactors between the originating postal operators or carriers and the destination postal operators or carriers, for example transportation contractors as defined below.

Agents involved in mail unit acceptance, induction, processing, transportation and delivery are various automated, semi-automated and manual systems and their operators such as cullers, facers/cancellers, mail sorters, containerisation systems, scanning devices, mail transportation vehicles, railroad cars, airplanes, mail clerks and the like.

Parties participating in the mail communication system are usually involved in mail units physical handling (e.g. sorting, transportation, delivery), in mail units-related information handling (e.g. tracking information capture and communication) and/or in mail units-related financial transaction handling (e.g. postage payment). The defining characteristic of a party is its legal status as an entity that is entrusted in the execution of any of the aforementioned aspects or activities of the mail communication process.

NOTE 1 All parties and agents considered in this document must be uniquely identifiable within the context of a given application. Methods of assigning identifiers to various parties and objects are addressed by ISO Standards and UPU standards: ISO/IEC 15418, ISO/IEC 15434, ISO/IEC 15459-1, UPU S25 and UPU S27.

NOTE 2 Roles of the parties and agents involved in the mail communication systems can be codified and published (i.e. made available to all interested parties) in the form of standardised code lists.

NOTE 3 It should be stressed that the list of parties, their agents and their roles is not exhaustive and intended for illustrative purposes. New parties and agents are continuously introduced when mail communication systems are undergoing complex changes associated with the introduction of new technology, change of ownership (privatisation) or change in the legal status of protected services (liberalisation). The framework of the present document is designed to accommodate the introduction of new parties and agents.

5.2.1 Party attribute

Party attribute is a useful concept that enables the capture and storage of information related to the party, that is not covered by the party name or its identifier. Examples of party attributes are the party's functional role in the process, its classification code according to the industry classification system, identifier for a contract that governs the party's relationship with another party or parties, various restrictions concerning the party's role and similar parameters.

5.2.2 Agent attribute

Agent attribute is a useful concept that enables the capture and storage of information related to the agent that is not covered by the agent name or its identifier. Examples of agent attributes are the agent's functional role in the process, year of production (in case of equipment), name of the manufacturer, various technical parameters such as scanning resolution, number of output bins, and similar parameters.

5.3 Physical objects

5.3.1 Mail item

Mail item is a single (indivisible) object that is physically moved through the postal distribution network from sender to recipient. Mail items typically carry a recipient destination address or a pointer to that address. Examples of mail items are post cards, letters, flats, express mail items, parcels and packets.

5.3.2 Mail unit

The concept of mail unit is a generalization of the concept of mail item. Mail unit is one of the central and most fundamental concepts in mail communications. Mail unit is a physical object that is transported at least through a portion of the mail communication network. Mail units by definition are either individual mail items or containers that consist of mail items and receptacles. Mail units are distinguished from empty mail containers that are defined as receptacles. Examples of mail units are post cards, letters, flats, parcels, packages, irregular parcels and pieces, and various receptacles containing mail such as flat trays, letter trays, IPC trays, sacks, pallets, bundles, baskets, roller cages, containers, refrigerated containers, unit load devices and transportation units. Each mail unit has a lifetime that is understood as the period of time between creating a mail unit or its entry into, exit from or dismantling of the mail communication system (in the case of composite mail units that are collections of mail items or other mail units).

Mail units can be a single (individual, indivisible, atomic) or compound. Single mail units are post cards, letters, flats, packages, parcels and similar objects. Compound mail units are collections of single mail units such as a tray, a bundle, a sack, a pallet, a roller cage containing a collection of trays, several pallets containing trays that are loaded onto a vehicle or an airplane. As a physical unit (object), a mail unit has a unique and identifiable location at any given point in time (date) during its lifetime. The mail unit is usually one of the primary targets of analysis and monitoring (the atomic object). The mail unit is characterized by its attributes. Mail units can be assembled together in a single container or a collection of containers for the purpose of transportation or processing. Mail units could be nested in the sense that smaller size containers can be assembled together in larger size containers, for example trays assembled together in a palette. Each individual container together with mail units contained therein is a mail unit in its own right that can be referenced through its identifier(s) and is fully characterised by its attributes.

All mail units considered in this document must be uniquely identifiable within a given application.

5.3.3 Mail receptacle

Mail units are transported using various types of containers. It is frequently important to distinguish between empty containers and containers that carry mail units. Mail receptacle is a generic term that is used to indicate an empty container. Examples of mail receptacles are trays, IPC trays, sacks, pallets, baskets, roller cages, refrigerated containers and unit load devices. Mail receptacles may or may not have unique identifiers. RFID technology is frequently used for identifying large containers carrying cross border mail units.

5.3.4 Aggregate

Unlike a mail unit, an aggregate is not constrained to form a physical unit and does not necessarily have a single defined location at any given point in time (for example, a part of an aggregate might be in one place, while another part could be in another place). Examples of aggregates are mailing, mailing submission, induction unit, submission group, consignment and mail action. Specifically, mailing is an instance of the an aggregate that corresponds to the collection of mail units (e.g. letters) to be generated as a result of a specific business process, such as an invoicing or an advertising campaign.

All aggregates considered in this document must be uniquely identifiable within the context of a given application.

5.3.5 Mailing submission, acceptance and submission group

A mailing is an aggregate from the mailer's[2] perspective. Typically, it might correspond to the set of mail units (e.g. letters) generated as a result of a business process, such as an invoicing cycle or an advertising campaign.

The task of generating, finishing and handing mail over to the postal operator is carried out by the mail submitter. This may be the mail originator, or a separate party working on the mail originator's behalf. For major mailings, the process may be spread over a number of days, or even weeks, necessitating that the mailing is broken down into sub-units which can be separately produced and handed over. Each of these units is called a *mailing submission* or *submission*. The mail submitter determines the breakdown of a mailing into submissions. All mail items that constitute a submission are handled as a unit and are presented to the postal operator on the same date and location (the place of the single hand-over transaction or acceptance/entry location). Each mailing submission is always associated with one date (the date of submission). The single hand-over transaction is the purpose (application) for the aggregate defined as the mailing submission.

Each submission thus consolidates a set of mail units forming part of a mailing, which is handed over together for acceptance, verification and postal processing. However, the actual hand-over process, referred to as *induction*, is usually organised in accordance with some schedule: typically, either the postal operator will collect submissions, or the mail submitter will deliver them to a postal facility, at one or more scheduled times each day. Given this, a single hand-over transaction may involve several submissions collectively referred to as an induction unit (see UPU glossary for definition).

The concept of *mailing* concerns only the mailer and reflects the mailer's view of the information related to the mail units as they support the mailer's business process (e.g. a batch of invoices or an advertising campaign). As a result, the mailing identifier is typically useful only to the mailer and it does not have any meaning outside the mailer domain (e.g. for the postal operator). Similarly, the concept of an induction unit reflects the postal operator's process of acceptance, verification and subsequent processing of mail items, and reflects the Post's view of the information related to the mail units involved. The induction unit identifier is typically meaningful only for the postal operator or its authorised agents. Normally, an induction unit consists of multiple mailing submissions accepted (or rejected) as part of a single hand-over transaction. These multiple mailing submissions are considered together (as a unit) to meet postal operator's financial or operational information processing needs. The concept of a *submission group* is useful when it is desirable or convenient to consider multiple mailing submissions as a group, regardless of whether these submissions form part of a

[2] The use of the term mailer is meant to cover the mailer and any party that acts on the mailer's behalf (mailer's agents).

single hand-over transaction. This could happen, for example when all mailing submissions in a group share the same *contract*.*attribute* (e.g. contract identifier). In this case various contractual obligations specified in *the contact* between a mailer and a postal operator (e.g. minimal number of mailing submissions required from the mailer during a given period of time to meet postage discount requirements) can be automatically verified using computerised information contained within SMS.

All submission groups must be uniquely identifiable within the context of a given application.

The mailing submission is the interface point between the mailer and postal processes. The mailing submission is the only set of mail units that is viewed as a unit both by the mailer and by the postal operator. Mailing submission identifier must be created by the mailer (or its authorised agent) according to the postal operator's regulations. As a result, the information sent by the mailer to the postal operator is organised to reflect and describe each submission. This information is defined as the *statement of mailing submission (SMS)*. It is assumed that for most practical purposes the SMS is an electronic document containing computerised information. The organisation of information in the SMS is the primary object of this specification.

The following diagram illustrates the relationships between mailings, mailing submissions, submission groups and induction units. The diagram shows three mailings, A, B and C, each divided into a number of submissions: five (numbered A:1 to A:5), in the case of mailing A, three each in the case of mailings B and C. Submissions A:1 and B:1 are produced on Monday and form one induction unit, handed over for postal processing at the end of the day; submissions A:2, B:2 and C:1 form a second induction unit, and so on. Submission A:4 is finished too late to join Thursday's induction, so is added to that on Friday. Submissions A:3, A;5, B:1 and C;2 form a Submission Group 1. They are grouped together because they were submitted by the mail submitter on behalf of a mailer that is different than other mailers involved in Mailings A, B and C and thus must be accounted for separately from other submissions.

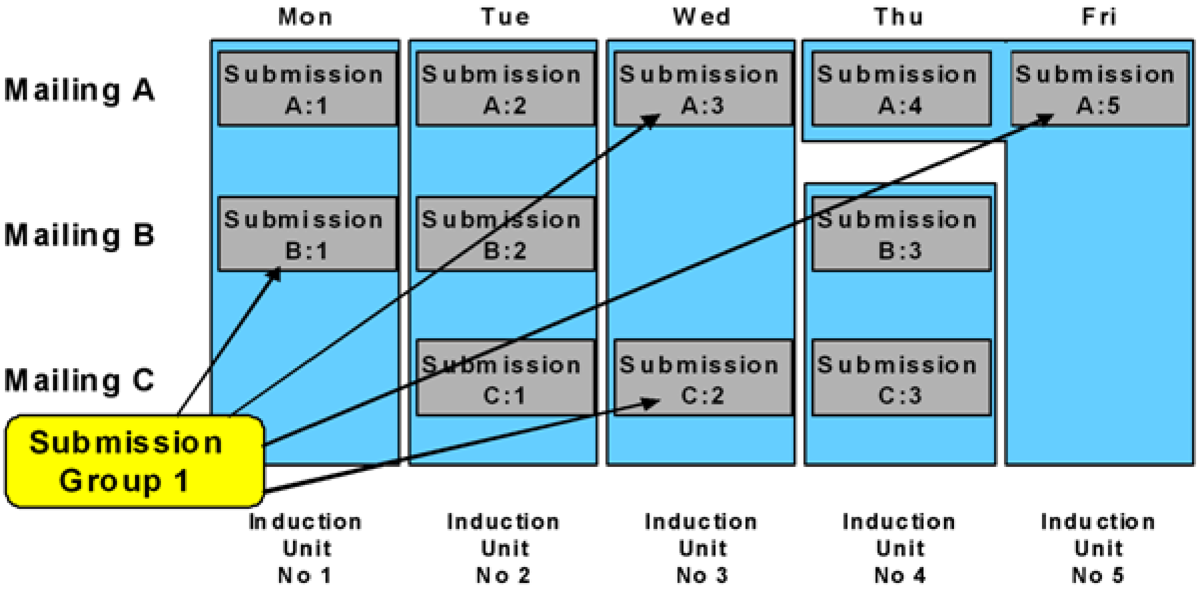


Figure 2 – Relationships between mailings, submissions, submission groups and induction units

The mapping between the internal production processes of the mailer (and other possible parties in the mailer's domain involved in mail production, finishing and induction) and submissions are typically maintained by the mailer and is outside of the scope of the present specification, as having no significance to the postal operator.

The SMS is created primarily for use by the postal operator or its authorised agents since it is the postal operator who is the recipient of the information. The mailing submission is the unit of analysis for financial operations and marketing organisations of the postal operator.

The SMS supports the process of mail acceptance and as a result, is used to detect discrepancies between the attributes of actual mail units as determined by the postal operator during the acceptance process and the information provided by the mailer or its agents in the form of the SMS. Additionally, the SMS is used to document discrepancies. Handling the resolution of discrepancies between the information contained in the SMS and the information obtained from the physical examination of the mailing submission corresponding to the SMS is outside of the scope of the present specification, as it is a matter of policies and procedures.

From a mailer viewpoint mailing submission consists of mail units that are hierarchically organised, for example into letters, trays of letters, various receptacles containing trays of letters etc. These mail units typically have directly measurable characteristics (attributes).

It should be noted that directly measurable characteristic means that the characteristic of the mail unit can be obtained by a direct measurement as opposed to the computation (e.g. weight of an aggregate can only be computed as the sum of the weights of its component mail units, while the weight of a mail unit is typically directly measurable).

All mailing submissions must be uniquely identifiable within the context of a given application.

5.4 Informational objects

This clause provides a detailed explanation concerning various informational objects that form the entity-relationship model of the mail communication system.

5.4.1 Mail unit attribute

Mail unit attribute is a central concept in the entity-relationship model describing a mail communication system. All mail units (including mail items) are fully characterised by their attributes. Mail unit attributes can be either primary or derived (composite). Values of the primary attributes are usually stored, while values of the derived attributes are usually computed when needed. Values of the primary attributes are either directly measured or assigned, while values of the derived attributes are computed from the values of other primary or composite attributes.

Mail unit attributes are always referred to by name. Since all mail unit attributes can be represented by a data value, a pair (mail unit attribute name, mail unit attribute value) contains all application-required information for a given attribute. For brevity, the pair (mail unit attribute name, mail unit attribute value) is frequently referred to as the *name-value pair*.

The definition of the mail unit attribute is not constructive in the sense that it does not allow for a constructive test that would determine whether a given object related to the mail unit is in fact the mail unit attribute. Mail unit attributes are empirically selected, listed, classified and explained in more detail in UPU M33 standard. The list of mail unit attributes is a living list and is open to additions, changes and deletions as experience in using the concept mail unit attribute evolves.

All mail unit attributes have initial or “null” value. Value of a mail unit attribute is set to “null” value when there is no available information as to the actual value of the attribute.

Different types of mail units have different attributes, although some attributes characterise mail units of all types. For example, mail items such as letters could have ink colour used to create a destination address and envelope substrate colour as their single valued attributes, while compound mail units such as pallets may not. On the other hand all mail units have a weight as their attribute.

The value of a mail unit attribute is a function of time. However, the time itself is not an attribute of mail unit, but rather a parameter on which some mail unit attributes are dependent. In this document time is expressed as a date in accordance with a commonly accepted practice in international standards, namely in the following format yyyy-mm-dd-T:HH:minmin:ssZ, where “yyyy” is the year, “mm” is the month, “dd” is the day, “HH” is the hour, “minmin” is the minute, “ss” is the second etc.

The mail unit attributes could come from a variety of sources, for example: mail unit itself or a database of information related to the mail unit. Some attributes may have the same nature, but originate from different sources (e.g. the destination address information as present on the mail unit (printed) and the destination address information stored in a postal database). The trustworthiness of mail unit attribute value is a function of its source, communication channel and an ability of the party concerned with the veracity of the information to compare values of attributes obtained from multiple sources.

Mail unit attributes fall into two broad categories, attributes that are time and process dependent and all other attributes. A prime example of a time-dependent attribute is the mail unit location, which is the fundamental attribute of track and trace application.

The attributes could be inherent or assigned. An example of an inherent attribute is the attribute “type” that takes the value of “letter”, “postcard”, “tray”, “roller cage”, “sack”, “palette”, transportation unit, etc. (these values are usually codified and published in a commonly accessible code list “mail unit type code list”). Another example is the attribute “position at the time of the last observation”. It signifies when and where the mail unit was last observed.

Other examples of inherent attributes are “weight”, “dimensions” and general physical characteristics such as colour.

It should be mentioned that the actual values of weight, dimensions, and other inherent mail unit attributes are rarely known with absolute certainty and precision.

Mail units usually carry a variety of markings containing data elements required for their processing and delivery. These markings include destination and origination addresses, digital postage mark, various endorsements (e.g. “par avion”), tracking identifier, special service indicator, etc. Location, size and other characteristics (e.g. print quality defects) of markings present on mail units are examples of assigned mail units attributes as they are in essence “assigned” either by the mail creator or by the consolidator or by the postal operator during mail creation or processing.

Examples of commonly encountered mail unit attributes are:

- mailunit.acceptance-location;
- mailunit.original-delivery-address;
- mailunit.originator;
- mailunit.payer;
- mailunit.return-address.

These and many other mail unit attributes are defined in UPU M33 standard.

5.4.2 Mail receptacle attribute

The concept of mail receptacle attribute allows the expression of basic physical parameters that are common to all receptacles. These include type, weight, dimensions, nominal capacity, construction material, handling constraints and the like. Examples are:

- mailreceptacle.weight;
- mailreceptacle.dimensions;
- mailreceptacle.nominal-capacity;

- mailreceptacle.construction-material;
- mailreceptacle.handling-constraints.

5.4.3 Aggregate attribute

Similar to mail units, aggregates are fully characterised by their attributes. Most of the comments concerning the concept of mail unit attributes in 5.4.1 are also applicable aggregates. The fundamental difference between the concept of mail unit and aggregate is the fact that an aggregate cannot be constrained to form a physical unit and therefore certain attributes applicable to mail units are not applicable to aggregates. A prime example is the (single) value of the attribute mailunit.location at a given moment in time. Another example is a (triple) value of mailunit.dimensions.

Examples of commonly encountered aggregate attributes are:

- aggregate.application.name;
- aggregate.component;
- aggregate.originator;
- aggregate.accounting-method;
- aggregate.component.mailunit.ID.

These and many other aggregate attributes are defined in UPU M34 standard.

5.4.4 Aggregate catalogue

The concept of the aggregate catalogue is motivated by the need to distinguish between the names and the values of different attributes considered in entity-relationship models. When attributes of a subset of mail units included in the catalogue of a aggregate acquire values in the context of a particular application, the resulting informational object becomes a statement. For example, when the application is a submission of mail, then the corresponding informational object is the statement of mailing submission.

5.4.5 Statement of mailing submission

The statement of mailing submission is an informational object that contains all information describing physical objects (aggregate) defined as a mailing submission. The following table provides the mapping between the physical world of mail units and aggregates and the world of informational objects that represent physical world in computer data models (e.g. in entity-relationship models).

Physical world	Description (Information)
— aggregate	— catalogue of aggregate
— mailing submission	— statement of mailing submission
— induction unit	— statement of induction unit

Statements of mailing submissions must be uniquely identifiable within the context of a given application.

5.4.6 Electronically exchanged message

The concept of an electronically exchanged message is a useful generalization for a variety of computerised documents that are commonly encountered in a mail communication system. Many application requirements are relevant to all EEMs and not just specific types, such as a statement of mailing submission. For example, communication channel security requirements may be applicable to many or all EEMs.

Electronically Exchanged Messages may be sent and received through electronic communication networks, public or private, as well as through portable electronic media such as CD ROMs, magnetic diskettes, tapes and machine-readable documents. Examples of EEMs include statement of mailing submission (SMS) and in general, a statement of aggregate.

All EEMs must be uniquely identifiable within the context of a given application.

5.4.7 Observation

Observation is one of the most important informational objects defined in this document. It contains all recorded (or stored) information about a mail unit at a given date. A collection of observations provides a description of a mail unit progression through the mail communication system at discrete moments in time. The observed information is stored and/or communicated in a data structure referred to as the observation record. There could be multiple records of the same observation. The observation record does not reflect the method used to obtain information contained in the record. The notion of how observation information has been obtained is reflected in the concept of observation attribute explained below.

There are circumstances when the value of a mail unit attribute cannot be captured with complete certainty. In this case the value may be treated as a random variable with a known or unknown distribution, and parameters of this distribution such as its expected value and standard deviation can be reported instead of the absolute value of the attribute.

As all other object observation considered in this document must be uniquely identifiable within a given application.

Formal description of the observation can take a form.

$$\text{Observation [mailunit (ID)]} = \{(A1), (A2), \dots , (AN)\} / \text{Date},$$

where *mailunit (ID)* is an identifier for the mail unit that is being observed and *(A1), (A2), …, (AN)* are values of the attributes *A1, A2,…, AN* respectively taken at the moment of time defined by the date (e.g. yyyy-mm-dd-T:HH:minmin:ssZ).

5.4.8 Observation attribute

The purpose of the observation attribute is to collect important information that is not captured in the observation record. Examples of observation attributes are values describing conditions under which the observation (mail unit attribute values) was taken and identity, role and attributes of the party or agent responsible for actions taken at the date of the observation. The identity of the mail sorting machine (agent) that scanned a given mail unit identifier, as well as its scanning resolution and illuminating condition provide useful examples of observation attributes.

The date of the observation together with its identity and the identity of the mail unit being observed are the only unconditionally required attributes of the observation. This means that these three data elements must always be present in any observation.

There are multiple ways to identify the party responsible for the actions taken at the time of the observation. It may be identified through its assigned identifier, its postal address, its location expressed in terms of its geographical coordinates, or all of the above. The role of the party responsible for the action (party attribute named “role”) can be codified (see for example UPU code list 153).

5.4.9 Expectation

The purpose expectation is to allow for a formal expression of needs and desires of concerned parties regarding mail units when these mail units are not under direct control of such parties. Expectations that are created by customers and communicated to postal operators serve to specify desired services and identify discrepancies between expected and performed services.

Expectation also allows for a formal definition of (custom-tailored) non-conditional services and forms a special case of postal product definition. Conditional services are services when the type of the information that could be made available to customers is dependent on the actions taken by the postal operator or location of the mail unit. For example, if a mail unit could not be delivered due to the absence of the recipient, the information about such an event, including information describing present location of the mail unit, could be made available to the sender.

Unlike observations, expectations can be defined over a range of dates. The amount of information held in a record for an expectation defined over a date range is larger than the amount of information held in a record for an expectation defined for a date.

The expectation information is stored and/or communicated in a data structure referred to as the expectation record. There could be multiple records for the same expectation. The expectation record contains anticipated attribute values, the consistency of which, however, cannot be ascertained in the same way as consistency of attribute values in observations.

All expectations considered in this document must be uniquely identifiable within a given application.

NOTE There is no analog to observation attributes in the context of expectations because it is not reasonable to assume that customers or other parties would anticipate, know or impose conditions, parameters or identities for actual measurements of mail unit attribute values.

5.4.10 Postal product/service

The main purpose of a formal definition for a postal product is to provide a set of automatically executable instructions for mail creator and postal operator aimed at smooth delivery of postal products. How then, can a postal product/service be formally defined using a set of concepts and definitions introduced in this standard? A straightforward and somewhat naïve approach would be to look at existing services and identify and generalise their defining characteristics. For example, a period of time elapsed from the deposit/induction of the mail item to the moment of its delivery (however delivery is defined) is one of the most common parameters of the service definition. In many European countries, “first” class mail is defined by this parameter when it is equal to “D+1”, where “D” is the day of induction. In addition, the first class mail service is also defined by the rule governing exception processing, namely that the first class mail service requires return of the undeliverable mail item to the mail item originator or its authorised agent or agents. Further, other parameters such as “security” or “guarantees” can be introduced as additional features of the service. A prime example of these features is “track & trace” information that is expected to be supplied to the originator of the mail item or entity or its agent(s). Still further parameters that could be specified by the originator are mail item or entity pick-up time, processing constraints (e.g. registered mail) and the like. Yet still further parameters reflect the nature of the mail unit itself as it affects the cost and salient characteristics of its processing within the postal distribution network (e.g. size, weight, worksharing level). This suggests that a comprehensive definition of the postal product capable of accommodating a broad variety of existing and future products should be specified in terms of rules that operate on mail unit attributes (defining mail unit) and observations (defining information reflective of postal processing and their distribution and access), where mail unit attributes are understood very broadly. Finally such rules should be agreed upon between postal operators and customers in such a manner that products offered by operators and products requested by customers should match and cause no confusion on either side. Thus the definition of the postal product is an agreed-upon set of rules operating on the values of the mail unit attributes governing both actions to be taken on the mail unit and communication of observations to all authorised parties. Several important observations are as follows.

The domain for the rule defining the product in terms of attributes is a subset (possibly proper subset) of mail unit attributes and their values. The domain is specified by the rule itself.

