

Postal services — Digital postage marks — Applications, security and design

The European Standard EN 14615:2005 has the status of a
British Standard

ICS 03.240

National foreword

This British Standard is the official English language version of EN 14615:2005.

The UK participation in its preparation was entrusted to Technical Committee SVS/4, Postal services, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

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

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

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

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 117 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 18 February 2005

© BSI 18 February 2005

ISBN 0 580 45451 7

English version

Postal services - Digital postage marks - Applications, security and design

Services postaux - Marques d'affranchissement digitales -
Applications, sécurité et design

Postalische Deinstleistungen - Digitale
Freimachungsvermerke - Inhalte, Sicherheit und
Gestaltung

This European Standard was approved by CEN on 26 August 2004.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

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



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

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

	page
Foreword.....	6
1 Scope	8
2 Normative references	8
3 Terms and definitions	9
4 Symbols and abbreviations	11
5 DPM applications and design process	12
5.1 Introduction	12
5.2 DPM business planning	13
5.3 DPM systems analysis	14
5.4 DPM security analysis	14
5.5 DPM design	15
Annex A (normative) Specification checklists	16
A.1 DPM applications specifications	16
A.2 System specification	16
A.3 Security specification	16
A.4 DPM specification	16
Annex B (informative) Business planning considerations	17
B.1 Possible applications	17
B.2 Market segmentation	18
B.2.1 Approach	18
B.2.2 Mailer segmentation	18
B.2.3 Postal access and induction	19
B.2.4 Payment	19
B.3 Applications selection	20
B.3.1 Approach	20
B.3.2 Infrastructure requirements and constraints	20
B.3.3 Other factors	21
Annex C (informative) Security analysis considerations	22
C.1 Context	22
C.2 Security objectives, policy and economics	23
C.3 Threats and vulnerabilities	24
C.3.1 Introduction	24
C.3.2 Environmental context	24
C.3.3 General threats to DPM systems	25
C.4 Applications and message level security	27
C.5 Security services and message level countermeasures	29
C.6 Applications level countermeasures	31
C.6.1 Introduction	31
C.6.2 Access and usage controls	31
C.6.3 Duplicate detection	34
C.6.4 Induction control	36
C.6.5 Inspection & forensic analysis	37
C.6.6 Investigation	37
C.6.7 Postal item verification	38
C.6.8 Obliteration countermeasures	40
C.6.9 Security service management	40
C.6.10 Volume and revenue controls	40
C.7 Countermeasure selection	41

C.8	Application of countermeasures.....	42
C.9	Message security implementation options.....	43
C.9.1	Introduction.....	43
C.9.2	Digital signatures.....	43
C.9.3	Message authentication codes	44
C.9.4	Exchange validation codes	45
C.9.5	Selection of message security techniques.....	47
C.9.6	Application of verification techniques	47
Annex D	(informative) Systems analysis considerations	48
D.1	Requirements analysis.....	48
D.2	Functional description	49
D.2.1	Approach	49
D.2.2	Postal item production.....	49
D.2.3	Rating.....	49
D.2.4	Accounting.....	50
D.2.5	DPM generation	50
D.2.6	DPM printing	50
D.2.7	Payment.....	50
D.2.8	Induction.....	50
D.2.9	Mail processing: sorting, transportation and delivery	50
D.2.10	Component management.....	51
D.2.11	Security management	51
D.2.12	Audit.....	51
D.2.13	Application services.....	51
D.3	Function allocation and architecture design.....	51
D.4	Other detailed design aspects	52
D.4.1	Introduction.....	52
D.4.2	Data requirements and sourcing	52
D.4.3	DPM printing	53
D.4.4	DPM data capture	54
D.4.5	Applications processing.....	55
D.4.6	Security analysis	56
D.4.7	Exception handling.....	56
Annex E	(informative) DPM design considerations	57
E.1	Data content.....	57
E.2	Data entry	58
E.3	Data construct mapping.....	58
E.4	Symbology	59
E.5	Human readable information.....	60
E.6	Layout, facing & aesthetics	61
E.7	Performance and test criteria.....	62
Annex F	(informative) Statistical analysis of DPM verification.....	63
F.1	Introduction.....	63
F.2	Purpose and scope of postal item verification.....	63
F.3	Detection of DPMs with invalid validation code.....	64
F.3.1	Introduction.....	64
F.3.2	Parameters	64
F.3.3	Possible Outcomes	65
F.3.4	Analysis of Outcomes	65
F.3.5	Calculation of Fraud Incidence	66
F.4	Influence of CVC length on fraud detection.....	68
F.5	Detection of duplicate DPMs	69
Annex G	(informative) Message security algorithms	71
G.1	Introduction.....	71
G.2	Hash functions used in message security services	71
G.3	Asymmetric (public key) cryptographic algorithms	71
G.3.1	DSA	71
G.3.2	RSA	72
G.3.3	ECDSA	72

G.3.4	Hybrid digital signatures with partial message recovery	73
G.3.5	Other digital signature methods	74
G.4	Message authentication code (MAC) algorithms	74
G.4.1	CBC DES	74
G.4.2	Advanced Encryption Standard (AES)	75
G.4.3	HMAC	75
G.4.4	MAC truncation and CVC size	76
G.5	Exchange validation code generation	77
G.6	Selection of algorithms for CVC implementation	78
G.6.1	Introduction	78
G.6.2	Cryptographic strength of commonly used algorithms	78
G.6.3	Validation code size and size inflation	80
G.6.4	Generation and verification complexity	81
G.6.5	Key generation complexity	82
G.6.6	Key management infrastructure	82
G.6.7	Intellectual property rights	82
G.6.8	Legality of use; export and import approval	83
Annex H (informative)	CVC generation and verification data	84
H.1	Introduction	84
H.2	Sources of data for verification	84
H.2.1	Introduction	84
H.2.2	Data encoded on the item	85
H.2.3	Data accessed by database look up	85
H.3	Selection of data used in the verification process	85
H.3.1	Introduction	85
H.3.2	Acceptance control code	87
H.3.3	Batch identifier and item number; licence plate	87
H.3.4	CVC	88
H.3.5	Date / time	88
H.3.6	Delivery security code	88
H.3.7	Device identifier, customer identifier or licence number	89
H.3.8	Postage value	89
H.3.9	Public key certificate identifier	89
H.3.10	Rating parameter(s), including service indicator	89
Annex I (informative)	Architecture examples	91
I.1	Introduction	91
I.2	The REMPI architecture	91
I.2.1	Introduction	91
I.2.2	Mailer systems	91
I.2.3	Mail finishing system	91
I.2.4	Mail finishing print subsystem	91
I.2.5	Secure accounting system	92
I.2.6	Announcement system	93
I.2.7	Acceptance system	93
I.2.8	Postal item verification system	93
I.2.9	Reconciliation & support systems	94
I.2.10	Bank	94
I.2.11	Post systems	94
I.2.12	Mail handling infrastructure	94
I.2.13	Customer information system	94
I.2.14	Enquiry & data system	94
I.3	USPS IBIP configurations	95
I.3.1	Introduction	95
I.3.2	System components	96
I.3.3	Configuration A	96
I.3.4	Configuration B	98
Annex J (informative)	Examples of digital postage marks (not to scale)	99
J.1	Australia Post	99
J.2	Canada Post	99
J.3	Deutsche Post	99

J.4	Die Post, Switzerland	101
J.5	Royal Mail	102
J.6	United States Postal Service (USPS)	102
Annex K (informative)	Relevant intellectual property rights (IPR)	104
K.1	Introduction	104
K.2	Massachusetts Institute of Technology	104
K.3	Neopost	104
K.4	Pitney Bowes Inc	104
K.5	Pitney Bowes Inc, together with Certicom Corp	105
K.6	United States Department of Commerce	105
K.7	United States Postal Service	105
Annex L (informative)	DPM design charts	106
L.1	Applicability of countermeasures against identified threats	106
	Application Countermeasure	107
L.2	Data elements used by typical applications & countermeasures	108
L.3	Mapping data elements onto data source & DPM data constructs	112
	Bibliography	114

Foreword

This document (EN 14615:2005) has been prepared by Technical Committee CEN/TC 331 "Postal Services", the secretariat of which is held by NEN, in collaboration with the UPU.

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

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2005, and conflicting national standards shall be withdrawn at the latest by July 2005.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

This document (EN 14615:2005) is the CEN equivalent of UPU¹⁾ standard S36-4. It may be amended only after prior consultation, between CEN/TC 331 and the UPU Standards Board, in accordance with the Memorandum of Understanding between CEN and the UPU.

The UPU's contribution to the standard was made, by the UPU Standards Board²⁾ and its subgroups, in accordance with the rules given in Part V of the "General information on UPU standards".

This document is the first version of EN 14615, but corresponds to the fourth version (S36-4) of UPU standard S36, the revision history of which can be found in the Foreword of the UPU versions of the specification.

This document includes a Bibliography.

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

1) The Universal Postal Union (UPU) is the specialised institution of the United Nations that regulates the universal postal service. The postal services of its 189 member countries form the largest physical distribution network in the world. Some 5 million postal employees working in over 660 000 post offices all over the world handle an annual total of 425 billion letters-post items in the domestic service and almost 6,7 billion in the international service. Some 4,5 billion parcels are sent by post annually. Keeping pace with the changing communications market, posts are increasingly using new communication and information technologies to move beyond what is traditionally regarded as their core postal business. They are meeting higher customer expectations with an expanded range of products and value-added services.

2) 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 organisations. 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

The transition from letterpress to digital printing provides the opportunity for a more effective way to communicate information on postal items. Current Postmarks include information such as postage value, date of posting and equipment identification, but this information is not readily machine readable. The emergence of digital printing and image processing technologies offers the opportunity to encode critical data in the form of digital postage marks (DPMs) which are more suitable for computer data capture. However, the adoption of these technologies requires careful study, both to maximise the benefits from their introduction and because digital printing technology might bring with it the need for different security measures than those commonly used in association with letterpress printing.

The document identifies a variety of factors which need to be considered in the DPM design process. It has three main purposes. It is intended to serve as:

- a) **a standard process:** for the design of applications using digital postage marks;
- b) **a guide:** to help in structuring local standards for digital postage marks;
- c) **a cross reference:** to point to other standards and documents related to DPM applications.

It is stressed that the factors identified are intended to be representative and do not constitute an exhaustive list.

Similarly, the document provides many examples of possible architectures and design solutions to the issues which are raised. These are non-normative. They are given for illustrative purposes only and there certainly exists a wide range of other possibilities which are not described. It is not intended to suggest that any one architecture or design or technical solution described is in any way required or in any way superior to any other, whether described herein or not.

