SLOVENSKI STANDARD
SIST-TS CEN/TS 15121-2:2012

01-marec-2012

Poštne storitve - Hibridna pošta - 2. del: Specifikacija vmesnika varovane elektronske poštne storitve (SePS) - Storitev ECPM

Postal Services - Hybrid Mail - Part 2: Secured electronic postal services (SePS) interface specification - ECPM Service

Postalische Dienstleistungen - Hybride Sendungen - Part 2: Schnittstellen-Spezifikation für Gesicherte elektronische postalische Dienste (SePS) - ECPM Service

/

Ta slovenski standard je istoveten z: CEN/TS 15121-2:2011

ICS:

03.240	Poštne storitve	Postal services

SIST-TS CEN/TS 15121-2:2012 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15121-2

January 2011

ICS 03.240

English Version

Postal Services - Hybrid Mail - Part 2: Secured electronic postal services (SePS) interface specification - ECPM Service

Postalische Dienstleistungen - Hybride Sendungen - Part 2: Schnittstellen-Spezifikation für Gesicherte elektronische postalische Dienste (SePS) - ECPM Service

This Technical Specification (CEN/TS) was approved by CEN on 9 August 2010 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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 15121-2:2011: E

Contents

Page

Foreword

This document (CEN/TS 15121-2:2011) 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 [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document forms Part 2 of a multi-part CEN standard, CEN/TS 15121, *Postal Services - Hybrid Mail*. CEN/TS 15121 was originally published as a UPU standard S43 and was adopted by CEN under the current Memorandum of Understanding between UPU and CEN. UPU S43 was a single part standard covering only secured electronic postal services, but has been split into parts to allow the standard to be extended to cover other services based on the same concepts and service primitives.

These concepts and service primitives are now documented in Part 1 of the standard, CEN/TS 15121-1, and UPU S43a.

This part provides the specification of the Electronic Postal Certification Mark (EPCM) service which conforms with the definition in Article 257bis of the UPU Letter Post Regulations.

CEN/TC 331 WG2 decided to adopt the UPU S43-b as it was an integrative part of UPU S43 during the time of the decision to adopt the UPU S43 under the current Memorandum of Understanding between UPU and CEN in 2005.

According to the Memorandum of Understanding (MoU) between the UPU and CEN, signed Oct. 22nd, 2001; 3.3 CEN notifies the following deviation from the source text:

> The term *"postal administration"* meaning a postal service designated by one member country of the UPU was changed according with the wording of the Postal Directive to *"postal service"*.

According to the CEN/CENELEC Internal Regulations, the national standards organizations 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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

This document provides the specification of the Electronic Postal Certification Mark (EPCM) service which conforms with the definition in Article RL 257bis of the UPU Letter Post Regulations. It is based on a subset of the verbs or operations defined in CEN/TS 15121-1, *Postal Services — Hybrid Mail — Part 1: Secured electronic postal services (SePS) interface specification — Concepts, schemas and operations*, to which the reader is referred.

An EPCM is essentially a digital signature verification and timestamping authority which verifies, and logs as evidence, the content integrity of electronic information. The collection of technical services in an EPCM service can cryptographically verify and store electronic evidence in support of the resolution of potential disputes which challenge the authenticity of events within a cycle of one or more automated transactions involving a postal customer.

An EPCM service constructed to this specification can support the capture and reproduction of evidence data attesting to the fact that a target business transaction was conducted and completed in an environment of integrity and trustworthiness with respect to one or more of the following attributes:

— the transaction originator;

— the party, if any, who closed or terminated the transaction;

— other parties who participated in the transaction;

— were the terms, conditions, and commitments understood by all parties;

— when was the document agreed to by the stakeholders, and sent to each participating party;

— when was it received by each participating party;

— was the content intact throughout transmission;

— have all parties been notified of all agreed events of significance.

An EPCM service which complies with this specification can support the following capabilities:

— non-repudiation of origin;

— non-repudiation of submission;

— non-repudiation of delivery;

— non-repudiation of receipt.

An EPCM's non-repudiation service involves the use of selected combinations of SePS operations in order to ensure end-to-end transaction integrity and evidence collection in a confidential and auditable environment.

This specification has one main heading:

Clause No	Description of content
5	EPCM service definition: this defines the EPCM service by reference to the schemas and operations defined in CEN/TS 15121-1:2011.