The rules operating on the values of mail unit attributes could be expressed implicitly or explicitly. Some simple rules (and their corresponding postal products) can be expressed directly in terms of the concept of expectation defined in this standard. In the case of traditional postal products the rules are published together with their corresponding prices and referred to by conventional classification such as first class, second class or express mail service. In this case, the rules are implicitly referenced by putting endorsements on mail units (for example: first class mail) and the rules are selected and controlled by the service provider (no negotiation is involved). As an example, the first class mail service is defined as a rule operating on the values of two mail unit attributes, namely: mailunit.original-delivery-address and mailunit.class-of-service. By the default agreement, the rule is to deliver the mail unit to the location specified by the attribute mailunit.original-delivery-address within a specified time period (e.g. D+1). Another example is first class mail service with track and trace. The set of values for the mail unit attributes for the rule governing actions taken on the mail unit consist of mailunit.original-delivery-address and mailunit.class-of-service and mailunit.customer-applied-ID. The set of mail unit attributes for the communication of observations consists of all values of the attributes mailunit.location and mailunit.process. The rule is to deliver the mail unit to the location specified by the value of the attribute mailunit.original-delivery-address within a specified time period and make available to the mail unit originator, (or its agent(s) or other authorised parties) values of the mailunit.location attribute whenever and wherever possible.

A more complex example of a postal product is a product defined by the following set of requirements:

— mail item is required to be delivered on a given date (date-certain delivery);

— postal operator is required to provide mail originator with delivery confirmation in terms of an observation taken at the delivery of the mail item into recipient mailbox;

— postal operator is required to provide mail originator with address correction information in the case when the destination address as presented on the mail item contains errors;

— postal operator is required to provide mail originator with information describing print quality defects with regard to the mail item destination address and digital postage mark.

In this case the set of mail item attributes that are needed for the product description are:

— mailitem.ID;

— mailitem.delivery-date;

— mailitem.originator;

— mailitem.original-delivery-address;

— mailitem.replacement-delivery-address;

— mailitem.original-delivery-address-print-quality-defect;

— mailitem.dpm-print-quality-defect.

The observation of the last four attributes and the mailitem.ID is to be taken at the time of mail item processing (for example by a mail sorting machine) and the observation of the first two attributes is to be taken at the time of mail item delivery into a recipient mailbox.

Thus the rule defining the product is to deliver the mail item to the location defined by the value of the mailitem.original-delivery-address (if deliverable) or by the value of mailitem.replacement-delivery-address at the date defined by the value of mailitem.delivery-date and send information contained in the observations described above, including the value of mailitem.replacement-delivery-address (if it is not NULL value) to the party defined by the value of mailitem.originator.

It is conceivable that in the future, postal service providers will negotiate postal products with their customers and in this case the subset of mail unit attributes and their values and the rules might be explicitly communicated using either a mail unit itself as a carrier of information or a computer data structure referenced by a pointer on the mail unit.

The mail unit is sometimes implied (not explicitly associated) with the postal product, such as in the case of the address correction service which may not involve actually posting a mail unit into a postal distribution network. In this case the service is performed by the postal operator by correcting computerised address information provided by a would-be mailer without actual processing of the mail unit.

5.4.11 Postal product/service attribute

Postal product attribute is a useful informational object designed to capture information that is not captured in the postal product object. Postal products can also be codified. In this case, the code for the product is a postal product attribute that takes its value from a code list. Price for the postal product can also be considered as its attribute. Since the price is somewhat arbitrary and in principle can be negotiated, it makes sense to keep the price out of the product itself. It also allows for negotiations between postal operators and their customers without changing basic data structures defining products. Similarly, financial and technical details (such as refunds conditions, expiration date, allowed induction points and times etc.) of the contract between a mailer and a post can be considered as attributes of negotiated services as well as attributes of the contract. Thus, the concept of postal product attribute allows the system to separate informational needs of postal operations from informational needs of postal finance and marketing while simultaneously accommodating similar needs of mail senders.

5.4.12 Contract and contract attributes

Mailers that have reasonably large and regular mailing submissions usually enter into an agreement (contract) with a postal operator (or operators) that defines their mutual financial and service requirements and obligations. The contract specifies the minimum amount of mail to be submitted, pricing and applicable discounts, service to be provided, methods of verification, dispute resolution and similar parameters and conditions. Contracts could be highly specific for a given mailer and postal operator. For the purpose of SMS specification, the contract is understood as an informational object containing all computerised parameters and conditions of the agreement that can be referenced in the SMS. Such computerised parameters and conditions are referred to as contract attributes and may include a contract identifier, contract type, contract legal status and similar attributes.

Contracts must be uniquely identifiable within the context of a given application.

5.5 Mailer domain process

Processes in the integrated mail communication system must be linked or interfaced through appropriate exchanges of information. Thus, all processes that are referred to or considered in the present standard are viewed as computer-driven where computers collect relevant process information. Other processes, although always present in mail communication systems, do not result in computerised information that can be exchanged between parties involved and therefore are not considered here. Oval blocks in the diagrams representing processes in the three principal domains indicate points in the processes where informational objects described in this standard can be collected, formatted and communicated.

In mail communication systems, mail units are the subjects of continuous processes throughout their life-cycle (from inception to discard). The processes comprise both physical processes (e.g. mail unit reorientation as a result of facing or a mail unit transfer from one location to another) and information processes (e.g. capturing and interpretation of data present on mail unit).

From the point of view of the mail communication system reference model, processes, both physical and informational, can be represented and described as a series of events, each of which is described by a set of observations.

Mailer domain process is described here in the most generic terms and does not take into account many variations and exceptions that take place in practical, actually encountered environments. Real processes in the mailer domain are always country, application and volume dependant, and could not be described in any detailed fashion within the scope of the present standard. Some sub-processes (or activities) sketched here happen only in a large volume mailer environment and are highly automated and computer-driven, while some others are present in almost any environment, but might be performed in a totally manual manner without any equipment at all. The purpose of providing the following description is to establish terminology and the very basic common features for some very commonly encountered mailer domain processes.

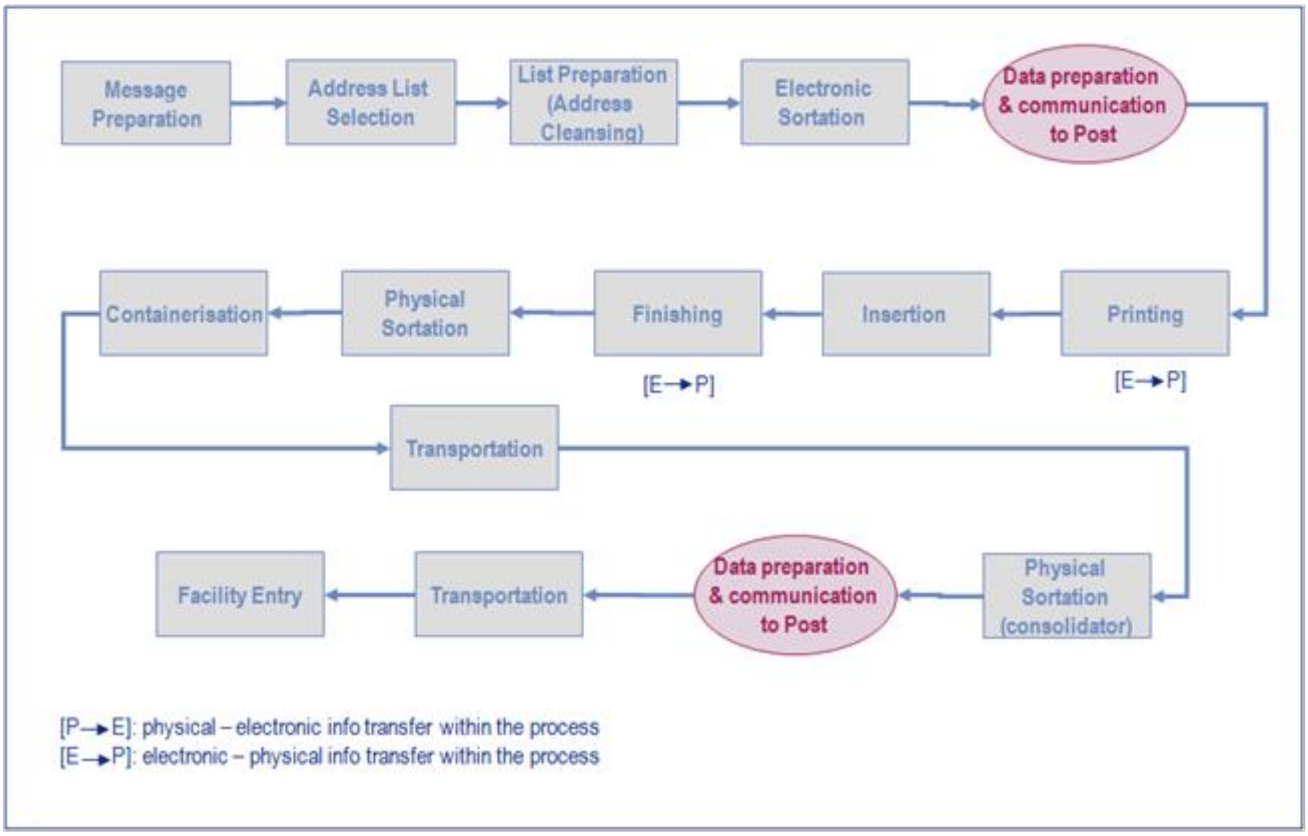

Message Preparation
Address List Selection
List Preparation (Address Cleansing)
Electronic Sortation
Data preparation & communication to Post
Printing
Insertion
Finishing
Physical Sortation
Containerisation
[E→P]
[E→P]
Transportation
Physical Sortation (consolidator)
Data preparation & communication to Post
Transportation
Facility Entry
[P→E]: physical – electronic info transfer within the process
[E→P]: electronic – physical info transfer within the process

Figure 3 – Mailer domain process

5.5.1 Message/content preparation

Message or content is information physically represented on a substrate or an object that is being sent by the mail unit originator to its recipient. Message/content is the sole reason for communication. Postal standards are typically not concerned with messages, nevertheless, message preparation is a critical part of the mail preparation process and may affect subsequent steps. Message is usually also linked and coordinated with the recipient mailing address.

5.5.2 List selection

The process of address list selection is typical for relatively large mailings. In the case of small mailings or a single mail unit the process of list selection is a simple process of recipient (destination) address selection for a given mail unit. As mentioned, the destination address has to be coordinated with the content of the mail unit.

5.5.3 List preparation

Address list preparation usually involves a process of quality control in order to avoid sending mail units that cannot be delivered or can be delivered only with additional expenses usually associated with exception processing. The process of address cleansing is executed when a party (e.g. postal operator) maintains a database of correct addresses and made available to mailers or their agents.

5.5.4 Electronic sortation

Electronic sortation is common when there is a discount offered to mailers for submitting their mailings already sorted (organised in a certain order that allows it to bypass certain processing steps that are otherwise necessary). This discount is sometimes referred to as a work-sharing discount. Electronic sortation is performed when mail units can be physically created without constraints concerning their “natural” order of creation. In some cases, mail units have to be produced in a specific sequence (e.g. according to a recipient account number or identifier) that may interfere with electronic sortation.

5.5.5 Printing

The process printing typically involves printing message(s) as well as printing the destination address. Sometimes when “window” envelopes are used, both the message and destination address are printed in one step. The printing process is typical for business-originated mail. Messages and addresses for mail units originated by individual mailers and households are sometimes handwritten, which may cause manual processing on the part of the postal operator.

5.5.6 Insertion

Insertion refers to a paper-handling mechanical process whereby mail units are assembled and inserted into a carrier envelope.

5.5.7 Finishing

Finishing typically involves printing a Digital Postage Mark (DPM) (sometimes referred to as an Indicium) and additional information such as Facing Identification Mark (FIM), mailer-selected advertising slogans etc. Finishing may require determining the mail unit rating parameters such as its weight or dimensions that are indicative of the tariff (postal rate or charge) to be paid by the payer for products/services that are expected to be rendered. The main purpose of finishing is to enable mailers to have effective access to postal products.

5.5.8 Physical sortation

The main purpose of physical sortation is to obtain a discount or better and faster service from the postal operator. Physical sortation can be performed by a mail originator or its agent (for example a consolidator or a contractor) depending on whether the mail originator has sufficient mail volume or required equipment and expertise. Physical sortation is more cumbersome and expensive than electronic sortation and is performed only when electronic sortation is not possible, for example when mail units created independently by different processes are merged or when mail units have to be prepared in certain order.

5.5.9 Containerisation

Containerisation is a necessary step since mail units could not be transported without containers. Containerisation involves the use of multiple receptacles that are country and application dependent.

5.5.10 Transportation

Transportation is a generic term. The nature and the sequence of specific activities comprising “transportation” may vary from mailer to mailer and is affected by the rules of induction that are country and postal facility dependent. Transportation usually involves loading and unloading of transportation vehicles.

5.5.11 Induction

The process of induction is common to both mailer and postal domains. The process of induction or entry occurs when an aggregate or a mail unit is presented for induction into the postal operator distribution network by the mail submitter. The process of induction includes the process of mailing submission verification (typically performed by the postal operator) that ensures that the submission complies with postal revenue protection and operational requirements. The process of induction typically applies only to controlled acceptance or controlled entry mail (CAM or CEM). The verification normally involves payment (or accounting) accuracy and mail quality check. The process of induction may result in acceptance or rejection of the mailing submission in part or as a whole. Acceptance of a mail unit or an aggregate may involve surcharges that are required to be paid by the submitter to the postal operator if the submission is found to be non-compliant with postal requirements.

5.6 Interfaces

Interfaces between mailer, recipient and postal domains are shown in Figure 1. All interfaces can be divided into two broad categories, namely interfaces that are enabled by physical mail units and electronic interfaces that are usually enabled by connecting computers in the mailer, recipient and postal domains through a private or public communication network (such as the internet).

Interfaces that make use of physical mail units are represented by the information printed or written directly on these mail units or attached to them via labels that are in turn either imprinted (machine printed) or inscribed with information (hand written). It is also possible to use specially designed electronic devices such as RF tags to exchange information between domains via mail units. In all cases, it is convenient to refer to the interface that is enabled by the mail units themselves as “material interface channel” or simply “material channel”.

Cost effective representation of information using mail units requires that information density should be sufficient to encode all application-required information for all classes of mail units, all business applications and all postal products. This should be accomplished for a broad variety of printing substrates. Effective automated capture of the information off mail units implies reliable scanning and interpretation of data present on said mail units.

It should be noted that electronic interfaces between domains could be implemented not only via electronic public communication networks such as the internet but also through portable electronic media such as magnetic disks, CD/DVD memories, flash memory etc. Electronic interfaces can be passive or active. A passive interface can be exemplified by a service provider (e.g. a postal operator) that allows access to information via a web service using browser software. An active interface can be exemplified by the direct transfer of information between domains using for example e-mail or FTP protocol when information is delivered to an explicitly identified recipient’s computer. The electronic interface channel is becoming an increasingly important aspect of the mail communication system by enabling true integration of the entire mail communication network.

Specific protocols, message content and structure are outside of the scope of a current standard. They are addressed in UPU and CEN standards dedicated to specific important applications (e.g. statement of mailing submission) and listed in the bibliography. This standard defines only a generic term of electronically exchanged message in order to address issues related to all such messages, for example security services (authentication, data integrity, privacy and no-repudiation).

NOTE 1 Although hand written information (such as address data) is frequently encountered in mail communication and can also be considered as a part of material interface it is typically not suitable for the effective exchange of information between domains and therefore excluded from the definition above.

NOTE 2 Electronic interface between domains can also be implemented via portable electronic media such as magnetic disks, CD/DVD memories, flash memory etc., however, these interfaces are less effective and are becoming increasingly unpopular.

6 Statement of mailing submission (SMS)

This clause describes the content of the SMS organised as a communication message, its format and communication protocol recommended for the transfer of SMS message from mailers to postal operators. It also provides a very brief description of recommended communication channel security requirements and gives basic references. The communication channel security is not specific to mail communication applications and is treated here, mainly as a necessary reminder to the reader, that all data exchanges through a public communication network have to be treated with appropriate caution.

Whenever the term “mailer” is used below without further clarification, it is meant to indicate any of the suitable parties in the sender/mailer domain that are defined in the present specification.

6.1 SMS structure

The information contained in the SMS document is divided into six sections: header, submission, parties, handover, mail units and aggregates.

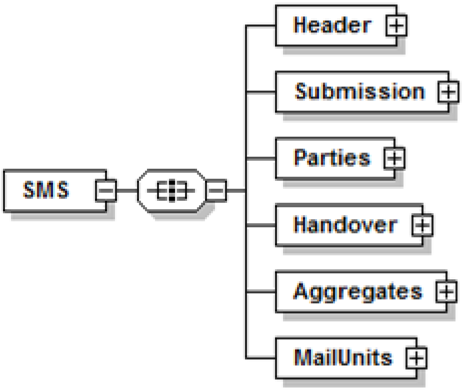


Figure 4 – The top level elements of the SMS structure

The header section contains information about the electronic message. This section is intended to be used by IT-personnel on both sides of the communication channel (Postal Operator and Customer) to help identify and solve message communications problems. This section contains information about the SMS-message itself and does not contain any information about the submission. As such, it does not contain any information relevant to Operations, Marketing or Finance (unless the timely and accurate transmission of an electronic SMS is part of the pricing process).

The submission section contains information needed to identify this mailing submission and its relation to other mailing submissions, when applicable.

The parties section contains information about the different parties involved in the submission process. The most important parties are the originator of the mail items, the submitter and the payer. A generic construction for adding other roles is also included.

The handover section contains information regarding the timing and location of the induction process. The section is relevant for Operations (i.e. transport if the induction is at a client’s site). It is less important for Finance and Marketing (unless the location or time of induction is part of the pricing process).

The aggregates section contains information about aggregates (see 0 mail aggregate), and the attributes that are common within each set, including postal services requested by the customer. When available, this section contains information describing relationships between aggregates and mail units, for example which aggregates are contained in given mail unit(s) and also which mail units are contained in a specified set.

All mail items that have identical values for at least some of their attributes are clustered together and the value of the respective attributes is specified only once. In this sense, the resulting clusters are aggregates since they are collections of mail units forming logical units.

The data elements and their structure support the efficient transfer of information when a large number of mail units are very similar, with only a few exceptions. In this case, the common attribute section of the aggregate indicates the default values for the entire set and the exceptions are listed in the mail items section (which can be thought of as the “itemized section”, while the aggregates section can be thought of as carrying the “default values” for the set).

The mail units section contains information about the structure of the mail units and their distribution inside receptacles (pallets, trays etc.). The section describes the hierarchy of mail units (which mail units are contained within other mail units). When available, this section contains information describing which mail unit belongs to a given set. Mail units are listed starting from the outermost mail units up to any level of detail agreed between the customer and the postal operator. The section provides support for optimizing transportation. The analysis of transportation needs is performed at the level of the largest mail units contained in the mailing submission.

6.2 Message Content

The SMS message has a tree structure and is organised hierarchically into six sections, several layers deep. In the SMS message, each section is represented by an XML element. The attributes of objects included in the SMS are always the leaves (terminal nodes of the tree structure). This organisation improves the readability of the document and clarifies the meaning of each attribute.

The remainder of this section provides a detailed description of the content of the statement of mailing submission (SMS).

6.2.1 SMS.Header

This subclause contains a description of an “electronic envelope” for the SMS. It is intended to be used by IT departments in Postal/Carrier and Sender/Mailer domains to organize effective exchanges of SMS messages. This section also contains information about the SMS-message itself, but does not contain any information specific to the mailing submission as a postal application. As such, it does not contain any information relevant to Operations, Marketing or Finance (unless the timing of the messages is significant from financial point of view).

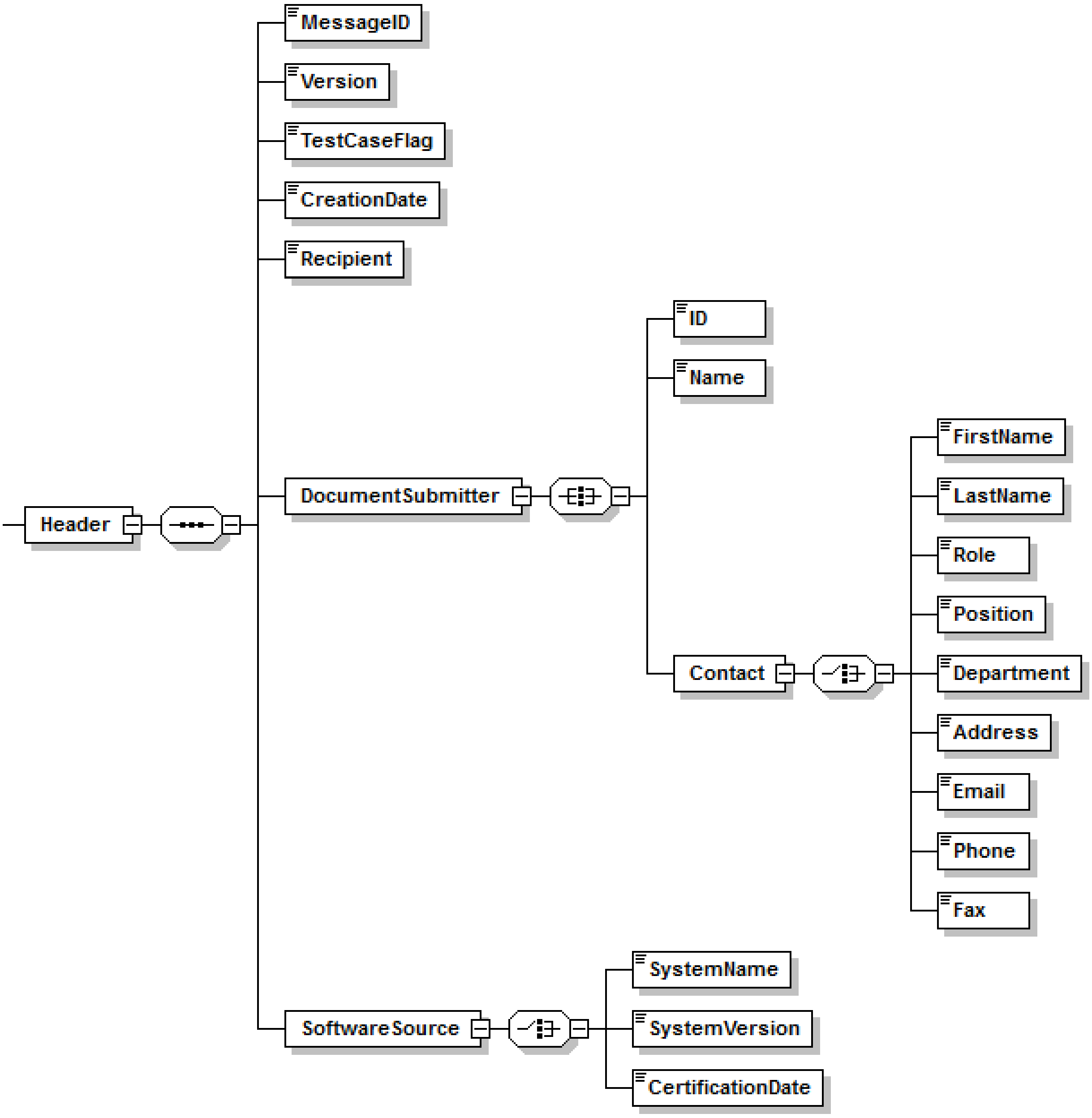


Figure 5 – The structure of SMS.Header element

6.2.1.1 SMS.Header.MessageID

The value of this attribute is a unique identifier for the SMS document.

6.2.1.2 SMS.Header.Version

The value of this attribute is the version of the SMS-format used to generate this message.

NOTE As the use of SMS by the postal operators evolves, different versions of SMS might be in use concurrently. The value of this attribute indicates the version of the schema used by the current SMS.

6.2.1.3 SMS.Header.TestCaseFlag

The value of this attribute is a flag that indicates whether the SMS is sent for testing purposes or as a real SMS for the production system.

NOTE The communication of the SMS requires implementing the SMS generation process within the mailer/sender’s software. It may be useful to exchange some test data before exchanging production SMS. This flag distinguishes between testing and production data.

6.2.1.4 SMS.Header.CreationDate

The value of this attribute is the creation date of the SMS document.

6.2.1.5 SMS.Header.Recipient

The value of this attribute is the name of the postal operator which is the intended recipient for the SMS.

6.2.1.6 SMS.Header.DocumentSubmitter

The value of this attribute is the party responsible for creating and communicating the SMS document to the postal operator.

NOTE This attribute is a part of the header section. It is not included in 6.2.3 to emphasize the distinction between the content of the header which only relates to the technical aspects of communicating the SMS message.

6.2.1.6.1 SMS.Header.DocumentSubmitter.ID

The value of this attribute is the unique customer identifier assigned by the postal administration to the document submitter.

6.2.1.6.2 SMS.Header.DocumentSubmitter.Name

The value of this attribute is the name of the document submitter.

