SLOVENSKI STANDARD
kSIST-TS FprCEN/TS 15130:2019

01-september-2019

Poštne storitve - Infrastruktura za elektrotehnične zaznamke pri frankiranju (DPM) - Informacije v podporo uporabi DPM

Postal services - DPM infrastructure - Messages supporting DPM applications

Postalische Dienstleistungen - Infrastruktur fÃ¼r Elektronische Freimachungsvermerke (DPM) - Nachrichten zur UnterstÃ¼tzung von Anwendungen der DPM; Englische Fassung CEN/TS 15130:2006

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

Ta slovenski standard je istoveten z: FprCEN/TS 15130

ICS:

03.240	Poštne storitve	Postal services
35.240.69	Uporabniške rešitve IT pri poštnih storitvah	IT applications in postal services

kSIST-TS FprCEN/TS 15130:2019 en,fr,de

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

FINAL DRAFT
FprCEN/TS 15130

June 2019

ICS

Will supersede 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 fÃ1/4r Elektronische Freimachungsvermerke (DPM) - Nachrichten zur UnterstÃ1/4tzung von Anwendungen der DPM; Englische Fassung CEN/TS 15130:2006

This draft Technical Specification is submitted to CEN members for Vote. It has been drawn up by the Technical Committee CEN/TC 331.

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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Specification.

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. FprCEN/TS 15130:2019 E

Contents

Page

European foreword

This document (FprCEN/TS 15130:2019) has been prepared by Technical Committee CEN/TC 331 “Postal Services”, the secretariat of which is held by NEN.

This document is currently submitted to the Vote on TS.

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.

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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
ascending register value
numerical value that is equal to the total accumulated value of postage that has been accounted for and printed by the mailing system (usually used in the context of a postage meter or a franking machine)

3.2
authentication
verification of the identity of a person, process or the origin of the data being exchanged

3.3
control sum
sum of the descending register value and ascending register value in a mailing system

3.4
cryptographic material
information used in conjunction with cryptographic methods of protecting information

3.5
cryptographic key
information that uniquely determines a bijection (one-to-one transformation) from the space of messages to the space of ciphertexts

3.6
Cryptographic Validation Codes
CVC
value, cryptographically derived from selected postal data, which may be used in verifying the integrity of such data and authenticating its origin

3.7
data integrity
property of a communication channel whereby data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source

3.8
descending register value
numerical value equal to the total value of unused postage remaining in the mailing system (usually used in the context of a postage meter or a franking machine)

3.9
Digital Postage Mark
DPM
postmark printed or otherwise attached to a mail item and containing information that may be captured and used by mail handling organizations and the recipient

3.10
DPM signature verification key
public key that is used for the DPM signature verification

3.11
DPM signing Key
DPM signature generation key
private key that is used for digital signing of DPM information

3.12
DPM verifier
verifier
postal equipment that is used for DPM verification

3.13
Exchange Validation Codes
EVC
code, known to or agreed between a mailer and a licensing post, which when applied to a postal item by the mailer may 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

3.14
implicit certificate
informational element that binds an entity's identity with its public cryptographic key allowing the verification of the digital signature by another entity using only information contained within the certificate itself

Note 1 to entry: In Digital Postage Mark verification systems based on public key cryptographic schemes, the verification key is public and can either be retrieved from a database (explicit certificate) or it can be computed from the information contained in the Digital Postage Mark (implicit certificate).

3.15
key management infrastructure
systems, policies and procedures used to create, store, distribute and update cryptographic keys

3.16
license
formal permission to account for postal charges and create an agreed upon evidence of payment for such charges given to qualified mailers by posts, carriers or their authorised agents

3.17
license number
informational element (typically numeric or alphanumeric code) that represents the fact that a mailer has obtained license from the post or a carrier authorising the mailer to account for postal charges and to print evidence of a paid postage

3.18
licensing post
postal organisation responsible for issuing licenses to qualified mailers

3.19
MAC key
DPM MAC key
Message Authentication Code (MAC) key used for the protection of the Digital Postal Mark (DPM) in DPM systems based on symmetric key cryptographic schemes

3.20
mailer
person or organization using the services of a post

3.21
mailing system
system which is used to account and evidence charges for postal services

Note 1 to entry: Variations of a mailing system include:

- franking machine or postage meter;
- personal computer with specialized software;
- online software service

3.22
Message Authentication Code
MAC
value, cryptographically derived from selected data, which allows data integrity and implicit data origin to be verified

Note 1 to entry: Since MACs are based on shared secret schemes they allow for weaker (implicit) data origin verification than digital signatures that are based on public key cryptographic schemes.

