# DIN EN 14615:2017-12 (E)

## Postal services - Digital postage marks - Applications, security and design

## Contents

Page


European foreword ..... 5

Introduction ..... 6

1 Scope ..... 8

2 Normative references ..... 8

3 Terms and definitions ..... 8

4 Symbols and abbreviations ..... 11

5 DPM applications and design process ..... 12
5.1 Introduction ..... 12
5.2 DPM business planning ..... 13
5.3 DPM systems analysis ..... 14
5.4 DPM security analysis ..... 15
5.5 DPM design ..... 16

Annex A (normative) Specification checklists ..... 17

A.1 Applications specifications ..... 17
A.2 System specification ..... 17
A.3 Security specification ..... 18
A.4 DPM specification ..... 18

Annex B (informative) Business planning considerations ..... 19

B.1 Possible applications ..... 19
B.2 Market segmentation ..... 20
B.3 Applications selection ..... 23

Annex C (informative) Security analysis considerations ..... 26

C.1 Context ..... 26
C.2 Security objectives, policy and economics ..... 27
C.3 Threats and vulnerabilities ..... 28
C.4 Applications and message level security ..... 32
C.5 Security services and message level countermeasures ..... 34
C.6 Applications level countermeasures ..... 36
C.7 Countermeasure selection ..... 47
C.8 Application of countermeasures ..... 49
C.9 Message security implementation options ..... 49

Annex D (informative) Systems analysis considerations ..... 56

D.1 Requirements analysis ..... 56
D.2 Functional description ..... 57

DIN EN 14615:2017-12 EN 14615:2017 (E) D.3 Function allocation and architecture design ..... 60
D.4 Other detailed design aspects ..... 60

**Annex E (informative) DPM design considerations ..... 67**

**E.1 Data content ..... 67**
**E.2 Data entry ..... 68**
**E.3 Data construct mapping ..... 69**
**E.4 Symbology ..... 70**
**E.5 Human readable information ..... 71**
**E.6 Layout, facing and aesthetics ..... 72**
**E.7 Performance and test criteria ..... 73**

**Annex F (informative) Statistical analysis of DPM verification ..... 74**

**F.1 Introduction ..... 74**
**F.2 Purpose and scope of postal item verification ..... 74**
**F.3 Detection of DPMs with invalid validation code ..... 75**
**F.4 Influence of CVC length on fraud detection ..... 80**
**F.5 Detection of duplicate DPMs ..... 81**

**Annex G (informative) Message security algorithms ..... 82**

**G.1 Introduction ..... 82**
**G.2 Hash functions used in message security services ..... 82**
**G.3 Asymmetric (public key) cryptographic algorithms ..... 83**
**G.4 Message authentication code (MAC) algorithms ..... 86**
**G.5 Exchange validation code generation ..... 90**
**G.6 Selection of algorithms for CVC implementation ..... 90**

**Annex H (informative) CVC generation and verification data ..... 96**

**H.1 Introduction ..... 96**
**H.2 Sources of data for verification ..... 96**
**H.3 Selection of data used in the verification process ..... 97**

**Annex I (informative) Architecture examples ..... 103**

**I.1 Introduction ..... 103**
**I.2 The REMPI architecture ..... 103**
**I.3 USPS IBIP configurations ..... 107**

**Annex J (informative) Examples of digital postage marks (not to scale) ..... 112**

**J.1 Australia Post ..... 112**
**J.2 Canada Post ..... 112**
**J.3 Deutsche Post ..... 112**
**J.4 Die Post, Switzerland ..... 114**
**J.5 Royal Mail ..... 115**
**J.6 United States Postal Service (USPS) ..... 116**

**DIN EN 14615:2017-12 EN 14615:2017 (E) Annex K (informative) Relevant intellectual property rights (IPR) ..... 118**

**K.1 Introduction ..... 118**
**K.2 Massachusetts Institute of Technology ..... 118**
**K.3 Neopost ..... 118**
**K.4 Pitney Bowes Inc ..... 119**
**K.5 Pitney Bowes Inc, together with Certicom Corp ..... 119**
**K.6 United States Department of Commerce ..... 120**
**K.7 United States Postal Service ..... 120**

**Annex L (informative) DPM design charts ..... 121**

**L.1 Applicability of countermeasures against identified threats ..... 121**

**L.2 Data elements used by typical applications and countermeasures .....125**
**L.3 Mapping data elements onto data source and DPM data constructs .....129**

**Bibliography .....131**