6.2.1.6.3 SMS.Header.DocumentSubmitter.Contact

The following attributes define the contact within the submitter’s organisation.

Table 1

SMS.Header.DocumentSubmitter.Contact.FirstName	First Name of the contact person
SMS.Header.DocumentSubmitter.Contact.LastName	Last Name of the contact person
SMS.Header.DocumentSubmitter.Contact.Role	Role of the contact person within the submitter's organisation
SMS.Header.DocumentSubmitter.Contact.Position	Position of the contact person within the submitter's organisation
SMS.Header.DocumentSubmitter.Contact.Department	Department, the contact person works in
SMS.Header.DocumentSubmitter.Contact.Address	Address of the contact person
SMS.Header.DocumentSubmitter.Contact.Email	Email-Address of the contact person
SMS.Header.DocumentSubmitter.Contact.Phone	Phone number of the contact person
SMS.Header.DocumentSubmitter.Contact.Fax	Fax number of the contact person

NOTE The contact information is a direct attribute of all parties and it has the same content as shown in 6.2.1.6.3.

6.2.1.7 SMS.Header.SoftwareSource

The value of this attribute identifies the software used for generating the SMS.

6.2.1.7.1 SMS.Header.SoftwareSource.SystemName

Name of the software/system generating the SMS.

6.2.1.7.2 SMS.Header.SoftwareSource.SystemVersion

Version of the software/system generating the SMS.

6.2.1.7.3 SMS.Header.SoftwareSource.CertificationDate

Date when the software/system was certified by the Postal Operator.

6.2.2 SMS.Submission

This subclause contains information that uniquely identifies a particular mailing submission and its relations to other mailing submissions, when applicable.

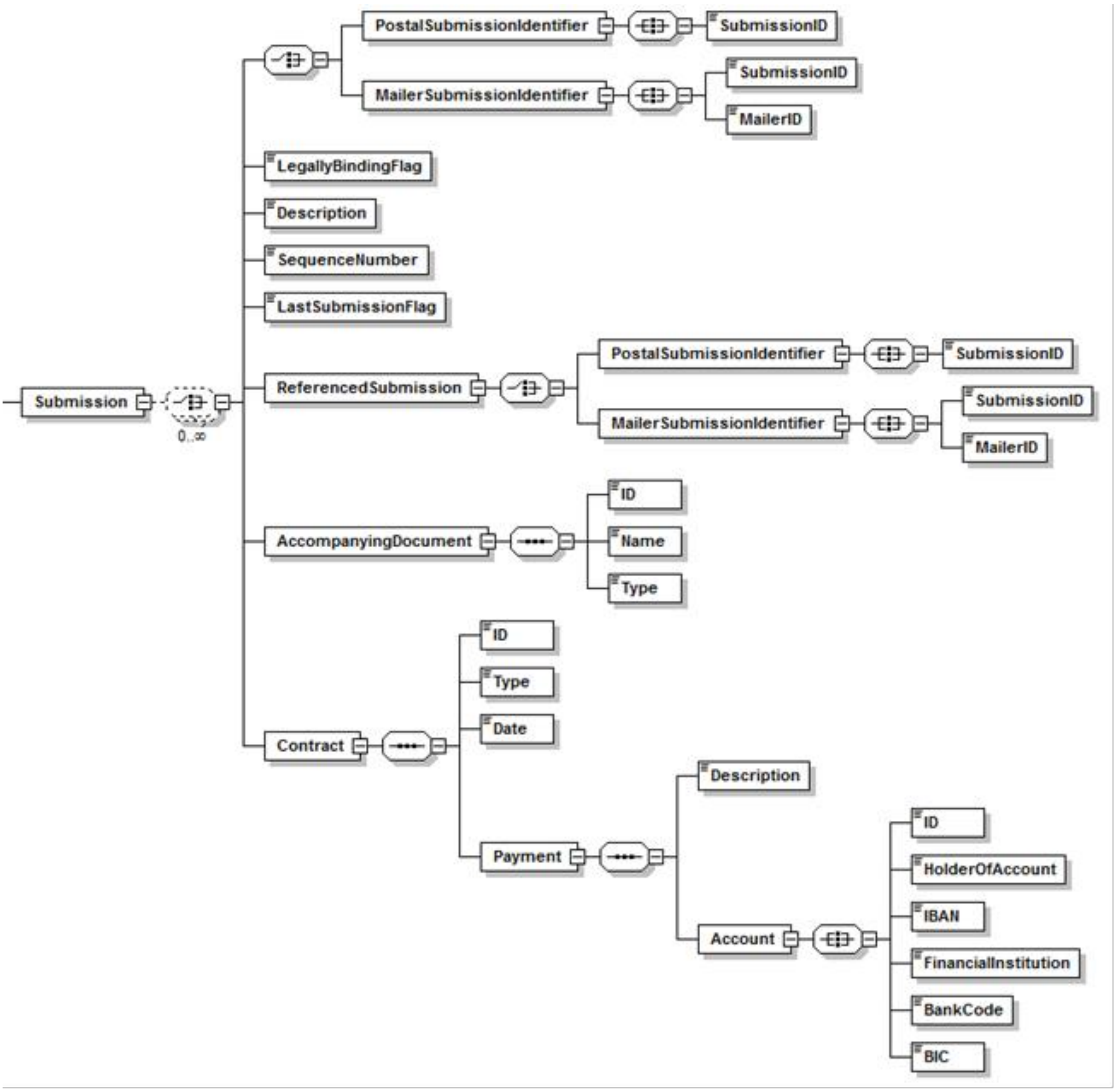


Figure 6 – The structure of SMS.Submission element

6.2.2.1 SMS.Submission.PostalSubmissionIdentifier

This element contains the mailing submission identifier assigned by the postal operator.

NOTE A mailing submission can be uniquely identified either by using an identifier generated by the postal operator or by the mailer or its authorized agent. In the former case, only one identifier is necessary and the postal operator is responsible for providing this unique identifier for use by the mailer. In the later case, each mailer is responsible for providing a unique submission identifier and then, when combined with the postal operator, assigned a unique mailer identifier which results in a unique identifier for submission. For this reason the SMS.Submission.PostalSubmissionIdentifier element contains only one attribute below it. This element is structured in this fashion only to maintain consistency with the structure of 6.2.2.2 (mailer-generated identifier for the submission).

6.2.2.1.1 SMS.Submission.PostalSubmissionIdentifier.SubmissionID

The value of this attribute is the actual submission identifier assigned by the postal operator (see NOTE above).

6.2.2.2 SMS.Submission.MailerSubmissionIdentifier

This element contains the mailing submission identifier assigned by the mailer.

6.2.2.2.1 SMS.Submission.MailerSubmissionIdentifier.SubmissionID

The value of this attribute is the actual submission identifier assigned by the mailer.

6.2.2.2.2 SMS.Submission.MailerSubmissionIdentifier.MailerID

The value of this attribute is the mailer identifier assigned by the postal operator.

6.2.2.3 SMS.Submission.LegallyBindingFlag

The value of this attribute is a flag which indicates the legal status of the SMS message.

NOTE This attribute indicates whether the SMS is a legally binding document. The default value for this flag is set to true (meaning that the SMS is legally binding, that is requiring meeting contractual obligations for both parties).

6.2.2.4 SMS.Submission.Description

The value of this attribute is a free-text attribute that can be used by the mailer to give a textual description of the submission, for example for a purpose internal to the mailer. This attribute consist of multiple informational elements serving different purposes.

6.2.2.5 SMS.Submission.SequenceNumber

The value of this attribute represents the serial number of the current mailing submission.

NOTE It is assumed that all mailing submissions are numbered in sequential order. If a mailing consists of multiple submissions, this attribute gives the sequential number of the present submission. It is convenient when there is a need to establish an ordered relationship between submissions (precedes or follows).

6.2.2.6 SMS.Submission.LastSubmissionFlag

The value of this attribute is a flag which, when set to “true”, indicates that this submission is the last of a given set of mailing submissions.

NOTE This attribute can be used to trigger a process that verifies fulfilment of contractual obligations on the part of the mailer. If a mailing consists of multiple submissions, this attribute indicates whether the present submission is the last submission within the mailing.

6.2.2.7 SMS.Submission.ReferencedSubmission

This is an element containing attributes that identify another submission which is part of the same mailing. This element contains two identifiers, structure of which is identical to the one described in 6.2.2.1 and 6.2.2.2.

6.2.2.7.1 SMS.Submission.ReferencedSubmission.PostalSubmissionIdentifier

The value of this attribute is the mailing submission identifier assigned by the postal operator to the referenced submission.

NOTE This element is structured in this fashion only to maintain consistency with the structure of 6.2.2.7.2 (mailer-generated identifier for the submission).

Table 2

SMS.Submission.ReferencedSubmission.PostalSubmissionIdentifier.SubmissionID	identifier assigned by the postal administrator to a submission referred to by this document

6.2.2.7.2 SMS.Submission.ReferencedSubmission.MailerSubmissionIdentifier

This element contains the mailing submission identifier assigned by the mailer to the referenced submission.

Table 3

SMS.Submission.ReferencedSubmission.MailerSubmissionIdentifier.SubmissionID	identifier assigned by the mailer to a submission referred to by this document
SMS.Submission.ReferencedSubmission.MailerSubmissionIdentifier.MailerID	mailer identifier assigned by the postal operator.

6.2.2.8 SMS.Submission.AccompanyingDocument

This element contains attributes that reference a physical document that accompanies this submission.

NOTE Having physical documents accompanying a mailing submission is not a requirement. This element provides a linkage to a physical document if needed.

6.2.2.8.1 SMS.Submission.AccompanyingDocument.ID

The value of this attribute is an identifier for the physical document accompanying the mailing submission.

6.2.2.8.2 SMS.Submission.AccompanyingDocument.Name

The value of this attribute is the name of the physical document accompanying the mailing submission.

6.2.2.8.3 SMS.Submission.AccompanyingDocument.Type

The value of this attribute defines the type of the physical document accompanying the mailing submission.

NOTE The document type reflects the nature of the document which simplifies non-computerised processing of the information. This could be “contract”, “list”, “manifest”, etc.

6.2.2.9 SMS.Submission.Contract

This element contains information identifying the negotiated agreement between the payer and the postal operator.

NOTE The implementation of SMS may have the contract information as a part of 6.2.3 under the Parties.Payer element, instead of being a part of 6.2.2.

6.2.2.9.1 SMS.Submission.Contract.ID

This is an attribute that identifies the contract which governs relationships between mailer and postal operator concerning the given submission.

6.2.2.9.2 SMS.Submission.Contract.Type

The value of this attribute is the type of the contract.

NOTE This attribute allows to classify contracts into different types for the convenience of the postal operator.

6.2.2.9.3 SMS.Submission.Contract.Date

The value of this attribute is the date of the contract.

6.2.2.9.4 SMS.Submission.Contract.Payment

This element contains attributes necessary and sufficient to transact the payment according to the terms of the contract.

Table 4

SMS.Submission.Contract.Payment.Account	This element contains a group of attributes describe the account used for payment
SMS.Submission.Contract.Payment.Account.ID	The value of this attribute is an identifier of the bank account used for settlement
SMS.Submission. Contract.Payment.Account.AccountHolder	The value of this attribute is the name of the holder of the account
SMS.Submission.Contract.Payment.Account.IBAN	The value of this attribute is the IBAN-Number of the account
SMS.Submission. Contract.Payment.Account.FinancialInstitution	The value of this attribute is the name of the bank where the payer holds the account
SMS.Submission. Contract.Payment.Account.BankCode	The value of this attribute is the code of the bank where the payer holds the account
SMS.Submission.Contract.Payment.Account.BIC	The value of this attribute is the BIC-Code of the payer's account

NOTE This element contains information concerning data elements necessary to transact payment within the framework of certain banking systems. It is not meant to exclude other possible payment arrangements that may exist in different countries and economic systems.

6.2.3 SMS.Parties

This subclause contains information about the different parties involved in the submission process. The most important parties are the originator of the mail units, the submitter and the payer. A generic construction for adding other roles is also included.

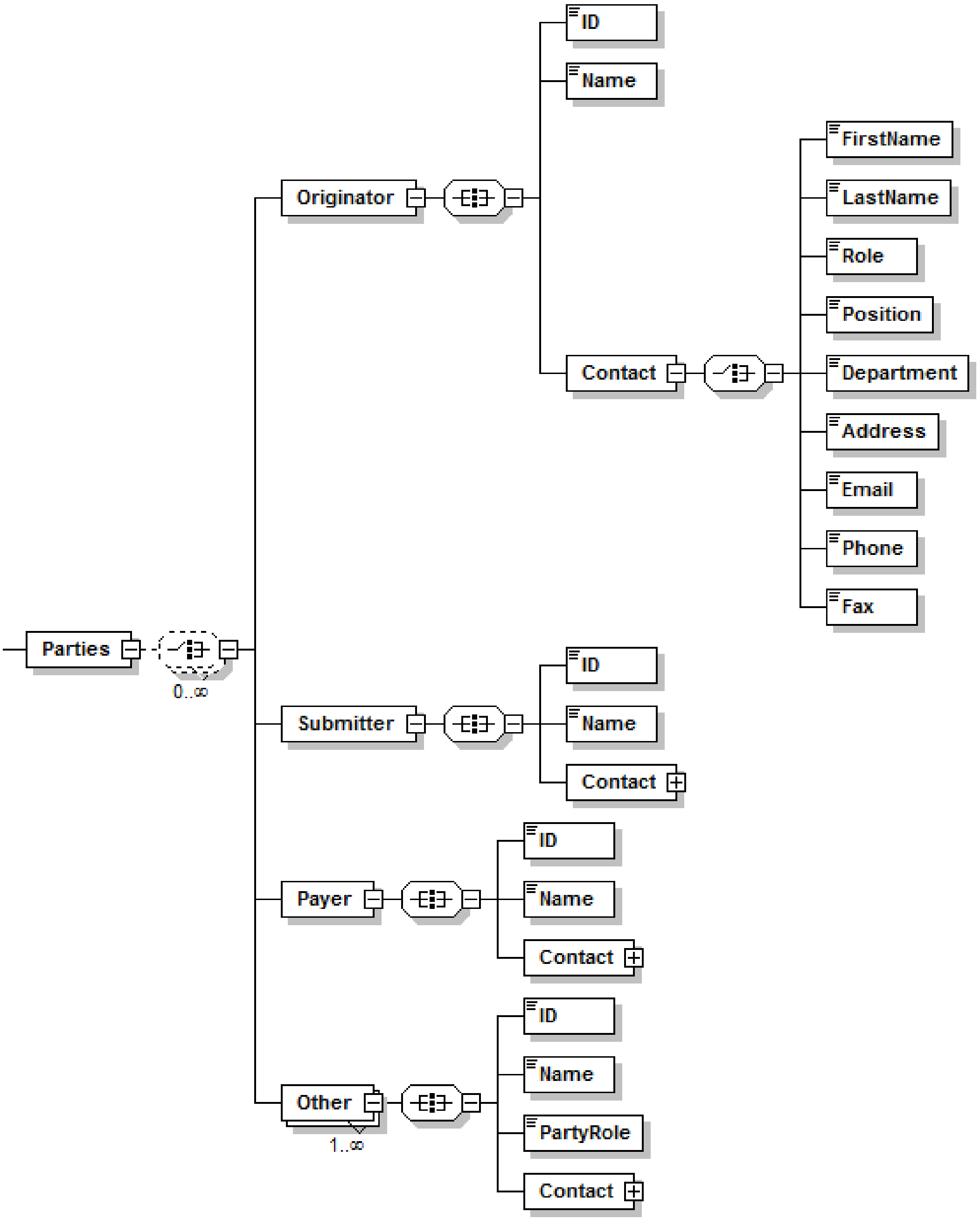


Figure 7 – The structure of SMS.Parties element

6.2.3.1 SMS.Parties.Originator

This element contains information about the originator of the mailing submission.

6.2.3.1.1 SMS.Parties.Originator.ID

The value of this attribute is the unique ID for the mailer.

6.2.3.1.2 SMS.Parties.Originator.Name

The value of this attribute is the name of the mailer.

6.2.3.1.3 SMS.Parties.Originator.Contact

The following attributes define a designated contact within the mailing submission originator organisation.

Table 5

SMS.Parties.Originator.Contact.FirstName	First Name of the contact person
SMS.Parties.Originator.Contact.LastName	Last Name of the contact person
SMS.Parties.Originator.Contact.Role	Role of the contact person within the originator's organisation
SMS.Parties.Originator.Contact.Position	Position of the contact person within the originator's organisation
SMS.Parties.Originator.Contact.Department	Department, the contact person works in
SMS.Parties.Originator.Contact.Address	Address of the contact person
SMS.Parties.Originator.Contact.Email	Email-Address of the contact person
SMS.Parties.Originator.Contact.Phone	Phone number of the contact person
SMS.Parties.Originator.Contact.Fax	Fax number of the contact person

6.2.3.2 SMS.Parties.Submitter

This is an element that defines the submitter of the given mailing submission.

6.2.3.2.1 SMS.Parties.Submitter.ID

The value of this attribute is the unique ID for the submitter of the mailing submission.

6.2.3.2.2 SMS.Parties.Submitter.Name

The value of this attribute is the name of the submitter.

6.2.3.2.3 SMS.Parties.Submitter.Contact

The following attributes define the contact within the customer's organisation having the role of submitter.

Table 6

SMS.Parties.Submitter.Contact.FirstName	First Name of the contact person
SMS.Parties.Submitter.Contact.LastName	Last Name of the contact person
SMS.Parties.Submitter.Contact.Role	Role of the contact person within the submitter's organisation
SMS.Parties.Submitter.Contact.Position	Position of the contact person within the submitter's organisation
SMS.Parties.Submitter.Contact.Department	Department, the contact person works in
SMS.Parties.Submitter.Contact.Address	Address of the contact person
SMS.Parties.Submitter.Contact.Email	Email-Address of the contact person
SMS.Parties.Submitter.Contact.Phone	Phone number of the contact person
SMS.Parties.Submitter.Contact.Fax	Fax number of the contact person

6.2.3.3 SMS.Parties.Payer

This element identifies the payer for the given mailing submission.

NOTE The implementation of SMS may have the contract information as a part of 6.2.3 under the Parties.Payer element, instead of being a part of 6.2.2.

6.2.3.3.1 SMS.Parties.Payer.ID

The value of this attribute is the unique ID for the payer.

6.2.3.3.2 SMS.Parties.Payer.Name

The value of this attribute is the name of the payer.

6.2.3.3.3 SMS.Parties.Payer.Contact

This element contains the following attributes defining the contact within the payer's organisation.

Table 7

SMS.Parties.Payer.Contact.FirstName	First Name of the contact person
SMS.Parties.Payer.Contact.LastName	Last Name of the contact person
SMS.Parties.Payer.Contact.PartyRole	Role of the contact person within the payer's organisation
SMS.Parties.Payer.Contact.Position	Position of the contact person within the payer's organisation
SMS.Parties.Payer.Contact.Department	Department, the contact person works in
SMS.Parties.Payer.Contact.Address	Address of the contact person
SMS.Parties.Payer.Contact.Email	Email-Address of the contact person
SMS.Parties.Payer.Contact.Phone	Phone number of the contact person
SMS.Parties.Payer.Contact.Fax	Fax number of the contact person

6.2.3.4 SMS.Parties.Other

This is a element that contains information about any additional party involved with the mailing submission.

NOTE 1 In some instances, major parties (originator, payer, and submitter) may not be the only parties involved with mailing submission. This element provides a mechanism to incorporate information about other parties into the SMS. Important examples of other parties are creator and consolidator.

NOTE 2 This element allows for multiple instances (when more than one other party needs to be included).

6.2.3.4.1 SMS.Parties.Other.ID

The value of this attribute is the unique ID for the other party.

6.2.3.4.2 SMS.Parties.Other.Name

The value of this attribute is the name of the other party.

6.2.3.4.3 SMS.Parties.Other.Role

The value of this attribute defines the role of the other party.

NOTE This role can be, for example mailing list broker.

6.2.3.4.4 SMS.Parties.Other.Contact

This element contains the following attributes defining the contact within the other party’s organisation.

Table 8

SMS.Parties.Other.Contact.FirstName	First Name of the contact person
SMS.Parties.Other.Contact.LastName	Last Name of the contact person
SMS.Parties.Other.Contact.Role	Role of the contact person within the other party's organisation
SMS.Parties.Other.Contact.Position	Position of the contact person within the other party's organisation
SMS.Parties.Other.Contact.Department	Department, the contact person works in
SMS.Parties.Other.Contact.Address	Address of the contact person
SMS.Parties.Other.Contact.Email	Email-Address of the contact person
SMS.Parties.Other.Contact.Phone	Phone number of the contact person
SMS.Parties.Other.Contact.Fax	Fax number of the contact person

6.2.4 SMS.Handover

The handover section contains information regarding the timing and location of the induction process. This information is most relevant for postal operations.

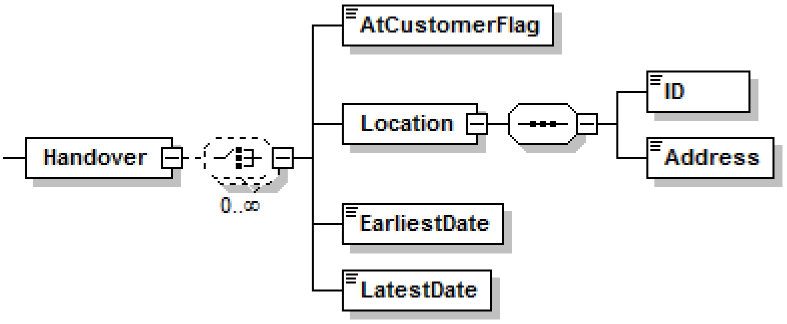


Figure 8 – The structure of SMS.Handover element

6.2.4.1 SMS.Handover.AtCustomerFlag

This attribute is a flag which, when set to “true”, indicates that the handover takes place at the submitter site. The default value of this flag is set to “false” and it indicates that the handover takes place at a postal facility.

6.2.4.2 SMS.Handover.Location

This element contains information about the location of the handover.

6.2.4.2.1 SMS.Handover.Location.ID

The value of this attribute is an identifier of the location of handover as assigned by the postal operator.

6.2.4.2.2 SMS.Handover.Location.Address

The value of this attribute is the location of handover expressed as a postal address.

NOTE The format used to express postal addresses is defined in other applicable standards (see EN 14142-1)

6.2.4.3 SMS.Handover.EarliestDate

The value of this attribute is the earliest date of handover.

6.2.4.4 SMS.Handover.LatestDate

The value of this attribute is the latest date of handover.

NOTE If the value of this attribute does not represent a valid date (e.g. expressed as a NULL value) then the earliest date of handover is the actual date of handover.

6.2.5 SMS.Aggregates

The element contains information about aggregates (defined in 0 mail aggregate), including the common attributes of mail units included in each set.

The purpose of this element is to communicate information about:

- Aggregates which contain mail items which are not individually identified and have common attributes (for example: size, destination, weight, postage amount). In some case, the count of mail items for the set may be sufficient.

- Aggregates which contain mail items which are individually identified and have common attributes (default attribute values). Specifying the common attributes for the majority of the mail items in the set leads to better use of resources (storage, communication and computation). Mail item attributes that are different from the defaults are expected to be listed individually under the MailUnits element (6.2.6).

- Aggregates containing mail items which have identifiers in defined ranges. Specifying mail unit ID ranges is a practical alternative to individually listing each mail unit.

The information in this element is organized as a hierarchy. At the top level is the element "Aggregates" which represents the section itself. At the next level below it are one or more sets as shown in Figure 9.

