BSI Standards Publication

Postal Services — Hybrid Mail

Part 2: Secured electronic postal services (SePS) interface specification — ECPM Service

National foreword

This Draft for Development is the UK implementation of CEN/TS 15121-2:2011.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion to an international standard. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards.*

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee SVS/4, Postal services.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2011

ISBN 978 0 580 70586 1

ICS 03.240

Compliance with a British Standard cannot confer immunity from legal obligations.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 January 2011.

Amendments issued since publication

Date	Text affected

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.

5.1.6 Event logging

The storage of the evidence (i.e. escrow) data associated with business transactions is a core capability of the EPCM service. EPCM service records are maintained by the service provider for as long as is needed to satisfy customer, postal service and local legal requirements.

EXAMPLE   USPS maintains records for at least seven years, the Government of Canada has mandated that Canada Post maintain its records for a minimum of 11 years.

5.2   Compliance with the SePS specification

EPCM services which comply with this specification shall support the CheckIntegrity, PostMark, RetrieveResults, Sign and Verify operations in accordance with the specifications of these operations in CEN/TS 15121-1.

Support for the SePS operations Decrypt, Encrypt, Locate, LogEvent, RetrievePostalAttributes, RetrieveSummary and StartLifecycle is not required for EPCM compliance. However, if one or more of them is supported, the operation(s) concerned shall function in accordance with specification in CEN/TS 15121-1.

Support for operations and options which are not defined in UPU standard S43a is permitted. However:

— any such operations and options shall not simply duplicate the functionality of one of the standard operations and/or options defined in CEN/TS 15121-1;

— users of the EPCM service shall not be required to make use of such operations and/or options in order to make use of the standard operations defined in CEN/TS 15121-1.

5.3   Backwards compatibility

The SePS schema specification in CEN/TS 15121-1 is discreet and version specific. Posts are free to select which discrete interface versions they support. However, except in the case of upgrades to V1.15 adopted to ensure cross-border compatibility, postal services who upgrade from older versions of the SePS specification (e.g. from V1.14) to a newer one are required to support backward compatibility of previously supported versions of the SePS interface specification as it applies to both processing requests/responses and honoring previously issued PostMarkedReceipts. Individual posts are free to address this backward compatibility challenge as they see fit. The `Version` element which is present in every request and which is included in the `PostMarkedReceipt` can be used to support this backwards compatibility requirement.

5.4   Cross-border provision of the EPCM service

The provision of an EPCM service across borders shall be governed by a bilateral or multi-lateral agreement between participating administrations. This agreement shall:

NOTE 1   An administration can participate in multiple agreements relating to EPCM services offered across different groups of countries.

— specify the provisions required to provide the EPCM service across borders;

— obligate participating services to comply with its provisions;

— define a Trust Model based on mutual authentication of the participant service;

— define an EPCM service logo which shall be used, wherever possible, to identify the EPCM service concerned and to provide for human readable representation of the fact that the service has been applied to an electronic document when the content of that document is rendered in a human readable form;

NOTE 2   The XML-formatted `PostMarkedReceipt` represents the SePS standardized definition of the composition of an EPCM.

— reflect and complement the applicable provisions contained in the UPU Letter Post Regulations.

NOTE 3   The Regulations impose additional requirements, in particular that verification of an EPCM should be free of additional charges, regardless of where the EPCM was applied.

For the purposes of the Trust Model, each participating service shall be digitally identified by means of a unique EPCM digital identifier (a string or a token) that unequivocally identifies that service when interacting, for EPCM cross-border transactions purposes, with other services and their users. This EPCM digital identifier shall be obtained from a trusted third-party digital identity provider and shall be communicated to all other participating services.

Annex A
(informative)

Relevant intellectual property rights (IPR)

A.1 Introduction

This informative annex lists all Intellectual Property Rights (trademarks, patents and patent applications), the use of which has been advised as possibly being implied by the application of this standard. It is stressed that the content of this annex is not exhaustive and is provided on a 'without prejudice' basis. That is:

— mention herein of a particular IPR indicates only that some party has expressed, to the Secretariat of CEN/TC 331 and/or the UPU Standards Board, the view that use of the standard might, in some circumstances, infringe the mentioned right. It should not be taken as in any way confirming the validity of such view and users of this standard should conduct their own searches to determine whether the mentioned IPR is in fact applicable to their specific case;

— the descriptive text associated with mention of a particular IPR is intended to provide only a general indication of the field of application of the right concerned. It should not be taken as implying that the right or its application is limited, in scope, to the description given;

— the absence of reference to any IPR is indicative only of the fact that the Secretariats of CEN/TC 331 and/or the UPU Standards Board had, up to the time of publication of this standard, received no suggestion that the said IPR could potentially be infringed by the use of this standard. Neither the UPU nor CEN has conducted any patent, trademark or other searches relevant to the subject matter of this standard and cannot accept any responsibility in case of infringement, on the part of users of this document, of any third party intellectual property rights.