The implementation of certain of the techniques described in the informative sections of this specification might involve the use of intellectual property that is the subject of patent rights. It is the responsibility of users of the standard to conduct any necessary patent searches and to ensure that any pertinent patents are in the public domain; are licensed³⁾ or are avoided. Neither CEN nor the UPU can accept any responsibility in case of infringement, on the part of users of this document, of any third party intellectual property rights. Nevertheless, document users and owners of such rights are encouraged to advise the Secretariat of the UPU Standards Board and/or of CEN/TC 331 of any explicit claim that any technique or solution described herein is protected by patent in any CEN or UPU member country. Any such claims will, without prejudice, be documented in the next update of this standard, or otherwise at the discretion of the Standards Board, respectively CEN/TC 331. Annex K of this document lists the intellectual property rights brought to the attention of CEN/TC 331 and the UPU Standards Board prior to approval of the publication of this version of the standard.

NOTE The mention of intellectual property rights, in Annex K, is on a 'without prejudice' basis. That is, such mention indicates only that some party has expressed the view that use of the standard might, in some circumstances, infringe the mentioned intellectual property rights. It should not be taken as in any way confirming the validity of such view and users should conduct their own patent searches to determine whether the mentioned IPR is in fact applicable to their specific case.

3) Mail service contractors are advised to ensure that reliance on patented approaches does not inadvertently lead to the creation of an effective monopoly. This could occur, even if usage of the approaches concerned is licensed by the mail service contractor, unless the terms of the licensing agreement commit the patent holder to making licences available, on appropriate terms, to the mail service contractors customers and suppliers, including competitors of the patent holder.

1 Scope

This document specifies a recommended procedure for the development of specifications for applications of digital postage marks (DPMs) – i.e. applications linked to the use of digital printing and image data capture technologies in the postal industry, most particularly for the evidencing of postage accounting and/or payment. It is not intended to prescribe or to recommend any particular architecture or design for such applications, only to specify the process through which such an architecture or design should be developed.

NOTE 1 For this reason, the standard includes both normative and informative content. Clauses 1 to 5 and Annex A are normative, whilst the remaining annexes are informative. Non-normative (informative) clauses are indicated as such in the heading.

The process described is based on a cyclic model, involving business planning; systems analysis; security analysis and detailed DPM design.

The defined process is a recommended one only and DPM applications designers are not obligated to follow it. However, its use is intended to ensure both that all relevant aspects are taken into account in the design process and that the resulting specifications have a degree of commonality of structure which make them comparable with similar specifications produced by other parties. It is hoped that this will make them more easily intelligible, and less open to ambiguity, for implementers.

It is assumed that users of the standard are familiar with normal processes involved in the design of computer-based applications and the standard therefore limits itself to aspects which are specific to DPM applications design. In particular, the document covers only requirements and considerations relating to applications that use digital postage marks, on individual postal items, as a means of communicating data (messages). The clause on design covers only the design of the digital postage marks themselves. It does not cover other aspects of design, including the possible use of other messages, transported by other means (e.g. statements of mailing), to provide for the communication of additional data, even though these might be just as important.

The standard assumes, but does not require, that it is desired to implement digital postage marks which conform to UPU standards S27, S28 and S25 (see Bibliography) and provides a guide to the use of these standards. However, many of the guidelines, recommendations and checklists would apply equally to the design of DPM applications using digital postage marks based on symbologies other than those supported by S28, or requiring data which cannot be accommodated within S25-defined data constructs.

NOTE 2 Though S28 [7] applies only to representation using two-dimensional symbologies and restricts its scope to two of these: Data Matrix and PDF417, its extension to other symbologies, including linear barcodes and OCR representation of data, is open to consideration. Users who find that their requirements cannot be met within the defined constraints are therefore encouraged to contact the Secretariat of the UPU Standards Board, with a view to exploring possible extension of the standard.

NOTE 3 Though S25 [5] defines an initial set of data constructs, it is intended to extend this set on an as-needed basis. Users who find that their requirements cannot be met by existing data definitions are therefore encouraged to contact the Secretariat of the UPU Standards Board, with a view to extension of the standard.

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.

UPU Standards glossary⁴⁾

NOTE Though this standard was developed on the assumption that users would wish to base their digital postage mark implementations on UPU standards S28 [7] and S25 [5], this is not actually a requirement. These two standards, along with many other standards which are relevant and should desirably be taken into account in the digital postage mark definition process, are therefore listed in the (informative) Bibliography at the end of the standard.

4) UPU Standards are obtainable from the UPU International Bureau, whose contact details are given in the Bibliography; the UPU Standards glossary is freely accessible on URL <http://www.upu.int>

3 Terms and definitions

For the purposes of this document, the terms and definitions given in the UPU Standards glossary and the following apply.

3.1

alteration

deliberate changing of information present in a DPM

3.2

authentication

process of verifying that the information encoded on a postal item, including in its DPM, is internally consistent and originates from the source identified on the item

3.3

collusion

cooperation between two or more parties with fraudulent intent

3.4

copying

duplication of an original DPM to produce identical copies and unauthorised use of these copies on postal items deposited into the postal system

3.5

counterfeiting

unauthorised creation of a symbol that is similar to, or apparently identical with, a legitimate DPM in an attempt to perpetrate fraud

3.6

countermeasure

action, law, procedure, mechanism or combination thereof that can be taken to detect, deter, frustrate and/or prevent adversarial attacks on, or inadvertent errors in, a DPM applications system and/or to control or limit the damage resulting from the occurrence of such attacks or errors

3.7

cryptanalysis

use of mathematical techniques in an attempt to defeat the use of cryptographic methods, particularly in the context of information security services

3.8

cryptographic validation code

CVC

value, cryptographically derived from selected postal item data, which can be used in verifying the integrity of such data and authenticating its origin

NOTE A truncated MAC (based on a symmetric cryptographic algorithm) or a digital signature (based on an asymmetric algorithm) can be used as a CVC. See also exchange validation code (EVC) and C.9.2 and C.9.3.

3.9

data capture

data read

capture and decoding of the machine representation of information contained in a DPM

3.10

data read

see under data capture

3.11

digital postage mark validation

DPM validation

process providing cryptographic or other authentication of the origin and integrity of digital postage mark data

3.12

digital signature

value, cryptographically derived from selected data using a public key algorithm, which, when associated with the corresponding public key and its owner, allows a recipient of the data to authenticate its origin and verify its integrity

NOTE See C.9.2. The use of digital signatures protects:

- the sender against forgery by third parties or the recipient, and
- the recipient against forgery by third parties and repudiation by the sender.

3.13

exchange validation code

EVC

code, known to or agreed between a mailer and a licensing post, which when applied to a postal item by the mailer, can be used by the licensing post to authenticate the origin of the item and, under appropriate circumstances, to verify the integrity of agreed upon DPM data

NOTE See also cryptographic validation code (CVC) and C.9.4.

3.14

forgery

fraudulent completion or alteration of a legitimate DPM

3.15

licensing post

mail service contractor which licenses a particular mailer to use DPMs on mail submitted to that mail service contractor

3.16

message authentication code

MAC

value, cryptographically derived from selected data, that allows data integrity and implicit data origin to be verified

NOTE 1 The above definition differs from that in the UPU Standards glossary.

NOTE 2 MACs provide weaker authentication of data origin than digital signatures (q.v.) because they do not protect against forgery by the recipient or against sender repudiation, unless the cryptographic key is known only to, and verification is performed by, a trusted third party.

NOTE 3 MACs are based on a shared secret (a private cryptographic key) between the sender and the verifier. Data integrity is established as long as the shared secret is not compromised, and subject to the probability of a third party, without knowledge of the secret, correctly guessing the MAC by random chance or by oracle attack. See C.9.3; G.4 and G.6.2 for further information.

3.17

obliteration

defacing a DPM with the intent of circumventing the verification process and thus avoiding payment

3.18

payment validation

process of validating that the correct payment amount for a postal item and its postal service has been accounted for

3.19

postal item data

information, related to a particular postal item, which is either known to or communicated between the mailer and the licensing post, or which can be captured from the postal item itself

NOTE That is, postal item data can include:

- physically measurable characteristics of an item, such as its weight;
- information encoded or represented on the item, whether this is in human readable form or in the form of a bar code or DPM;
- information which is communicated by other means, e.g. in an EDI message.

3.20

replay

re-use or re-transmission of a message (including a DPM) with fraudulent intent

NOTE Copying of a DPM is treated under the heading "Copying"; Replay refers to re-use of an original DPM (compare with Sampling).

3.21**security feature****security technique**

characteristic of a DPM that adds complexity and makes the DPM harder to reproduce or change without detection

NOTE See C.9.5.

3.22**threat**

method of mounting an attack on a DPM applications system that, if successfully applied, would cause damage to a mail service contractor, its agents and/or its customers

3.23**truncated MAC**

special case of a message authentication code, which is a non-empty proper subset of the result of applying the cryptographic algorithm selected for MAC calculation

NOTE Truncation is used to reduce the length of the MAC (to save space in the DPM) and to increase the difficulty of exhaustive key extraction attacks. However, the truncation should not be too severe (i.e. the truncated MAC should not be too short) – see C.9.3 and G.4.4.

3.24**vulnerability**

point of weakness; susceptibility to damage through adversarial attack or inadvertent error

4 Symbols and abbreviations

For the purposes of this document, the symbols and abbreviations given in the UPU Standards glossary and the following apply.

CVC:	Cryptographic Validation Code
EVC:	Exchange Validation Code
FIPS:	(United States of America) Federal Information Processing Standard
FIPS PUB:	reference to a FIPS Publication, issued by the (American) National Institute of Standards & Technology (NIST). The number following PUB refers to the publication number being referenced.
NIST:	(United States of America) National Institute of Standards and Technology
$x _m$:	modulus m value of x, i.e. $x - m \cdot \text{INT}(x/m)$

5 DPM applications and design process

5.1 Introduction

Digital postage marks, or DPMs, are postmarks containing information that can be read and processed by mailers, postal handling organisations and the mail recipients, having three distinct features:

- the information content is expressed in the form of a message, containing internationally standardised data constructs;
- the message is represented on the postal item in the form of one or more machine readable symbols;
- the read rate and accuracy of data capture from the symbols is improved by the inclusion of error detection and correction data.

DPMs can be used to support a wide variety of computer-based postal applications which require information to be encoded on postal items in a form which can be readily captured by automated equipment. Such applications include proof of postage accounting and/or payment, together with applications intended to provide added value services such as proof of posting; tracking and tracing; time certain delivery, etc.