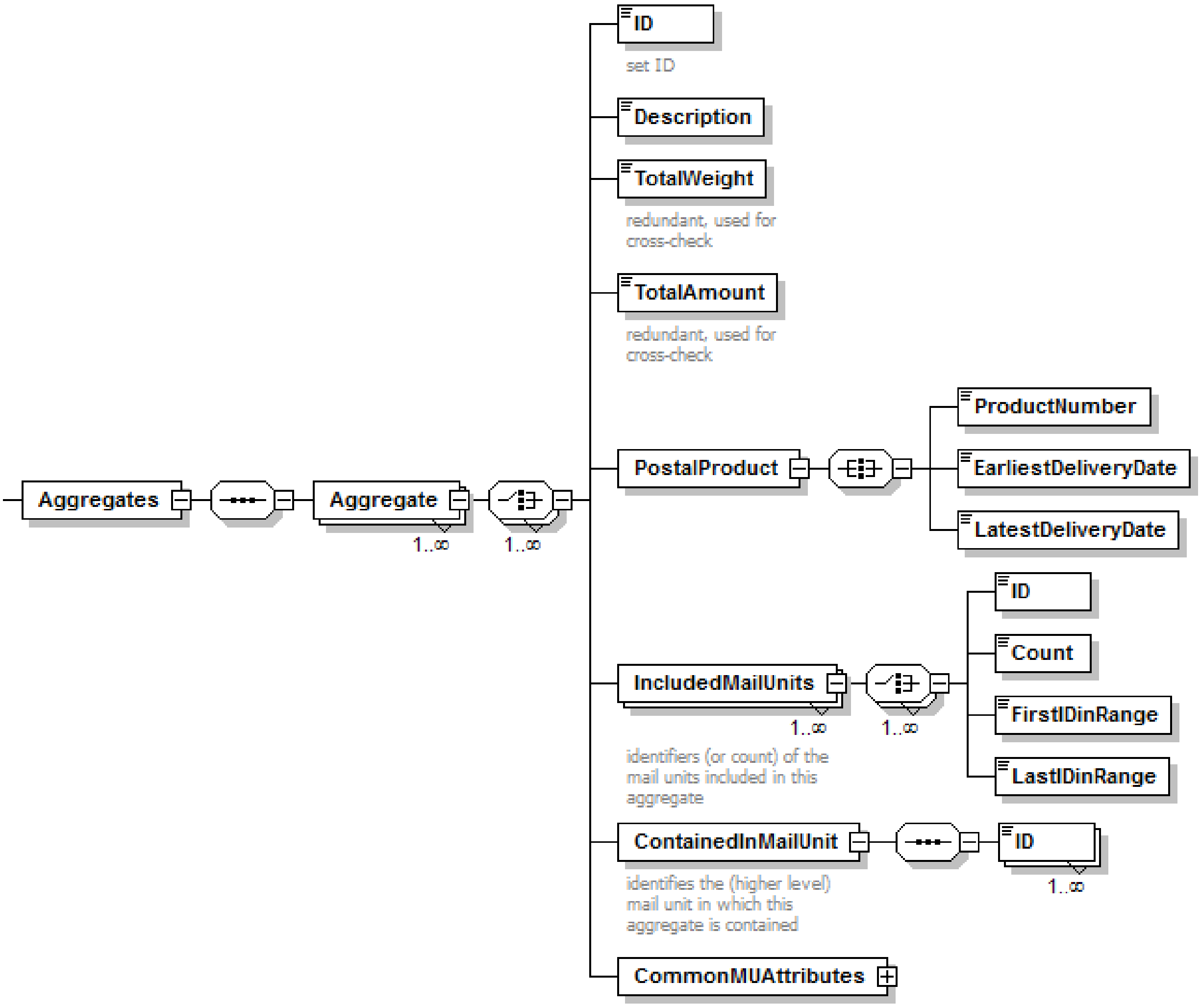


Figure 9 – The structure of SMS.Aggregates element

6.2.5.1 SMS.Aggregates.Aggregate

This element contains information describing one set. The lower level element "CommonAttributes" identifies the mail unit's attributes that are common to all mail units in this particular set.

6.2.5.1.1 SMS.Aggregates.Aggregate.ID

The value of this attribute is the set identifier assigned by its creator.

6.2.5.1.2 SMS.Aggregates.Aggregate.Description

The value of this attribute is text describing the aggregate.

6.2.5.1.3 SMS.Aggregates.Aggregate.TotalWeight

The value of this attribute is the total weight of all the mail units included in the set.

6.2.5.1.4 SMS.Aggregates.Aggregate.TotalAmount

The value of this attribute is the total price paid by the mailer for all the mail units included in the set.

6.2.5.1.5 SMS.Aggregates.Aggregate.PostalProduct

This element contains postal product information common to all mail items in the set, as described in the table below. The values contained in this element are the PostalProduct default values for all items in the set. Individual mail units that use other postal services may be listed under the SMS.MailUnits (6.2.6) element.

Table 9

SMS.MailUnits.Mailunit.PostalProduct.ProductNumber	The value of this attribute is an identifier of a postal product taken from a code list
SMS.MailUnits.Mailunit.PostalProduct.EarliestDeliveryDate	The value of this attribute is the earliest date, the mail item should be delivered to the addressee
SMS.MailUnits.Mailunit.PostalProduct.LatestDeliveryDate	The value of this attribute is the latest date, the mail item should be delivered to the addressee

NOTE The XML schema in Figure 9 implies that all mail units included in the given mail set wiil be associated with the same postal product. In case when this constraint is not necessary, the postal product attribute can be left empty, allowing for flexibility of constructing mail sets comprised of mail units associated with different postal products.

6.2.5.1.6 SMS.Aggregates.Aggregate.IncludedMailUnits

This element contains information about the mail units included in the set, as described in the following table.

Table 10

SMS.MailUnits.Mailunit.IncludedAggregate.ID	The value of this attribute is a list of IDs of mail units included in the set
SMS.MailUnits.Mailunit.IncludedAggregate.Count	The value of this attribute specifies the number of mail units in the set
SMS.MailUnits.Mailunit.IncludedAggregate.FirstIDinRange	The value of this attribute specifies the value of the first mail unit ID in the set, when the IDs are specified as a range of sequential numbers
SMS.MailUnits.Mailunit.IncludedAggregate.LastIDinRange	The value of this attribute specifies the value of the last mail unit ID in the set, when the IDs are specified as a range of sequential numbers

6.2.5.1.7 SMS.Aggregates.Aggregate.ContainedInMailUnit

This element contains information about the mail unit which contains the set.

Table 11

SMS.MailUnits.Mailunit.IncludedAggregate.ID	The value of this attribute identifies the mail unit which completely contains the aggregate, when applicable

6.2.5.1.8 SMS.Aggregates.Aggregate.CommonMUAttributes

This element contains the attributes that are common to all mail units in the set. These values are thought of as “defaults” and are superseded by the values of attributes of mail units listed individually under the SMS.MailUnits element (6.2.6), when applicable. The attributes in this section are the same as the attributes described above in the SMS.MailUnits.Mailunit.Attributes section (6.2.6.1.1). There are two attributes that are not on the list of CommonMUAttributes: the mail unit ID and OuterMailUnitFlag (the ID cannot be common to an aggregate and the OuterMailUnitFlag must be always false for all mail units in an aggregate).

NOTE 1 More than one action and observation may apply to each mail unit (for example: first class, insured, tracking). In this case, the combination of actions to be taken is identified by a unique product identifier from a code list.

NOTE 2 Aggregate earliest and latest delivery date must be consistent with the timing aspects of the product referenced by the product code.

6.2.6 SMS.MailUnits

This element of SMS contains information about individual mail units, their attributes and their physical hierarchy (i.e. how mail units are aggregated together into larger mail units). From the information describing the physical hierarchy it is possible to derive information describing the assignment of mail units to receptacles (pallets, trays etc.) in the mailing submission. The MailUnits element includes the information necessary and sufficient to identify the outermost mail units to facilitate the process of mail acceptance and resource planning, including optimization of transportation. Information about outermost mail units is grouped in the element OuterMailUnits. Lastly, this element contains information regarding mapping of aggregates to mail units.

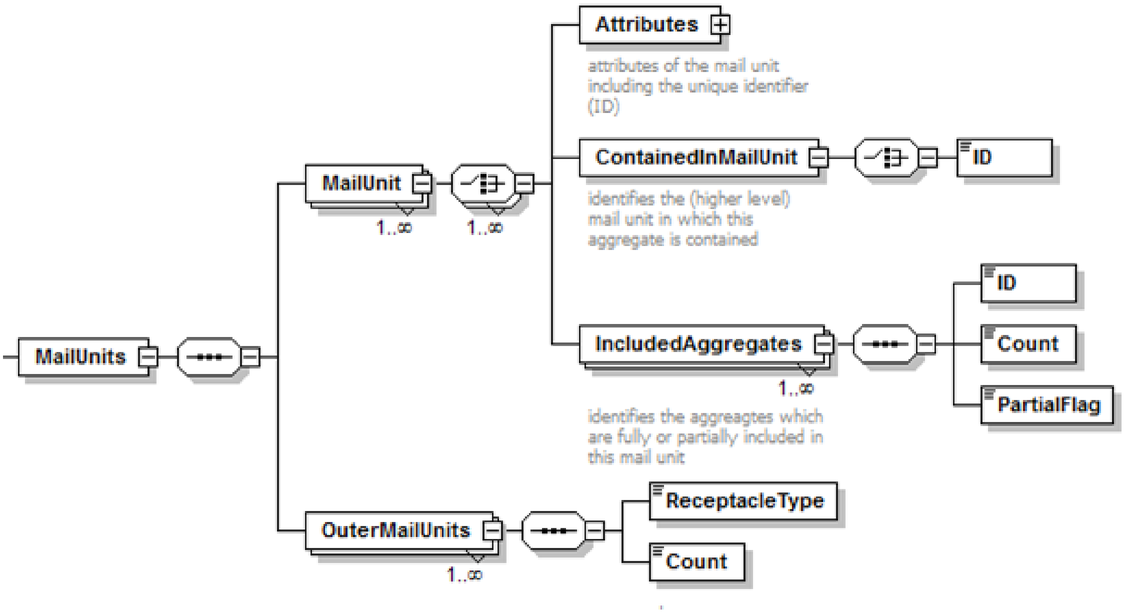

Attributes
attributes of the mail unit including the unique identifier (ID)
ContainedInMailUnit
ID
identifies the (higher level) mail unit in which this aggregate is contained
MailUnit
1..∞
1..∞
ID
Count
PartialFlag
MailUnits
IncludedAggregates
1..∞
identifies the aggreagtes which are fully or partially included in this mail unit
ReceptacleType
OuterMailUnits
Count
1..∞

Figure 10 – The structure of SMS.MailUnits element

Figure 10 illustrates the structure of the MailUnits element of the SMS schema. The elements MailUnits.Mailunit.Attributes contain additional elements which are not shown here to enhance the readability of the diagram. Mail unit attributes are illustrated in Figure 11.

6.2.6.1 SMS.MailUnits.MailUnit

This element contains information describing mail units which can be individually identified (the mail unit attribute ID is known). This element may have an unlimited number of instances; each instance of the SMS.MailUnits.MailUnit element represents one mail unit.

6.2.6.1.1 SMS.MailUnits.Mailunit.Attributes

This element includes attributes of individual mail units (i.e. envelopes, postcards) and aggregates (i.e. trays, sacks). Tables 12, 13, 14 and Figure 11 illustrate only the attributes most commonly used. Mailers and posts may agree to communicate additional attributes not listed here, as indicated by the presence of an element labeled OtherAttributes.

Table 12

SMS.MailUnits.Mailunit.Attributes.ID	Unique identifier of the mail unit.
SMS.MailUnits.Mailunit.Attributes.DestinationPostalCode	The value of this attribute is the destination of the mail unit expressed as a postal code
SMS.MailUnits.Mailunit.Attributes.Weight	The value of this attribute is the weight of the mail unit
SMS.MailUnits.Mailunit.Attributes.Dimensions	The value of this attribute is a set of dimensions of the mail unit
SMS.MailUnits.Mailunit.Attributes.Length	The value of this attribute is the length of the mail unit (applicable to mail items)
SMS.MailUnits.Mailunit.Attributes.Width	The value of this attribute is the width of the mail unit (applicable to mail items)
SMS.MailUnits.Mailunit.Attributes.Thickness	The value of this attribute is the thickness of the mail unit (applicable to mail items)
SMS.MailUnits.Mailunit.Attributes.OtherAttributes	This is a placeholder for mail unit attributes not listed here, but agreed upon between mailers and posts. It also a reminder that this list is likely to be updated

The following mail unit attributes are normally used for single mail items:

Table 13

SMS.MailUnits.Mailunit.Attributes.Machinable	The value of this attribute indicates if the mail items can be processed by an automated equipment (e.g. sorting machines)
SMS.MailUnits.Mailunit.Attributes.MachineReadable	The value of this attribute is indicates if the destination addresses on the mail units is expected to be read by an automated equipment (e.g. OCR, barcode readers)
SMS.MailUnits.Mailunit.Attributes.Addressed	The value of this attribute indicates if the mail items carry specific addresses, or not
SMS.MailUnits.Mailunit.Attributes.EquipmentID	The value of this attribute is a code which identifies the equipment used to produce the mail unit
SMS.MailUnits.Mailunit.Attributes.EquipmentType	The value of this attribute is the type of equipment used to produce the mail unit
SMS.MailUnits.Mailunit.Attributes.FormFactor	The value of this attribute is the form factor of the mail unit. This also could be aspect ratio of length and width or a code for mailing envelope size (e.g. A4 or #9)
SMS.MailUnits.Mailunit.Attributes.InsuredValue	The value of this attribute is the insured value of the mail unit (applicable to mail items)
SMS.MailUnits.Mailunit.Attributes.CODAmount	The value of this attribute is the amount expected as COD for the mail unit (applicable to mail items)
SMS.MailUnits.Mailunit.Attributes.NonDeliveryDisposition	The value of this attribute is taken from a code list to indicate what has to be done with the mail item if it cannot be delivered
SMS.MailUnits.Mailunit.Attributes.Inserts	This element contains information about any enclosures inserted into the mail unit that affect the price of the service
SMS.MailUnits.Mailunit.Attributes.Inserts.Type	The value of this attribute is the type of insert (e.g. business reply card).
SMS.MailUnits.Mailunit.Attributes.Inserts.Weight	The value of this attribute is the weight of the insert
SMS.MailUnits.Mailunit.Attributes.Inserts.Thickness	The value of this attribute is the thickness of insert
SMS.MailUnits.Mailunit.Attributes.Inserts.Count	The value of this attribute is the number of inserts
SMS.MailUnits.Mailunit. Attributes.PostalProduct	This element contains mail unit postal product information (applicable to mail items)
SMS.MailUnits.Mailunit. Attributes.PostalProduct.ProductNumber	The value of this attribute is an identifier of a postal product taken from a code list

SMS.MailUnits.Mailunit. Attributes.PostalProduct.EarliestDeliveryDate	The value of this attribute is the earliest date, the mail item should be delivered to the addressee
SMS.MailUnits.Mailunit. Attributes.PostalProduct.LatestDeliveryDate	The value of this attribute is the latest date, the mail item should be delivered to the addressee
SMS.MailUnits.Mailunit. Attributes.Payment	This element contains mail unit payment information (applicable to mail items)
SMS.MailUnits.Mailunit. Attributes.Payment.Type	The value of this attribute indicates the type of payment evidencing (e.g. franking, postage stamps)
SMS.MailUnits.Mailunit. Attributes.Payment.PostageAsEvidenced	The value of this attribute is the amount of postage applied to the individual mail item
SMS.MailUnits.Mailunit. Attributes.Payment.FrankingMachineID	The value of this attribute is the identifier of the franking machine used for payment evidencing.

The following mail unit attributes are normally used for packages:

Table 14

SMS.MailUnits.Mailunit.Attributes.OuterMailUnitFlag	When “true”, the value of this attribute indicates that the mail unit is visible without opening other mail units. In most cases it contains other mail units.
SMS.MailUnits.Mailunit.Attributes.ReceptacleType	The value of this attribute is the type of receptacle holding the mail unit (for example: envelope, tray, sack).
SMS.MailUnits.Mailunit.Attributes.SortMethod	The value of this attribute indicates the method used to group smaller mail units included in the given mail unit. The value of this attribute is taken from a code list.
SMS.MailUnits.Mailunit.Attributes.StackableFlag	The value of this attribute is a flag which, when set to be “true”, indicates that the mail unit can be stacked (one on the top of another).

Figure 11 illustrates the structure of the SMS.MailUnits.Mailunit.Attributes element. The attributes are defined in Tables 12 to 14.

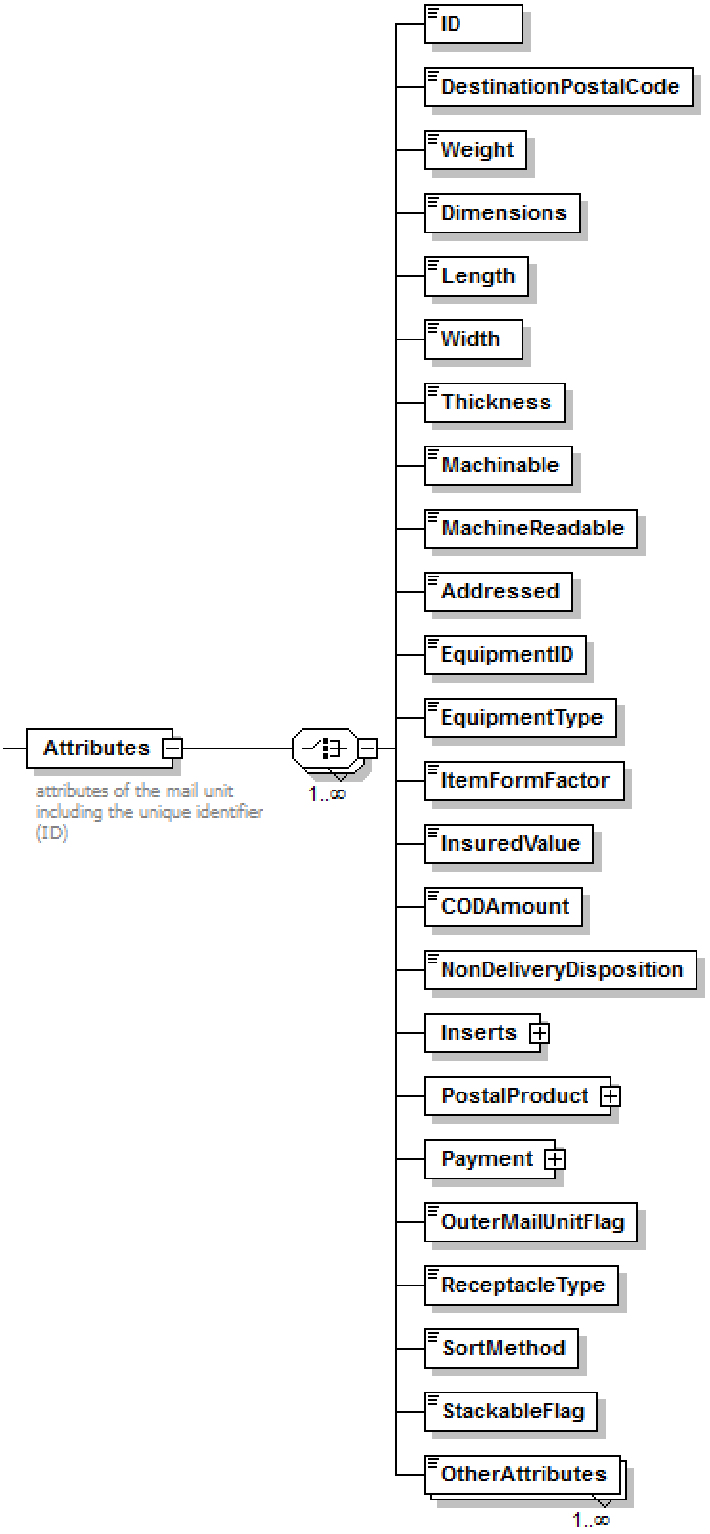


Figure 11 – Structure of mail unit attributes

6.2.6.1.2 SMS.MailUnits.Mailunit.ContainedInMailUnit

This element identifies the larger mail unit that contains the given mail unit.

Table 15

SMS.MailUnits.Mailunit.IncludedInMailunit.ID	The value of this attribute identifies the mail unit which contains the given mail unit (points to the aggregate which includes the mail unit)

6.2.6.1.3 SMS.MailUnits.Mailunit.IncludedAggregate

This element identifies the aggregate to which items contained in the given mail unit belong to. For example, the given mail unit is a tray which contains items which are part of an aggregate identified by the value of the ID attribute below. Some of the items from the given set are included in the tray. Their number is expressed by the count element. The element PartialFlag, when true, indicates that not all mail units from the set are included in the given mail unit.

Table 16

SMS.MailUnits.Mailunit.IncludedAggregate.ID	The value of this attribute identifies the aggregate completely included in the mail unit
SMS.MailUnits.Mailunit.IncludedAggregate.Count	The value of this element indicates the number of mail units from the set which are included in the given mail item
SMS.MailUnits.Mailunit.IncludedAggregate.PartialFlag	The value of this element, when true, indicates that only some of the mail units from the set are included in the given mail unit

The information elements defining the set are described in 6.2.5.

6.2.6.2 SMS.MailUnits.OuterMailUnits

This element contains information about the largest mail units (outer mail units). This information about outer mail units (container type and count) can be computed by analyzing all MailUnit elements, when sufficient information is provided. It is possible that in certain cases mailers will provide only information regarding the outer mail units, for example, a submission contains two roller cages. Multiple instances of this element are allowed, one for each type of receptacle.

6.2.6.2.1 SMS.MailUnits.OuterMailUnits.ReceptacleType

The value of this attribute is the type of receptacle of outer mail units.

6.2.6.2.2 SMS.MailUnits.OuterMailUnits.Count

The value of this attribute is the number of individual outer mail units of the corresponding type.

6.3 Message Format

For reasons of convenience and communications efficiency, (sets of) SMS will generally be sent in batches, rather than singly, preceded by a header identifying the message. The content of the header is outside the scope of this Technical Specification.

The recommended format of each message has the following structure:

Table 17

Header	
1 to 99	SMS

NOTE The number of 99 possible SMS is arbitrary. It is assumed that 99 possible SMS within one communication message is sufficient to cover present and foreseeable needs of mailers and postal operators.

6.4 Communication Protocol

The communication protocol between the submitter and the post is as follows:

Step 1: The submitter sends a message containing 1 SMS to 99 SMS to the post.

Step 2: Upon successful receipt, the post sends an acknowledgement message to the submitter.

6.5 Communication channel security

The implementation of services that rely on information transfers between a postal operator and its customers require the use of secure communication channels. Such communication channels between the customer (e.g. mailer or its authorised agents) and the postal operator can be established using traditional (standard) methods of digital encryption and digital signatures as described in ISO/IEC 9798-3:1998 and ISO 10126-2:1991. This secure communication channel between the postal customer and the postal operator is referred to as the customer-post channel. An established secure customer-post channel provides for mutual authentication (and non-repudiation when needed) between a customer and a postal operator before any transmission of data occurs through the channel. The channel is also able to protect the integrity of all data exchanged through the channel by allowing both the customer and the postal operator to check that received data has not been altered during transmission process. This is accomplished through digital signing of all information contained the messages. Finally, the privacy of information contained in messages communicated through this channel is protected against disclosure to unauthorized parties by using digital encryption.

Communications described in the present technical specification enable the services of authentication, non-repudiation, data integrity and privacy independently of each other, as needed. Whenever a reference is made to the Customer-Post channel and it is not specified otherwise, it is assumed that all four security services are enabled.

Threats and countermeasures related to Customer-Post channel infrastructure are described in EN 14615 and UPU S36-4). More information is available in the draft of CEN DPM Infrastructure standard.

The techniques required to secure the Customer-Post Channel are generic to any computer-to-computer communication channel and as such are adequately described in the aforementioned international standards. That is why this specification does not give any specific recommendation for implementing channel security. The techniques specific to SMS applications are described in detail in Clause 7.

7 Application Security

7.1 Introduction

Any consideration of security should be set in the context of an overall security policy, defining objectives and constraints which apply. In its approach to security this clause follows the methodology adapted by EN 14615 and UPU S36-4. These standards identify all commonly encountered threats (attacks) against systems that use digital postage marks (DPMs) and recommend effective countermeasures. Special attention is paid to the attacks that may result in sizable postal revenue losses. The approach taken by these standards essentially assumes (because the DPM is their focus) that the DPM is the main (and in some cases the only) source of information available to postal operators for protecting postal revenues. While this is the case for a collection mail (that is the mail that is anonymously deposited into street letter boxes typically by individuals and small to medium size commercial mailers) it is not the case for the class of mail known as Bulk Mail or a Controlled Acceptance Mail or Controlled Entry Mail (CAM or CEM). The CEM is normally packaged (or containerised) and either brought for induction into a postal facility by a mailer (or its agent) or collected by postal personnel at the mailer’s premises. In either case, the CEM is normally examined by postal personnel before being accepted for processing which explains the meaning of the term “Controlled Acceptance/Entry”. The Electronic Data Interchange across the Mailer-Post Interface fully applies to this type of mail. This means that mailers and Posts can collect and subsequent to collection, electronically exchange certain relevant data in addition to a more traditional exchange of data via (physical) mail units. In the case of CEM effective revenue, protection measures are greatly enriched by the availability and use of information that can be electronically interchanged between mailers and post.