Users of the standard are encouraged to conduct any necessary searches and to ensure that any pertinent IPR is either in the public domain; is licensed from the holder(s) or is avoided.

A.2 USPS Trademarks

The United States Postal Service claims the registration or pending registration of the trademark "ELECTRONIC POSTMARK", "USPS ELECTRONIC POSTMARK", "EPM" and "USPS EPM", "UNITED STATES POSTAL SERVICE ELECTRONIC POSTMARK" and a figurative trademark in the following countries and regions:

COUNTRY / REGION	MARK	CLASSES	REG.NO.	RENEWAL DEADLINE
ARGENTINIA	ELECTRONIC POSTMARK	9 16 25 35 39 42	1760166 1760165 1760164 1760163 1760162 1760161	20091102 20091102 20091102 20091102 20091102 20091102
BRAZIL	ELECTRONIC POSTMARK	9 16 25 35	820980552 820980617 820980595 820980587	20130930 20150607 20110619 20151129

		39	820980609	20151129
		42	200072366	20151129
CHILE	ELECTRONIC POSTMARK	25	530543	20081223
CHINA	ELECTRONIC POSTMARK	25	1323353	20091013
COLOMBIA	ELECTRONIC POSTMARK	9	220679	20090903
		35	217744	20090420
		39	218217	20090429
		42	217456	20090331
CHINA	ELECTRONIC POSTMARK	25	1323353	20091013
COLOMBIA	ELECTRONIC POSTMARK	9	220679	20090903
		35	217744	20090420
		39	218217	20090429
		42	217456	20090331
CTM	ELECTRONIC POSTMARK	9, 16, 25, 35, 39, 42	853606	20080617
ECUADOR	ELECTRONIC POSTMARK	9	2100	20100406
		16	2099	20100406
		25	2098	20100406
		35	615	20100321
		39	614	20100321
		42	617	20100321
INDIA	ELECTRONIC POSTMARK	9	813229	n/a (pending)
		16	813230	20080803
		25	813231	20080803
INDONESIA	ELECTRONIC POSTMARK	9	444088	20080911
		25	441745	20080804
		16	441749	20080804
		35	441751	20080804
		39	441752	20080911
		42	441750	20080804
JAPAN	ELECTRONIC POSTMARK	9, 16, 25, 35, 39, 42	4701818	20130915
MALAYSIA	ELECTRONIC POSTMARK	9	98/10171	n/a (pending)
		25	98/10172	20080309
		16	98/10176	20080309
		35	98/10174	20080309
		39	98/10173	20080309
		42	98/10175	20080309
MEXICO	ELECTRONIC POSTMARK		337103	n/a (pending)
			618525	20080623
			585698	20080623
			598976	20080806
			597202	20080623
			617541	20080623
NEW ZEALAND	ELECTRONIC POSTMARK	25	295834	20150729
NEW ZEALAND 9	USPS ELECTRONIC POSTMARK	9	642643	20080730
		16	642644	20080730
		35	642645	20080730
		39	642646	20080730
		42	642647	20080730
NORWAY	ELECTRONIC POSTMARK	16, 25	207990	20110419
		35, 39, 42	215283	20120812
PARAGUAY	ELECTRONIC POSTMARK	9	218294	20090710
		16	218293	20090710
		25	223166	20100303
		35	223165	20100303
		39	223164	20100303

		42	223163	20100303
PERU	ELECTRONIC POSTMARK	9 16 25 35 39 42	50103 50104 49697 16468 16467 15999	20081104 20081104 20081022 20081218 20081218 20081027
PHILIPPINES	ELECTRONIC POSTMARK	9, 16, 25, 35, 39, 42	4-1998- 005617	Aff/Use due 20100118
SINGAPORE	ELECTRONIC POSTMARK	9 16 25 35 39 42	T9807802D T9807803B T9807804J T9807805I T9807806G T9807807E	20080731 20080731 20080731 20080731 20080731 20080731
SWITZERLAND	ELECTRONIC POSTMARK	9, 16, 25, 35, 39, 42	466979	20091026
TAIWAN	ELECTRONIC POSTMARK	16 25 35 42	985087 1011897 159955 163421	20120215 20120815 20120229 20120430
UNITED STATES	ELECTRONIC POSTMARK	42	2451150	§8/15 due 20070515
UNITED STATES	USPS ELECTRONIC POSTMARK	42	2451172	§8/15 due 20070515
UNITED STATES	EPM	35, 38, 39, 42	2874196	§8/15 due 20100817
UNITED STATES	USPS EPM	9, 35, 39, 45	2934455	§8/15 due 20110322
UNITED STATES	UNITED STATES POSTAL SERVICE ELECTRONICPOSTMARK	42	2485456	§8/15 due 20070904

In a letter dated 31 March 2006, the USPS has indicated its belief that ELECTRONIC POSTMARK – treated and maintained as a trademark – would support the controlled and regulated provision of authenticated time/date stamp services across international boundaries.

A.3 Patents

See CEN/TS 15121-1.

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™