TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16326

January 2013

ICS 03.240

English Version

Postal Services - Hybrid Mail - Functional Specification for postal registered electronic mail

Services postaux - Courrier hybride - Spécifications fonctionnelles pour le courrier recommandé électronique

Postalische Dienstleistungen - Hybride Sendungen - Funktionale Spezifikation für elektronische Posteinschreibsendungen

This Technical Specification (CEN/TS) was approved by CEN on 7 February 2012 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey 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 16326:2013: E

Contents

Page

Foreword

This document (CEN/TS 16326:2013) 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.

Keeping pace with the changing communications market, postal operators 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.

Standards are important prerequisites for effective postal operations and for interconnecting the global network. The European Committee for Standardization, their Technical Committee 331 "Postal Services" develops and maintains a growing number of standards to improve the exchange of postal-related information between postal operators, postal handling organisations, customers, suppliers and other partners, including various international organisations.

This functional specification has been developed in close relationship with the following technical standards:

— CEN/TS 15121-1:2011;

— ETSI TS 102 640-1.

The use of this Technical Specification as a basis for any implementation is at the risk of the user. Any party intending such use is strongly advised to seek close contact with the appropriate working group, so that it can be kept informed of ongoing work.

The CEN/TS 16326 was originally published as a UPU standard S52-1and was adopted by CEN under the current Memorandum of Understanding between UPU and CEN.

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

This document describes the functional specification for a postal operator to build or implement the postal registered electronic mail (abbreviated hereinafter to PReM) system which can be offered to the customers of the postal operator as part of the Secure electronic Postal Services (SePS).

PReM is an electronic version of the traditional postal registered mail service. It uses state-of-the-art cryptographic technologies to provide strong role authentication, protection of message confidentiality and integrity and to add non-repudiation attributes to evidence of events and operations. Therefore, the goal of a PReM is to enhance the traditional e-mail service so as to provide an end-to-end trusted electronic communication service, encompassing both evidence of submission and delivery between authenticated parties.

The service is embodied in the secured and trusted exchange of electronic mail, as every step of the process is logged for future evidence tracing and any entity involved is authenticated. The PReM service comprises the following features:

— secured message forwarding and delivery: ensures the PReM Message confidentiality (encryption) and integrity (no modification); and authenticity and non-repudiation of users (mailer and addressee) and postal operators (origin and destination). In addition, PReM messages will be securely transported from mailer to addressee/mailee;

— evidence generation: all significant events within a complete operation cycle are traceable. Types of evidence and evidence formats are described in 7.2;

— event notification: notification that a particular event/operation has occurred will be generated and sent to corresponding parties;

— archival of evidence: storage of generated evidence for future attestation.

The implementation of part or all of this functional specification might involve the use of intellectual property which is the subject of patent and/or trademark rights. Since the specification was developed in close relationship with ETSI TS 102 640, these might include rights held by ETSI. 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, or are avoided. CEN/TC 331 cannot 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 or the Secretariat of CEN/TC 331 or CEN/TC 331 WG2 of any explicit claim that any technique or solution described herein is protected by such right in any 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 or Secretariat of the CEN/TC 331 WG2.

Annex C of this document lists the intellectual property rights brought to the attention of the UPU Standards Board or CEN/TC 331 WG2 prior to approval of the publication of this version of the standard.

1 Scope

This Technical Specification constitutes the functional specification of a secure electronic postal service, referred to as the postal registered electronic mail or PReM service. PReM provides a trusted and certified electronic mail exchange between mailer, postal operators and addressee/mailee. In addition, evidence of corresponding events and operations within the scope of PReM will be generated and archived for future attestation.

The PReM service is defined by reference to the concepts, schemas and operations defined in CEN/TS 15121-1:2011. It utilises six SePS operational verbs (CheckIntegrity, LogEvent, Postmark, RetrieveResults, Sign and Verify) and the five additional server-side operational verbs (SendMessagetoDestination, Subscribe Notification, UnscbscribeNotification, RejectMessage and ReceiveNotification) to fulfil the operational requirements of a PReM System.

Return of Investment (ROI), market potential, revenues model, business plan and pricing policy are outside the scope of this functional specification. Postal operators are advised to make the necessary marketing study and research prior to considering leasing, procuring or developing such a PReM system in accordance with this functional specification.

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.

a) European Telecommunications Standards Institute (ETSI) Standards

NOTE ETSI standards are available at www.etsi.org.

ETSI TS 102 640-1, *Electronic Signatures and Infrastructures (ESI);Registered Electronic Mail (REM); Part 1: Architecture*

ETSI TS 101 862 V1.3.3 (2006-01), *Qualified Certificate Profile*

b) European Committee for Standardization (CEN)

NOTE CEN standards can be obtained from national standardization institutes of CEN National Members (see http://www.cen.eu)

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

CWA 14169, *Secure Signature-Creation Devices "EAL 4+"*

c) Internet Engineering Task Force Public Key Infrastructure X.509 working group (IETF PKIX)

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R.Housley, W.Polk, available from: http://www.rfc-editor.org/rfc/pdfrfc/rfc5280.txt.pdf

d) Universal Postal Union (UPU) Standards

NOTE UPU standards are available on subscription from the UPU International Bureau: Weltpoststrasse 4, Case postale, 3000 Berne 15, SWITZERLAND; Tel: +41 31 350 3111; Fax: +41 31 350 3110; http://www.upu.int

UPU Technical Standard S43a, *Secured electronic postal services (SePS) interface specification — Part A: Concepts, schemas and operations*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in the UPU Standards glossary, in the documents referred to in Clause 2 and in Bibliography, and the following apply. The definition of other frequently used or particularly important terms as well as other terms introduced in this document is given below.

3.1
Advanced Electronic Signature
signature, uniquely linked to and capable of identifying the signatory, which was created by a signature creation device in the sole control of the signatory and which is linked to data in such a way that subsequent change to such data is detectable

3.2
postal operator
entity officially designated by a UPU member country to operate postal services and to fulfil some or all of the related obligations arising out of the Acts of the UPU in its territory

3.3
postal operator Trust List
list of registered and authenticated postal operators which is maintained by the UPU International Bureau

3.4
Email Client Software
software which supports the creation, sending, reception and storage of messages intended to be or actually transmitted over electronic communication systems in accordance with the Simple Mail Transfer Protocol

3.5
notification
message that informs the involved parties that a PReM operation has been performed or a PReM event has taken place

3.6
PReM Dispatch
PReM Message together with all previously collected evidence related thereto the PReM Message

3.7
PReM Object
electronic message or file(s) that mailer intends to send to addressee/mailee

3.8
PReM Policy Domain
collection of PReM enabled postal operators which belong to a group that it is managed according to agreed rules and regulations agreed by the group

3.9
PReM Message
S/MIME object consisting of one or more PReM Objects