DIN CEN/TS 15121-1:2011-03 (E)

Postal Services_- Hybrid Mail_- Part_1: Secured electronic postal services (SePS) interface specification_- Concepts, schemas and operations; English version CEN/TS_15121-1:2011

Contents

Page

Foreword 5

Introduction 6

1 Scope 8

2 Normative references 9
2.1 UPU standards 9
2.2 Internet Engineering Task Force (IETF) documents 9
2.3 Organization for the Advancement of Structured Information Standards (OASIS) 10

3 Terms and definitions 10

4 Symbols and abbreviations 13

5 Key SePS concepts 14
5.1 Authentication 14
5.2 Digital signature verification 15
5.3 Error handling 15
5.4 Event logging 15
5.5 Lifecycle management 16
5.6 Non-repudiation 16
5.7 PostMarking 16
5.8 Processing directives or options 17
5.9 Protection of confidentiality 17
5.10 Time stamping 17
5.11 Transaction handling 17

6 Overview of SePS operations 17
6.1 General 17
6.2 CheckIntegrity 18
6.3 Decrypt 19
6.4 Encrypt 19
6.4.1 General 19
6.4.2 Delegated Confidentiality Service 19
6.5 Locate 19
6.6 LogEvent 20
6.7 PostMark 20
6.8 RetrievePostalAttributes 20
6.9 RetrieveResults 20
6.10 RetrieveSummary 20
6.11 Sign 21
6.12 StartLifecycle 21
6.13 Verify 21

7 Common schema types used across SePS operations 22
7.1 Introduction 22
7.2 AccessScope and Scopes 22
7.3 ClaimedIdentity 23
7.4 ClientApplication 26
7.5 ContentIdentifier 26
7.6 ContentMetadata 26
7.7 EncryptResponse Option 27
7.8 Event 29
7.9 OriginalContentType 29
7.10 ParticipatingPartyType 30

7.11 PostMarkedReceipt 31
7.12 PostMarkedReceipt (XMLDSIG considerations) 36
7.13 QualifiedDataType 38
7.14 SignatureInfoType 38
7.15 SignaturePolicyIdentifier 39
7.16 TransactionKeyType 40
7.17 TransactionStatus and TransactionStatusDetailType 41
7.18 ValidOperation 41
7.19 ValidOption 42
7.20 Version 42
7.21 X509InfoType 42

8 Detailed specification of SePS operations 44
8.1 Introduction 44
8.2 CheckIntegrity 44
8.2.1 CheckIntegrity Edit Rules Summary 44
8.2.2 CheckIntegrityOptions Request Flags 45
8.2.3 CheckIntegrity Request Elements 46
8.2.4 CheckIntegrity Response Object 48
8.3 Decrypt 51
8.3.1 Decrypt Edit Rules Summary 51
8.3.2 DecryptOptions Request Flags 52
8.3.3 Decrypt Request Elements 53
8.3.4 Decrypt Response Object 53
8.4 Encrypt 54
8.4.1 Encrypt Edit Rules Summary 54
8.4.2 EncryptOptions Request Flags 55
8.4.3 Encrypt Request Elements 56
8.4.4 Encrypt Response Object 57
8.5 Locate 58
8.5.1 Locate Edit Rules Summary 58
8.5.2 LocateOptions Request Flags 58
8.5.3 Locate Request Elements 59
8.5.4 Locate Response Object 60
8.6 LogEvent 60
8.6.1 LogEvent Edit Rules Summary 60
8.6.2 LogEventOptions Request Flags 61
8.6.3 LogEvent Request Elements 61
8.6.4 LogEvent Response Object 62
8.7 PostMark 62
8.7.1 PostMark Edit Rules Summary 62
8.7.2 PostMarkOptions Request Flags 63
8.7.3 Postmark Request Elements 63
8.7.4 PostMark Response Object 65
8.8 RetrievePostalAttributes — RetrievePostalAttributes Edit Rules Summary 66
8.9 RetrieveResults 67
8.9.1 RetrieveResults Edit Rules Summary 67
8.9.2 RetrieveResultsOptions Request Flags 68
8.9.3 RetrieveResults Request Elements 69
8.9.4 RetrieveResults Response Object 70
8.10 RetrieveSummary 73
8.10.1 RetrieveSummary Edit Rules Summary 73
8.10.2 RetrieveSummaryOptions Request Flags 73
8.10.3 RetrieveSummary Request Elements 73
8.10.4 RetrieveSummary Response Object 74
8.11 Sign 75
8.11.1 Sign Edit Rules Summary 75
8.11.2 SignOptions Request Flags 76
8.11.3 Sign Request Elements 77
8.11.4 Sign Response Object 78

8.12 StartLifeCycle ... **79**
8.12.1 StartLifecycle Edit Rules Summary ... **79**
8.12.2 StartLifecycleOptions Request Flags ... **79**
8.12.3 StartLifecycle Request Elements ... **80**
8.12.4 StartLifecycle Response Object ... **80**
8.13 Verify ... **81**
8.13.1 Verify Edit Rules Summary ... **81**
8.13.2 VerifyOptions Request Flags ... **81**
8.13.3 Verify Request Elements ... **83**
8.13.4 Verify Response Object ... **87**

Annex A (normative) **SePS XML Schema V1.15** ... **89**

Annex B (normative) **Web Service Description Language (WSDL) V1.15** ... **108**

Annex C (informative) **Examples** ... **117**
C.1 General ... **117**
C.2 Standalone PostMarkedReceipt over a verified signature ... **117**
C.3 Standalone <PostMarkedReceipt> over data when using PostMark operation ... **120**
C.4 Embedded <PostMarkedReceipt> over a verified signature ... **122**
C.5 RequesterSignature over TransactionKey for any operation in protected Lifecycle ... **125**
C.6 RequesterSignature over OriginalContent when used in a CheckIntegrity operation ... **126**

Annex D (informative) **European and international standards inter-relationships and evolution** ... **128**

Annex E (informative) **Relevant intellectual property rights (IPR)** ... **129**
E.1 Introduction ... **129**
E.2 USPS Patents ... **130**

Bibliography ... **131**