

DIN CEN/TS 15130

ICS 03.240

Ersatz für
DIN CEN/TS 15130:2006-07**Postalische Dienstleistungen –
Infrastruktur für Elektronische Freimachungsvermerke (DPM) –
Nachrichten zur Unterstützung von Anwendungen der DPM;
Englische Fassung CEN/TS 15130:2020**

Postal services –
DPM infrastructure –
Messages supporting DPM applications;
English version CEN/TS 15130:2020

Services Postaux –
Affranchissement électronique, Infrastructure du système –
Messages pris en charge par les applications;
Version anglaise CEN/TS 15130:2020

Gesamtumfang 52 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (CEN/TS 15130:2020) wurde vom Technischen Komitee CEN/TC 331 „Postalische Dienstleistungen“ erarbeitet, dessen Sekretariat von NEN (Niederlande) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-03-04 AA „Postalische Dienstleistungen“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden Technischen Spezifikation wurde kein Entwurf veröffentlicht.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung von CEN/TS 15130:2020.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Erfahrungen mit dieser Technischen Spezifikation sind erbeten:

- vorzugsweise als Datei per E-Mail an nia@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter <http://www.din.de/stellungnahme> abgerufen werden;
- oder in Papierform an den Normenausschuss „Informationstechnik und Anwendungen (NIA)“ im DIN Deutsches Institut für Normung e. V., 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Änderungen

Gegenüber DIN CEN/TS 15130:2006-07 wurden folgende Änderungen vorgenommen:

- a) Begriffe aktualisiert;
- b) Norm redaktionell überarbeitet.

Frühere Ausgaben

DIN CEN/TS 15130: 2006-07

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerung der folgenden Begriffe ist identisch mit der Benummerung in der englischen Fassung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

aufsteigender Registerwert

numerischer Wert, der dem Gesamtwert des angefallenen Portos entspricht, das von dem Versandsystem (üblicherweise im Zusammenhang mit einem Freistempler oder einer Frankiermaschine genutzt) ausgewiesen und ausgedruckt wurde

3.2

Authentisierung

Verifizierung der Identität einer Person, eines Prozesses oder des Ursprungs der ausgetauschten Daten

3.3

Kontrollsumme

Summe aus dem absteigenden Registerwert und dem aufsteigenden Registerwert in einem Versandsystem

3.4

kryptographisches Material

Informationen, die im Zusammenhang mit kryptographischen Verfahren zum Schutz von Informationen genutzt werden

3.5

kryptographischer Schlüssel

Information, die eine Bijektion (Eins-zu-eins-Umwandlung) von Nachrichten zu chiffrierten Texten eindeutig definiert

3.6

kryptographische Validierungscodes

CVC, en: Cryptographic Validation Codes

aus ausgewählten Postdaten kryptographisch abgeleiteter Wert, der bei der Verifizierung der Integrität solcher Daten und der Authentisierung ihres Ursprungs genutzt werden darf

3.7

Datenintegrität

Eigenschaft eines Kommunikationskanals, wonach Daten seit dem Zeitpunkt ihrer Erstellung, Übertragung oder Speicherung durch eine autorisierte Quelle nicht auf unzulässige Weise abgeändert wurden

3.8

absteigender Registerwert

numerischer Wert, der dem Gesamtwert des nicht genutzten Portos entspricht, das in dem Versandsystem (üblicherweise im Zusammenhang mit einem Freistempler oder einer Frankiermaschine genutzt) verbleibt

3.9

elektronischer Freimachungsvermerk

DPM, en: Digital Postage Mark

Poststempel, der auf eine Sendung gestempelt oder einer Sendung anderweitig beigelegt wird und Informationen beinhaltet, die von sendungsverarbeitenden Organisationen und vom Empfänger erfasst und genutzt werden können

3.10

DPM-Signatur-Verifizierungsschlüssel

öffentlicher Schlüssel, der für die Verifizierung einer DPM-Signatur genutzt wird

3.11

DPM-Signierschlüssel

DPM-Schlüssel zur Erstellung einer digitalen Signatur

privater Schlüssel, der zum digitalen Signieren von DPM-Informationen genutzt wird