The implementation of digital postage marks should be driven by overall business objectives and strategies. It is assumed that these are already known and that it has been determined that digital postage mark applications will provide an important contribution to their fulfilment.

The design of a DPM application shall follow a four step cyclic process; with interlocking cycles for Business Planning, Systems Analysis, Security Analysis and DPM Design. These cycles should be interactive and iterative. Figure 1 below shows the overall process. This starts with Business Planning, followed by parallel work on Systems and Security Analysis, and is completed by DPM Design. The detailed design of other system aspects will require similar design activity, but this falls outside the scope of this document.

The Business Planning cycle shall be conducted in accordance with 5.2 and shall result in **DPM** (and possibly other) **Applications Specifications** which take into consideration both business requirements and constraints. The adequacy of the scope of these specifications shall be verified by reference to the checklist in A.1.

The Applications Specifications shall be used as input to the DPM Systems Analysis cycle. This shall be conducted in accordance with 5.3, resulting in the **System Specification** which takes into consideration both system requirements and constraints. The adequacy of the scope of this specification shall be verified by reference to the checklist in A.3.

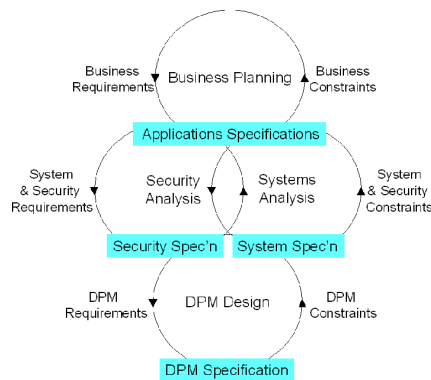


Figure 1 — DPM Applications and Design Process

Most, though not necessarily all, DPM applications are expected to involve postage evidencing and/or the unique identification of individual postal items. This standard therefore covers Security Analysis and the design of the security infrastructure, justifying separate treatment of this aspect of systems analysis. This shall be conducted in accordance with 5.4, resulting in a separate **Security Specification**. The adequacy of the scope of this specification shall be verified by reference to the checklist in A.2.

The System and Security Specifications are the input to the fourth step, covering design of the DPM itself. This shall be conducted in accordance with 5.5, resulting in the **DPM Specification**, addressing both the message content and encoding and other aspects, such as the incorporation of human readable data, overall aesthetics, placement and printing. The adequacy of the scope of this specification shall be verified by reference to the checklist in A.4.

All stages should involve close cooperation between customers (mailers and recipients); technical solutions providers, such as suppliers of mail finishing equipment and mail processing systems, and mail service contractors.

It is stressed that the process might require iteration: during later stages, problems might well be encountered which cannot satisfactorily be resolved within the specification(s) prepared in the previous stage(s). In this case, it will be necessary to iterate back to resolve these.

5.2 DPM business planning

Business planning is a required precursor to the successful introduction of DPM applications. The first step in the business planning cycle is to decide on the objective: what is to be achieved by the DPM application(s) and how does this relate to overall business objectives and strategies? Both short and longer term aspects need to be considered.

Annex B provides informative guidelines to the main topics which need to be addressed. The key issue is to define which applications (see B.1) are to be supported, for which market segments (B.2). Decisions on these issues will be influenced by the mail service contractor's business objectives and priorities, as well as by features of the existing business, including technical infrastructure. An introduction to some of the considerations which are likely to arise in the selection process is provided in B.3.

The results of this planning shall be documented in a form which can provide the basis for management approval and serve as the high level definition from which more detailed requirements specifications and designs can be developed. The output of the Business Planning Cycle is thus one or more documents, together comprising the **Applications Specifications**. These present the business requirements for the DPM application(s) in sufficient detail to give boundary conditions within which the system design can be prepared.

The specifications outline the scope of the DPM application(s) to be implemented; define the objectives to be met and the constraints within which they are to be implemented and operated. The means to resource the application(s) and fulfil the objectives and the expected benefits should also be covered.

The list below defines a minimal recommended scope for the Applications Specifications, a checklist for which is provided in A.1. Users of the standard are free to add to this scope and/or to map it onto their own preferred documentation structure, but shall ensure that the result covers at least the topics which are identified:

- a) **Business Environment and Objectives:** a specification of the overall context within which it is proposed to implement DPM applications;
- b) **Role of DPM Applications:** a specification of which DPM applications are to be supported, for which segments of the market, with an indication of how they are expected to contribute to overall business objectives;
- c) **Description of Selected Applications:** a description of the selected DPM applications that should provide sufficient detail to serve as the basis for systems and security analysis and DPM design. This should cover:
 - how accounting is to be performed and controlled;
 - how mail is inducted into the postal system;
 - the use made of the DPM in mail processing;
 - the main interfaces to other postal systems, including those for accounting, revenue control, payment management and mail handling operations.
- d) **Infrastructure and Design Constraints:** a description of the characteristics of the technical infrastructure into which the planned DPM applications have to be integrated and how is this expected to change, together with a specification of the resulting constraints on DPM application design and implementation;
- e) **Implementation Policy and Priorities:** a description of how the planned DPM applications relate to other ongoing and planned developments;
- f) **Business Impact:** an analysis of how the DPM applications will impact the parties involved – customers (both mailers and recipients); the mail service contractor itself and third parties, including other postal handling organisations, service providers and mailing system and equipment suppliers;
- g) **Implementation Plan, including Timing, Resources and Investment:** a plan describing how the applications are to be implemented, including a list of the key milestones and their timing, a specification of what resources are needed and what costs will be incurred;
- h) **Benefits and Cost Justification:** an analysis of the quantitative and qualitative benefits that are expected to result; how these are related to costs and the expected return, both for the mail service contractor and for the other affected parties. Consideration should be given to whether all parties are properly incented;
- i) **Critical Success Factors:** a description of the key factors which will influence the success of the implementation and subsequent operation and of the measures that need to be taken to control these factors;
- j) **Management Control and Evaluation:** a specification of how the implementation and subsequent operations will be managed and controlled. In particular, this should address the key decision points and what quantitative measures need to be available to support management decision processes.

5.3 DPM systems analysis

The second stage in the DPM applications & design process is that of Systems Analysis. This should be undertaken in parallel with development of the Security Specification (see 5.4) since the two topics are closely interrelated: at least in payment related applications, many applications functions correspond to security countermeasures.

Normal systems analysis and design processes should be followed, but there might be a need to pay particular attention to the phasing of development and introduction. It could well be that longer term objectives cannot be economically realised in the context of the existing postal system infrastructure and designs and plans for implementation should take into account the phasing in of infrastructure developments.

The output of this stage shall be a control document, the System Specification, that describes the architecture for the system required to support the selected DPM applications and presents the system design in sufficient detail to give a boundary condition within which the detailed design of DPM applications can be prepared. The System Specification shall cover all systems requirements which need to be met in order to satisfy business objectives. At least the following topics, most of which are discussed at more length in informative Annex D, shall be addressed:

- a) requirements analysis;
- b) functional description;
- c) function allocation and architecture design;
- d) performance criteria;
- e) systems architecture;
- f) applications processes;
- g) input data requirement;
- h) source of data;
- i) DPM data capture;
- j) sampling methods;
- k) exception handling;
- l) infrastructure requirements and constraints.

5.4 DPM security analysis

The third stage in the DPM applications & design process is the development of a Security Specification. This should be done in parallel with Systems Analysis, described in 5.3.

Security requirements need to be defined in the context of overall business objectives. The security system should be designed around these requirements, taking into account the rapidly developing state-of-the-art in information security techniques. The most cost effective security system design is likely to be affected by the existing postal infrastructure; the cost base of the mail processing system; the value of digital postage marks and the cultural and legal framework within which DPM applications are to be introduced. Annex C provides an informative guide to some of the key issues which need to be considered.

The result of the analysis shall be documented in a Security Specification. As a minimum, this should cover the following aspects:

- a) **Security Objectives, Policy and Economics**, setting the framework within which the security analysis is performed;
- b) **Threats to and Vulnerabilities** of the system, with emphasis on those that could endanger the mail service contractor's revenue;
- c) **Countermeasures** which can be applied to deter attacks on the system, assist in the detection of security breaches, identify their source and collect evidence of attempted fraud;
NOTE As explained in C.4 below, countermeasures fall into two classes: Message Level Security Services, designed to protect the security of the DPM itself, and Applications Level Countermeasures, which address applications-specific issues.
- d) **Security Economics and Countermeasure Selection**, defining and justifying the package of countermeasures selected for implementation;
- e) **Application of Countermeasures**, detailing when, where and how the various selected countermeasures are to be applied;
- f) **Implementation Options**, particularly for message level security services, where there is a wide choice of methods and techniques which can be applied.

5.5 DPM design

The final phase covers the detailed design of the DPM itself, some examples of which are given in (informative) Annex J. The design is likely to involve the making of compromises between conflicting requirements. Such compromises should take into account both application requirements and environmental constraints. The business objectives, documented in the Applications Specifications that result from DPM Business Planning (see 5.2), should not be lost during this process.

NOTE Annex E provides an informative introduction to some of the key issues which are likely to arise. It does not address the design of complementary system elements required to implement DPM applications as these are outside the scope of this document.

The output of this cycle shall be a control document, the **DPM Specification**, that specifies the DPM in sufficient detail to permit the development of equipment and/or software by knowledgeable implementers. It should cover at least:

- a) data content;
- b) data entry;
- c) representation and data construct mapping;
- d) symbology;
- e) human readable information;
- f) layout, aesthetics and placement;
- g) performance and test criteria.

Annex A (normative)

Specification checklists

A.1 DPM applications specifications

The following list of topics shall be used to verify the adequacy of the scope of DPM applications specifications developed in accordance with 5.2:

- a) Business Environment and Objectives
- b) Role of DPM Applications
- c) Description of Selected Applications
- d) Infrastructure and Design Constraints
- e) Implementation Policy and Priorities
- f) Business Impact: customers/mail service contractor/third parties
- g) Implementation Plan: timing, resources, investment
- h) Benefits and Cost Justification
- i) Critical Success Factors
- j) Management Control and Evaluation; decision points, quantitative measures

A.2 System specification

The following list of topics shall be used to verify the adequacy of the scope of the system specification developed in accordance with 5.3:

- a) Requirements Analysis
- b) Functional Description
- c) Function Allocation and Architecture Design;
- d) Performance Criteria
- e) Systems Architecture
- f) Applications Processes
- g) Input Data Requirement
- h) Source of Data
- i) DPM Data Capture
- j) Sampling Methods
- k) Exception Handling
- l) Infrastructure Requirements and Constraints

A.3 Security specification

The following list of topics shall be used to verify the adequacy of the scope of the security specification developed in accordance with 5.4:

- a) Security Objectives, Policy and Economics
- b) Threats and Vulnerabilities
- c) Message Level Security Service Analysis
- d) Applications Level Countermeasure Analysis
- e) Countermeasure Selection
- f) Application of Countermeasures
- g) Message Level Security Implementation

A.4 DPM specification

The following list of topics shall be used to verify the adequacy of the scope of the DPM specification developed in accordance with 5.5:

- a) Data Content
- b) Data Entry
- c) Representation and Data Constructs
- d) Symbolology
- e) Human Readable Information
- f) Layout, Aesthetics and Placement
- g) Performance and Test Criteria

Annex B (informative)

Business planning considerations

B.1 Possible applications

A DPM contains a message to be used alone or in conjunction with other messages and/or pre-stored data, for one or more mailing applications. DPMs can be used to support a wide variety of postal applications, providing added value for both the mail service contractor and the mailer. The initial application for DPM is most likely to include validation of postage accounted (payment validation) and this is assumed in what follows, though similar considerations would apply to DPM applications which did not include validation of postage.

