SLOVENSKI STANDARD
SIST-TS CEN/TS 15121-1:2012

01-januar-2012

Poštne storitve - Hibridna pošta - 1. del: Specifikacija vmesnika varovane elektronske poštne storitve (SePS) - Koncepti, sheme in delovanje

Postal Services - Hybrid Mail - Part 1: Secured electronic postal services (SePS) interface specification - Concepts, schemas and operations

Postalische Dienstleistungen - Hybride Sendungen - Part 1: Schnittstellen-Spezifikation für Gesicherte elektronische Postdienste (SePS) - Begriffe, Schemata und Betrieb

Ta slovenski standard je istoveten z: CEN/TS 15121-1:2011

ICS:

03.240	Poštne storitve	Postal services

SIST-TS CEN/TS 15121-1:2012 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15121-1

January 2011

ICS 03.240

English Version

Postal Services - Hybrid Mail - Part 1: Secured electronic postal services (SePS) interface specification - Concepts, schemas and operations

Postalische Dienstleistungen - Hybride Sendungen - Part 1: Schnittstellen-Spezifikation für Gesicherte elektronische Postdienste (SePS) - Begriffe, Schemata und Betrieb

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 15121-1:2011: E

Contents

Page

Foreword

This document (CEN/TS 15121-1:2011) 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.

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"*.

This document is the equivalent to Part 1 of a multi-part UPU standard, S43: Secured electronic postal services (SePS) interface specification. S43 was originally published as a single part standard covering only one secured electronic postal service, but has been split into parts to allow the standard to be extended to cover other services based on the same concepts, schemas and operations. Part 1 defines these concepts, schemas and operations.

Part 2 defines EPCM Services, and uses the specification of Part 1.

The specification is complemented by five annexes. Annex A and Annex B are normative; Annex C, Annex D and Annex E are informative. The specification contains a Bibliography.

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 interface specification describes a standardized way for postal services or its system development teams to build a secured electronic postal services (SePS) capability which can be offered to customers as part of an electronic service inventory.

A SePS is a postal service which is accessed electronically through the use of an interface based on an appropriate subset of the operations (verbs) specified in this document. Together these define a set of standardized application layer software security services aimed at facilitating the introduction and integration of the following capabilities into a target customer's business applications:

— digital signature verification;

— certificate status verification;

— timestamping of verified signatures (i.e. a PostMarkedReceipt);

— receipt issuance;

— content timestamping;

— digital signature creation;

— capture of signature intent (context and user commitment);

— creation of encrypted envelopes;

— decryption of encrypted envelopes;

— evidence logging of all SePS events;

— logging of user events deemed relevant to the business transaction;

— tying together of SePS events into a business transaction Lifecycle;

— retrieval of evidence data in support of dispute resolution and future challenges in a non-repudiation context.

Individual SePS services may support different subsets of the defined operations. For example, the electronic postal certification mark (EPCM) service, defined in part B of the standard (see UPU standard S43b) uses the CheckIntegrity, PostMark, RetrieveResults, Sign and Verify operations to support the capture and reproduction of evidence data attesting to the fact that a business transaction was conducted and completed in an environment of integrity and trustworthiness.

The process of integrating SePS features into an automated application is termed "SePS-enabling" the target application. Each call to a SePS can be looked at as a non-repudiable SePS event or SePS transaction within the application's overall business workflow. These non-repudiable events can be logically linked and tracked within an application's business workflow to provide additional business context to an arbitrator should a challenge to the event's authenticity be presented by any of the involved parties.

This specification describes the SePS interface standard and contains four main clauses and five annexes:

Clause No	Description of content
5	*Key SePS concepts:* introduces a number of key concepts which are drawn on in the remainder of the specification;
6	*Overview of SePS operations*: provides an overview of the standard operations, supported by the schema defined in Annex A, which can be combined to implement secured electronic postal services which comply with this specification;
7	*Common schema types used across SePS operations*: defines common WSDL element types that are sent to and returned from the SePS;
8	*Detailed specification of SePS operations*: provides a detailed definition of the operations which were introduced in Clause 6;
Annex A	*(normative) SePS XML Schema V1.15:* provides the formal XML Schema for the SePS interface;
Annex B	*(normative) Web Service Description Language (WSDL) V1.15:* provides the formal WSDL specification of the SePS interface;
Annex C	*Examples:* provides specific examples illustrating the various constructs used within the interface;
Annex D	*(informative) European and international standards inter-relationships and evolution:* provides background information on other signature standards which exist in the same domain as the SePS interface specification. Their influence and role in shaping this standard and its evolution is also covered;
Annex E	*(informative) Relevant intellectual property rights (IPR):* provides information about intellectual property rights whose use has been reported as possibly being implied by certain implementations of the specification.

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 E 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 E, 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 standard XML interface that will enable software applications to call a secured electronic postal service (SePS), provided by a postal service, which is based on the concepts, schemas and operations described herein.

The specification provides:

— a definition of standard operations which can be combined to support secured electronic postal services;

— a full description of all mandatory and optional request parameters required for use of these operations;

— a full description of all response elements and the detailed circumstances under which they are returned.