3.12

DPM-Verifizierer

Verifizierer

postalische Einrichtung, die zur DPM-Verifizierung genutzt wird

3.13

Validierungscodes des Datenaustauschs

EVC, en: Exchange Validation Codes

Code, der einem Versender und einer lizenzierenden Post bekannt ist oder zwischen ihnen vereinbart wurde und, wenn er vom Versender auf einer Sendung angewendet wurde, von der lizenzierenden Post genutzt werden darf, um den Ursprung der Sendung zu authentisieren und unter entsprechenden Umständen die Integrität der vereinbarten DPM-Daten zu verifizieren

3.14

implizites Zertifikat

Informationselement, das die Identität einer Instanz an ihren öffentlichen kryptographischen Schlüssel bindet, um die Verifizierung der digitalen Signatur durch eine andere Instanz ausschließlich anhand von Informationen, die in dem Zertifikat selbst enthalten sind, zu ermöglichen

Anmerkung 1 zum Begriff: In Systemen zur Verifizierung von elektronischen Freimachungsvermerken auf der Grundlage von kryptographischen Verfahren mit öffentlichen Schlüsseln ist der Verifizierungsschlüssel öffentlich und kann entweder aus einer Datenbank abgerufen (explizites Zertifikat) oder aus den Informationen, die im elektronischen Freimachungsvermerk enthalten sind, errechnet werden (implizites Zertifikat).

3.15

Infrastruktur der Schlüsselverwaltung

Systeme, Richtlinien und Verfahren zur Erstellung, Speicherung, Vergabe und Aktualisierung von kryptographischen Schlüsseln

3.16

Lizenz

formelle Erlaubnis zur Auszeichnung von Portokosten sowie zur Erstellung eines vereinbarten Zahlungsnachweises für solche Kosten, die qualifizierten Versendern durch die Post, durch Spediteure oder durch deren bevollmächtigte Vertreter erteilt wird

3.17**Lizenznummer**

Informationselement (üblicherweise ein numerischer oder alphanumerischer Code), der die Tatsache darstellt, dass ein Versender durch die Post oder einen Spediteur eine Lizenz erhalten hat, die es dem Versender ermöglicht, Portokosten auszuweisen sowie einen Nachweis über ein solches gezahltes Porto zu drucken

3.18**lizensierende Post**

postalische Organisation, die für die Ausgabe von Lizenzen an qualifizierte Versender verantwortlich ist

3.19**MAC-Schlüssel****DPM-MAC-Schlüssel**

Schlüssel für den Nachrichtenauthentisierungscode (MAC, en: Message Authentication Code), der zum Schutz des elektronischen Freimachungsvermerks (DPM) in DPM-Systemen auf der Grundlage von kryptographischen Verfahren mit symmetrischen Schlüsseln genutzt wird

3.20**Versender**

Person oder Organisation, die die Dienstleistung einer Post in Anspruch nimmt

3.21**Versandsystem**

System, das genutzt wird, um Kosten für postalische Dienstleistungen auszuweisen und nachzuweisen

Anmerkung 1 zum Begriff: Zu den Variationen eines Versandsystems gehören unter anderem:

- Frankiermaschinen oder Freistempler;
- Personal-Computer mit spezieller Software;
- Online-Software-Dienste.

3.22**Nachrichtenauthentisierungscode**

MAC, en: Message Authentication Code

aus ausgewählten Daten kryptographisch abgeleiteter Wert, der eine Verifizierung der Datenintegrität und des Ursprungs von impliziten Daten ermöglicht

Anmerkung 1 zum Begriff: Da MACs auf Verfahren geteilter Sicherheitsinformationen beruhen, ermöglichen sie die Verifizierung des Ursprungs von schwächeren (impliziten) Daten als digitale Signaturen, die auf kryptographischen Verfahren mit öffentlichen Schlüsseln beruhen.