Possible applications include, but are not limited to:

- a) **Mailer Postage Accounting** covers the case in which the mailer, or, more probably, equipment used by the mailer, performs the postage accounting function, using the DPM to evidence that accounting has taken place. In this case, the aim is to provide the mail service contractor with a means to validate that DPMs, generated and applied to postal items by mailers, have been properly accounted for and correctly correspond with item characteristics such as requested service, size and weight. This requires the validation of information contained in the DPM and in any other related accounting messages generated by the mailer. This implies identifying the mailer, determining the required service and capturing sufficient item attributes to validate the postage value. The results can then be correlated with accounting records and corresponding payments, in such a way as to provide an acceptable level of postal revenue protection.
- b) **Mail Service Contractor Postage Accounting** covers the case in which the mail service contractor performs the accounting function and generates invoices for the postal items processed, using data obtained from DPMs on the items and/or from related messages, such as acceptance control documents or statements of mailing. In this case, the application should provide mechanisms to allow the mailer to validate the invoices he receives. The (automated) invoicing of business reply mail provides an obvious example of this mode of accounting. Normal (business generated) mail could also be accounted for in this way if desired, though this is likely to involve security and other considerations which are not addressed in this standard.
- c) **Business Reply Mail Accounting and Control:** In the case of business reply items, the DPM can contain the business reply licence number or other identification of the origin of the item. This can be used both to validate the destination address and to control the collection of statistics and the generation of invoices;
- d) **Service Identification**, in which the DPM is used by the postal handling system to determine the mailer's timing, processing and delivery requirements for a postal item;
- e) **Quality of Service Measurement**, where the DPM contains a unique identifier, for the postal item, which is used to capture tracking data as the postal item passes through the mail handling process, in order to measure the quality of service provided. The identification can be read together with actual date/time information at different points in the mailstream. This information can then be used to provide timely reports on the quality of service achieved compared to standards. Selected information can be made accessible to customers where appropriate. This application might have consequences for the data content and design of the DPM. For example, if separate reports are required for different products and services, it could be necessary to include Service Data (see UPU standard S25 [5]) in the DPM. Similarly, if performance data are to be recorded through to the point of delivery then a means of data capture at the point of delivery is needed. This might have a consequence on the choice of symbology and the design of the DPM;

NOTE Many posts are expected to prefer to use post-applied identifiers, known as ID-tags, for quality of service measurement. However, the data can still be correlated with customer-applied identifiers if the association between the ID-tag and DPM is recorded at some point in the mail handling process.

- f) **Cross Border Handling**, in which information in the DPM is shared among postal handling organisations with the aim of improving the efficiency of processing of the postal item. For example, the DPM could

include identification of special items and provide service and terminal dues accounting data. This requires that UPU standards are followed in the design of the DPM;

- g) **Customer Enquiry Handling**, in which identification and service data in the DPM is used to support the provision of service information to the mailer. Examples include proof of posting (certificate of mailing); reporting of the location of a postal item in the mail handling process (tracing); notification of undeliverable mail; provision of time and proof of delivery reports, etc.;
- h) **Mailer Defined Applications**: mailers can define their own applications, such as pre-classifying reply items, by assigning specific information to the Customer Data Field in the DPM. Three categories of mailer-specific application can be distinguished:
 - i) mailer to post; where there is an agreement, for support of a specific application, between the mailer and the mail service contractor;
 - ii) mailer to the recipient, for example, using data in the DPM to support internal sorting at the recipient's premises;
 - iii) mailer to himself, for business reply mail, or in case of return of undeliverable mail.

These applications are supported by a data field in a DPM for use by the mailer: the «Customer Data Field». The mailer will define the application and its data contents. The data in the Customer Data Field will normally be ignored by the postal system unless there is a specific joint application, as in case (i) above. Where a joint application is defined, the quality of source information in the Customer Data Field should be controlled.

B.2 Market segmentation

B.2.1 Approach

The implementation of DPM technology should be considered separately for each of the different market segments. These are typically defined by reference to mailer characteristics; to the method of mail induction and to the means of payment.

B.2.2 Mailer segmentation

The basis for mailer segmentation could be:

- a) mailer organisation type (risk related);
- b) volume of postal items;
- c) method/technology used to produce the postal item: generating, assembly and finishing;
- d) information processing tools available to the mailer;
- e) postal induction and acceptance methods.

Each segment has specific needs and capabilities. A possible segmentation based on the volume of postal items processed by mailers is presented below, though individual mail service contractors may choose different parameters:

- **Mailcentre**: large volume mailer employing several dedicated operators and highly specialised mail processing systems. Mail activities are frequently charged back to internal cost centres;
- **Mailroom**: medium volume mailers employing dedicated operators and specialised mailing equipment;
- **Office**: small volume mailers employing non dedicated operators and a shared piece of mailing equipment;
- **Desktop**: typically an individual or small group of mailers using a PC and printer combination, generating mail using standard office or desktop publishing software. A small piece of mailing equipment, such as a franking machine, could also be used. Groups of PC users within the same organisation might be networked.

B.2.3 Postal access and induction

DPM applications will need to accommodate existing access methods and open the way to improve further the ease by which mailers can access postal services. Existing access methods which might need to be taken into account include:

- a) **Uncontrolled entry - Collection Mail**, including:
 - i) Mail entered into the mailstream through a publicly accessible/street collection box;
 - ii) Self service retail points.
- b) **Controlled entry**, including:
 - i) Mail handed in to a postal counter clerk;
 - ii) Mail accepted through a controlled acceptance point;
 - iii) Metered mail from special boxes;
 - iv) Mail received in special pouches or envelopes;
 - v) Mail collected from mailers premises.

It is stressed that applications need not necessarily address all access methods. Depending on a mail service contractor's priorities and objectives, it may be decided to implement DPMs for only one access method initially. Thus, for example, the first USPS DPM initiative⁵⁾ was aimed at small and home office mailers, operating in an uncontrolled acceptance environment, whereas the Deutsche Post and Royal Mail started⁶⁾ with medium to high volume mailers, operating in a controlled acceptance environment in which details of mailings are communicated electronically, prior to induction.

B.2.4 Payment

Different payment methods and systems are in use. Many are automated, using computer-based systems, and extensive use is made of systems which support remote resetting of approved postal devices or equipment. In such cases, it is advantageous for payment validation purposes that information available from these computer payment systems are used in conjunction with the information obtained from DPM data capture.

In addressing payment, three issues need consideration: timing, means and control.

- a) **Payment Timing**. This can be based on:
 - i) prepayment: Payment made in advance of mailing. This method applies to advance purchase and use of stamps and is often used for postage metering systems. The payments made can, but need not, directly correspond to one or more submissions of postal items to be mailed;
 - ii) post-payment: Payment made after a mailing service for postal items has been received. Invoices for specific mailings, monthly payment accounts and authorisation limit-based systems are common. Again, meters are often used for accounting and credit control;
 - iii) just-in-time payment or Pay-per-use: Payment corresponding to a specific submission or mailing of postal items made at the time of, or immediately prior to, posting. Inter-alia, this corresponds to payment being made, over a post office counter, at the time of mail induction.
- b) **Payment Means**. A number of payment means are well established; some common ones are listed below:
 - i) Cash: normally associated with payments made at the postal counter;
 - ii) Cheque: payment commonly made through the post;
 - iii) EFT (Electronic Funds Transfer): electronic alternative to cheque payment;
 - iv) Direct debit: a debit made directly from a customers bank account with customer prior authorisation. Generally the payment transaction is electronic;
 - v) Charge cards⁷⁾: accepted more by smaller customers, for example, SOHO (Small Office/Home Office) mailers.
- c) **Payment Controls**. The DPM validation approach should take into consideration the method of accounting, including any credit terms, and data consolidation for postage purchased or postage used. Control methods include:
 - i) Metering: customer mailing equipment controls credit and usage limits. Metering could be local to the customer or remote;
 - ii) Controlled Acceptance: Acceptance procedures ensure that customers do not exceed credit limits (or present adequate payment) at the time of mail submission.

⁵⁾ This refers to the IBIP: Information-Based Indicium Programme.

⁶⁾ This refers to the REMPI: Re-Engineering the Mailer-Post Interface project.

⁷⁾ Including credit and debit cards and electronic purses.

B.3 Applications selection

B.3.1 Approach

For each mail service contractor the priorities and practical constraints will shape the criteria upon which to base applications selection. For each proposed application a systematic evaluation process should be followed, with close consultation between the different parties (internal and external) responsible for making the application successful. The choice between possible options can follow traditional decision making methods⁸⁾. Account should be taken of the relative importance of the various criteria.

One of the key decision factors is likely to relate to the fact that different applications have different processing and postal infrastructure implications.

B.3.2 Infrastructure requirements and constraints

Mail service contractors already have a significant investment in their automated processing equipment infrastructure. The capabilities and performance of this infrastructure differ from one operator to another. Also, the level of automation could vary geographically for any single operator.

The objectives of a DPM application might not be fully realisable within the constraints of the existing postal infrastructure and trade-offs might need to be made between applications objectives and the required investment in infrastructure improvements. Plans for changing or upgrading the technical infrastructure are likely to be a significant factor in the implementation of most DPM applications.

The financial and human resources required to effect any necessary change in the postal infrastructure should be understood and accepted prior to completing the business planning cycle. It might be desirable to use a phased approach, allowing rapid implementation of a limited applications capability, with later extension to provide full support for the envisaged applications. For example, it might be possible to support some applications on the basis of using portable or hand held scanners to capture DPM data from only a selected sample of postal items and to defer others until support for full on-line reading of DPMs has been implemented.