The specification also describes the functionality and edit rules of the actual technical specification artifacts, which are represented by an XML Schema (XSD) and an associated Web Services Definition Language (WSDL) specification. The versions of these applicable at the date of publication of this version of the specification are contained in this document as Annex A and Annex B respectively. These can also be obtained in electronic format from the UPU Technical Standards CD-ROM or from the UPU Standards Secretariat.

In case of any conflict between Annex A and other provisions of this specification, Annex A shall be regarded as definitive.

The SePS schema specification in Annex A is discreet and version specific. Postal Services 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 schema (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.

The requirement for backward compatibility does not apply to cross-border scenarios where V1.15 has been adopted to ensure compatibility. The SePS Interface specification includes a digital signature platform supporting basic cryptographic service operations as well as a comprehensive framework for the delivery of evidentiary, witnessing, and non-repudiation services. The specification provides for continued support of legacy CMS/PKCS7 binary signatures. This approach allows subscribing applications to leverage the strengths of both protocols and can aid in the migration from one to the other. The schema will continue to support, in an interchangeable way, use of both CMS/PKCS7 and XMLDSIG artifacts.

SePS implementations are free to support the "XML Signature Syntax and Processing" standard (i.e. XMLDSIG) for all elements presently carrying PKCS7 content. Selection of either format is supported across the two prevalent signature formats within this domain. XML Encryption is also supported.

The specification:

— complies with IETF RFC 3161 in respect of time stamp tokens, time stamp values and other time stamp attributes;

— complies with all mandatory requirements (i.e. qualified as "required" or "shall" in the text) of IETF RFC 3126 and ETSI TS 101 733 as they apply to Electronic Signatures – Complete (i.e. ES-C);

— complies with the IETF RFC 2630 ASN.1 layout for all PKCS objects utilised in the specification;

— supports XMLDSIG signature formatting as defined in IETF RFC 3275;

— complies with IETF RFC 2560 in respect of the `ValidationData` element.

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.

2.1 UPU standards

UPU Standards glossary

NOTE UPU Standards are obtainable from the UPU International Bureau, whose contact details are given in the Bibliography; the UPU Standards glossary is freely accessible on URL http://www.upu.int.

2.2 Internet Engineering Task Force (IETF) documents

NOTE Internet RFCs (Requests for Comment) are available from the Internet Engineering Task Force, c/o the Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 20191-5434, U.S.A. Tel: (+1 703) 620 8990, Fax: (+1 703) 620 9071, www.ietf.org. RFCs can also be obtained from www.faqs.org/rfcs/.

RFC 2315[2)] – PKCS #7 Version 1.5

RFC 2560[3)] – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (June 1999), M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams

RFC 2617 – HTTP Authentication: Basic and Digest Access Authentication (June 1999) J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart

RFC 2822 – Internet Message Format

---

2) This defines the ASN.1 layout for all relevant PKCS objects utilised by the SePS.

3) The ValidationData element defined in the WSDL interface specification (Annex B) refers directly to this RFC. If a SePS described in this RFC as it pertains to ValidationData required at non-repudiation challenge time for successful evidencing. This can be accomplished through CRL evidence capture as well as signed OCSP responses, the latter being more credible. This new version of the specification provides an extensibility model whereby individual posts may implement their own ValidationData complexType to extend the abstract GenericValidationData now in the schema.

RFC 3126[4] – Electronic Signature Formats for long term electronic signatures (September 2001), D. Pinkas, J. Ross, N. Pope

RFC 3161[5] – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (August 2001), C. Adams, P. Cain, D. Pinkas, R. Zuccherato

RFC 3275[6] – XML-Signature Syntax and Processing (March 2002), D. Eastlake, J. Reagle, D. Solo

RFC 3447 – Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

2.3 Organization for the Advancement of Structured Information Standards (OASIS)

NOTE OASIS (Organization for the Advancement of Structured Information Standards) is a non-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces web services standards along with standards for security, e-business, and standardisation efforts in the public sector and for application-specific markets. OASIS specifications can be obtained via its web site, www.oasis-open.org, which also provides contact details for written communications.

oasis-sstc-saml-core-1.1 – Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS Standard, September 2003, E. Maler et al., http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

OASIS DSS – Digital Signature Services (DSS) Technical Committee, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

OASIS DSS – Digital Signature Services (DSS) - EPM Profile, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

3 Terms and definitions

For the purposes of this document, the terms and definitions given in the UPU Standards glossary and the following apply.

3.1
asymmetric cryptographic algorithm
cryptographic algorithm using two related keys, a public key and a private key, and in which one key can decrypt what has been encrypted with the other one

3.2
certificate (e.g. X509)
public CA certified portion of a key pair in a PKI environment which binds an entity's unique name and their public key to the corresponding privately-generated private key

4) This RFC is considered by most authorities to be the essential definition of what constitutes a legitimate non-repudiation service. It describes the technical criteria and pre-requisites for minimum compliance as a non-repudiation service capability. The SePS interface specification honours ES-C mandatory requirements, i.e. qualified as “required” or “shall” in the text.