This clause defines threats (attacks) and countermeasures based on the use of both electronically (via SMS) and physically (via DPM) supplied information. The attacks that are considered here are concerned, for the most part, with monetary gains that may be expected by perpetrators of such attacks and that may result in revenue losses to postal operators. However, in addition to revenue protection concerns, the electronic interchange of data across Mailer-Post interface poses other challenges typically present in the general case of the electronic exchange of valuable information. These challenges primarily deal with the protection of information that is deemed to be private (confidential) to both communicating parties, i.e. mailer and post. Yet another set of issues with the electronic communication of data may include data integrity and data source authentication, impersonation, denial of service attacks and other similar threats that are not aimed at defrauding the Post of its revenue, but rather at damaging other aspects of mailer’s and postal operations. These threats are, for the most part, not specific to postal applications. The present section provides only basic recommendations and refers interested readers to commonly available published standards and literature on the matter of attacks that are not specific to postal applications (see [1]).

7.2 Threats and Vulnerabilities

In spirit this subclause closely follows the subclause on threats and vulnerabilities in EN 14615 and UPU S36-4. Descriptions of some threats were modified, while some other threats were added to reflect more precisely the environment typical for the Controlled Entry Mail (CEM).

The most typical and common threats in the CEM environment are aimed at adding unpaid or underpaid mail items (or mail units) to mailing submissions or claiming unauthorized (and therefore illegitimate) discounts for mail items that are not qualified for such discounts. Electronically Exchanged Messages (EEM) and Digital Postage Marks provide powerful tool to counter these threats.

It is assumed that accounting for the CEM is typically done by the original mailer or its agent(s) and that the accounting information (postage values, postage amounts, various totals, registers values etc.) and the directly associated information (weight of individual mail items, total weight for mailing submission, number of mail items in the submission, ranges of unique identification numbers for mail items in the mailing submission etc.) are collected within secure boundaries of a Postal Security Device (PSD). If this is not the case, the accounting information collected by the mailer and/or its agents and submitted to a postal operator for processing cannot be trusted in terms of authenticity of its source and data integrity.

After completing the mail preparation process, the accounting information is communicated electronically to the postal operator that would process the mailing submission (the information can possibly be submitted directly to a postal controlled entry point' computer) via one (or several) of Electronically Exchanged Messages such as the SMS. It is also assumed that individual mail items within mailing submission carry DPMs, albeit the exact design and security mechanism of the DPMs used may vary depending on threat assessment and risk analysis related to a particular mailing application, trustworthiness of the mailer and other factors. For example, it is possible in many applications to use a DPM containing only postage value and an unique identification number without any cryptographic data protection (such as the Cryptographic Validation Code – see EN 14615 and UPU S36-4 for definitions and discussion) and yet to retain a sufficient level of revenue protection control. In other applications, particularly when the threat of *Collusion* is real it may become necessary to use mail items carrying cryptographically protected information within the DPM.

Threats or *attacks* correspond to methods of attacking a system with the objective of causing damage to it, its operators or users. For a detailed discussion of threats or attacks the reader is referred to EN 14615 and UPU S36-4. Threat analysis, in the context of a postage payment process, is concerned with identifying all possible attacks at each step or link in the process and analysis of the consequences of such attacks to all involved parties. Fundamental to this analysis are questions as to who is liable in the event of a breach of security and who bears the cost of providing necessary security measures. These questions can only be addressed in the context of a particular business model which delineates operating responsibility and business liability. Several different legal entities (parties) might be involved in mail creation, preparation, processing and delivery. Knowledge of the parties involved may be helpful in resolving the issue of liability.

The remainder of this subclause is devoted to identifying a number of threats that are common to Controlled Entry Mail payment systems. It is stressed that the list given below is not exhaustive. Most of the threats identified involve the disclosure, modification, copying or substitution of data, though other categories of threat, including physical attacks and attempts to prevent reliable operation, should not be ignored. The other categories, however, are not specific to CEM payment and adequately addressed elsewhere, for example in the aforementioned EN 14615 and UPU S36-4.

Each postal operator has a unique environment that may preclude some of the following threats, but more importantly, may yield to threats that have not been addressed. It is important to conduct a thorough analysis and to complement the list of applicable threats when needed and give proper consideration to each one. The analysis should address at least:

a) Alteration of DPM: in the context of this standard, alteration involves the deliberate changing of information present in a legitimately created DPM. For example, a DPM containing a low postage value may be altered to indicate a (much) larger amount of postage. Note that alterations may be made to the computer readable data in the DPM, to the human readable data, or to both.

b) Alteration of Electronically Exchanged Message (EEM): in the context of this standard, alteration involves the deliberate changing of information present in any of the electronically exchanged messages, most importantly in the Statement of Mailing Submission (SMS). For example, a SMS containing one value of the total weight for the mailing submission can be altered to indicate a lower weight in order to submit (for processing and delivery by Post) unaccounted (and consequently unpaid) mail items.

c) Collusion: involves cooperation between two or more parties with fraudulent intent. It may occur between postal customers (mailers and recipients), between a customer and a supplier, or between one of these and a corrupt postal employee. For example, an individual employed by one mailer may assist another mailer to generate mail purporting to originate in his own organisation, or a mailer may bribe a postal employee to by-pass controlled entry mail acceptance controls (see Inappropriate Induction below). Collusion attacks could not be totally prevented, but properly organised systems are designed to be vulnerable only to collusion between several (i.e. more than two or three) individuals and to have multiple verification processes which support the detection of collusion.

d) Copying: involves the duplication of an original DPM to produce (unpaid for) identical copies and using these copies on mail units deposited into the postal system. Unlike counterfeiting (see below), this requires access to, or detailed knowledge of, a legitimate Digital Postage Mark. In the CEM environment copying of DPM may be used by unscrupulous mailers or third parties involved in mailing preparation or submission to add unpaid (but if taken by themselves properly verifiable) mail units to mailing submissions containing legitimately paid mail.

e) Counterfeiting of DPM: unauthorised creation of a printed symbol that is similar to, or apparently identical with, a legitimate DPM in an attempt to perpetrate fraud. It includes creating original, apparently legitimate, but unauthorised, DPMs containing guessed or predicted Cryptographic Validation Code or Exchange Validation Code values (see UPU S36-4 and EN 14615 for definitions and discussion). Unauthorised access to DPM authentication devices (verifiers) may be used to create counterfeit DPMs in which the guessed CVC or EVC is known to be correct, making detection difficult or impossible. For this reason, access to verifiers must be protected. In the CEM environment a counterfeiting of DPM may be used by unscrupulous mailers or third parties involved in mailing preparation or submission other than original mailers to add unpaid mail units to mailing submissions containing legitimately paid mail. As noted, counterfeiting does not require knowledge of legitimately computed DPMs or their unique identification numbers and therefore is more simple for perpetrators to execute than copying (especially in a large volume mail environment).

f) Cryptanalysis: use of mathematical techniques in an attempt to defeat the use of cryptographic methods, particularly in the context of information security services. It is normally aimed at recovering cryptographic keys by exploiting knowledge of the cryptographic algorithm, data that forms input of and/or output from the algorithm, or both. Since well-known cryptographic algorithms are endorsed and standardised only after extensive expert examination, the threat from cryptanalysis when using such endorsed and standardised algorithms is considered minimal. However, algorithms and their parameter values should be carefully selected for use in protecting both EEM and DPM-based systems. The most common algorithms are described, and minimal acceptable values of their relevant parameters given, in the UPU S36-4 and EN 14615.

g) Device Modification: illegitimate alteration of a genuine PSD (postal security device designed to compute information for DPM and execute security services required for the protection of EEM) with fraudulent intent. For example, unauthorised manipulation of ascending and/or descending registers of a franking device could result in postage payment avoidance.

h) Illegitimate Key Access: access to the secret cryptographic key or keys of a legitimate postal security device or a user by an unauthorised party, thereby allowing the party concerned to masquerade (cryptographically) as the legitimate device or user. Illegitimate access to cryptographic keys would put at risk any cryptographically protected features of the system. Prevention of such access therefore deserves careful design of the key management and protection system and also needs to address the procedures for dealing with any illegitimate key access that may be detected.

i) Illegitimate Use of Device: operation or manipulation of a genuine device for the purpose of perpetrating fraud. For example, unauthorised use of a pre-payment-based metering (franking) device could result in damage to the legitimate user, since the metered postage used by the perpetrator would no longer be available to the legitimate user. There may also be circumstances in which the device supplier and/or the postal administration may be impacted (e.g. in a credit based systems, the mailer from whom a metering device is stolen may refuse to pay for postage subsequently accounted for by the device).

j) Impersonation: occurs when one mailer introduces mail items into the postal system, claiming that they have been originated by another mailer. For example, in a situation in which accounting is done by the Post, DPMs could be modified to include a device or licence identifier belonging to another mailer. The postal items concerned would then be interpreted as, and charged to the mailer whose device identifier or licence number appeared in the DPMs, rather than the mailer which actually generated the mail. Another example specific to CEM is the situation when an unauthorised mailer adds mail units marked with the authorised mailer’s identity to a mailing submission of the authorised mailer with or without knowledge of the authorised mailer. This situation may occur, for example, when unpaid mail units added to paid mail units in a mailing submission while the mailing submission is in transit from a legitimate and authorised mailer’s facility to an entry point in the postal distribution network.

Note that, depending on the specific characteristics of the application, system and DPM design, impersonation may be a special case of *Alteration*, of *Device Modification* and/or of *Illegitimate Use of Device*. It may also be associated with *Inappropriate Induction*.

k) Inappropriate Induction: introduction of mail units into the mail system in an improper way that may result in the by-passing of normal induction/acceptance controls. For example, a dishonest mass mailer could possibly arrange to have mail inducted through an Office of Exchange, resulting in it being treated as inter-administration mail. This threat would normally be associated with collusion (see above) between the mailer and a postal system employee.

In the case of CEM, a dishonest mailer may attempt to avoid normal acceptance control procedures by breaking a (fairly) large mailing submission into smaller units and by depositing such units through (many, potentially very many) street letter boxes.

l) IT System Infiltration: covers the range of threats which are common to IT systems. For example, a deceitful postal employee with access to the financial database that maintains records of the funds paid in by mailers and suppliers, could modify the database records to the advantage of the mailer and the disadvantage of the post. Each element of the IT system must be examined to minimise the possibility of undetected, unauthorised access to, change or deletion of data.

m) Miss-application: covers any case in which a DPM generated for one mail item is in fact applied to another, or in which the parameters used for generating a DPM do not correspond with the attributes of the item to which it is applied. This will result in a loss of revenue to the postal operator if the postage accounted for is less than that which should properly be due for the mail unit to which the DPM is actually applied, for example, if payment was for a lower weight class, or if a discount rate is applied inappropriately. However, proof of intentional fraud may be difficult, as miss-application may be accidental, as well as deliberate.

Of particular interest to the CEM environment is inappropriate (and especially deliberately fraudulent) claiming of worksharing (e.g. pre-sort) discounts for unqualified mailings. Such discounts can be legitimately claimed for mailing that has undergone special preparation designed to bypass one or several postal processing steps that are normally required for unqualified mailings. For example, substantial discounts are frequently available to mailers for pre-sort and mailer-applied sorting (routing) barcodes.

n) Obliteration / Read-rate Manipulation: defacing a DPM so that it cannot be interpreted by automatic scanners and/or human operators, with the intent of circumventing the verification process and thus avoiding payment. There are many ways in which the DPM can be rendered illegible, including folding, spindling, mutilating, smudging, etc. Detecting obliteration may be difficult, as read-rates are never perfect and may be adversely impacted by accident or equipment malfunction.

o) Refund Requests: refund policies, and the threats associated with them, will vary from one postal administration to the next. Particular attention needs to be paid to refunds of unused pre-paid postage and to refunds for spoiled mail and DPMs.

p) Replay: involves the re-use or re-transmission of a message (including a DPM[3)]) with fraudulent intent. Examples include the re-use of envelopes carrying DPMs and, probably of more significance, the repeat of communications (transmissions), such as postage download messages, between subsystems. Unlike counterfeiting (q.v.), replay requires access to or detailed knowledge of a legitimate original message.

q) Repudiation: occurs when one of the parties to a transaction denies his or her involvement. For example, in a CEM environment a mailer could attempt to deny sending an SMS to a postal operator in order to avoid responsibility while the actual mailing submission has later been found to have significant discrepancies with the received SMS. Similarly, in a system based on postal administration postage accounting (see UPU S36-4 and EN 14615), a mailer could attempt to deny responsibility for the origination of the mail.

[3)] Note that copying of a DPM is treated under the heading “Copying”. Here reference is made to re-use of an original DPM (compare with stamp washing).

r) Re-Use: see Replay

s) Security System Infiltration: penetration of the security system with the objective of disabling it or reducing its effectiveness. If the security system can be penetrated and disabled, any vulnerabilities of such a security system may be exposed and advantage taken of them. Fraudulent key insertion, in which an unauthorised key value is inserted into the set of authorised keys supported by the security system, provides a second example.

t) Side Channel Attack: non-invasive attacks which take advantage of the physical nature of the computational process to obtain information about the secret information stored within a system or a device (e.g. secret key). The execution of cryptographic operations involves physical processes that consume energy and require time to perform. Analysis of timing and/or power consumption data may reveal information about the value of the key used, even in situations in which the equipment concerned is tamper/protected.

   Side channel attacks fall into two categories: timing attacks and power consumption attacks. In a timing attack, an adversary with knowledge of the algorithm attempts to learn bits of the secret key by measuring the time required to execute cryptographic transformations on known plain text. Power consumption attacks exploit differences between the levels of power consumption that normally occur during the execution of cryptographic algorithms. Typically, if a bit of the secret key is zero, the power consumed during execution differs from the power consumed when the bit is equal to one. Power consumption attacks are also known as Simple Power Analysis, Differential Power Analysis and Inferential Power Analysis and may involve the use of sophisticated statistical techniques applied to thousands of power measurements taken during the execution of the algorithm. These attacks, if not adequately protected against, can result in a total breakdown of the system, since the attacker may gain access to cryptographic keys without leaving any trace.

u) Substitution: involves the interception of a legitimate mail item and its replacement by single or multiple other items. In a DPM-based environment, the substitute item would have to bear a copy of the DPM taken from the original, possibly giving rise to a case of Miss-Application (see above). If this is not the case, substitution has no direct revenue consequences for the postal administration, but it obviously affects the mailer of the original item, which will not be delivered, and could give rise to claims that the item has been lost by the postal service. In the CEM environment a single item of relatively high weight may be replaced in the mailing submission with multiple items of lower weight, in such a manner that the total weight of the mailing as reported in the SMS remains unchanged. In this case, if substitution is undetected and depending on the structure of postal tariffs, the postal operator may suffer considerable loss of revenue.

v) Substitution of Electronically Exchanged Message (EEM): substitution of one EEM (legitimate and genuine) by another. It involves interception of a legitimate EEM and its replacement by another EEM. Substitution normally involves either alteration of the message or alteration of its source in order to change the message itself or to convince the receiver that the message has been originated by a party different than the actual sender. See also *Alteration of EEM and Repudiation*.

w) Underpayment: see Miss-Application

Not all entries in this list of threats are of equal relevance for security/postal revenue protection in the CEM environment. Some threats are generic in nature, for example cryptanalysis, IT system infiltration, side-channel attacks, illegitimate key access and illegitimate use of the PSD. These attacks are either dealt with in sufficient detail in UPU S36-4 and EN 14615 or in widely available specialized standards and literature on information security. For this reason this specification does not discuss these threats any further. On the other hand threats specific to Controlled Entry Mail such as Alteration of Electronically Exchanged Message, Collusion, Impersonation, Substitution of EEM and Inappropriate induction are discussed in detail.

7.3 Applications and Message Level Security

The purpose of any security system is to reduce the protected system’s vulnerability to applicable threats to the extent that is economically, organisationally and technically feasible. Clearly, elimination of such vulnerability is preferable, but all practical systems suffer from weaknesses and total elimination is unlikely to be possible and still less to be cost effective. Security system design is therefore generally based on two principles:

— damage control;

— deterrence.

Damage control is concerned with minimising the costs and consequences associated with attacks on and errors in the system. This requires a high rate of detection of security breaches, coupled with an appropriate reaction. This reaction may either relate to a particular breach of security giving rise to it, and/or be directed against the possibility of similar breaches in the future. Thus, for example, reaction to the detection, through sampling, of a mail item carrying an inappropriate or unreadable digital postage mark may involve either interception of the item for investigation or its delivery, possibly combined with the initiation of a closer investigation of the responsible mailer, to determine the incidence of such mail items.

The problem with a pure damage control approach is that it provides no disincentive to potential attackers. Deterrence is therefore concerned with increasing the costs of mounting an attack on the system, reducing the probability of such an attack being successful and minimising the benefit to the attacker. Such an approach requires a higher and more consistent capability of detecting security breaches, coupled with reactions designed to impact the attacker, rather than being designed to minimise the immediate impact on the system.

Apprehension and punishment of attackers represents one of the most powerful, but difficult to achieve, means of deterrence. In addition to a high rate of attack detection, it requires the identification of the perpetrator of an attack, support for the investigation and prosecution and the application of a suitable penalty. The deterrent effect requires that the probability of apprehension and the penalty for proven offenders are balanced, so that the overall risk to the attacker is high in relation to the rewards which may be gained in cases in which the security breach is either not detected or in which the perpetrator is not apprehended. There is a need for a clear regulatory framework, providing for additional charges in case of avoidable error and for stiff legal penalties in case of successful prosecution of attempted fraud. The latter requires the security system to provide for the collection of legally admissible evidence of fraud. In some cultures, even a low rate of prosecutions may offer sufficient deterrence if the penalties are high enough. This may make detection and apprehension by random sampling a workable strategy if the sampling rate is chosen to give the right level of probability to reliably identify an attacker.

Countermeasures are techniques designed to deter adversarial attacks, enable detection of such attacks and also inadvertent errors which can be misconstrued as deliberate attacks, and, where possible, to reduce or eliminate vulnerability to possible threats. They do so by:

a) providing controls designed to detect and respond to the occurrence of errors and/or possible attacks, reducing the system vulnerability to the associated threats;

b) increasing the cost of mounting an adversarial attack and/or reducing the expected benefit, to an attacker, thereby making attack less rewarding;

c) increasing the probability of identification of an attacker and/or increasing the ‘cost’ of being caught, thereby creating a risk which will deter all but the most determined attacker.

Countermeasures may consist of mechanisms, procedures, laws, etc., or combinations thereof. This standard, like UPU S27, considers them under two categories corresponding to the S27 definitions of *Message-* and *Applications Security*.

Thus, for the Controlled Entry Mail the postal revenue protection countermeasures are aimed at four objectives:

1) *Detection* of postage accounting errors, specifically when the accounted postage amount serves as a basis for payment and when the accounting for the postal charges was performed by the mailer or its agent.

2) *Determination* of the nature of the accounting errors e.g. whether they are inadvertent or deliberate.

3) *Identification* of the party (or parties) responsible for accounting for postal charges and its associated errors (if any); in the case of CEM, identification may be accomplished by associating ownership of mailing submission with the identity of the party that presents mailing submission for the entry into the postal distribution system. In most cases, the entry of CEM into the postal distribution network is not anonymous, which implies that the identity of mail owner or more generally the identity of the legally responsible party can be ascertained without difficulty.

4) *Production* of (legally) admissible evidence of deliberate errors and support of the ensuing investigation and prosecution in the case where errors were determined to be of deliberate nature.

Achievement of the afore-mentioned four objectives depends primarily on the information available to a postal operator or, more generally, to a verification party. The sources of this information are various electronically exchanged messages (EEM), information present on mail units (e.g. DPM) and system-wide information available from postal information systems, suppliers and other third parties. This specification is mostly concerned with the description of techniques making use of messages electronically exchanged between mailer and postal operator in combination with the information that can be captured from individual mail units.

Message-level security is concerned with countermeasures to protect against deliberate communication errors, and specifically attacks against communications employed to convey falsified information between parties involved. These include the interception and/or modification or discovery of exchanged messages by third (unauthorised) parties; the impersonation, by third parties, of authorised senders and repudiation of messages by their sender or receiver. Message-level security covers:

a) protection of message *confidentiality*, i.e. measures to prevent unauthorised parties from intercepting messages and/or from understanding any private content of messages which they may have access to (whether legitimately or otherwise);

b) protection of message *integrity*, i.e. measures taken to prevent accidental (e.g. through communications error) and/or deliberate modification of messages during their transport from sender to receiver;

c) *message source authentication*, i.e. methods used to validate that a message originated from a specific authorised sender and not from any other party;

d) *message non-repudiation*, i.e. methods used to ensure that the sender of a message cannot plausibly deny having sent it and/or to ensure that the recipient(s) of a message cannot plausibly deny having received it.

Application-level security deals with countermeasures which cannot be handled on an individual message level, including the correlation of data between different messages, and between messages and data held in postal, mailer's and third parties' computer systems. Examples include:

a) validation of mailing submission' parameters as reported in an EEM (e.g. SMS) against actually measured parameters of the mailing submission; and

b) comparison of total postage accounted by a PSD device against records of refills and mailing activities (volumes of inducted mail units).

7.4 Security Services and Message-level Countermeasures

Postal administrations desiring to implement an effective postage payment system for CEM are strongly recommended to protect the security of the information contained in the EEMs and the DPMs by using an appropriate combination of the four security services, namely Authentication; Confidentiality; Data Integrity and Non-Repudiation. The application of security services to DPMs are covered in detail in UPU S36-4 and EN 14615 and is not discussed any further in this standard unless such an application is used in combination with other counter measures related to the EEMs.

7.4.1 Authentication is a security service that provides assurance of the identity of an entity involved in a transaction. In particular, it seeks, through the use of information that is, in principle, known only to a particular authorised message sender, to ensure that received messages are genuine – i.e. were validly created and sent by the party from which they purport to have originated.

Authentication primarily acts as a countermeasure to the *substitute* and *impersonation* threats.

The purpose of applying an authentication service to the EEMs is to ensure that only authorised devices and/or authorised mailers can create legitimate EEMs and to assist in the identification of the mailers concerned and in detection of *Substitution of Electronically Exchanged Messages.*

Implementation of an authentication service is recommended. Where this is done, the authentication service should be applied to all EEMs. Authentication is usually achieved by using cryptographic techniques such as digital signatures and message authentication codes, though other approaches are possible. These cryptographic techniques are discussed in detail in the UPU S36-4 and CEN EN 14615 standards and in other national and international standards (see ISO/IEC 9798-3:1998 and ISO 10126-2:1991).

7.4.2 Confidentiality is a security service that provides a means of preventing unauthorised entities from interpreting (protected parts of) the content of a message. As a result, the message may be stored or transmitted without any fear that the protected information content will become known to a third party.

Confidentiality may be an important service for the EEMs that contain commercially sensitive or private information. For example if confidentiality of SMS is not protected then an interested third party (e.g. competitor) may learn information indicative of the number of mailer's customers, their addresses and other potentially damaging to the original mailer information.

Where required, confidentiality is normally achieved by the implementation of a (reversible) encryption of the data to be protected, using either a public key of a public/private key pair of which the private key is known only to the intended recipient of the message, or using a secret key shared between the sender and the intended recipient.

7.4.3 Data Integrity is a security service that provides an assurance that protected data has not been altered by either intentional or accidental means. It thus prevents the undetected substitution of invalid or incorrect data for legitimate, protected, data.

Data integrity acts primarily as a countermeasure for the threats of *Alteration, Alteration of Electronically Exchanged Messages*, but may also be used to protect against *miss-application* if integrity protection is extended to include data which is intrinsic to the correct EEM or the mail unit.

The implementation of a data integrity service is strongly recommended. Moreover, the service should be applied to all EEMs to provide evidence of deliberate alteration for fraudulent purposes.

Like authentication, data integrity is usually achieved by using cryptographic techniques such as digital signatures and message authentication codes. Other, non-cryptographic, techniques may be used in cases in which the requirement is to protect against communications error, rather than against deliberate alteration of message content. UPU S36-4 and EN 14615 provide guidelines on possible implementation approaches.

7.4.4 Non-repudiation is a security service that binds an entity to a transaction in which it participates, i.e. it provides (legally admissible) evidence of a given party's participation in the transaction and acts as a countermeasure to the threat of *repudiation*. The purpose of the non-repudiation service is to prevent the sender of a message from successfully denying the fact of sending it (sender non-repudiation) and/or to prevent the receiver from successfully denying the fact of receiving it (receiver non-repudiation). This may be particularly relevant in any prosecution of (attempted) fraud, in which it may be essential to prove the identity of the perpetrator.