In any event, the gap between what data capture and processing is required and what is currently possible should be determined and the approach to resolution of these differences defined.

- a) **Data Source:** As discussed in D.4.2, the data required for DPM applications can come from several sources, of which the DPM itself is only one. Other important sources include Databases; On-line Messages from the customer; Item Attribute information and Process Data resulting from postal item processing. However data is sourced, there could be implications for the postal processing infrastructure:
 - i) **DPM:** impacts the need for appropriate data capture equipment, particularly where there is a need to capture data from all postal items carrying DPMs;
 - ii) **Databases:** access to postal databases presupposes the existence of a suitable infrastructure, capable of accessing and delivering the data required by DPM applications processes within the time frame in which it is required;
 - iii) **On-Line Messages:** the extraction of data from mailer-post interface messages presupposes the existence of appropriate electronic data interchange and message routing and storage capabilities;
 - iv) **Item Attributes:** as for the capture of data from DPMs, the capture of other postal item attributes, such as destination address or item dimensions or weight, presupposes the existence of appropriate data capture facilities;
 - v) **Process Data:** access to earlier results of processing a particular postal item requires (a) that the item carry a readily accessible identifier, such as an ID-tag, and (b) that an integrated processing infrastructure, capable of delivering the required data within operationally necessary timeframes, exists.

⁸⁾ For example, a well defined option can be used as a reference, with other options being evaluated by comparing them with this reference. The comparison could be either subjective and qualitative (same, better or worse) or might need to be objective and quantitative, depending on the importance of the factor being considered.

- b) **DPM Data Capture:** Data capture can be required anywhere in the postal processing system from the point of access through to the point of delivery. The point and frequency of data capture depend on the required level of validation, service and management control, which might evolve with time. Data can be captured either using available automated mail processing equipment (which might require upgrade of both hardware and software) or using hand held or portable systems.
- c) **Data Processing:** Data processing can be on-line and/or off-line and can be performed either locally and/or centrally. Local processing might have the benefit of faster response times, whilst central processing could simplify data correlation and consolidation, for example, to allow correlation of DPM data with resetting data and statistics. Local and central data processing systems also have different management characteristics, for example, central systems might be easier to control than local or distributed systems. Of course, it is possible to use hybrid solutions where some data is processed locally and other data is processed centrally. For example, DPM validation could be made locally in real time, with duplicate detection being made centrally on a post-delivery basis. The choices made heavily impact communications requirements and the possible need for upgrading the telecommunications infrastructure should also be taken into account.

The decision to process data on-line or off-line depends on available processing power, timing requirements and expense. It is useful to consider timing requirements in relation to three different time intervals, namely real time, deferred and post delivery:

- i) **Real Time:** where the reaction time is fast enough to influence the operation of the current mail handling process - for example, by influencing sorting bin selection during the passage of a postal item through a sorting machine;
- ii) **Deferred:** where the reaction time is fast enough to be able to influence the operation of a later mail processing step - for example, by using information captured during outward sorting of a postal item to intercept it during inward sorting or delivery sequencing;
- iii) **Post-Delivery:** where the result of processing the information captured from a postal item is only available after the item has left the control of the postal system. This information can be used for statistical purposes, to prompt investigative action or to influence the processing of subsequent postal items from the same source. It is possible to use post-delivery processing results to decide on the time interval used for processing future mailings, for example, to flag as suspect and perform real time processing on selected mail.

B.3.3 Other factors

The selection of applications might also be influenced by other factors, including the responses to the following questions:

- a) **Objectives/priorities:** where is the focus of attention directed: enhancing or providing new services and products; easing customer access to postal services and products; improving management information or providing better postal revenue security?
- b) **Customer impact and acceptance:** how will proposed applications impact customers, what costs will they incur and what benefits will accrue to them? Will customers have to change their mode of operation or implement new technology: how long will this take and are incentives needed to accelerate the process?
- c) **Legal issues:** are proposals impacted by legislation with respect to data protection and the use of cryptographic technology; constraints imposed by fair trade legislation or the terms of any reserved area monopoly?
- d) **IPR issues:** do proposed applications and design solutions rely on the use of third party intellectual property; what will be the impact of this on possible suppliers of equipment and technology and what is the organisation's policy concerning licensing or avoidance of third party IPR?
- e) **Organisational impact:** what impact will proposed applications have on the organisation of the mail service contractor and on the roles and responsibilities of different organisational functions, including technology supply, data capture and processing, security, inspection/investigation, operational management, quality control, etc?
- f) **Investment & Funding:** what investments are required, of which parties and over what time frame; what returns can be expected and how are investments to be funded?
- g) **Technology & Standards Status:** how robust are the envisaged technologies; have they been fully proven elsewhere and can developments be based on widely accepted standards?
- h) **Timing:** how long will it take to implement proposed applications and to realise their full potential; how does this fit in with market requirements?
- i) **Competitive position:** how will possible applications impact the mail service contractor's competitive position?

Annex C (informative)

Security analysis considerations

C.1 Context

Every system has vulnerabilities that render it potentially prone to malfunction, whether caused by accident or design, and to misuse. Such malfunction or misuse, if it occurs in practice, can have detrimental economic, operational and/or human safety consequences. Malevolent parties can attempt to induce these consequences by mounting attacks on the system.

Security analysis is concerned with identifying a system's vulnerabilities, the potential threats or methods of attack that might be used to exploit them and the measures that can be taken to protect against such threats and to reduce the consequences of any malfunction or misuse that nevertheless occurs.

This informative annex is intended to provide the reader with guidance on security analysis for DPM applications systems. It introduces the need for this to be set in the context of a security policy (C.2), identifies some of the threats and vulnerabilities that might need to be considered (C.3), defines different levels at which protective measures (countermeasures) can be taken (C.4), identifies some of the specific countermeasures that are likely to be applicable (C.5 and C.6), discusses the selection of which countermeasures should be implemented (C.7), considers the extent to which the selected countermeasures should be applied (C.8) and provides guidance on the options for implementing message level security (C.9).

The fundamental security requirement is that a DPM application, with the security measures selected as a result of this analysis in place, should:

- accurately account for postal funds;
- provide all information necessary for the verification of postage payment;
- deter attacks on the system by thwarting them, making them highly risky for the perpetrators and/or making them economically unrewarding;
- detect attempted or actual postal fraud, identifying the perpetrators and supporting the collection of legally admissible evidence for use in their prosecution.

It is stressed that security is an economic and operational issue: no security system can prevent the occurrence of errors or the mounting of attacks and it is not possible to totally exclude the possibility of such errors or attacks leading to malfunction. Increasing security can, however, reduce the incidence of errors and attacks and can prevent or mitigate the negative consequences of their occurrence. However, this comes at the cost of increasing system complexity and reducing operational convenience, both of which have an economic cost which should be weighed against the benefits. The task of security analysis is therefore that set of countermeasures that result in optimal protection of the system. Ideally, the result of applying these countermeasures should be such that:

- no party or parties should be able to benefit, from a successful attack on the system, without having to expend time and resources, to mount the attack, which are disproportionately large in comparison with the benefits obtained;

NOTE 1 Benefit is used here in its widest possible sense, not in a narrow purely economic sense: malevolent parties can benefit by causing disruption and economic damage to the system operator or users, without necessarily enjoying any direct economic benefit to themselves. Internet 'denial of service' attacks provide an example of this.

- for an attacker, whether successful or otherwise, the probability of apprehension should be high in relation to any benefits which might be anticipated from a successful attack;

NOTE 2 Even If the first point above is true, potential attackers might not be aware that the cost of success exceeds the benefits they might expect, or might simply hope to be lucky (viz. participation in lotteries). A mechanism to identify such attackers, so that other (external to the system) means can be used to prevent them from mounting further attacks, is therefore desirable.

- the level of security should be optimal in the sense that the economic and operational costs of increased security should be higher than the probable benefits obtained through the resulting reduction in vulnerability of the system, whilst the savings from reducing security should be lower than probable cost of the resulting increase in the system's vulnerability.

C.2 Security objectives, policy and economics

Any consideration of security should be set in the context of an overall security policy, defining the objectives and constraints which apply. Topics which should be considered include:

- a) **Business Objectives:** security is concerned with cost effective protection of a system against adversarial attack and/or inadvertent error, but the objective can be approached from different perspectives: for example, is the objective simply to minimise losses through fraud and error, or does account have to be taken of the impact of security measures on service use and revenues as well?

NOTE 1 Some measures might be very effective in security terms, but at the cost of destroying the business that the security system exists to protect. For example, verification of handwritten signatures is a traditional way of authenticating transactions in a face-to-face environment. But studies have shown that, at least for credit card transactions, strict application of signature verification at the point of sale could result in a 24 % reduction in the number of perfectly valid transactions.

- b) **Security Policy:** the complete elimination of all possibility of attack or error is not practical, so security policy should focus on what level of security is to be achieved, at what cost. The policy needs to set clear guidelines: how important is prevention, as compared with detection; is the emphasis on deterrence through raising the cost of mounting an attack, or through increasing the cost and probability of being caught?

- c) **Economics:** the overall economic goal of security analysis is to minimise any vulnerability that the system might possess within acceptable cost/benefit and quality trade-offs. The approach is to make error improbable and attack unrewarding, not to try to completely eliminate all possibility of attack or error. For example, if the mounting of an attack costs the perpetrator significantly more than can be gained, then perpetration is probably not worthwhile. Conversely, it might not be economically worthwhile to implement a particular countermeasure or security technique if the cost of implementation is high, whilst the potential damage which results from its absence is small. At the same time, account should be taken of the market and business impact of a given security system: the level of security which is optimal from the perspective of its direct impact could be far from optimal in an overall business sense. If security is too strict, it might make matters so difficult for customers that they take their business elsewhere; if it is perceived to be too lax, customers might be mistrustful and, again, take their business elsewhere.

NOTE 2 Perception can be as important as reality. In an internet environment, people avoid doing business with sites which acquire a reputation for poor security, whether or not this is justified. In a postal environment based on the use of digital postage marks, one can imagine the impact of even one widely published report of "how I managed to successfully send 1 000 postal items without paying."

- d) **Architecture:** security measures are most effective when designed into a system at the outset. In other words, to overlay a security design onto an already designed system usually results in less effective security. Further, in considering security during initial system design, it is often best, from an economic standpoint, to define a security boundary within the overall system and, if possible, to include all security techniques within this boundary. For example, the physical means (such as tamper protection and/or tamper detection mechanisms) that are needed to counter physical penetration threats can be made less expensive when applied only to a well defined and confined subset of system elements (i.e. those within the boundary) than to the entire system. Additionally, the architecture of the system plays a role in the security techniques that will be required. For example, the example architectures described in Annex I have different architecture dependent security requirements. In the REMPI (I.2) and USPS Configuration A (I.3.3) architectures, a Security/Revenue Sensitive/Accounting module is co-located with the customer. This is not the case in USPS Configuration B (I.3.4), which has different security requirements as a result.

