ICS 03.240 PREDBEŽNÁ SLOVENSKÁ TECHNICKÁ NORMA August 2020

STN P	**Poštové služby** **Infraštruktúra DPM (digitálne poštové značky)** **DPM aplikácie pre podporu informácií**	**STN P** **CEN/TS 15130** 96 1016

Postal services - DPM infrastructure - Messages supporting DPM applications

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. 07/20

Táto predbežná STN je určená na overenie. Pripomienky zasielajte ÚNMS SR najneskôr do 1. 3. 2022.

Obsahuje: CEN/TS 15130:2020

131278

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN/TS 15130

April 2020

ICS 03.240 Supersedes CEN/TS 15130:2006

English Version

Postal services - DPM infrastructure - Messages supporting DPM applications

Services Postaux - Affranchissement électronique, Infrastructure du système - Messages pris en charge par les applications

Postalische Dienstleistungen - Infrastruktur für Elektronische Freimachungsvermerke (DPM) - Nachrichten zur Unterstützung von Anwendungen der DPM

This Technical Specification (CEN/TS) was approved by CEN on 21 October 2019 for provisional application.

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

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

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, 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: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 15130:2020 E

Contents

Page

European foreword

This document (CEN/TS 15130:2020) has been prepared by Technical Committee CEN/TC 331 “Postal Services”, the secretariat of which is held by NEN.

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

This document will supersede CEN/TS 15130:2006.

In comparison with the previous edition, the following technical modifications have been made:

a) Normative Annex A Implicit certification process, has been updated with reference to a state-of-the-art algorithm for new applications of digital signature generation and verification.

b) The Bibliography has been updated accordingly.

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

Introduction

The purpose of this document is to define a consistent and complete set of messages between vendors and posts infrastructures in support of DPM applications.

It is assumed that the reader of this document is familiar with computer-related technologies normally used to design and implement applications requiring an interaction between computer systems. This document makes use of industry-accepted technical standards and concepts like public key cryptography and communication protocols.

This document defines the significant content and the format for data exchanges and messages, consistent with current industry practices. Also, consistent with the concepts of extensibility and flexibility, this document allows for extensions supporting specific (local) implementations using additional data elements.

1 Scope

This document specifies the information exchanges between various parties' infrastructures that take place in support of DPM applications. It complements standards that address the design, security, applications and readability of Digital Postage Marks.

The following items will be addressed by this document:

— identification of parties participating in exchanges of information described by this document;

— identification of functions (interactions, use cases);

— definition of parties' responsibilities in the context of above functions;

— definition of messages between parties: message meaning and definition of communication protocols to support each function;

— definition of significant content (payload) for each message;

— security mechanisms providing required security services, such as authentication, privacy, integrity and non-repudiation.

This document does not address:

— design of DPM supporting infrastructure for applications internal to providers and carriers;

— design of DPM devices and applications for applications internal to end-users.

NOTE Although there are other communications between various parties involved in postal communications, this document covers only DPM-related aspects of such communications.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9798-3, *IT Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques*

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