Sender non-repudiation is very important to EEMs, particularly containing financial/postal accounting and binding contractual information. It has to be recognised that sender non-repudiation applies to the legal entity which generated the information used in provision of the non-repudiation service. Depending on the business and application scenario, this may not be the mailer. For example, it might be the mailer's franking device

(PSD which could conceivably be the subject of unauthorised use) or a party responsible for mail finishing which works on behalf of the mailer and which might, knowingly or inadvertently, generate mail purporting to be, but not actually, that of the mailer. If the identity verification process used by the key certification authority is weak, it could even be a third party which impersonated the mailer at the time of key issuance or registration.

Protection against sender repudiation is closely linked to the issue of authentication (see above) – if the approach taken to this is secure and makes use of information (such as the private key of a public-private key pair) known only to the sender, sender repudiation is unlikely to be successful; if the approach is weak, the sender may find it easier to claim that the message was generated by a third party.

As is the case with authentication, sender non-repudiation is typically implemented using cryptographic (information security) techniques. Digital signatures and message authentication codes can both provide this service. However, whilst digital signatures provide for explicit sender non-repudiation, message authentication codes provide it implicitly since at least two parties participating in a transaction secured by a message authentication code must have shared access to the protected secret key. As a result, the sender can always try to claim that a disputed message was generated by the receiver, or that the receiver's key security has been compromised. For this reason, use of secret key cryptographic algorithms for non-repudiation purposes is limited to situations in which either the receiver is beyond reproach, or recourse is made to a third party, which is fully trusted by both sender and receiver.

Receiver repudiation – the claim by a receiver that he/she did not receive a message, or received it at a time other than that of its real receipt – may also present a risk in certain cases, particularly in case of messages relating to special classes of mail. Protection against this eventuality is normally afforded by requiring the receiver to acknowledge receipt. Such acknowledgements can, as necessary, be protected using authentication and sender non-repudiation services. Many well-designed communication protocols include acknowledgement messages. Actual examples of acknowledgements are outside of the scope of the present specification.

Security of access to the message communications channel may also play a role in protection against both sender and receiver repudiation. For example, in the case of messages submitted on physical media such as CD ROM or magnetic disk, acceptance control procedures may be used to validate sender identity at the point of message hand-over; similarly, signing procedures are traditionally used (c.f. registered mail) to confirm acceptance of the message.

7.5 Application-level Countermeasures

The following subsections outline most important of the application-level countermeasures that may be applied. It should be stressed that those outlined should in no way be construed as representing a complete list of possibilities and postal administrations are encouraged to creatively consider other techniques.

Given the scope of the present specification and as noted above, the following subsections concentrate on countermeasures which relate, in some way, to the EEMs and their linkage to the DPMs whose primary purpose is to detect errors in postage accounting, identify responsible party or parties and provide evidence of fraud when applicable. This evidence should enable the postal administration (or its authorised agent) to improve its ability to conduct effective investigation and prosecution of postal fraud as well as deliver desired deterrence effect for potential perpetrators of fraud.

7.5.1 Access and Usage Controls

A wide variety of threats may be effectively countered by limiting access to, or controlling the usage of sensitive parts of the system. Access and Usage are not specific to the CEM environment and discussed in detail in UPU S36-4 and EN 14615. However, two specific comments related to tamper protection and watchdog timers in the CEM environments are as follows.

The response to tampering may include reporting to a device management system, modification of critical device data or disabling of the device. To guard against the threats of *illegitimate key access* and *security system infiltration*, it is desirable that the tamper response includes the destruction (e.g. zeroisation) of any cryptographic parameters stored in the device. In the case of the EEMs requiring security protection, disablement may not always be the best option as given the data carrying characteristics of the EEMs, it may be preferable, instead, to allow the device to continue to operate, but to flag information collected as invalid due to tampering (c.f. the principle of silent alarms for physical access control).

Watchdog timers are timers which must be periodically reset by an authorised inspection engineer or through contact with a device management system, failing which they disable the device associated with them. Disablement may be permanent or temporary (i.e. until the next inspection or contact). Two cases may be considered. In the first, the timer is implemented in the device itself. This requires that physical access to the device is controlled or that the device is provided with tamper protection (q.v.), since it might otherwise be possible for an unauthorised party to reset the timer. In the second case, the timer is remote from the device (e.g. in the management system) and operates by logically controlling the operation of the device, e.g. by refusing connection to a network, or (in the case of EEMs) by causing EEMs produced with the help of devices which have timed out to be rejected as invalid.

Access and usage controls may be used in combination with each other, and with other types of countermeasure. However, there may be limited value in implementing excessive controls.

7.5.2 Countermeasures against Counterfeiting

As noted in the CEM environment, counterfeiting of the DPM may be used by unscrupulous mailers or third parties involved in mail preparation or submission to add unpaid mail items to mailing submissions containing legitimately paid mail. The counterfeiting of the DPM may be used in combination with the *alteration of an EEM, such as the SMS,* in order to avoid detection and prosecution. The countermeasure against alterating the SMS is use of digital signatures or message authentication codes. It allows detection of any alteration that has been made to the SMS after it has been digitally signed by the PSD or any other security device. If the SMS has not been altered, it contains information about some directly measurable (by a verifier), characteristics of the mailing submission (such as its total weight or total number of mail units contained in the submission or other characteristics) as well as identities of mail items included in the mailing submission and that have been accounted for by the PSD. A significant discrepancy between the directly measured and the PSD-reported total weight (or other characteristic) would indicate a possible presence within the mailing submission of mail items with counterfeited DPMs. The information indicative of the identities of mail items in the mailing submission may simply be a range of serial numbers for the properly accounted mail items. Unaccounted mail items, therefore, must bear serial numbers that either are *duplicates of the legitimately accounted for items* or are outside of the range of mail unit identifiers reported in the SMS.

Thus, unpaid mail items imprinted (or otherwise supplied) with the counterfeited DPMs will be detectable by direct examination as either not having any discernible identities at all or having identities that are in clear contradiction with the (verified) information provided in the SMS. Finding such items in the mailing would normally provide solid evidence of fraudulent intent.

Effective use of the counterfeiting countermeasures requires that at least several data elements must be included in the digitally signed portion of the SMS. These data elements are:

- range of unique serial numbers or other unique identifiers for the mail items contained in the mailing submission;
- net and gross weights of the mailing submission;
- mail item weight distribution (for mail items contained in the mailing submission);
- postage rates (tariffs) and postage paid (or accounted for) for the mail items included in the SMS in various homogeneous postage rate categories;
- total postage paid.

7.5.3 Countermeasures against Duplication (copying)

Fraudulent duplication (or replication) of DPMs represents a potentially significant source of postal revenue loss. Duplicate detection seeks to counter this threat by detecting cases of duplication so that appropriate action can be taken.

To prove duplication in the case of CEM beyond any doubt, it is necessary to find within the mailing submission at least two different mail units (e.g. letters) that carry the same DPM. In the case of CEM environment this can be effectively achieved during acceptance process through the use of a two-step procedure:

i) By measuring physical properties of the mailing submission such as its total weight and determining any significant (e.g. outside of a pre-defined level of tolerance) discrepancy between total weight of the mailing submission as reported in the SMS and the total weight directly measured at the acceptance time by trusted postal personnel. Any significant discrepancy would indicate that the mailing submission may contain unreported (and therefore unaccounted for) mail items.

ii) If unaccounted mail items carry DPMs that are duplicates of the legitimate DPMs, then two or more items with the identical DPMs can always be found. This can be done by the direct physical examination of mail items contained in the mailing submission, for example by sampling and comparison. If all DPMs carry human readable identification information this in principle can be done by a simple manual examination and observation. Otherwise appropriate hand-held or automatic-feed scanning equipment can be employed for this purpose.

For this approach to work, each legitimate DPM must be unique. This can be achieved in a variety of ways, for example by the inclusion in the DPM information:

- (non-resettable) counter that always increases;
- value of the PSD device’s ascending register;
- date/time stamp to the appropriate granularity.

All suitable techniques are described in UPU S36-4 and EN 14615.

Remarkably, the two-step procedure outlined above allows for both detecting the fraudulent attempt and for the production of legally admissible evidence of such an attempt, providing that two different mail units with the identical DPMs do constitute such evidence. This should in principle, create a very powerful deterrence effect as noted above.

In this way the CEM environment bears a very favourable comparison with the collection mail environment with regard to duplicate detection, which is in the case of the CEM is considerably simplified due to the fact that a) adding unaccounted duplicates of mail units changes directly measurable (compared to reported) parameters of the mailing submission and b) normally the *entire mailing submission* is available for examination at the time of acceptance thus avoiding the problem of discrimination between a genuine and a duplicate DPM (see UPU S36-4 and EN 14615 for discussion of duplicate detection based on the information available on the mail unit itself). One significant convenience and cost saving consequence of this fact is that the destination address information for each mail unit need not be included in the cryptographically protected portion of the DPM for an effective duplicate detection.

Effective use of counterfeiting countermeasure requires that at least several data elements must be included in the digitally signed portion of the EEMs (e.g. SMS). These data elements are:

- range of unique serial numbers of mail items contained in the mailing submission;
- net and gross weights of mailing submission;

- mail item weight distribution in the mailing submission;
- postage rates (tariffs) and postage accounted for the mail items in various homogeneous postage rate categories (clusters) included in the submission;
- total postage.

7.5.4 Countermeasures against Inappropriate Induction

Induction control covers procedures that may be applied to mail at the point of its induction into the postal distribution network, the result of which determines whether, and under what conditions, the mail concerned will be accepted for further processing.

Induction control is normally considered primarily in relation to CEM submissions from individual medium to high volume mailers or their agents using a manifest or statement of mailing submission (SMS). As noted, a primary threat by mass mailers against induction control can be described as breaking a mailing submission into sufficiently small units that can be deposited anonymously for example through street letter boxes. This threat is easily thwarted by application of countermeasures normal in the collection mail environment. For example, all collection mail may be required to carry a verifiable evidence of postage paid such as a postage stamp or a DPM. Thus, any mail item that is found in collection mail and does not have verifiable evidence of postage can be detected and diverted for further investigation. UPU S36-4 and EN 14615 provide detailed analysis of security measures for collection mail.

7.5.5 Countermeasures against Miss-Application

As noted miss-application (underpayment) in the CEM environment frequently manifests itself in the underrating of mail items, in particular by using wrong rating parameters (e.g. weight, size) or claiming inappropriate (and especially deliberately fraudulent) worksharing discounts for unqualified mail items.

The case of wrong rating parameters that are directly measurable from the mail unit itself is discussed in UPU S36-4 and EN 14615. In addition, the underrating that is based on the use of wrong (lower than actual) weights for mail units can be detected in the case of the CEM by using the EEMs such as the SMS and by directly measuring the total weight of the mailing submission as described above. Once the discrepancy between the reported and the measured total weights has been found, the mailing submission can be (manually) searched for the mail items that display a discrepancy between the applied rate and the directly measurable weight. Such items in principle constitute admissible evidence of fraud.

The case of incorrectly used rating parameters other than weight or size such as incorrectly claimed discounts for pre-sort or for customer applied sorting (routing) bar code is more complicated. No direct measurements based on the entire mailing submission can detect incorrect pre-sort or incorrectly applied (or totally missing) sorting bar codes on individual mail units. Thus, the detection of such a miss-application at the time of the acceptance (entry) into the postal network can be done either by manual examinations of (sampled) mail items or by specialised automated equipment. The detection of such miss-application can also be performed during the normal mail sorting operation. The manual examination may be time consuming and costly. Any specialised equipment requires economic justification and must be designed to satisfy application requirements for the controlled entry mail. One possible alternative to the detection of this type of miss-application at the time of acceptance is detection at later stages of normal mail processing as mentioned above. During the process of sorting and delivery, incorrectly pre-sorted or pre-barcoded items can be flagged, out-sorted and presented as evidence of miss-application. The issue here is proof that miss-application was intended and was not a result of some random equipment malfunction or an inadvertent operator's error. This proof, at least partially, can be provided with the help of the EEMs, such as the SMS. For example, pre-sorting is frequently done using software in a data processing environment before the physical mail generation process begins. If a PSD is interfaced with a data processing computer to receive an electronic pre-sort qualification statement (as a part of the SMS) at the end of data processing cycle, then this pre-sort qualification statement together with other data included in SMS can be digitally signed within the secure boundary of the PSD and electronically transmitted with the digital signature to a postal operator. Mail items that do not qualify for a discount (sometimes referred to as "residuals") can be reported in the SMS. If the number of non-qualifying mail items reported in the digitally signed and verifiable SMS differs from the number of actually discovered non-qualifying items, then any significant discrepancy may indicate deliberate miss-application. This is due to the fact that normal pre-sorting software process results in a documented qualification report automatically consistent with the composition of actual mailing submission. Similar approach works for the case of miss-application for customer applied bar codes.

7.5.6 Countermeasures against collusion

Manifestation of collusion in the case of Controlled Entry Mail is partial or total abandonment of proper control acceptance procedures. The result of such abandonment is that completely unpaid or incorrectly paid mail units enter the postal processing stream where no postage payment verification procedures may be applied to such mail units. This is a serious threat, especially when it involves malicious behaviour by what would be normally trusted postal employees.

Since execution of a normal acceptance process cannot be expected in the case of collusion, postal operators are advised to organise a collusion detection process for the CEM environment at the stages of postal processing subsequent to the acceptance. Such a detection process must be organised based on examination of the DPMs present on individual mail items since mailing submissions most likely will loose their integrity after acceptance as a result of sorting and distribution. Thus, a detection process may start in a sampling of mail units downstream from the acceptance (e.g. at a final machine sort in a postal facility prior to delivery) with a certain number of mail items randomly selected for verification. If all mail items are required to carry DPM, several outcomes of verification are possible:

1) Mail units (e.g. letters) with cryptographically secured DPM (i.e. DPM containing CVC) display internally or externally inconsistent data indicating counterfeiting or copying. In this case, if the DPMs are required to contain cryptographically-protected reference information to the SMS where they are supposed to be recorded, then finding counterfeited or copied DPMs would indicate a collusion and the SMS together with the found inconsistent mail units will indicate the coordinates of point(s) of induction and dates/times where and when the collusion has occurred and will constitute sufficient evidence of collusion at induction facilities identified by the aforementioned coordinates (e.g. postal codes).

2) Mail units (e.g. letters) without cryptographically secured DPMs contain at least unique identification number and a reference to the SMS where they are supposed to be recorded. If such mail units display duplicate DPMs or identities out of the range reported in the SMS, then such mail units would be indicative of potential collusion. It must be stressed however that in the case when the cryptographically secured DPM is not required, fully trusting any information in the DPM is not possible. Therefore, clever attackers may find an easy way to defeat postal countermeasures by colluding with postal employees with a very little risk of detection or of a giving a (legally admissible) proof of fraudulent activity if the DPMs without cryptographic protection are allowed.

It is worthwhile mentioning that different requirements may be applied to different mailers at the discretion of postal operators. For example, trustworthy mailers may be allowed to use mail without cryptographically secured DPMs, while other mailers may be required to apply cryptographically protected DPMs to all of their mail units. This may provide the desired deterrence effect as noted above.

7.5.7 Countermeasures against Impersonation

As noted, impersonation occurs when a mailer wants to hide its identity typically in order to avoid making payment for mail or in order to avoid responsibility for mailing materials prohibited for mailing by law (e.g. dangerous materials, explosives, “hate” mail etc.). The present specification is primarily concerned with the security of payment and does not discuss detection and prosecution of unlawful mailings except when the theft of postal funds is involved.

Two possible outcomes of impersonation aimed at payment avoidance are:

1) impersonating mailer attempts to defraud a postal operator;

2) impersonating mailer attempts to defraud other mailer or mailers.

In the second case, the postal operator normally does not suffer any monetary losses and the attempt may or may not be detectable by a postal operator except when a concerned defrauded mailer notifies the postal operator about improper charges. If the mailing submission has been properly paid for or expected to be properly paid for by a mailer, the postal operator may have no choice but to accept and process mail as submitted. Only if there is a direct indication of a possible impersonation aimed at defrauding other mailer, the postal operator may begin an investigation depending on the applicable laws. The present specification does deal with such cases explicitly.

The impersonation aimed at defrauding a postal operator inevitably results in the submission of unpaid or improperly paid mail. This may happen if and only if the impersonating mailer uses one or several of the already discussed attacks. For example, if unpaid mail units added to paid mail units in a mailing submission by the impersonating mailer while the mailing submission is in transit from a legitimate and authorised mailer's facility to an entry point in the postal distribution network, then this inevitably changes directly measurable characteristics of the mailing submission. Thus, during the acceptance process a significant discrepancy can be found between reported and measured characteristics of mailing submission as described above. Then, also, legally admissible evidence of fraud can be produced by finding mail units with internally or externally inconsistent DPM information as has already has been described. Identification of the impersonating mailer may require opening a mail item or other similar measures that would have to be executed under appropriate legal supervision. It has to be stressed that in some cases mail units that are produced by the impersonating mailer may not carry any detectable identity of the responsible mailer at all. In this case the identification cannot proceed based on the information available from the mailing and it must use other sources of information.

Effective use of impersonation countermeasure requires that at least several data elements must be included in the digitally signed portion of the EEMs (e.g. SMS). These data elements are:

- mailer's identity information (e.g. mailer's account number and/or PSD ID);
- EEM's identity information (e.g. SMS ID).

7.5.8 Obliteration countermeasures

General DPM obliteration countermeasures are described in full detail in UPU S36-4 and EN 14615. In the case of CEM the effective use of obliteration by dishonest mailers can be made more difficult compared to the case of collection mail since some critical information (e.g. mail unit identity) can be made redundant, for example by requiring it to be presented on the mail unit in both human and machine-readable format. This is because the design of the DPM for the CEM has considerably more flexibility due to the availability of an electronic channel for communication of information from the mailer to the postal operator. Deliberate obliteration of the redundant information is difficult to mask and, due to the nature of acceptance process, direct examination of mail units would reveal such obliteration, thus providing evidence of fraudulent activity on the part of the mailer.

7.5.9 Countermeasures against inappropriate Refund Request

In the CEM environment the verification of the fact that certain mail units have been paid for but have not been mailed is particularly easy. If, for example, the SMS clearly identifies a number of mail units as paid for, those paid for mail units are physically present at the time of acceptance, and if the total weight of the actual mailing submission is less than the total weight reported in the SMS, then the refund can be issued after completion of the appropriate acceptance process as described above. More importantly, due to the efficiency of duplicate detection countermeasures for the CEM, it is possible to automatically correct for malfunctions of the mail preparation equipment that otherwise would result in mail units that have been paid for but could not be mailed. This is so because the DPM information that is ultimately destined for a non-mailable mail unit, can be in practice automatically re-used on another mail unit with the identical postage rating characteristics. The result of such re-use is the mailing submission that is in perfect harmony with its associated (and typically automatically created) SMS.

Selection and application of countermeasures is discussed in detail in EN 14615 and UPU S36-4.

Annex A
(informative)

Examples of SMS documents

Mailing submissions can be classified based on the method used to identify mail pieces they contain. There are three categories of practical interest:

- mail pieces are uniquely identified and listed in the SMS;
- mail pieces are uniquely identified, the identifiers are within defined ranges and only the ranges are captured in the SMS;
- mail pieces are not uniquely identified, but they share one or more common attributes (which indicates that they belong to a aggregate).

Any mailing submission may include mail items from any or all categories described above. The following table illustrates the possible combinations:

Table A.1

Example	Uniquely identified	Range	Not uniquely identified
A1			✓
A2		✓	
A3		✓	✓
A4	✓		
A5	✓		✓
A6	✓	✓	
A7	✓	✓	✓

In Table A.1, only examples A1, A2 and A4 are distinct. The other four examples (A3, A5, A6 and A7) are combinations of the other examples and they can be implemented using the elements described in A1, A2 and A4.

Examples in this annex contain both the XML document and a snapshot of the file being displayed using an XML editor. The XML documents in this example are valid when checked against the XML schema described throughout this document and listed in ?.

The use of this particular XML editor does not constitute an endorsement.

A.1 Identical postcards

The submission contains 10 000 identical postcards. The postcards do not carry unique IDs. The mailer delivers the postcards in 25 trays, each containing 400 postcards. Each tray is identified (for example, from 1 to 25). All trays are placed in a roller cage.

- Mail units:
  - Mail unit list contains 26 elements:
    - 1 element: roller cage (ID)
    - 25 elements: trays (IDs, attributes, contained in identified roller cage)
  - Outer mail units list contains 1 element:
    - 1 element: roller cage, 1
- Aggregates:
  - Aggregate list contains 1 element:
    - 1 element: MU set with a count of 10 000 contained in the roller cage (ID)

NOTE The mail unit which fully contains the aggregate is the roller cage.

A.1.1 Text of the XML document:

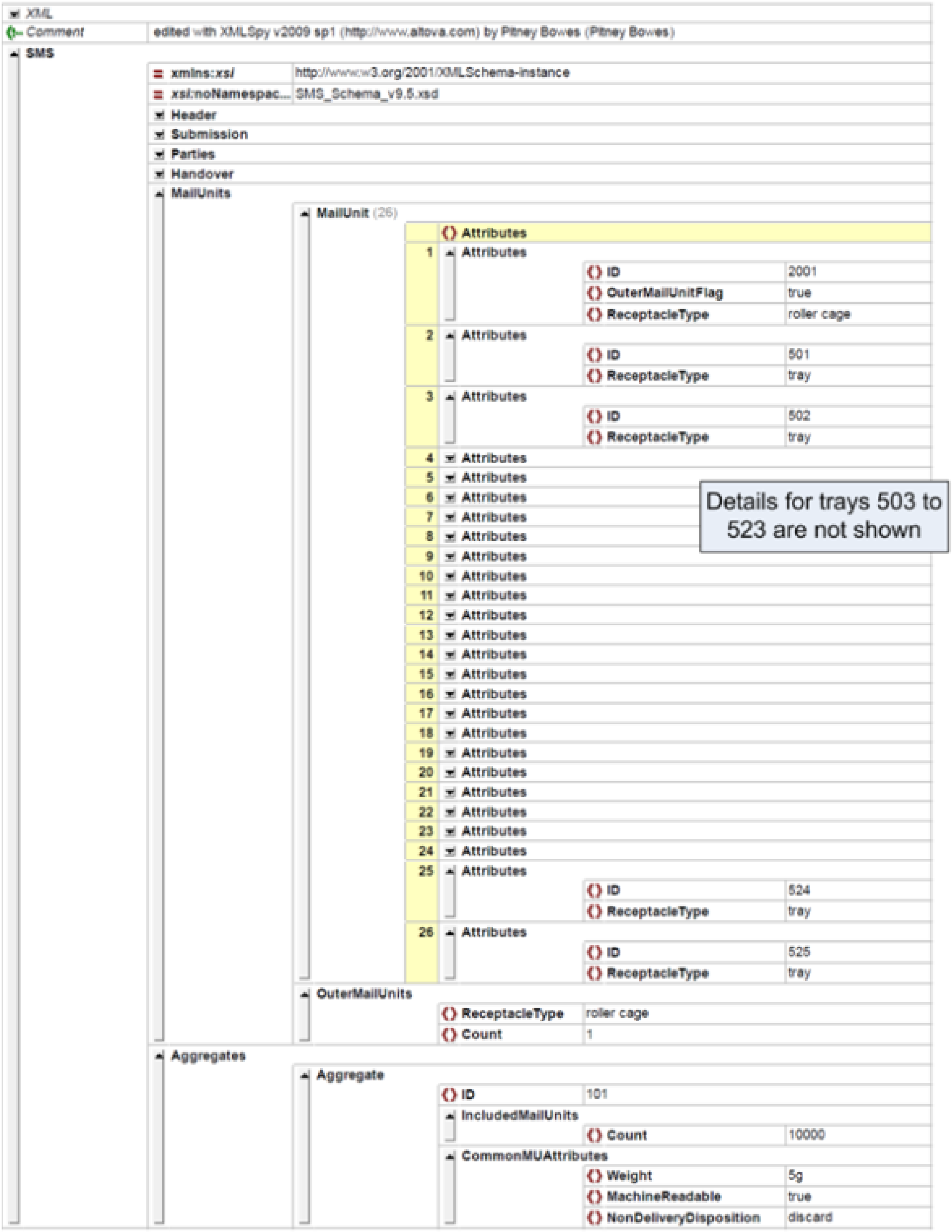
```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2009 sp1 (http://www.altova.com) by Andrei Obrea (Pitney
Bowes) -->
<SMS                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="SMS_Schema_v9.5.xsd">
   <Header>
      <MessageID/>
      <Version/>
      <TestCaseFlag/>
      <CreationDate/>
      <Recipient/>
      <DocumentSubmitter>
         <ID/>
         <Name/>
         <Contact>
            <FirstName/>
         </Contact>
      </DocumentSubmitter>
      <SoftwareSource>
         <SystemName/>
      </SoftwareSource>
   </Header>
   <Submission>
      <PostalSubmissionIdentifier>
         <SubmissionID/>
      </PostalSubmissionIdentifier>
      <LegallyBindingFlag/>
      <Description/>
      <SequenceNumber/>
      <LastSubmissionFlag/>
      <ReferencedSubmission>
         <PostalSubmissionIdentifier>
            <SubmissionID/>
         </PostalSubmissionIdentifier>
      </ReferencedSubmission>
      <AccompanyingDocument>
         <ID/>
         <Name/>
         <Type/>
      </AccompanyingDocument>
      <Contract>
         <ID/>
         <Type/>
         <Date/>
         <Payment>
            <Description/>
            <Account>
               <ID/>
               <HolderOfAccount/>
               <IBAN/>
               <FinancialInstitution/>
               <BankCode/>
               <BIC/>
            </Account>
         </Payment>
      </Contract>
   </Submission>
```

```
<Parties>
   <Originator>
      <ID/>
      <Name/>
      <Contact>
         <FirstName/>
      </Contact>
   </Originator>
   <Submitter>
      <ID/>
      <Name/>
      <Contact>
         <FirstName/>
      </Contact>
   </Submitter>
   <Payer>
      <ID/>
      <Name/>
      <Contact>
         <FirstName/>
      </Contact>
   </Payer>
   <Other>
      <ID/>
      <Name/>
      <PartyRole/>
      <Contact>
         <FirstName/>
      </Contact>
   </Other>
</Parties>
<Handover>
   <AtCustomerFlag/>
   <Location>
      <ID/>
      <Address/>
   </Location>
   <EarliestDate/>
   <LatestDate/>
</Handover>
<MailUnits>
   <MailUnit>
      <Attributes>
         <ID>2001</ID>
         <OuterMailUnitFlag>true</OuterMailUnitFlag>
         <ReceptacleType>roller cage</ReceptacleType>
      </Attributes>
   </MailUnit>
   <MailUnit>
      <Attributes>
         <ID>501</ID>
         <ReceptacleType>tray</ReceptacleType>
      </Attributes>
   </MailUnit>
   <MailUnit>
      <Attributes>
         <ID>502</ID>
         <ReceptacleType>tray</ReceptacleType>
      </Attributes>
```

```
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>503</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>504</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>505</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>506</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>507</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>508</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>509</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>510</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>511</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>512</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>513</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>514</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>515</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>516</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>517</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>518</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>519</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>520</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>521</ID>
      <ReceptacleType>tray</ReceptacleType>
   </Attributes>
</MailUnit>
<MailUnit>
   <Attributes>
      <ID>522</ID>
```

```
            <ReceptacleType>tray</ReceptacleType>
         </Attributes>
      </MailUnit>
      <MailUnit>
         <Attributes>
            <ID>523</ID>
            <ReceptacleType>tray</ReceptacleType>
         </Attributes>
      </MailUnit>
      <MailUnit>
         <Attributes>
            <ID>524</ID>
            <ReceptacleType>tray</ReceptacleType>
         </Attributes>
      </MailUnit>
      <MailUnit>
         <Attributes>
            <ID>525</ID>
            <ReceptacleType>tray</ReceptacleType>
         </Attributes>
      </MailUnit>
      <OuterMailUnits>
         <ReceptacleType>roller cage</ReceptacleType>
         <Count>1</Count>
      </OuterMailUnits>
   </MailUnits>
   <Aggregates>
      <Aggregate>
         <ID>101</ID>
         <IncludedMailUnits>
            <Count>10000</Count>
         </IncludedMailUnits>
         <CommonMUAttributes>
            <Weight>5g</Weight>
            <MachineReadable>true</MachineReadable>
            <NonDeliveryDisposition>discard</NonDeliveryDisposition>
         </CommonMUAttributes>
      </Aggregate>
   </Aggregates>
</SMS>
```

A.1.2 Screen snapshot of XML document



```
XML
Comment   edited with XMLSpy v2009 sp1 (http://www.altova.com) by Pitney Bowes (Pitney Bowes)
SMS
    xmlns:xsi            http://www.w3.org/2001/XMLSchema-instance
    xsi:noNamespac...    SMS_Schema_v9.5.xsd
    Header
    Submission
    Parties
    Handover
    MailUnits
        MailUnit (26)
                 Attributes
             1   Attributes
                     ID                  2001
                     OuterMailUnitFlag   true
                     ReceptacleType      roller cage
             2   Attributes
                     ID                  501
                     ReceptacleType      tray
             3   Attributes
                     ID                  502
                     ReceptacleType      tray
             4   Attributes
             5   Attributes
             6   Attributes
             7   Attributes
             8   Attributes
             9   Attributes
            10   Attributes
            11   Attributes
            12   Attributes
            13   Attributes
            14   Attributes
            15   Attributes
            16   Attributes
            17   Attributes
            18   Attributes
            19   Attributes
            20   Attributes
            21   Attributes
            22   Attributes
            23   Attributes
            24   Attributes
            25   Attributes
                     ID                  524
                     ReceptacleType      tray
            26   Attributes
                     ID                  525
                     ReceptacleType      tray
        OuterMailUnits
                 ReceptacleType      roller cage
                 Count               1
    Aggregates
        Aggregate
                 ID                  101
                 IncludedMailUnits
                     Count               10000
                 CommonMUAttributes
                     Weight                   5g
                     MachineReadable          true
                     NonDeliveryDisposition   discard
```

Details for trays 503 to 523 are not shown

Figure A.1

A.2 First class envelopes with ranges of unique identifiers

The submission contains 600 uniquely identified first class envelopes. The identifiers are serialized and they span two ranges: the first range is from 500 to 899 and the second range is from 1 100 to 1 299. The mailer delivers the submission in three trays. The first two trays contain the envelopes in the first range and the third tray contains the envelopes in the second range.

- Mail units:
    - Mail unit list contains 3 elements:
        - 3 elements: trays (IDs, attributes)
    - Outer mail units list contains 1 element:
        - 1 elements: tray, 3
- Aggregates:
    - Aggregate list contains 2 elements:
        - 2 elements: MU set with ID in a range with the first ID = 500 and last ID = 899 is contained in the first and second trays; MU set with ID in a range from 1 100 to 1 299 is contained in the third tray.

NOTE In this example it was possible to identify the trays containing each MU set. In other cases, trays may contain MEs from more than one set. In those cases it is not possible to identify the tray which contains the set.

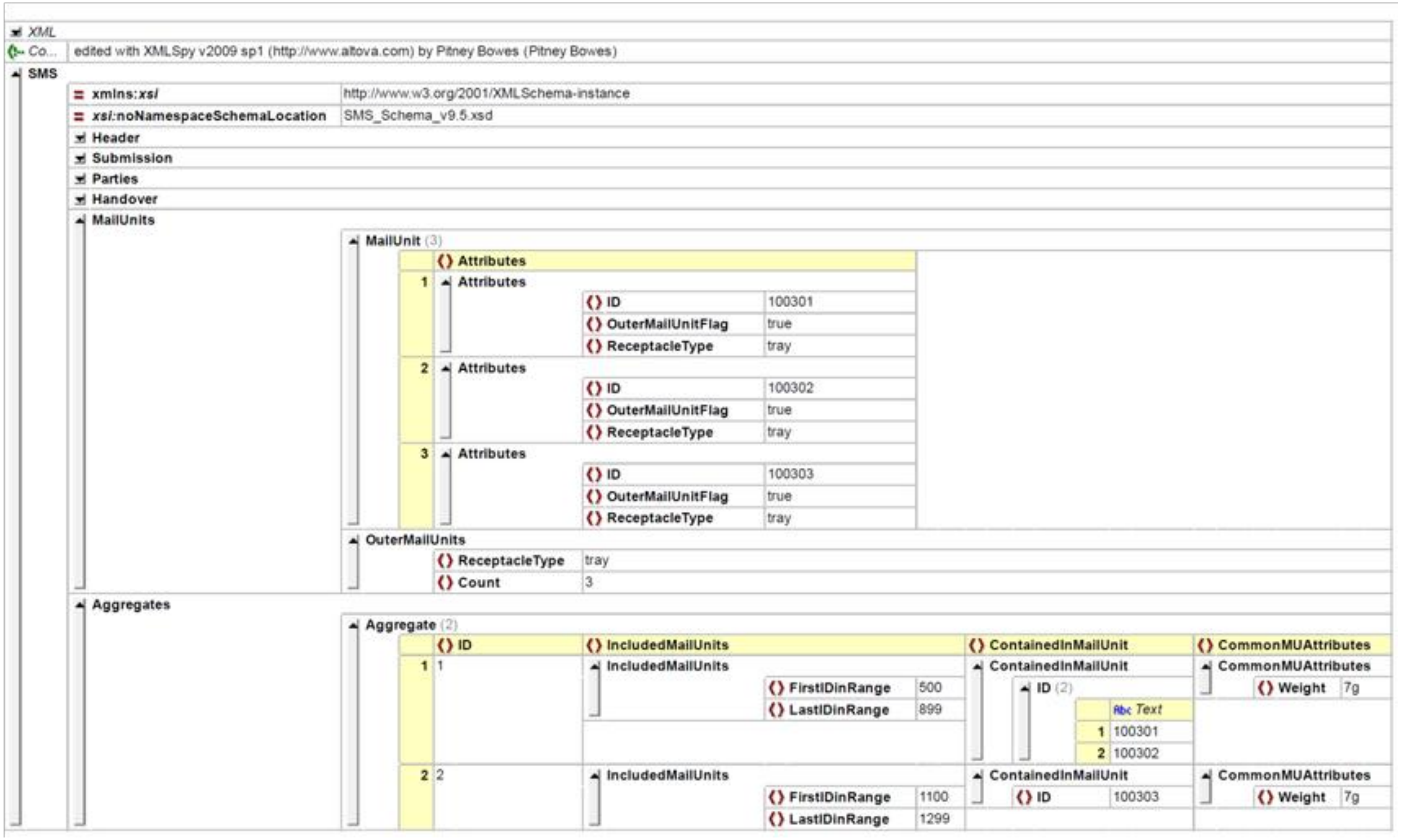
A.2.1 Text of the XML document:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2009 sp1 (http://www.altova.com) by Andrei Obrea (Pitney
Bowes) -->
<SMS                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="SMS_Schema_v9.5.xsd">
   <Header>
      <MessageID/>
      <Version/>
      <TestCaseFlag/>
      <CreationDate/>
      <Recipient/>
      <DocumentSubmitter>
         <ID/>
         <Name/>
         <Contact>
            <FirstName/>
         </Contact>
      </DocumentSubmitter>
      <SoftwareSource>
         <SystemName/>
      </SoftwareSource>
   </Header>
   <Submission>
      <PostalSubmissionIdentifier>
         <SubmissionID/>
      </PostalSubmissionIdentifier>
      <LegallyBindingFlag/>
      <Description/>
      <SequenceNumber/>
      <LastSubmissionFlag/>
      <ReferencedSubmission>
         <PostalSubmissionIdentifier>
            <SubmissionID/>
         </PostalSubmissionIdentifier>
      </ReferencedSubmission>
      <AccompanyingDocument>
         <ID/>
         <Name/>
         <Type/>
      </AccompanyingDocument>
      <Contract>
         <ID/>
         <Type/>
         <Date/>
         <Payment>
            <Description/>
            <Account>
               <ID/>
               <HolderOfAccount/>
               <IBAN/>
               <FinancialInstitution/>
               <BankCode/>
               <BIC/>
            </Account>
         </Payment>
      </Contract>
   </Submission>
```

```
<Parties>
   <Originator>
      <ID/>
      <Name/>
      <Contact>
         <FirstName/>
      </Contact>
   </Originator>
   <Submitter>
      <ID/>
      <Name/>
      <Contact>
         <FirstName/>
      </Contact>
   </Submitter>
   <Payer>
      <ID/>
      <Name/>
      <Contact>
         <FirstName/>
      </Contact>
   </Payer>
   <Other>
      <ID/>
      <Name/>
      <PartyRole/>
      <Contact>
         <FirstName/>
      </Contact>
   </Other>
</Parties>
<Handover>
   <AtCustomerFlag/>
   <Location>
      <ID/>
      <Address/>
   </Location>
   <EarliestDate/>
   <LatestDate/>
</Handover>
<MailUnits>
   <MailUnit>
      <Attributes>
         <ID>100301</ID>
         <OuterMailUnitFlag>true</OuterMailUnitFlag>
         <ReceptacleType>tray</ReceptacleType>
      </Attributes>
   </MailUnit>
   <MailUnit>
      <Attributes>
         <ID>100302</ID>
         <OuterMailUnitFlag>true</OuterMailUnitFlag>
         <ReceptacleType>tray</ReceptacleType>
      </Attributes>
   </MailUnit>
   <MailUnit>
      <Attributes>
         <ID>100303</ID>
         <OuterMailUnitFlag>true</OuterMailUnitFlag>
```

```
            <ReceptacleType>tray</ReceptacleType>
         </Attributes>
      </MailUnit>
      <OuterMailUnits>
         <ReceptacleType>tray</ReceptacleType>
         <Count>3</Count>
      </OuterMailUnits>
   </MailUnits>
   <Aggregates>
      <Aggregate>
         <ID>1</ID>
         <IncludedMailUnits>
            <FirstIDinRange>500</FirstIDinRange>
            <LastIDinRange>899</LastIDinRange>
         </IncludedMailUnits>
         <ContainedInMailUnit>
            <ID>100301</ID>
            <ID>100302</ID>
         </ContainedInMailUnit>
         <CommonMUAttributes>
            <Weight>7g</Weight>
         </CommonMUAttributes>
      </Aggregate>
      <Aggregate>
         <ID>2</ID>
         <IncludedMailUnits>
            <FirstIDinRange>1100</FirstIDinRange>
            <LastIDinRange>1299</LastIDinRange>
         </IncludedMailUnits>
         <ContainedInMailUnit>
            <ID>100303</ID>
         </ContainedInMailUnit>
         <CommonMUAttributes>
            <Weight>7g</Weight>
         </CommonMUAttributes>
      </Aggregate>
   </Aggregates>
</SMS>
```

A.2.2 Screen snapshot of XML document



```
XML
Co...  edited with XMLSpy v2009 sp1 (http://www.altova.com) by Pitney Bowes (Pitney Bowes)
SMS
   = xmlns:xsi                       http://www.w3.org/2001/XMLSchema-instance
   = xsi:noNamespaceSchemaLocation   SMS_Schema_v9.5.xsd
   Header
   Submission
   Parties
   Handover
   MailUnits
                                     MailUnit (3)
                                           () Attributes
                                        1  Attributes
                                                       () ID                   100301
                                                       () OuterMailUnitFlag    true
                                                       () ReceptacleType       tray
                                        2  Attributes
                                                       () ID                   100302
                                                       () OuterMailUnitFlag    true
                                                       () ReceptacleType       tray
                                        3  Attributes
                                                       () ID                   100303
                                                       () OuterMailUnitFlag    true
                                                       () ReceptacleType       tray
                                     OuterMailUnits
                                           () ReceptacleType  tray
                                           () Count           3
   Aggregates
                                     Aggregate (2)
                                           () ID   () IncludedMailUnits                     () ContainedInMailUnit        () CommonMUAttributes
                                        1  1       IncludedMailUnits                        ContainedInMailUnit           CommonMUAttributes
                                                            () FirstIDinRange   500            ID (2)                        () Weight  7g
                                                            () LastIDinRange    899                       Text
                                                                                                        1 100301
                                                                                                        2 100302
                                        2  2       IncludedMailUnits                        ContainedInMailUnit           CommonMUAttributes
                                                            () FirstIDinRange   1100           () ID   100303                () Weight  7g
                                                            () LastIDinRange    1299
```

Figure A.2

A.3 Uniquely identified first class envelopes

The submission contains 10 000 first class uniquely identified envelopes. The mailer delivers the envelopes in 40 uniquely identified trays, each carrying 250 envelopes. The trays are placed in two uniquely identified roller cages.

- Mail units:
  - Mail unit list contains 10 042 elements:
    - 2 elements: roller cage (ID, attributes)
    - 40 elements: tray (ID, attributes, contained in identified roller cage)
    - 10 000 elements: envelope (ID, attributes, contained in identified tray)
  - Outer mail units list contains 1 element:
    - 1 elements: roller cage, 2
- Aggregates:
  - Aggregate list contains 1 element:
    - 1 element: ME set with a count of 10 000

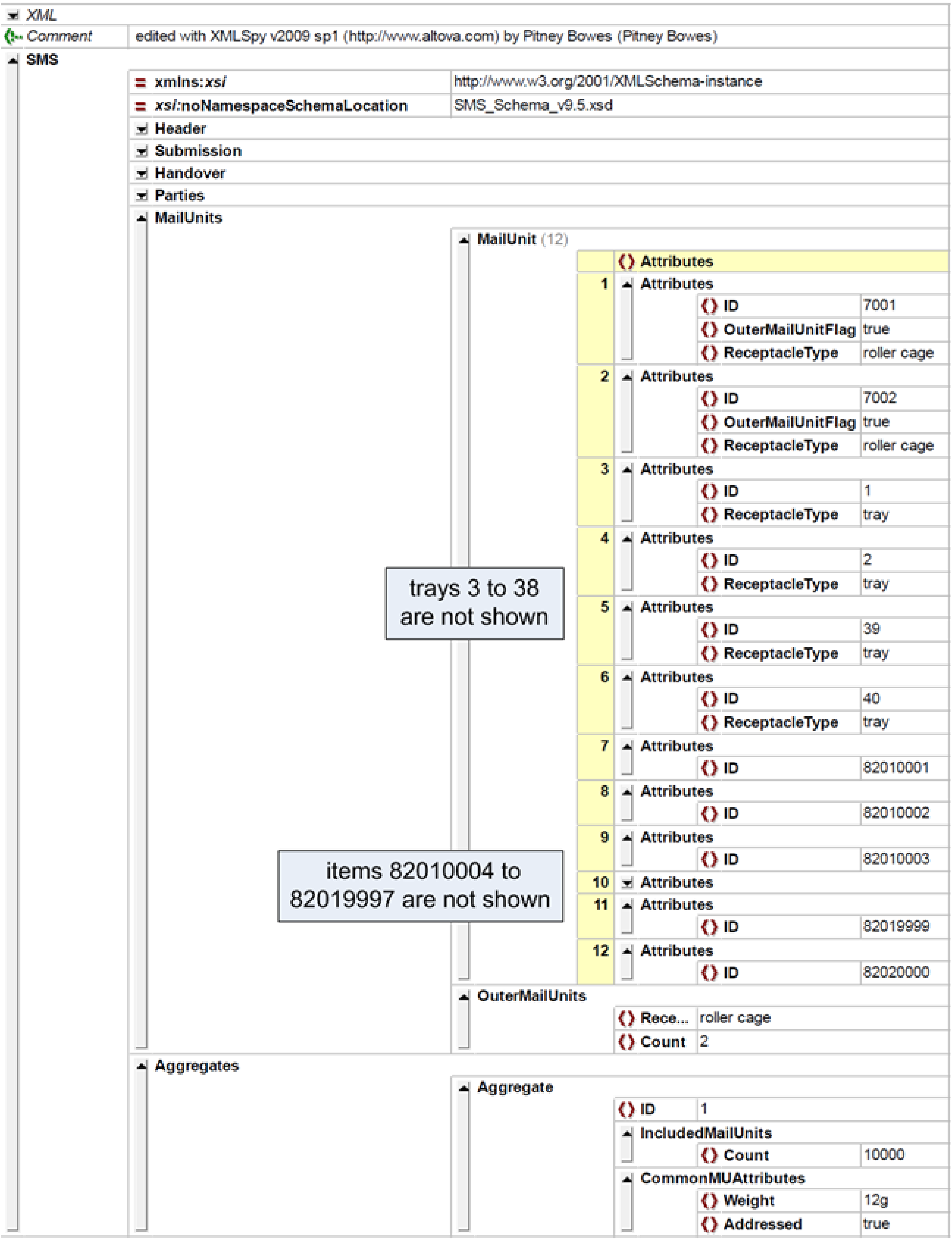
A.3.1 Text of the XML document:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2009 sp1 (http://www.altova.com) by Andrei Obrea (Pitney
Bowes) -->
<SMS                         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="SMS_Schema_v9.5.xsd">
    <Header>
        <MessageID/>
        <Version/>
        <TestCaseFlag/>
        <CreationDate/>
        <Recipient/>
        <DocumentSubmitter>
            <ID/>
            <Name/>
            <Contact>
                <FirstName/>
            </Contact>
        </DocumentSubmitter>
        <SoftwareSource>
            <SystemName/>
        </SoftwareSource>
    </Header>
    <Submission>
        <PostalSubmissionIdentifier>
            <SubmissionID/>
        </PostalSubmissionIdentifier>
        <LegallyBindingFlag/>
        <Description/>
        <SequenceNumber/>
```

```
      <LastSubmissionFlag/>
      <ReferencedSubmission>
         <PostalSubmissionIdentifier>
            <SubmissionID/>
         </PostalSubmissionIdentifier>
      </ReferencedSubmission>
      <AccompanyingDocument>
         <ID/>
         <Name/>
         <Type/>
      </AccompanyingDocument>
      <Contract>
         <ID/>
         <Type/>
         <Date/>
         <Payment>
            <Description/>
            <Account>
               <ID/>
               <HolderOfAccount/>
               <IBAN/>
               <FinancialInstitution/>
               <BankCode/>
               <BIC/>
            </Account>
         </Payment>
      </Contract>
   </Submission>
   <Handover>
      <AtCustomerFlag/>
      <Location>
         <ID/>
         <Address/>
      </Location>
      <EarliestDate/>
      <LatestDate/>
   </Handover>
   <Parties>
      <Originator>
         <ID/>
         <Name/>
         <Contact>
            <FirstName/>
         </Contact>
      </Originator>
      <Submitter>
         <ID/>
         <Name/>
         <Contact>
            <FirstName/>
         </Contact>
      </Submitter>
      <Payer>
         <ID/>
         <Name/>
         <Contact>
            <FirstName/>
         </Contact>
      </Payer>
```

```
         <Other>
            <ID/>
            <Name/>
            <PartyRole/>
            <Contact>
               <FirstName/>
            </Contact>
         </Other>
      </Parties>
      <MailUnits>
         <MailUnit>
            <Attributes>
               <ID>7001</ID>
               <OuterMailUnitFlag>true</OuterMailUnitFlag>
               <ReceptacleType>roller cage</ReceptacleType>
            </Attributes>
         </MailUnit>
         <MailUnit>
            <Attributes>
               <ID>7002</ID>
               <OuterMailUnitFlag>true</OuterMailUnitFlag>
               <ReceptacleType>roller cage</ReceptacleType>
            </Attributes>
         </MailUnit>
         <MailUnit>
            <Attributes>
               <ID>1</ID>
               <ReceptacleType>tray</ReceptacleType>
            </Attributes>
         </MailUnit>
         <MailUnit>
            <Attributes>
               <ID>2</ID>
               <ReceptacleType>tray</ReceptacleType>
            </Attributes>
         </MailUnit>
         <MailUnit>
            <Attributes>
               <ID>39</ID>
               <ReceptacleType>tray</ReceptacleType>
            </Attributes>
         </MailUnit>
         <MailUnit>
            <Attributes>
               <ID>40</ID>
               <ReceptacleType>tray</ReceptacleType>
            </Attributes>
         </MailUnit>
         <MailUnit>
            <Attributes>
               <ID>82010001</ID>
            </Attributes>
         </MailUnit>
         <MailUnit>
            <Attributes>
               <ID>82010002</ID>
            </Attributes>
         </MailUnit>
         <MailUnit>
         <Attributes>
            <ID>82010003</ID>
         </Attributes>
      </MailUnit>
      <MailUnit>
         <Attributes>
            <ID>82019998</ID>
         </Attributes>
      </MailUnit>
      <MailUnit>
         <Attributes>
            <ID>82019999</ID>
         </Attributes>
      </MailUnit>
      <MailUnit>
         <Attributes>
            <ID>82020000</ID>
         </Attributes>
      </MailUnit>
      <OuterMailUnits>
         <ReceptacleType>roller cage</ReceptacleType>
         <Count>2</Count>
      </OuterMailUnits>
   </MailUnits>
   <Aggregates>
      <Aggregate>
         <ID>1</ID>
         <IncludedMailUnits>
            <Count>10000</Count>
         </IncludedMailUnits>
         <CommonMUAttributes>
            <Weight>12g</Weight>
            <Addressed>true</Addressed>
         </CommonMUAttributes>
      </Aggregate>
   </Aggregates>
</SMS>
```