- e) **Infrastructure Constraints:** what constraints are imposed by the existing infrastructure and the mail service contractor's capability to develop and extend this? For example:

- i) is automated mail handling equipment capable of capturing (or being extended to capture) DPM data on-line?
- ii) are there operational or timing constraints on the ability to access data from corporate databases, or from mail processing systems?
- iii) to what extent does the existing infrastructure support electronic data interchange with customers?

- f) **Legal Framework:** the legislative framework can have considerable impact on the security measures which may be employed. Particular issues of concern include data protection and privacy requirements, legislative constraints on the use and/or export of cryptographic systems and the legal recourse which is available against perpetrators of postal fraud. In some countries, such redress is limited and the deterrent effect of being caught might consequently be reduced.

C.3 Threats and vulnerabilities

C.3.1 Introduction

Threats correspond to methods of attacking a system with the objective of causing damage to it, its operators or users. Actual attacks could combine several such methods. The damage caused need not be directly measurable in financial terms (i.e. might not necessarily result in direct revenue loss to the mail service contractor) and need not lead to direct benefit to the attacker. Damage can also occur through reductions in productivity; loss of business as a result of lack of customer confidence and through legal liability for damage suffered by customers, suppliers or third parties (see ANSI X9.49 [18]). For example, the obtaining and disclosure of information which is intended to be private could bring the system into disrepute, resulting in indirect loss of business, rather than causing direct damage to either the system operator or the owner of the information concerned.

Generally, threats are aimed at exploiting weaknesses or vulnerabilities in the system. Such weaknesses can also result in damage through inadvertent error.

The first step in any system security analysis is to identify and evaluate the potential threats to, and vulnerabilities of, the system. In this process, it can be useful to consider that possible threats can arise in a multitude of ways, from a variety of vulnerabilities and from a range of sources. Possible sources include:

- a) dishonest system users with a proclivity for attempting to defraud the system;
- b) dishonest suppliers taking advantage of a system vulnerability known to them;
- c) disgruntled or dishonest mail service contractor employees who can take advantage of privileged access to the system;
- d) unrelated third parties (e.g. network hackers in a network-based architecture).

For each identified threat, or combination of threats, an assessment should be made as to:

- a) the relevance of the threat in the context of the particular DPM system under development;
- b) the vulnerability of the system to the threat, or combination of threats, in question (what is the likelihood of damage occurring);
- c) the extent of probable damage, and
- d) the need for countermeasures (see C.4 to C.8).

C.3.2 Environmental context

The issue of context is particularly important. In a postage payment business process context, threat analysis is essentially concerned with identifying all possible attacks, at each step or link in the process, and analysing the consequences to the business of such attacks. 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. For example, in some scenarios, the supplier of a digital postage mark generation device or issuing service might take responsibility for verification and be liable for the consequences of failures in this process; in others, the mail service contractor might be responsible and therefore need to take measures to protect against fraud.

The analysis also needs to take into account the environment resulting from the proposed architecture of the system. This is almost certain to involve some components that are under the direct physical control of the mail service contractor; others that are under the control of suppliers and subcontractors and still others that are under user control. Threats related to equipment or system components located at a mailer's site (or indeed in any location not under the control of a trusted party) are of special concern because such equipment is in an environment where an attacker might have essentially unrestricted access. Particular care is needed where the equipment concerned is supplied by third parties and has not been subject to mail service contractor approval procedures such as those specified in UPU standard S30. In DPM applications, this is most likely to be the case for printing equipment and security analysis should therefore pay special attention to this equipment and its interface with accounting and cryptographic subsystems.

C.3.3 General threats to DPM systems

The following text identifies a number of threats which are likely to be common to DPM 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.

Each mail service contractor will have a unique environment that might preclude some of the following, but more importantly, might give rise to threats that have not been addressed. It is important to conduct a thorough analysis; to complement the list of applicable threats and to give proper consideration to each one. The analysis should address at least:

- a) **Alteration:** in the context of this standard, alteration involves the deliberate changing of information present in a DPM. For example, a DPM containing a low postage value could be altered to indicate a much larger amount of postage or identification data might be changed, resulting in the DPM being attributed to another party. Note that alterations might be made to the computer readable data in the DPM, to the human readable data, or to both.
- b) **Collusion:** collusion involves cooperation between two or more parties with fraudulent intent. It can occur between customers, between a customer and a supplier, or between one of these and a corrupt postal employee. For example, an individual employed by one mailer could assist another mailer to generate mail purporting to originate in his own organisation, or a mailer could bribe a postal employee to bypass bulk mail acceptance controls (see Inappropriate Induction below). Collusion attacks can not be totally prevented, but properly designed 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.
- c) **Copying:** copying involves the duplication of an original DPM to produce (unpaid for) identical copies and use of these copies on postal items deposited into the postal system. Unlike counterfeiting (see below) this requires access to, or detailed knowledge of, a legitimate digital postage mark. The level of difficulty involved could depend on whether DPM production requires the use of special equipment or supplies (see C.6.5 a).
- d) **Counterfeiting:** counterfeiting is unauthorised creation of a symbol that is similar to, or apparently identical with, a legitimate DPM in an attempt to perpetrate fraud. It includes the creation of original, apparently legitimate, but unauthorised, DPMs containing guessed or predicted CVC or EVC values. Unauthorised access to DPM authentication devices (verifiers) could 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 should be protected.
- e) **Cryptanalysis:** cryptanalysis is the 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 the recovery of 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 only after extensive expert examination, the threat from cryptanalysis when properly using such endorsed algorithms is considered to be minimal. However, algorithms and their parameter values should be carefully selected for use in DPM systems. The most common algorithms are described, and minimal acceptable values of their relevant parameters given, in Annex G.
- f) **Device Modification:** this covers the illegitimate alteration of a genuine DPM device with fraudulent intent. For example, the unauthorised manipulation of the ascending and/or descending registers of a metering device could result in postage payment avoidance.
- g) **Direct Drive:** this involves transmission of data to a printing subsystem from an unauthorised source with the objective of producing a fraudulent DPM, either using replay (see q) or counterfeiting (see d).
- h) **Illegitimate Key Access:** this covers access to the secret cryptographic key or keys of a legitimate device or 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 place at risk any cryptographically protected features of the system. The prevention of such access therefore deserves careful design of the key management and protection system. This also needs to address the procedures for dealing with any illegitimate key access which is detected.

- i) **Illegitimate Use of Device:** this is defined as the operation or manipulation of a genuine device for the purpose of perpetrating fraud. For example, unauthorised use of a prepayment-based metering 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 could also be circumstances in which the device supplier and/or the mail service contractor is impacted (e.g. in a credit-based systems, the mailer from whom a metering device is stolen might refuse to pay for postage subsequently accounted for by the device).
- j) **Impersonation:** impersonation occurs when one mailer introduces postal 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 mail service contractor, 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. Note that, depending on the specific characteristics of the applications system and DPM design, impersonation can be a special case of Alteration, of Device Modification and/or of Illegitimate Use of Device. It can also be associated with Inappropriate Induction.
- k) **Inappropriate Induction:** the introduction of postal items into the mail system in an improper way might result in the bypassing of normal induction controls. For example, a dishonest mass mailer could possibly arrange to have mail induced through an Office of Exchange, resulting in its being treated as inter administration mail. This threat would normally be associated with collusion (see above) between the mailer and a postal system employee.
- l) **Induced Malfunction:** operating a system outside of its intended operating range can cause information such as cryptographic keys to be leaked or the device to grant unauthorised access to operations or services (e.g., modifying funds stored in a register). Malfunctions might be induced in a focused or random manner. Further information can be found in FIPS 140 [23] and UPU standard S30 [8].
- m) **IT System Infiltration:** this 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/providers, could modify the database records to the advantage of the mailer and the disadvantage of the mail service contractor. Each element of the IT system should be examined to minimise the possibility of undetected, unauthorised access to, change or deletion of data.
- n) **Miss-Application:** this covers any case in which a DPM generated for one postal 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 postal item to which it is applied. This will result in loss of revenue to the postal service if the postage accounted for is less than that which is properly due for the item 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 fraud might be difficult, as miss-application can be accidental, as well as deliberate.
- o) **Obliteration / Read rate Manipulation:** obliteration is defined as defacing a DPM in such a way that it can not 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. Detection of obliteration might be difficult, as read rates are never perfect and can be adversely impacted by accident or equipment malfunction.
- p) **Refund Requests:** refund policies, and the threats associated with them, will vary from one mail service contractor to the next. Particular attention should be paid to refund of unused prepaid postage and to refunds for spoiled items and DPMs.
- q) **Replay:** this involves the re-use or re-transmission of a message (including a DPM) 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. Replay of this could be used to create copies that are forensically indistinguishable from the originals, potentially circumventing image related countermeasures such as those discussed in C.6.5. Apart from envelope re-use, there are two principle methods of replaying data:
 - 1) record and replay: this involves recording a data transmission and replaying it at a later time either to the same printing subsystem or a different printing subsystem;
 - 2) real-time replay: this involves routing a data transmission to multiple printing subsystems at the same time (for example using a specially constructed cable or software spooling program).

NOTE copying of a DPM is treated under the heading "Copying"; Replay refers to re-use of an original DPM (compare with stamp washing).

- r) **Repudiation:** repudiation occurs when one of the parties to a transaction denies his or her involvement in it. For example, in a metering system, the sending of a postage value download to a customer's meter represents the transfer of money. If the customer subsequently claims that the download was never received, the mail service contractor could lose revenue if it is unable to tie the download transaction to the customer's subsystem (e.g. through an undeniable audit trail or transaction history). Similarly, in a system based on mail service contractor postage accounting (see 5.4), a mailer could attempt to deny responsibility for the origination of items.
- s) **Re-Use:** see Replay
- t) **Security System Infiltration:** security system infiltration is defined as 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 that the security system insulated could be exposed and advantage taken of them. Fraudulent key insertion, in which an unauthorised key value is inserted into the set of keys supported by the security system, provides a second example.
- u) **Side Channel Attack:** Side channel attacks are non invasive attacks which take advantage of the physical nature of the computational process to obtain information about the secret key. The execution of cryptographic operations involves physical processes that consume energy and require time to perform. For example, analysis of timing and/or power consumption data might reveal information about the value of the key used, even in situations in which the equipment concerned is tamper protected. Further information can be found in FIPS 140 [23] and UPU standard S30 [8].
- v) **Substitution:** substitution involves the interception of a legitimate postal item and its replacement by another. 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 mail service contractor, 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.
- w) **Underpayment:** see Miss-Application.