The implementation of part or all of this specification might involve the use of intellectual property that is the subject of patent and/or trademark rights. It is the responsibility of users of the standard to conduct any necessary searches and to ensure that any pertinent rights are in the public domain; are licensed[1)] 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 such rights 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 A 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 A, 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 searches to determine whether the mentioned IPR is in fact applicable to their specific case.

1) Mail service contractors are advised to ensure that reliance on intellectual property that is not in the public domain does not inadvertently lead to the creation of an effective monopoly. This could occur, even if usage of the intellectual property concerned is licensed by the mail service contractor, unless the terms of the licensing agreement commit the IPR holder to making licences available, on appropriate terms, to the mail service contractor's customers and suppliers, including competitors of the IPR holder.

1 Scope

This document specifies a secured electronic postal service, referred to as the Electronic Postal Certification Mark (EPCM) service, which provides a chain of evidence, stored by an administration as a trusted third party, to prove the existence of an electronic event, for a certain content, at a certain date and time, and involving one or more identified parties.

The service is defined by reference to the concepts, schemas and operations defined in CEN/TS 15121-1, *Postal Services — Hybrid Mail — Part 1: Secured electronic postal services (SePS) interface specification — Concepts, schemas and operations*. It requires support for five core SePS operations and permits optional support seven others.

This version of the specification does **not** cover:

— a description of the issues surrounding inter-operability between multiple postal SePS implementations when a business transaction Lifecycle requires the participation of more than one SePS implementation in a cross-border scenario involving two or more postal services;

— issues surrounding SePS usage in a ‘multiple Certificate Authority’ scenario where inter-operating posts are participating in a cross-border transaction as described above;

— examination of “Certificate Authority deployment model” alternatives necessitated by the cross-border scenarios described above.

2 Normative references

The following referenced documents are indispensable for the application 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.

CEN/TS 15121-1:2011, *Postal Services — Hybrid Mail — Part 1: Secured electronic postal services (SePS) interface specification — Concepts, schemas and operations*

NOTE See Part 1 of the standard (CEN/TS 15121-1).

3 Terms and definitions

For the purposes of this document, the terms and definitions given in CEN/TS 15121-1:2011 apply.

4 Symbols and abbreviations

For the purposes of this document, the symbols and abbreviations given in CEN/TS 15121-1:2011 apply.

5 EPCM service definition

5.1 Service description

5.1.1 Outline

The EPCM service provides a mechanism whereby a party to an electronic transaction, which might involve multiple electronic exchanges of data between participating parties, can register an electronic document as

forming part of the transaction lifecycle, with all participating parties and/or authorised third parties subsequently being able to verify this registration and its timing. As a corollary, it also provides a mechanism to prevent repudiation of registered documents and to support repudiation of changes made to documents subsequent to their registration.

The service is based on five components: digital signature verification; time stamping; protection of confidentiality; non-repudiation and event logging. These components are described below.

5.1.2 Digital signature verification

Digital signatures are used both to verify the identity of the party submitting or registering an electronic document and to ensure the integrity of the document content. All input is maintained as evidence and can be re-verified at any point in the future should authenticity be challenged. Digital signature integrity and certificate status are verified using PKI-based digital fingerprinting and signature verification technologies to check for both content and certificate integrity.

5.1.3 Time stamping

Signature verification services are time stamped with a unique electronic postal certification mark (EPCM) or value attesting to the fact that the post providing the EPCM stands behind the evidence gathered during the signing ceremony, as well as the subsequent verification status. Additionally the date at which the transaction was conducted is captured both in the EPCM service's logging facility and within the verified signatures themselves.

5.1.4 Protection of confidentiality

PKI-based encryption services are used to provide a high degree of confidence that sensitive business information is hidden from all but the intended recipients. Encryption at origin and decryption at destination guarantees absolute security and privacy for business transaction stakeholders.

5.1.5 Non-repudiation

The EPCM service retains all customer-required tracking and evidence records of significance within the business transaction life cycle. These records are used to support the following non-repudiation services:

— non-repudiation of Origin;

— non-repudiation of Submission;

— non-repudiation of Delivery;

— non-repudiation of Receipt.

Combined with user-authentication, timestamping, and message integrity, these non-repudiation services ensure an extremely trustworthy end-to-end business transaction process. It is intended that the EPCM service, through the implementation of jurisdiction-specific legislative requirements, can act as a legally binding transaction notarization service both within and across postal domains.

Where required to do so, the EPCM service provider can provide any authorised individual or organization with any and all required evidence of the existence, integrity, and logged date of any business transaction tracked by the service. This information can be re-produced digitally or physically and can be sent to any required arbitrating party for their assessment.