SLOVENSKI STANDARD
SIST EN 14615:2005

01-maj-2005

Poğtne storitve ï Digitalne poğtne oznaļ be ï Uporaba, varnost in oblikovanje

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

Postalische Deinstleistungen - Digitale Freimachungsvermerke - Inhalte, Sicherheit und Gestaltung

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

Ta slovenski standard je istoveten z: **EN 14615:2005**

ICS:

03.240	Poštne storitve	Postal services

SIST EN 14615:2005 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 14615

January 2005

ICS 03.240

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

Ref. No. EN 14615:2005: E

Contents

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 UPU[1] 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 Board[2] 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 licensed[3] 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 glossary[4)]

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 stamp washing).

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•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:

a) the information content is expressed in the form of a message, containing internationally standardised data constructs;

b) the message is represented on the postal item in the form of one or more machine readable symbols;

c) 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.

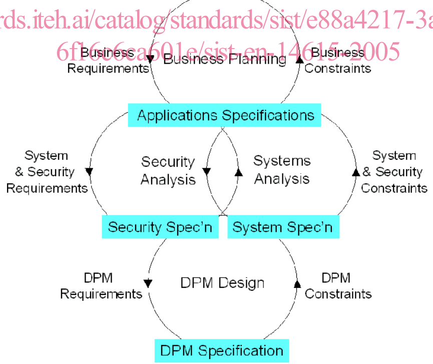

Figure 1 — DPM Applications and Design Process

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.