C.4 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 this is economically, organisationally and technically feasible. Clearly, the elimination of such vulnerability is preferable, but all practical systems suffer from weaknesses and total elimination is unlikely to be possible, 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 can either relate to the particular breach of security giving rise to it, and/or be directed against the possibility of similar breaches in the future. Thus, for example, the reaction to the detection, through sampling, of a postal item carrying an inappropriate or unreadable digital postage mark might involve either interception of the item for investigation or its delivery, possibly combined with the initiation of a closer investigation of the mailer to determine the incidence of such 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. Thus, the reaction to a postal item found to carry a duplicate digital postage mark might involve:

- returning the item instead of delivering it;
- delivering it but mounting an investigation of the mailer;
- delivering it together with an appropriate advice to the recipient;
- intercepting and opening it (in a facility authorised for this purpose) to aid in confirming the identity of the perpetrator and in collecting legally admissible evidence of fraud (see below).

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 detection, it requires the identification of the perpetrator of an attack 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 might 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. In some cultures, even a low rate of prosecutions could offer sufficient deterrence if the penalties are high enough. This might make detection and apprehension by random sampling a workable strategy if the sampling rate is chosen to give the right level of probability to catch an attacker.

Countermeasures are techniques designed to deter adversarial attacks, to enable detection of such attacks and inadvertent errors, 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.

Care should be exercised in the implementation and application of countermeasures: if they are not implemented or applied correctly and by appropriately knowledgeable personnel, additional vulnerabilities might be introduced.

Countermeasures can consist of mechanisms, procedures, laws, etc., or combinations thereof. This standard, like UPU standard S27 [6], considers them under two categories, corresponding to the S27 definitions of Message- and Applications Security.

Message security is concerned with countermeasures to protect against communications errors; the interception and/or modification of messages by third parties; the impersonation, by third parties, of authorised senders and to repudiation of messages by their sender or receiver. Message security can cover:

- a) protection of confidentiality, i.e. measures to prevent unauthorised parties from intercepting messages and/or from understanding any private content of messages which they have access to (whether legitimately or otherwise)
- b) protection of 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) authentication, i.e. methods used to validate that a message originated from a specific authorised sender and not from any other party
- d) non-repudiation, i.e. methods used to ensure that the sender of a message cannot deny having sent it and/or to ensure that the recipient(s) of a message cannot deny having received it.

Whilst DPMs are defined as containing messages and are therefore subject to message level security measures, they are not the only messages to which this applies. Many, if not all, DPM applications will also involve other messages, such as electronic messages used for credit resetting purposes, electronic or hard copy manifests (statements of mailing submission and statements of induction) and messages used by cryptographic key management systems. Though these are not dealt with within the scope of this standard, such messages are candidates for message level security and should be considered during security analysis: it is vital to ensure the integrity of **all** information flows associated with DPM applications.

Applications 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 on postal computer systems. Examples include:

- a) validation of information in a DPM against delivery or return address data;
- b) validation of information in a DPM against human readable representations of the same data (e.g. postage paid or date of intended posting);
- c) checking of total postage applied by a metering device against records of meter refills and mailing activity (volumes).

C.5 Security services and message level countermeasures

Mail service contractors desiring to implement a DPM-based postage payment system are strongly recommended to protect the security of the messages encoded in DPMs by using an appropriate combination of the four security services, namely Authentication; Confidentiality; Data Integrity and Non-Repudiation.

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 which is, in principle, known only to a particular authorised message sender, to ensure that the source of a received message is genuine – i.e. that the message was validly created and sent by the party from which it purports to have originated.

Authentication primarily acts as a countermeasure to the counterfeit and impersonation threats, but can, in some circumstances, also address the threat of illegitimate use of device. The purpose of applying an authentication service to DPMs is therefore to ensure that only authorised devices and/or users create DPMs and to assist in the identification of the users concerned. The implementation of an authentication service is recommended. Where this is done, the service should be applied to all DPMs for which capture of the encoded data occurs in practice.

Authentication is usually achieved by using cryptographic techniques such as digital signatures and message authentication codes, though other approaches are possible. Guidelines on possible implementation approaches are provided in C.9.

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 can be stored or transmitted without any fear that the protected information content will become known to a third party.

Confidentiality is addressed at the threat of IT system infiltration. However, its applicability to DPM message content is expected to be limited to cases in which:

- use is made of EVCs (see C.9.4);
- it is required to protect the identity of the mailer or DPM generation device, to prevent this from being used, by a third party (such as another postal handling organisation which legitimately handles the postal item) as a basis for estimating the mailer's traffic volumes, and /or
- the DPM contains information which the mailer wishes to keep confidential.

The confidentiality service also has clear applicability in cases in which generation and printing of the DPM are separated by an intervening network – though this provides an example of application of the service to electronic messages containing DPM data, rather than to the protection of the DPM message when encoded on a postal item. In particular, the service can be used to prevent the unauthorised interception and subsequent printing of the DPM by an intruder on the network. If they were not protected and an intruder intercepted and used them, a duplicate database countermeasure (see C.6.3) would certainly detect such unauthorised use; however, the information available to postal inspectors would lead back to the authorised mailer, not to the intruder.

Where required, confidentiality is normally implemented by encrypting (cryptographically transforming) the data to be protected, using either the public key of a complementary public/private key pair of which the private key is known only to the intended recipient of the message, or using a secret key known only to the sender and intended recipient.

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 threat of alteration, but can also be used to protect against miss-application if integrity protection is extended to include data which is intrinsic to the correct postal item. In this case, applying the DPM to the wrong postal item will result in a change to this intrinsic data, resulting in a case of alteration.

The implementation of a data integrity service is recommended. Moreover, the service should be applied to all DPMs for which capture of the encoded data occurs in practice. It is also important for the protection of electronic messages, such as statements of mailing submission and credit resetting messages, which could be associated with many DPM applications.

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. Guidelines on possible implementation approaches are provided in C.9.

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 having sent it (sender non-repudiation) and/or to prevent the receiver from successfully denying having received it (receiver non-repudiation). This could be particularly relevant in any prosecution of (attempted) fraud, in which it might be essential to prove the identity of the perpetrator.

Sender non-repudiation has clear applicability to electronic and other non-DPM messages that are exchanged between the mailer, the mail service contractor and their agents. However, because of the threat of copying and the possibility that a particular DPM might not actually be read by the postal handling system, it has limited applicability to DPM messages themselves.

The result of sender non-repudiation applied to a DPM message can provide a reasonable guarantee (counterfeits excepted) that the mailer or DPM generation device indicated by the DPM indeed generated a DPM with corresponding content. However, postal item transport is generally insecure, so the postal item could, in principle, be seen by multiple parties during its creation and processing. Any of these parties could take a copy of the DPM and apply it to another postal item. Thus, unless all copied DPMs can be proven to result in misapplication, it is possible for the mailer to claim that the item bearing a particular DPM was not created by him, but carries a copy of one of his DPMs. To avoid any counterclaim that this would have resulted in detection of a duplicate by the postal system, he might go on to claim either that the genuine item has already been delivered, without its DPM data being captured, or that the item concerned was never actually mailed. Given this, sender non-repudiation applied to a DPM message can, at best, serve to support other evidence (e.g. content) of the origin of a postal item.

Sender non-repudiation also applies to the entity which generated the information used in provision of the non-repudiation service. Depending on the business and applications scenario, this might not be the mailer: for example, it might be the mailer's metering device (which could conceivably be the subject of unauthorised use) or a mail finisher which works on behalf of the mailer and which might, knowingly or in error, 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 might 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 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 necessarily have 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, the 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 did not receive a message, or received it at a time other than that of its real receipt – can 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.

Security of access to the message communications channel can also play a role in protection against both sender and receiver repudiation: for example, in the case of messages submitted on physical supports, acceptance control procedures can be used to validate sender identity at the point of message handover; similarly, signing procedures are traditionally used (c.f. registered mail) to confirm reception. However, this consideration cannot apply to DPMs themselves, since these have to be presumed accessible to any party with access to the postal item.

C.6 Applications level countermeasures

C.6.1 Introduction

The following outlines some of the applications level countermeasures that may be applied. It is stressed that those outlined should in no way be construed as representing a complete list of possibilities and mail service contractors are encouraged to creatively consider other techniques.

Given the scope of this standard, the following concentrates on countermeasures which relate, in some way, to digital postage marks whose primary purpose is to provide evidence of, or the basis for, postage accounting. This evidence is intended to enable the mail service contractor (or its agent) to improve its ability to detect attempted postal fraud. Where (possibly) fraudulent activity is detected, the information in the DPM, together with other information present on (and in appropriate circumstances, in) the postal item, can assist in identification of the responsible party and provide legally admissible evidence. This is only possible if the DPM contains appropriate data elements (see Annex E) which are protected from manipulation (see data integrity in C.5) and are consistent with other (audit) information that is available within the postal payment system.

C.6.2 Access and usage controls

A wide variety of threats can be effectively countered by limiting access to, or controlling the usage of, sensitive parts of the system. In non-DPM-based postage metering systems, it is normal to control usage through credit resetting procedures and watchdog timers and to protect against device modification by controlling physical access using tamper detection techniques. Such approaches are also likely to be needed in a DPM applications environment, in particular for the protection of cryptographic keys and funds related data. FIPS PUB 140-2 [23] and UPU standard S30 [8] provide guidance in assuring that cryptographic keys are managed securely within a module. Similar principles should be applied to the protection of funds related data. It should be noted that the particular countermeasures employed [see particularly b), d), f) and g) below] could depend upon the DPM system topology and location of the accounting and cryptographic subsystems.

Approaches which should be considered include:

- a) **Credit Control:** credit controls are value counters which, in postage accounting applications, limit the amount of postage which may be accounted for by an accounting device. Typically, the limit can be reset through credit resetting procedures linked either to inspection of the device, or to contact with a credit resetting (device management) system. Two cases can be considered. In the first, the control 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 credit limit. In the second case, the control 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 DPMs) by causing DPMs produced by devices which have used up their credit limit to be rejected as invalid.
- b) **Electronic Access Control:** this involves the use of logical means to limit access to sensitive functions or services to authorised entities (individual users, programs, processes, or systems). This requires authentication (i.e. verification that the accessing entity is indeed the entity which it claims to be). As described in FIPS 140-2 [23] clause 4.3, authentication can be based on the use of logical keys (passwords or PINs); physical keys, such as smart cards, and intrinsic attributes, such as fingerprints or other biometric characteristics.