3.23**Nichtabstreitbarkeit**

Sicherheitsdienstleistung, die eine Instanz daran hindert, vorherige Verpflichtungen oder Tätigkeiten zu leugnen

3.24**Parametrisierung**

Verfahren zur Versorgung eines Systems oder eines Gerätes mit sämtlichen Eingabeinformationen, die für einen ordnungsgemäßen Betrieb erforderlich sind, einschließlich der Zuweisung spezifischer numerischer Werte zu benannten Variablen, die bei der Berechnung von Ausgabewerten, wie z. B. Datenelementen von DPM, genutzt werden

3.25

Post

Postverwaltung

3.26

Postbehörde

Organisation, die vom WPV-Mitgliedsstaat oder -gebiet als Betreiber benannt wurde, der für die Erfüllung gewisser oder sämtlicher Pflichten des Mitgliedes, die aus der Einhaltung des/der WPV-Vertrags und -Vereinbarungen entstehen, verantwortlich ist

3.27

Postleitzahl

numerischer oder alphanumerischer Wert, der einen geographischen Ort eines Elementes einer postalischen Bearbeitung und eines Versandnetzwerkes, einschließlich postverarbeitender Einrichtungen, Ladengeschäfte, Zustellungseinheiten und Briefkästen einzelner Empfänger, eindeutig angibt

3.28

Privatsphäre

Vertraulichkeit

Sicherheitsdienstleistung, die genutzt wird, um den (bedeutenden) Inhalt der Informationen von all denjenigen fernzuhalten, denen der Zugang hierzu nicht gestattet ist

3.29

asymmetrische Kryptographie

Kryptosystem, das zwei Schlüssel nutzt: einen öffentlichen Schlüssel, der allen Parteien zugänglich ist, und einen privaten oder geheimen Schlüssel, der nur einer Partei (entweder dem Sender oder dem Empfänger der Nachricht, je nach Nutzung des Systems) bekannt ist

Anmerkung 1 zum Begriff: Ein wichtiger Aspekt des Systems öffentlicher Schlüssel besteht darin, dass die öffentlichen und privaten Schlüssel auf eindeutige Weise miteinander verbunden sind und es rein rechnerisch nicht möglich ist, den privaten Schlüssel aus der Kenntnis des öffentlichen Schlüssels zu errechnen.

3.30

Public-Key-Infrastruktur

PKI, en: Public Key Infrastructure

System von digitalen Zertifikaten, Zertifizierungsstellen und Registrierungsstellen oder Vertretern, das die Authentisierung sämtlicher Parteien, die an Kommunikations- und Datenaustauschverfahren beteiligt sind, ermöglicht

3.31

symmetrische Kryptographie

Verschlüsselungssystem, bei dem der Sender und Empfänger einer Nachricht eine einzige gemeinsame geheime Information (Schlüssel) nutzen, um Nachrichten, die ausgetauscht werden, sowohl zu verschlüsseln als auch zu entschlüsseln

3.32

Zeitstempel

Wert der aktuellen Zeit, der von einem System gespeichert wird, um anzugeben, wann eine bestimmte Transaktion stattgefunden hat

3.33

koordinierte Weltzeit

UTC, en: Coordinated Universal Time

universelle Zeit unter Berücksichtigung der jährlichen Einfügung oder Auslassung von Schaltsekunden durch Atomuhren zum Ausgleich von Änderungen in der Erdrotation (mittlere Greenwich-Zeit aktualisiert anhand von Schaltsekunden)

3.34

Lieferant

Anbieter und/oder Betreiber von Versandsystemen

3.35

World Wide Web Consortium

W3C

internationales Gremium von Unternehmen, das an der Entwicklung von offenen Standards für das Internet und das Web beteiligt ist

3.36

XML

erweiterbare Auszeichnungssprache

(en: Extensible Mark-up Language)

Untergruppe der SGML, die eine bestimmte Textauszeichnungssprache für den Austausch von strukturierten Daten darstellt

3.37

XML-Schema

XML-Schema ist eine XML-Sprache zur Beschreibung und Beschränkung des Inhaltes von XML-Dokumenten

— Leerseite —

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

Contents	Page
European foreword	3
Introduction	4
1 Scope.....	5
2 Normative references.....	5
3 Terms and definitions	5
4 Requirements.....	10
5 Description of the models (system architecture and interaction diagrams).....	14
Annex A (normative) Implicit certification process.....	38
Annex B (normative) Message structure.....	40
Annex C (informative) Development principles	43
Bibliography	44

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*

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 <https://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

3.26

post

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

3.27

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

3.28

privacy

confidentiality

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