

# DIN EN 14615:2017-12 (D)

## Postalische Dienstleistungen - Digitale Freimachungsvermerke - Anwendungen, Sicherheit und Gestaltung; Deutsche Fassung EN 14615:2017

---

Inhalt	Seite
Europäisches Vorwort.....	4
Einleitung .....	6
1 Anwendungsbereich.....	8
2 Normative Verweisungen .....	8
3 Begriffe .....	8
4 Symbole und Abkürzungen .....	11
5 DPM-Anwendungen und Gestaltungsprozess .....	12
5.1 Einleitung.....	12
5.2 DPM-Unternehmensplanung.....	13
5.3 DPM-Systemanalyse .....	15
5.4 DPM-Sicherheitsanalyse .....	15
5.5 DPM-Gestaltung .....	16
Anhang A (normativ) Spezifikations-Prüflisten.....	17
A.1 Anwendungsspezifikationen .....	17
A.2 Systemspezifikation .....	17
A.3 Sicherheitsspezifikation .....	18
A.4 DPM-Spezifikation.....	18
Anhang B (informativ) Überlegungen hinsichtlich der Unternehmensplanung .....	19
B.1 Mögliche Anwendungen .....	19
B.2 Marktsegmentierung.....	21
B.3 Anwendungsauswahl .....	23
Anhang C (informativ) Überlegungen hinsichtlich der Sicherheitsanalyse.....	27
C.1 Kontext.....	27
C.2 Sicherheitstechnische Ziele, Verfahren und ökonomische Aspekte.....	28
C.3 Bedrohungen und Schwachstellen.....	30
C.4 Sicherheit auf Anwendungs- und Mitteilungsebene .....	34
C.5 Sicherheitsfunktionen und Gegenmaßnahmen auf Mitteilungsebene .....	36
C.6 Gegenmaßnahmen auf Anwendungsebene .....	39
C.7 Auswahl von Gegenmaßnahmen .....	53
C.8 Anwendung von Gegenmaßnahmen .....	54
C.9 Optionen zur Implementierung der Mitteilungssicherheit.....	55
Anhang D (informativ) Überlegungen hinsichtlich der Systemanalyse .....	62
D.1 Bedarfsanalyse.....	62
D.2 Funktionsbeschreibung .....	63
D.3 Aufgabenzuweisung und Architekturplanung.....	66
D.4 Weitere ausführliche Planungsaspekte .....	67
Anhang E (informativ) Überlegungen zu DPM-Gestaltung .....	74
E.1 Dateninhalt.....	74
E.2 Dateneintrag .....	75
E.3 Datenkonstruktabbildung.....	76
E.4 Symbologie .....	78
E.5 Klartextinformationen .....	79

E.6	Layout, Ausrichtung und Aussehen .....	79
E.7	Leistungs- und Prüfkriterien.....	80
<b>Anhang F (informativ) Statistische Analyse der DPM-Prüfung.....</b>		<b>82</b>
F.1	Einleitung.....	82
F.2	Ziel und Umfang der Überprüfung von Postsendungen .....	82
F.3	Erkennung von DPMs mit ungültigem Gültigkeitscode .....	83
F.4	Einfluss der CVC-Länge auf die Betrugserkennung.....	89
F.5	Erkennung von kopierten DPMs .....	89
<b>Anhang G (informativ) Mitteilungssicherheitsalgorithmen .....</b>		<b>91</b>
G.1	Einleitung.....	91
G.2	In Mitteilungssicherheitsdiensten verwendete Hash-Funktionen .....	91
G.3	Asymmetrische kryptographische Algorithmen (öffentliche Schlüssel) .....	92
G.4	Mitteilungsauthentisierungscode(MAC)-Algorithmen .....	96
G.5	Erzeugung des Austauschgültigkeitscodes (EVC) .....	99
G.6	Algorithmusauswahl für die CVC-Implementierung.....	100
<b>Anhang H (informativ) CVC-Erzeugungs- und Verifizierungsdaten .....</b>		<b>107</b>
H.1	Einleitung.....	107
H.2	Datenquellen zur Verifizierung.....	107
H.3	Während des Verifizierungsprozesses verwendete Datenauswahl .....	108
<b>Anhang I (informativ) Architekturbeispiele .....</b>		<b>114</b>
I.1	Einleitung.....	114
I.2	REMPI-Architektur .....	114
I.3	USPS IBIP-Konfigurationen.....	118
<b>Anhang J (informativ) Beispiele digitaler Freimachungsvermerke (nicht maßstabsgetreu) .....</b>		<b>123</b>
J.1	Australia Post .....	123
J.2	Canada Post.....	123
J.3	Deutsche Post .....	124
J.4	Die Post, Schweiz .....	125
J.5	Royal Mail .....	126
J.6	United States Postal Service (USPS) .....	127
<b>Anhang K (informativ) Relevante geistige Eigentumsrechte .....</b>		<b>128</b>
K.1	Einleitung.....	128
K.2	Massachusetts Institute of Technology .....	128
K.3	Neopost.....	128
K.4	Pitney Bowes Inc .....	129
K.5	Pitney Bowes Inc, zusammen mit der Certicom Corp.....	130
K.6	Handelministerium der Vereinigten Staaten von Amerika.....	130
K.7	United States Postal Service (Postdienst der Vereinigte Staaten von Amerika) .....	130
<b>Anhang L (informativ) Schaubilder über die DPM-Gestaltung .....</b>		<b>131</b>
L.1	Anwendbarkeit von Gegenmaßnahmen gegen festgestellte Bedrohungen .....	131
L.2	Von typischen Anwendungen und Gegenmaßnahmen verwendete Datenelemente.....	133
L.3	Zuordnung von Datenelementen zu Datenquellen und DPM-Datenkonstrukten.....	138
<b>Literaturhinweise .....</b>		<b>140</b>