The purpose of applying an electronic access control technique within a DPM system can be twofold: to ensure that only specific entities can access the sensitive functionality concerned and/or to aid in binding an entity to the instance of use of the functionality, as a means of preventing repudiation.

It is recommended that at least postage accounting, credit re-setting, supervisory and security functions are protected by means of electronic access control. Sensitive systems should be implemented with multiple levels of access control, so that accessing entities with different operational roles and levels of security clearance can have different access rights. Where necessary, such access rights should enforce requirements for several independent entities to be involved in the activation of critical functions. For example, manual entry of a cryptographic key, if required, should be achieved by having different individuals enter different components of the key, so that no one can (in the absence of collusion) acquire knowledge of the full key. Similarly, reset of critical systems, such as the DPM verification system, should require at least two separate and independent operations.

If electronic access control is implemented using passwords or PINS, measures should be taken to ensure that:

- these are changed on a regular basis;
- they are not stored on the application's operating platform, but entered by the entity seeking access to the application;
- individual users and systems designers are made fully conscious of the need for security.

Electronic access control might need to be bi-directional. That is, an entity (person or applications process) which is required to prove its identity to an accessed applications service or function, might need to have the application concerned prove its identity in return.

This requirement for bi-directional electronic access control is particularly evident in the case of two applications processes, each of which needs to be sure of the software and version number of its counterpart.

It is recommended that a configuration management system is used to provide assurance that applications software components:

- are correctly installed and configured before being permitted to operate, and
- are regularly monitored to verify their configuration, version number and integrity (i.e. that they have not been modified).

NOTE 1 This can be achieved in a variety of ways. For example, each process could request a (variable) hash total calculation on the other.

NOTE 2 It is emphasised that configuration management provides non adversarial users with a tool for bi-directional electronic access control, while enabling detection of the use of inappropriate software.

c) **Lost & Stolen Device Management:** lost and stolen devices are defined as devices that are no longer in the possession of the authorised entity. This can apply to highly sensitive equipment used by authorised providers of electronic postage and to DPM verifiers as well as to meters and other security devices used by mailers. It is almost certainly appropriate for sensitive equipment to be uniquely identifiable, with records being retained of authorised usage. Transactions involving a particular device should include, or allow access to, the device identifier, so that corrective action (such as rejection of all DPMs) can be taken in case of use of a device which has been registered as lost or stolen. Ideally, it should be possible to remotely deactivate devices when they contact the management system, e.g. for credit or watchdog timer resetting purposes.

d) **Physical Access Control:** physical access to a sensitive device can be controlled by housing the device in a facility to which physical entrance is limited to authorised persons. The requirements for such physical access control systems are comparable with those applying in the case of other sensitive computer-based systems, and are not considered further in this standard.

Physical access controls may be applied at any scale, from site, through building and room, to individual enclosure. Access control systems themselves should be provided with tamper protection (see below). Subject to this, physical access control might be adequate, without the further tamper protection of individual devices, in the case of devices housed in postal system facilities, and even, subject to postal security audit, in the case of devices operated by approved suppliers (e.g. dispensers of electronic postage value), but is unlikely to be appropriate in cases in which sensitive equipment is housed on customer premises. In such cases, consideration should be given to providing the devices concerned with tamper protection (see below).

e) **Secure Link of Printing & Accounting:** one of the key potential problems with the use of digital printing technology is the ease with which print images can be reproduced. At least in cases in which there is no other adequate way of detecting the use of such duplicates (see C.6.3), it might be desirable to make this more difficult by securely linking the DPM printer to a postage accounting module, preventing use of the printer for (unaccounted) reproduction of DPMs. Though this countermeasure does not prevent the copying of DPMs (e.g. by digitally scanning them and reprinting the image using another printer), it might help in ensuring that the resulting prints are forensically distinguishable from original prints, produced by the authorised printer. The effectiveness of this measure can be enhanced by using DPM printers which have distinctive features.

- f) **Side channel leakage protection:** side channel attacks depend upon information gained from the analysis of cryptographic function execution timing and/or power consumption. Such attacks can be protected against by the use of techniques designed to mask variations in these physical parameters. The need for and complexity of such countermeasures is dependent on the type of computer chip and algorithm involved – some algorithms and chips are more susceptible to side channel attacks than others – and no clear standard has yet emerged in this area. As a minimum, it is recommended that security devices which execute cryptographic algorithms for the computation of CVCs should be tested against susceptibility to side channel attacks.
- g) **Tamper Protection:** as is the normal case with traditional postage meters, sensitive devices can be fitted with physical security features which result, with high probability, in unauthorised attempts at access, use, or modification of the device being either detected subsequent to the attempt by leaving visible signs (i.e. tamper evident), or being detected during the attempt (i.e. tamper detection) so that appropriate actions can be taken by the device to protect itself (i.e. tamper response). FIPS PUB 140-2 [23] and UPU standard S30 - International postage meter approval requirements (IPMAR) [8] provide requirements for device tamper protection mechanisms.

A device that has been engineered to be only tamper evident, does not provide protection in and of itself. However, when used in conjunction with a periodic physical device inspection, this can be an effective countermeasure.

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 DPM generation devices, disablement might not always be the best option: given the data carrying characteristics of the DPM, it might be preferable, instead, to continue to allow the device to continue to generate DPMs, but to flag these as invalid due to tampering (c.f. the principle of silent alarms for physical access control).

- h) **Usage Count Control:** usage count controls are usage counters which limit the number of times a device, or one of the services which it provides, can be used. They are particularly applicable to DPM verification devices, which are open to (miss-)use to test the validity of counterfeit DPMs with guessed security data.

Several levels of control might be desirable. For example:

- i) a limit on the number of attempts to validate a particular transaction (e.g. verification of DPM or validation of an access control password) within a given period (or consecutively);
- ii) a limit on the overall usage of the verification device or function (e.g. on the total number of validations performed in a day, or until reset of the device by a privileged user);
- iii) a limit on the overall number or rate of validation failures permitted either consecutively; within a given time period, and/or until the device is reset by a privileged user.

NOTE 3 This is potentially more powerful than an overall usage limit. For example, a high speed on-line verifier might be capable of performing around 30 verification operations per second – almost 2,6 million per day – but might (in normal circumstances) practically be used for only half that number. If such a verifier could be accessed by an attacker and used to check the validity of guessed counterfeit DPMs protected by a 10-bit cryptographic code, the counterfeiter, with a 1 in 1 024 probability of a correct guess each time, would be able to create 2 531 apparently valid counterfeit DPMs per day if there were no control and 1 465 per day if use of the verification device were limited to 1,5 million validations per day. However, if, in normal use, 95 % or more of DPMs validated were expected to be legitimate, a device 'validation failure' limit could be set to perhaps 100 000 per day. With this limit, the counterfeiter would only be able to check 100 098 guesses, resulting in 97 valid counterfeits, before the device disabled itself. Similarly, with a normal 95 % success rate, the probability of a string of 20 consecutive failures is about 1 in 10^{26} . For the counterfeiter, who has a success rate of only 1 in 1 024, the probability is around 0,98. So imposing a limit of 20 consecutive failures will rarely stop the verifier in normal operation (though the possibility of a bad 'batch' of DPMs does exist), but would have a good chance of stopping the counterfeiter before he was able to obtain a single valid DPM.

- i) **Watchdog Timers:** watchdog timers are timers which are 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 can be permanent or temporary (i.e. until the next inspection or contact). Two cases can 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 DPMs) by causing DPMs produced by 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, the implementation of excessive controls is of limited value.

C.6.3 Duplicate detection

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 beyond any shadow of doubt, it is necessary, when faced with one item, to show that some earlier item (which might have already been delivered and so have left the system) carried the same DPM. In principle this can be achieved through the use of a duplicates database:

- during the process of verifying a postal item, the DPM data is captured and compared to previously processed DPM data that is stored in the database;
- if the given DPM has not been encountered on a previous item, it is added to the database for use in future comparisons;
- if the DPM has been encountered before, the postal item carrying it **and** the previous item which carried an identical DPM are flagged as possible duplicates;
- other data are consulted (see below), or an investigation is carried out, to determine which (if either) of the two postal items is genuine, and which carries a copied DPM.

For this approach to work, each legitimate DPM has to be unique⁹⁾. This can be achieved in a variety of ways, including the inclusion in the DPM of either a (non-resettable) counter that always increases; the value of the metering device's ascending register, or a date/time stamp to the appropriate granularity, etc.

No matter which method is used to make each DPM unique, the approach requires access to a database of "used" DPMs during the postal item verification process. By its very nature, this database can grow very large: in a worst case scenario, with poor security system design, this could involve retaining, and searching through, details of **all** DPMs that have **ever** been used. Even given current computer and database technology, this would have severe cost and processing implications.

One way of reducing the cost would be to attempt duplicate detection for only a selected sample of postal items (see Annex F). This reduces both the size of the database and the processing required to search it. However, it also reduces the probability of finding a match, since, even if the postal item being examined carries a copied DPM, there is a good probability that the original was never sampled.

A second potential problem results from the fact that DPMs might be read at several different points in the mail handling process. Given this, the finding of a DPM which matches one which has already been seen need not necessarily imply that the DPM is a duplicate: it could simply be that the postal item carrying it has been intercepted for a second time, perhaps because it is, for some reason, being reprocessed. A mechanism which is independent of the DPM is therefore needed to distinguish between items.

ID-tags provide one mechanism for doing this. ID-tags are postal item identifiers which are applied by (or under the close supervision of) the mail service contractor, preferably during the first automated processing of a postal item (e.g. at induction; during facing and cancelling, or during outward sorting). Different postal items carrying identical DPMs would be assigned different ID-tags, allowing them to be distinguished from one another – and providing proof that DPM duplication has occurred. Note that customer applied identifiers cannot adequately fulfil this role: a fraudulent mailer would simply copy **both** the DPM and the item identifier.

Even where the occurrence of DPM duplication can be proven, the discrimination between paid and fraudulent postal items might be non trivial: which postal item carries a duplicate – the one resulting in duplicate detection, or the earlier one, which might have already been delivered?

⁹⁾ Strictly speaking, it is **not** necessary for DPMs to be unique. In some applications (e.g. PPI mail), it might be desirable to allow the same DPM to be applied to a whole batch of items. In this case, the requirement would not be to prevent duplication, but to ensure that a given DPM was not used more times than is accounted for. The database would need to keep a record of the authorised number of uses and to support comparison between this and the actual number of incidences of the DPM encountered.