3.23
non-repudiation
security service which prevents an entity from denying previous commitments or actions

3.24
parametrisation
process of supplying a system or a device with all input information required for proper operation, involving assignment of specific numerical values to named variables used in computation of output values such as data elements of DPM

3.25
post
postal administration postal authority

organization which has been designated by the UPU member country or territory as an operator responsible for fulfilling part or all of the member's obligations arising from adherence to the UPU convention and agreements

3.26
postal code
numeric or alphanumeric value that is uniquely indicative of a geographic location of an element of postal processing and delivery network, including postal processing facilities, retail offices, delivery units and individual recipient’s mailboxes

3.27
privacy
confidentiality
security service used to keep the (meaningful) content of the information from all but those authorised to have it

3.28
public key cryptography
cryptographic system that uses two keys: a public key accessible to all parties and a private or secret key known only to one party (either the sender or the recipient of the message depending on the use of the system)

Note 1 to entry: An important element of the public key system is that the public and private keys are uniquely related to each other and it is computationally infeasible to compute private key from the knowledge of public key.

3.29
Public Key Infrastructure
PKI
system of digital certificates, certificate authorities, and registration authorities or agents that allows for authentication of all parties involved in communication and data exchange processes

3.30
symmetric key cryptography
encryption system in which the sender and receiver of a message share a single, common secret information (key) that is used both to encrypt and decrypt messages that are being exchanged

3.31
time stamp
value of the current time stored by a system to indicate when a certain transaction took place

3.32
Universal Coordinated Time
UCT
universal time, taking into account the addition or omission of leap seconds by atomic clocks each year to compensate for changes in the rotation of the earth (Greenwich Mean Time updated with leap seconds)

3.33
vendor
provider and/or operator of mailing systems

3.34
World Wide Web Consortium
W3C
international consortium of companies involved with the development of open standards for internet and the web

3.35
XML
Extensible Mark-up Language
subset of SGML constituting a particular text mark-up language for interchange of structured data

3.36
XML schema
XML schema is an XML language for describing and constraining the content of XML documents

4 Requirements

4.1 Functional structure

This clause covers the organization of the logical layer of communication between post and vendor.

In the context of this document, a typical postal operator or a carrier of physical mail items is organized along well-defined functional elements. Specifically, typical functional elements are postal operations (including: mail collection, processing, sorting, transportation and delivery) and system administration and management control (including finance and marketing).

Since this document defines (for the major part) communications between vendor and post aimed at supporting postal revenue collection based on DPM, the postal operator is the main recipient and beneficiary of the information collected and communicated within the DPM supporting infrastructure.

Therefore, the functional requirements are organized to match the functional elements of the postal organization namely: postal operations and system administration and management control. Accordingly, Clause 5 of the present document is organized into the following major subclauses:

- key management processes;
- licensing and parameterization of mailing systems;
- data collection and reporting processes;
- audit-related process.

In this organization, key management processes support postal operations while licensing and parameterization, data collection and audit-related clauses support system administration and management control.

Postal revenue collection systems that are based on DPM require postal verification of accounting processes performed by mailers. In practice, this amounts to DPM verification that is performed on individual mail items and, as such, becomes a part of postal operations.

DPM verification requires that all verification equipment (verifiers) have access to DPM verification keys or key materials (symmetric or public).

For the purpose of this document these verification keys are supplied to verifiers from postal key management infrastructure. The postal key management infrastructure in its relation to vendor key management infrastructure is covered in subsequent clauses of this document.

4.2 Technical requirements

Technical requirements for this document are driven by the needs of posts and vendors to create and operate a cost-effective, functional and efficient infrastructure which allows them to exchange information as described in Clause 5.

This infrastructure will allow interoperability between systems owned and operated by vendors and posts eliminating the need for custom interfaces between specific parties. The use of established technologies and industry-standard solutions will minimize the cost of such infrastructure. The optimum set of solutions is highly dependent on specific conditions and the state of the technology at any given time.

Specific performance levels (like scalability, speed, reliability, availability) are outside the scope of this document, as they evolve quickly and they vary greatly between organizations.

Annex B includes as an example a specific implementation of the transport layer using XML schema standard for data representation.