A.3.2 Screen snapshot of XML document



```
XML
Comment    edited with XMLSpy v2009 sp1 (http://www.altova.com) by Pitney Bowes (Pitney Bowes)
SMS
    = xmlns:xsi                        http://www.w3.org/2001/XMLSchema-instance
    = xsi:noNamespaceSchemaLocation    SMS_Schema_v9.5.xsd
    Header
    Submission
    Handover
    Parties
    MailUnits
        MailUnit (12)
                () Attributes
            1   Attributes
                    () ID                  7001
                    () OuterMailUnitFlag   true
                    () ReceptacleType      roller cage
            2   Attributes
                    () ID                  7002
                    () OuterMailUnitFlag   true
                    () ReceptacleType      roller cage
            3   Attributes
                    () ID                  1
                    () ReceptacleType      tray
            4   Attributes
                    () ID                  2
                    () ReceptacleType      tray
            5   Attributes
                    () ID                  39
                    () ReceptacleType      tray
            6   Attributes
                    () ID                  40
                    () ReceptacleType      tray
            7   Attributes
                    () ID                  82010001
            8   Attributes
                    () ID                  82010002
            9   Attributes
                    () ID                  82010003
            10  Attributes
            11  Attributes
                    () ID                  82019999
            12  Attributes
                    () ID                  82020000
        OuterMailUnits
                () Rece...   roller cage
                () Count     2
    Aggregates
        Aggregate
                () ID        1
                IncludedMailUnits
                    () Count             10000
                CommonMUAttributes
                    () Weight            12g
                    () Addressed         true
```

trays 3 to 38 are not shown

items 82010004 to 82019997 are not shown

Figure A.3

Annex B
(informative)

Text of the XML Schema for SMS

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2009 sp1 (http://www.altova.com) by Andrei Obrea (Pitney
Bowes) -->
<xs:schema                            xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
   <xs:element name="SMS">
      <xs:complexType>
         <xs:all>
            <xs:element name="Header">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="MessageID"/>
                     <xs:element name="Version"/>
                     <xs:element name="TestCaseFlag"/>
                     <xs:element name="CreationDate"/>
                     <xs:element name="Recipient"/>
                     <xs:element name="DocumentSubmitter">
                        <xs:complexType>
                           <xs:all>
                              <xs:element name="ID"/>
                              <xs:element name="Name"/>
                              <xs:element name="Contact">
                                 <xs:complexType>
                                    <xs:choice>
                                       <xs:element name="FirstName"/>
                                       <xs:element name="LastName"/>
                                       <xs:element name="Role"/>
                                       <xs:element name="Position"/>
                                       <xs:element name="Department"/>
                                       <xs:element name="Address"/>
                                       <xs:element name="Email"/>
                                       <xs:element name="Phone"/>
                                       <xs:element name="Fax"/>
                                    </xs:choice>
                                 </xs:complexType>
                              </xs:element>
                           </xs:all>
                        </xs:complexType>
                     </xs:element>
                     <xs:element name="SoftwareSource">
                        <xs:complexType>
                           <xs:choice>
                              <xs:element name="SystemName"/>
                              <xs:element name="SystemVersion"/>
                              <xs:element name="CertificationDate"/>
                           </xs:choice>
                        </xs:complexType>
                     </xs:element>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
```

```
<xs:element name="Submission">
   <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
         <xs:choice>
            <xs:element name="PostalSubmissionIdentifier">
               <xs:complexType>
                  <xs:all>
                     <xs:element name="SubmissionID"/>
                  </xs:all>
               </xs:complexType>
            </xs:element>
            <xs:element name="MailerSubmissionIdentifier">
               <xs:complexType>
                  <xs:all>
                     <xs:element name="SubmissionID"/>
                     <xs:element name="MailerID"/>
                  </xs:all>
               </xs:complexType>
            </xs:element>
         </xs:choice>
         <xs:element name="LegallyBindingFlag"/>
         <xs:element name="Description"/>
         <xs:element name="SequenceNumber"/>
         <xs:element name="LastSubmissionFlag"/>
         <xs:element name="ReferencedSubmission">
            <xs:complexType>
               <xs:choice>
                  <xs:element name="PostalSubmissionIdentifier">
                     <xs:complexType>
                        <xs:all>
                           <xs:element name="SubmissionID"/>
                        </xs:all>
                     </xs:complexType>
                  </xs:element>
                  <xs:element name="MailerSubmissionIdentifier">
                     <xs:complexType>
                        <xs:all>
                           <xs:element name="SubmissionID"/>
                           <xs:element name="MailerID"/>
                        </xs:all>
                     </xs:complexType>
                  </xs:element>
               </xs:choice>
            </xs:complexType>
         </xs:element>
         <xs:element name="AccompanyingDocument">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="ID"/>
                  <xs:element name="Name"/>
                  <xs:element name="Type"/>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
         <xs:element name="Contract">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="ID"/>
                  <xs:element name="Type"/>
```

```
                              <xs:element name="Date"/>
                              <xs:element name="Payment">
                                 <xs:complexType>
                                    <xs:sequence>
                                       <xs:element name="Description"/>
                                       <xs:element name="Account">
                                          <xs:complexType>
                                             <xs:all>
                                                <xs:element name="ID"/>
                                                <xs:element

name="HolderOfAccount"/>
                                                <xs:element name="IBAN"/>
                                                <xs:element

name="FinancialInstitution"/>
                                                <xs:element
name="BankCode"/>
                                                <xs:element name="BIC"/>
                                             </xs:all>
                                          </xs:complexType>
                                       </xs:element>
                                    </xs:sequence>
                                 </xs:complexType>
                              </xs:element>
                           </xs:sequence>
                        </xs:complexType>
                     </xs:element>
                  </xs:choice>
               </xs:complexType>
            </xs:element>
            <xs:element name="Parties">
               <xs:complexType>
                  <xs:choice minOccurs="0" maxOccurs="unbounded">
                     <xs:element name="Originator">
                        <xs:complexType>
                           <xs:all>
                              <xs:element name="ID"/>
                              <xs:element name="Name"/>
                              <xs:element name="Contact">
                                 <xs:complexType>
                                    <xs:choice>
                                       <xs:element name="FirstName"/>
                                       <xs:element name="LastName"/>
                                       <xs:element name="Role"/>
                                       <xs:element name="Position"/>
                                       <xs:element name="Department"/>
                                       <xs:element name="Address"/>
                                       <xs:element name="Email"/>
                                       <xs:element name="Phone"/>
                                       <xs:element name="Fax"/>
                                    </xs:choice>
                                 </xs:complexType>
                              </xs:element>
                           </xs:all>
                        </xs:complexType>
                     </xs:element>
                     <xs:element name="Submitter">
                        <xs:complexType>
```

```
      <xs:all>
         <xs:element name="ID"/>
         <xs:element name="Name"/>
         <xs:element name="Contact">
            <xs:complexType>
               <xs:choice>
                  <xs:element name="FirstName"/>
                  <xs:element name="LastName"/>
                  <xs:element name="Role"/>
                  <xs:element name="Position"/>
                  <xs:element name="Department"/>
                  <xs:element name="Address"/>
                  <xs:element name="Email"/>
                  <xs:element name="Phone"/>
                  <xs:element name="Fax"/>
               </xs:choice>
            </xs:complexType>
         </xs:element>
      </xs:all>
   </xs:complexType>
</xs:element>
<xs:element name="Payer">
   <xs:complexType>
      <xs:all>
         <xs:element name="ID"/>
         <xs:element name="Name"/>
         <xs:element name="Contact">
            <xs:complexType>
               <xs:choice>
                  <xs:element name="FirstName"/>
                  <xs:element name="LastName"/>
                  <xs:element name="Role"/>
                  <xs:element name="Position"/>
                  <xs:element name="Department"/>
                  <xs:element name="Address"/>
                  <xs:element name="Email"/>
                  <xs:element name="Phone"/>
                  <xs:element name="Fax"/>
               </xs:choice>
            </xs:complexType>
         </xs:element>
      </xs:all>
   </xs:complexType>
</xs:element>
<xs:element name="Other" maxOccurs="unbounded">
   <xs:complexType>
      <xs:all>
         <xs:element name="ID"/>
         <xs:element name="Name"/>
         <xs:element name="PartyRole"/>
         <xs:element name="Contact">
            <xs:complexType>
               <xs:choice>
                  <xs:element name="FirstName"/>
                  <xs:element name="LastName"/>
                  <xs:element name="Role"/>
                  <xs:element name="Position"/>
                  <xs:element name="Department"/>
                  <xs:element name="Address"/>
```

```
                                           <xs:element name="Email"/>
                                           <xs:element name="Phone"/>
                                           <xs:element name="Fax"/>
                                        </xs:choice>
                                     </xs:complexType>
                                 </xs:element>
                              </xs:all>
                           </xs:complexType>
                       </xs:element>
                    </xs:choice>
                 </xs:complexType>
             </xs:element>
             <xs:element name="Handover">
                 <xs:complexType>
                    <xs:choice minOccurs="0" maxOccurs="unbounded">
                       <xs:element name="AtCustomerFlag"/>
                       <xs:element name="Location">
                           <xs:complexType>
                              <xs:sequence>
                                 <xs:element name="ID"/>
                                 <xs:element name="Address"/>
                              </xs:sequence>
                           </xs:complexType>
                       </xs:element>
                       <xs:element name="EarliestDate"/>
                       <xs:element name="LatestDate"/>
                    </xs:choice>
                 </xs:complexType>
             </xs:element>
             <xs:element name="Aggregates">
                 <xs:complexType>
                    <xs:sequence>
                       <xs:element name="Aggregate" maxOccurs="unbounded">
                           <xs:complexType>
                              <xs:choice maxOccurs="unbounded">
                                 <xs:element name="ID">
                                     <xs:annotation>
                                        <xs:documentation>set
ID</xs:documentation>
                                     </xs:annotation>
                                 </xs:element>
                                 <xs:element name="Description"/>
                                 <xs:element name="TotalWeight">
                                     <xs:annotation>
                                        <xs:documentation>redundant,   used   for
cross-

check</xs:documentation>
                                     </xs:annotation>
                                 </xs:element>
                                 <xs:element name="TotalAmount">
                                     <xs:annotation>
                                        <xs:documentation>redundant,   used   for
cross-

check</xs:documentation>
                                     </xs:annotation>
                                 </xs:element>
                                 <xs:element name="PostalProduct">
```

```
                                    <xs:complexType>
                                        <xs:all>
                                           <xs:element name="ProductNumber"/>
                                           <xs:element
name="EarliestDeliveryDate"/>
                                           <xs:element
name="LatestDeliveryDate"/>
                                        </xs:all>
                                    </xs:complexType>
                                 </xs:element>
                                 <xs:element             name="IncludedMailUnits"
maxOccurs="unbounded">
                                    <xs:annotation>
                                        <xs:documentation>identifiers  (or  count)
of the mail units

included in this aggregate</xs:documentation>
                                    </xs:annotation>
                                    <xs:complexType>
                                        <xs:choice maxOccurs="unbounded">
                                           <xs:element name="ID"/>
                                           <xs:element name="Count"/>
                                           <xs:element name="FirstIDinRange"/>
                                           <xs:element name="LastIDinRange"/>
                                        </xs:choice>
                                    </xs:complexType>
                                 </xs:element>
                                 <xs:element name="ContainedInMailUnit">
                                    <xs:annotation>
                                        <xs:documentation>identifies  the  (higher
level) mail unit in

which this aggregate is contained</xs:documentation>
                                    </xs:annotation>
                                    <xs:complexType>
                                        <xs:sequence>
                                           <xs:element                  name="ID"
maxOccurs="unbounded"/>
                                        </xs:sequence>
                                    </xs:complexType>
                                 </xs:element>
                                 <xs:element name="CommonMUAttributes">
                                    <xs:complexType>
                                        <xs:choice                  minOccurs="0"
maxOccurs="unbounded">
                                           <xs:element name="ReceptacleType"/>
                                           <xs:element
name="DestinationPostalCode"/>
                                           <xs:element name="Weight"/>
                                           <xs:element name="SortMethod"/>
                                           <xs:element name="StackableFlag"/>
                                           <xs:element name="Machinable"/>
                                           <xs:element name="MachineReadable"/>
                                           <xs:element name="Addressed"/>
                                           <xs:element name="EquipmentID"/>
                                           <xs:element name="EquipmentType"/>
                                           <xs:element name="Dimensions"/>
                                           <xs:element name="ItemFormFactor"/>
                                           <xs:element name="Length"/>
                                           <xs:element name="Width"/>
                                           <xs:element name="Thickness"/>
                                           <xs:element name="InsuredValue"/>
                                           <xs:element name="CODAmount"/>
                                           <xs:element
name="NonDeliveryDisposition"/>
                                           <xs:element name="Inserts">
                                               <xs:complexType>
                                                  <xs:choice>
                                                      <xs:element name="Type"/>
                                                      <xs:element name="Weight"/>
                                                      <xs:element
name="Thickness"/>
                                                      <xs:element name="Count"/>
                                                  </xs:choice>
                                               </xs:complexType>
                                           </xs:element>
                                           <xs:element name="Payment">
                                               <xs:complexType>
                                                  <xs:choice>
                                                      <xs:element name="Type"/>
                                                      <xs:element

name="PostageAsEvidenced"/>
                                                      <xs:element

name="FrankingMachineID"/>
                                                  </xs:choice>
                                               </xs:complexType>
                                           </xs:element>
                                           <xs:element name="OtherAttributes"

maxOccurs="unbounded"/>
                                        </xs:choice>
                                     </xs:complexType>
                                 </xs:element>
                              </xs:choice>
                           </xs:complexType>
                       </xs:element>
                    </xs:sequence>
                 </xs:complexType>
             </xs:element>
             <xs:element name="MailUnits">
                 <xs:complexType>
                    <xs:sequence>
                       <xs:element name="MailUnit" maxOccurs="unbounded">
                           <xs:complexType>
                              <xs:choice maxOccurs="unbounded">
                                 <xs:element name="Attributes">
                                     <xs:annotation>
                                        <xs:documentation>attributes  of  the  mail
unit including the

unique identifier (ID)</xs:documentation>
                                     </xs:annotation>
                                     <xs:complexType>
                                        <xs:choice maxOccurs="unbounded">
                                           <xs:element name="ID"/>
                                           <xs:element
name="DestinationPostalCode"/>
                                           <xs:element name="Weight"/>
                                           <xs:element name="Dimensions"/>
                                           <xs:element name="Length"/>
                                           <xs:element name="Width"/>
                                           <xs:element name="Thickness"/>
                                           <xs:element name="Machinable"/>
                                           <xs:element name="MachineReadable"/>
                                           <xs:element name="Addressed"/>
                                           <xs:element name="EquipmentID"/>
                                           <xs:element name="EquipmentType"/>
                                           <xs:element name="ItemFormFactor"/>
                                           <xs:element name="InsuredValue"/>
                                           <xs:element name="CODAmount"/>
                                           <xs:element
name="NonDeliveryDisposition"/>
                                           <xs:element name="Inserts">
                                              <xs:complexType>
                                                 <xs:choice>
                                                    <xs:element name="Type"/>
                                                    <xs:element name="Weight"/>
                                                    <xs:element
name="Thickness"/>
                                                    <xs:element name="Count"/>
                                                 </xs:choice>
                                              </xs:complexType>
                                           </xs:element>
                                           <xs:element name="PostalProduct">
                                              <xs:complexType>
                                                 <xs:all>
                                                    <xs:element

name="ProductNumber"/>
                                                    <xs:element

name="EarliestDeliveryDate"/>
                                                    <xs:element

name="LatestDeliveryDate"/>
                                                 </xs:all>
                                              </xs:complexType>
                                           </xs:element>
                                           <xs:element name="Payment">
                                              <xs:complexType>
                                                 <xs:choice>
                                                    <xs:element name="Type"/>
                                                    <xs:element

name="PostageAsEvidenced"/>
                                                    <xs:element

name="FrankingMachineID"/>
                                                 </xs:choice>
                                              </xs:complexType>
                                           </xs:element>
                                           <xs:element
name="OuterMailUnitFlag"/>
                                           <xs:element name="ReceptacleType"/>
```

```
                                       <xs:element name="SortMethod"/>
                                       <xs:element name="StackableFlag"/>
                                       <xs:element name="OtherAttributes"

maxOccurs="unbounded"/>
                                    </xs:choice>
                                 </xs:complexType>
                              </xs:element>
                              <xs:element name="ContainedInMailUnit">
                                 <xs:annotation>
                                    <xs:documentation>identifies  the  (higher
level) mail unit in

which this aggregate is contained </xs:documentation>
                                 </xs:annotation>
                                 <xs:complexType>
                                    <xs:choice>
                                       <xs:element name="ID"/>
                                    </xs:choice>
                                 </xs:complexType>
                              </xs:element>
                              <xs:element            name="IncludedAggregates"
maxOccurs="unbounded">
                                 <xs:annotation>
                                    <xs:documentation>identifies          the
aggreagtes which are fully or

partially included in this mail unit</xs:documentation>
                                 </xs:annotation>
                                 <xs:complexType>
                                    <xs:sequence>
                                       <xs:element name="ID"/>
                                       <xs:element name="Count"/>
                                       <xs:element name="PartialFlag"/>
                                    </xs:sequence>
                                 </xs:complexType>
                              </xs:element>
                           </xs:choice>
                        </xs:complexType>
                     </xs:element>
                     <xs:element name="OuterMailUnits" maxOccurs="unbounded">
                        <xs:complexType>
                           <xs:sequence>
                              <xs:element name="ReceptacleType"/>
                              <xs:element name="Count">
                                 <xs:annotation>
                                    <xs:documentation>.</xs:documentation>
                                 </xs:annotation>
                              </xs:element>
                           </xs:sequence>
                        </xs:complexType>
                     </xs:element>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
         </xs:all>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

Annex C
(informative)

Example of a protocol for secure communication of EEM

This annex describes an example of a secure protocol for communication of any suitable EEM, for example the SMS. The protocol allows authentication of the mailer or its agent that generated the EEM (data source) and protects integrity and confidentiality of the data contained in the EEM.

The process of mail generation/assembly and finishing in the CEM environment is assumed to be automated. It is also assumed that a typical mail assembly machine is computer controlled and equipped with a postal security device (PSD) that has been designed and built in accordance with postal security requirements (see EN 14615 and UPU S36-4 for details).

Finally it is also assumed that a public key cryptographic scheme with appropriate, carefully chosen values of security parameters, has been selected for use by a postal operator. This can be RSA, DSS or ECC or any other tested and trusted cryptographic scheme. Note that the choice of a cryptographic scheme for securing EEM in the CEM environment is far less critical that the choice of such a scheme for securing DPMs because there are no severe bandwidth and performance constraints requirements in the case of EEM compared to the case of DPM (see UPU S36-4 and EN 14615 for more detailed discussion).

In the following examples the Elliptic Curve Cryptography (ECC) scheme is used for the sake of concreteness. ECC is also widely accepted as the most economical of commonly used schemes. However the protocol that is described in this annex can be extended without difficulties to any other public key scheme.

Public parameters of the selected ECC scheme are assumed to be computed by the postal operator or a trusted third party and shared with all involved mailers, their agents and other interested parties.

C.1 Set up for ECDSA scheme

ECDSA makes use of the following mathematical objects:

— finite field F_q containing *q* elements, where q is either a prime number or an integral power of 2;

— elliptic curve E over F_q, being a set of points from the field F_q that satisfy a certain equation determined by two parameters *a* and *b*, which are also elements of the field F_q, for which the points on the curve form a cyclic group of prime order *n* with respect to a specially defined operation of addition;

NOTE NIST (USA) has published recommended elliptic curves. They have been tested and have no known weaknesses (http://csrc.nist.gov/publications/fips/index.htm).

— elliptic curve's point at infinity, denoted by ®;

— two underlying field elements denoted by x_p and y_p which define a base point $P = (x_p, y_p)$ on the curve E of prime order n. Common parameters shared between postal and mailer domain are (p, E, P, n).

1) Given these parameters, the postal operator computes two pairs of master keys, (K_pE, KE) and (K_pL, KL), where K_pE, and K_pL, are private keys known only to the postal operator and protected within the security perimeter of postal operations and where KE and KL are public keys distributed to PSD suppliers. These public keys KE and KL could be installed in all PSD prior to their installation at mailer' sites.

2) Given common parameters, a PSD connected to a mail assembly/finishing system of a mailer generates an ECDSA key pair as follows:

— private key, denoted by K_{pr}, is a statistically unique and unpredictable integer that is greater than 1 but less than *n* – 1, where *n* is the order of point P;

— corresponding public key, denoted by K_{pb} or (x_q,y_q), is the point on the curve E such that $K_{\text{pb}} = K_{\text{pr}}\ P$, i.e. one obtains K_{pb} by adding K_{pr} copies of the point P together.

For an SMS application, it is recommended that the domain parameters *q* and *n* satisfy the requirements recommended for all financial service industry applications, namely:

— $q > 2^{160}$ (but note that the United States National Institute of Science and Technology now recommends $q > 2^{190}$);

— $n > 2^{160}$.

3) The PSD sends K_{pb} together with mailer's *M* identity ID*M* to a postal operator secure certification server (postal certification server);

4) Certification server signs K_{pb} with its private master key K_{pL} using ECDSA, and creates X.509 certificate for K_{pb} denoted below as Cert (K_{pb} , ID*M*). The postal certification server sends the certificate Cert (K_{pb} , ID*M*) to the PSD.

5) Postal certification server distributes its master public keys KE and KL to all computers installed at controlled entry facilities of the postal operator that are expected to accept CEM.

C.2 Protocol

C.2.1 Part 1: Message generation

1) The PSD creates a session secret symmetric key K_{s} that can be used for any approved symmetric key cryptographic algorithm, for example triple DES or AES;

2) At the end of the mail preparation process and after completion of the accounting process the PSD encrypts plain text EEM selected for transmission to postal operator with the key K_{s} thus computing the cipher text E_{Ks} (EEM);

3) The PSD computes ECDSA-based digital signature of the EEM using its private key K_{pr} thus creating the cipher text DS_{Kpr} (EEM);

4) The PSD encrypts K_{s} with postal public key *KE* by computing the cipher text ECDSA_{KE} (K_{s});

5) The PSD composes communication message:

$$[\ \mathrm{E}_{\text{Ks}}\ (\text{EEM}),\ \text{ECDSA}_{\text{KE}}\ (K_s),\ \ \mathrm{DS}_{\text{Kpr}}\ (\text{EEM}),\ \text{Cert}\ (K_{\text{pb}}\ ,\ \text{ID}M\ )\ ]$$

and sends it to the postal controlled acceptance unit' computer and central archival server (if needed) of the postal operator.

C.2.2 Part 2: Message Verification

1) Controlled entry operation is presented with the physical mailing submission and (possibly some time before this in the case of pre-announcement of EEM) with the electronic message:

$$[\ \mathrm{E}_{\mathrm{Ks}}\ (\mathrm{EEM}),\ \mathrm{ECDSA}_{\mathrm{KE}}\ (K_{\mathrm{s}}),\ \mathrm{DS}_{\mathrm{Kpr}}\ (\mathrm{EEM}),\ \mathrm{Cert}\ (K_{\mathrm{pb}}\ ,\ \mathrm{ID}M\ )\ ].$$

2) Controlled entry computer verifies authenticity of the Cert (K_{pb} , IDM) by using public master key KL.

3) Controlled entry computer decrypts ECDSAKE (K_{s}) using K_{pE} and obtains K_{s}.

4) Postal controlled entry computer decrypts EK_{s} (EEM) with the *K*s and obtains plain text EEM.

5) Controlled entry computer verifies signature DSKpr(EEM) using the key K_{pb} and the plain text EEM.

Bibliography

[1] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997

[2] UPU M37, *Postal processing events and event reporting – Part A: General concepts and attribute definitions*

[3] EN 14142-1, *Postal services – Address databases – Part 1: Components of postal addresses*

[4] UPU S25, *Data constructs for the communication of information on postal items, batches and receptacles*

[5] UPU S27, *Framework for communication of information about postal items, batches and receptacles*

[6] UPU S36-4, *Digital Postage Marks (DPM) – Applications, Securityand Design*

[7] UPU M33, *Postal item attributes and the communication of item information*

[8] UPU M34, *Mail aggregate attributes and the communication of aggregate information*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™