5) References within the SePS WSDL specifications (Annex B) that pertain to time stamp tokens, time stamp values, or any other time stamp attributes should be assumed by any reader or implementer to be RFC 3161 compliant.

6) This RFC, commonly referred to as XMLDSIG, is the W3C's landmark standard to which nearly all XML-based attempts to capture ASN.1 PKCS7 syntax in XML refer. The WSDL interface specification (Annex B) allows for both PKCS7 binary ASN.1 formatting of signature objects as well as the more recent XMLDSIG signature formatting.

3.3
certificate Revocation List (CRL)
list of revoked certificates

3.4
certification
process of creating a public key certificate binding an entity's identity to its public key

3.5
certification Authority (CA)
entity trusted by one or more other entities to create, assign, revoke or suspend public key certificates

3.6
certification path
ordered sequence of certificates of entities which, together with the public key of the initial entity, can be processed to obtain the public key of the final entity in the path

3.7
cross-certification
mechanism by which two CAs exchange certificates to implement a trusted relationship

3.8
cryptographic key
parameter controlling the operation of a cryptographic function

3.9
cryptography
discipline embodying the principles, means and methods for the transformation of data in order to hide its information content, or to prevent its undetected modification, or to prevent its unauthorized use or any combination thereof

3.10
digital signature
value, cryptographically derived from selected data using a public key algorithm, which when associated with the corresponding public key and its owner, allows a recipient of the data to authenticate its origin and verify its integrity

3.11
distinguished name
globally unique name for an entity

3.12
end entity
person, organisation, computer system or group thereof that is the subject of or uses a certificate but is not a CA or RA

NOTE An end entity is a subscriber or a relying party or both.

3.13
entity
CA, RA or end entity

3.14
hash
one-way mathematical function that maps values from a large (possibly very large) domain into a smaller domain and that satisfies the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output

NOTE Hashing is used to reduce a potentially long message into a “hash value” or “message digest” of fixed length, which is sufficiently compact to be used as input to a digital signature algorithm.

3.15
key
see cryptographic key

3.16
key pair
set of keys, consisting of a public key and a private key, that are associated with an entity in a public key cryptography system

3.17
non-repudiation
service providing proof, beyond reasonable doubt, of the integrity and origin of data which can be validated by a third party

3.18
object identifier
sequence of integer components identifying an object such as an algorithm or attribute type

3.19
Public Key Infrastructure (PKI)
set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke certificates based on public key cryptography

3.20
Registration Authority (RA)
entity responsible for the identification and authentication of certificate subjects but which does not sign or issue certificates

3.21
relying party
recipient of a certificate who acts in reliance on that certificate and/or on a digital signature that is verified using that certificate

3.22
RSA algorithm
cryptographic method created by Rivest, Shamir, and Adelman for which the intellectual property rights are held by RSA Data Security

3.23
Secure Socket Layer (SSL)
protocol developed by Netscape for encrypted transmission over TCP/IP networks

3.24
subject
entity whose public key is certified in a public key certificate

3.25
subscriber
end entity or subject that is considered to have an account, with a SePS Provider, providing it with the ability to subscribe to the SePS as per some pre-determined contractual arrangement

3.26
Trusted Time Stamp (TTS)
record mathematically linking a data item to a date7 assured by a trusted time stamping authority

3.27
Time Stamp Authority (TSA)
trusted third party which issues and/or verifies trusted time stamps

3.28
X.509 V3 certificate extension
mechanism, defined in Version 3 of the X.509 standard, supporting the embedding of usage and policy information in a certificate

4 Symbols and abbreviations

For the purposes of this document, the symbols, abbreviations and acronyms given in the UPU Standards glossary and the following apply:

CMS Cryptographic Message Syntax (the evolution of PKCS#7)

EPCM Electronic Postal Certification Mark

NOTE 1 The acronym EPCM refers to a particular Regulation adopted by the Postal Operations Council within the UPU and describes a specific SePS which complies with the specification in Part B of this standard (S43b). Other (future) Regulations and standards might specify other services which comply with this part of the standard (S43a).

IETF Internet Engineering Task Force

LDAP Lightweight Directory Access Protocol

NA Not Applicable

OCSP Online Certificate Status Protocol

PS Postal Service

PKCS#n: Public Key Cryptography Standard #n (e.g. PKCS#7 or PKCS#1)

PKI Public Key Infrastructure

RDBMS Relational Database Management System

RFC Internet Request For Comments

RSA Short for Rivest, Shamir and Adelman, inventors of the RSA encryption algorithm owned by RSA Data Security, Inc.; frequently used to refer to the algorithm itself

SAML Security Assertion Markup Language

SePS Secured electronic postal service(s)

NOTE 2 The acronym SePS is used both to refer to a single implementation — a secured electronic postal service — and generically, to refer to services that comply with this specification. The appropriate interpretation (service or services) has to be determined from the context in which the acronym is used.

SNMP Simple Network Management Protocol

SSL Secure Socket Layer

TSA Time Stamp Authority

TSP Trusted Service Provider