ICS 03.240 SLOVENSKÁ TECHNICKÁ NORMA Marec 2018

STN	**Poštové služby Digitálne poštové známky Použitie, bezpečnosť a navrhovanie**	**STN EN 14615** 96 1015

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 02/18

Obsahuje: EN 14615:2017

Oznámením tejto normy sa ruší
STN EN 14615 (01 0130) z augusta 2005

126116

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2018
Podľa zákona č. 264/1999 Z. z. o technických požiadavkách na výrobky a o posudzovaní zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov sa slovenská technická norma a časti slovenskej technickej normy môžu rozmnožovať alebo rozširovať len so súhlasom slovenského národného normalizačného orgánu.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 14615

September 2017

ICS 03.240

Supersedes EN 14615:2005

English Version

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

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

Postalische Dienstleistungen - Digitale Freimachungsvermerke - Anwendungen, Sicherheit und Gestaltung

This European Standard was approved by CEN on 2 December 2016.

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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre has the same status as the official versions.

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2017 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 14615:2017 E

Contents

Page

European foreword 5
Introduction 6
1 Scope 8
2 Normative references 8
3 Terms and definitions 8
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 15
5.5 DPM design 16
Annex A (normative) Specification checklists 17
A.1 Applications specifications 17
A.2 System specification 17
A.3 Security specification 18
A.4 DPM specification 18
Annex B (informative) Business planning considerations 19
B.1 Possible applications 19
B.2 Market segmentation 20
B.3 Applications selection 23
Annex C (informative) Security analysis considerations 26
C.1 Context 26
C.2 Security objectives, policy and economics 27
C.3 Threats and vulnerabilities 28
C.4 Applications and message level security 32
C.5 Security services and message level countermeasures 34
C.6 Applications level countermeasures 36
C.7 Countermeasure selection 47
C.8 Application of countermeasures 49
C.9 Message security implementation options 49
Annex D (informative) Systems analysis considerations 56
D.1 Requirements analysis 56
D.2 Functional description 57

D.3 Function allocation and architecture design 60
D.4 Other detailed design aspects 60
Annex E (informative) DPM design considerations 67
E.1 Data content 67
E.2 Data entry 68
E.3 Data construct mapping 69
E.4 Symbology 70
E.5 Human readable information 71
E.6 Layout, facing and aesthetics 72
E.7 Performance and test criteria 73
Annex F (informative) Statistical analysis of DPM verification 74
F.1 Introduction 74
F.2 Purpose and scope of postal item verification 74
F.3 Detection of DPMs with invalid validation code 75
F.4 Influence of CVC length on fraud detection 80
F.5 Detection of duplicate DPMs 81
Annex G (informative) Message security algorithms 82
G.1 Introduction 82
G.2 Hash functions used in message security services 82
G.3 Asymmetric (public key) cryptographic algorithms 83
G.4 Message authentication code (MAC) algorithms 86
G.5 Exchange validation code generation 90
G.6 Selection of algorithms for CVC implementation 90
Annex H (informative) CVC generation and verification data 96
H.1 Introduction 96
H.2 Sources of data for verification 96
H.3 Selection of data used in the verification process 97
Annex I (informative) Architecture examples 103
I.1 Introduction 103
I.2 The REMPI architecture 103
I.3 USPS IBIP configurations 107
Annex J (informative) Examples of digital postage marks (not to scale) 112
J.1 Australia Post 112
J.2 Canada Post 112
J.3 Deutsche Post 112
J.4 Die Post, Switzerland 114
J.5 Royal Mail 115
J.6 United States Postal Service (USPS) 116

Annex K (informative) Relevant intellectual property rights (IPR) **118**
K.1 Introduction **118**
K.2 Massachusetts Institute of Technology **118**
K.3 Neopost **118**
K.4 Pitney Bowes Inc **119**
K.5 Pitney Bowes Inc, together with Certicom Corp **119**
K.6 United States Department of Commerce **120**
K.7 United States Postal Service **120**
Annex L (informative) DPM design charts **121**
L.1 Applicability of countermeasures against identified threats **121**
L.2 Data elements used by typical applications and countermeasures **125**
L.3 Mapping data elements onto data source and DPM data constructs **129**
Bibliography **131**

European foreword

This document (EN 14615:2017) 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 March 2018, and conflicting national standards shall be withdrawn at the latest by March 2018.

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

This document supersedes EN 14615:2005.

This document (EN 14615:2017) 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 second 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.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the 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 192 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 maximize 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.

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.

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

---

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.

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 [7], or requiring data which cannot be accommodated within S25-defined data constructs.

NOTE 1 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 2 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.

1 Scope

This European Standard 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 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.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, 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 and S25 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.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN