E DIN EN 14615:2016-09 (D/E)

Erscheinungsdatum: 2016-08-19

Postalische Dienstleistungen - Digitale Freimachungsvermerke - Anwendungen, Sicherheit und Gestaltung; Deutsche und Englische Fassung prEN 14615:2016

Postal services - Digital postage marks - Applications, security and design; German and English version prEN 14615:2016

Inhalt

Seite

Europäisches Vorwort 6

Einleitung 7

1 Anwendungsbereich 9

2 Normative Verweisungen 9

3 Begriffe 9

4 Symbole und Abkürzungen 13

5 DPM-Anwendungen und Gestaltungsprozess 13
5.1 Einleitung 13
5.2 Unternehmensplanung digitaler Freimachungsvermerke 15
5.3 Systemanalyse für digitale Freimachungsvermerke 16
5.4 Sicherheitsanalyse digitaler Freimachungsvermerke 17
5.5 Gestaltung digitaler Freimachungsvermerke 18

Anhang A (normativ) Spezifikations-Prüflisten 19
A.1 Anwendungsspezifikationen 19
A.2 Systembeschreibung 19
A.3 Sicherheitsbeschreibung 20
A.4 Beschreibung digitaler Freimachungsvermerke 20

Anhang B (informativ) Überlegungen hinsichtlich der Unternehmensplanung 21
B.1 Mögliche Anwendungen 21
B.2 Marktsegmentierung 23
B.2.1 Ansatz 23
B.2.2 Absendersegmentierung 23
B.2.3 Postzugang und Einlieferung 23
B.2.4 Zahlungsweise 24
B.3 Anwendungsauswahl 25
B.3.1 Ansatz 25
B.3.2 Infrastrukturelle Anforderungen und Beschränkungen 25
B.3.3 Sonstige Faktoren 27

Anhang C (informativ) Überlegungen hinsichtlich der Sicherheitsanalyse 29
C.1 Kontext 29
C.2 Sicherheitstechnische Ziele, Verfahren und ökonomische Aspekte 30
C.3 Bedrohungen und Schwachstellen 32
C.3.1 Einleitung 32
C.3.2 Umgebungskontext 32
C.3.3 Allgemeine Bedrohungen für Systeme digitaler Freimachungsvermerke 33
C.4 Sicherheit auf Anwendungs- und Mitteilungsebene 37
C.5 Sicherheitsfunktionen und Gegenmaßnahmen auf Mitteilungsebene 39
C.6 Gegenmaßnahmen auf Anwendungsebene 42
C.6.1 Einleitung 42
C.6.2 Zugangs- und Anwendungskontrollen 42

C.6.3 Dublettenerkennung 46
C.6.4 Einlieferungskontrolle 50
C.6.5 Prüfung und forensische Analyse 50
C.6.6 Untersuchung 51
C.6.7 Überprüfung von Postsendungen 51
C.6.8 Maßnahmen gegen Beschädigung 54
C.6.9 Security Service Management 55
C.6.10 Kontrollen des Sendungsaufkommens und der Einnahmen 55
C.7 Auswahl von Gegenmaßnahmen 56
C.8 Anwendung von Gegenmaßnahmen 57
C.9 Optionen zur Implementierung der Mitteilungssicherheit 58
C.9.1 Einleitung 58
C.9.2 Digitale Signaturen 59
C.9.3 Mitteilungsauthentisierungscodes 60
C.9.4 Austauschgültigkeitscodes (AGCs) 62
C.9.5 Technikauswahl zur Mitteilungssicherheit 64
C.9.6 Anwendung von Prüftechniken 64

Anhang D (informativ) Überlegungen hinsichtlich der Systemanalyse 65
D.1 Bedarfsanalyse 65
D.2 Funktionsbeschreibung 67
D.2.1 Ansatz 67
D.2.2 Erstellung von Postsendungen 67
D.2.3 Tarifgestaltung 67
D.2.4 Abrechnung 67
D.2.5 Erstellen der digitalen Freimachungsvermerke 67
D.2.6 Drucken der digitalen Freimachungsvermerke 68
D.2.7 Zahlungsweise 68
D.2.8 Einlieferung 68
D.2.9 Postbearbeitung: Sortierung, Beförderung, Zustellung 68
D.2.10 Komponentenmanagement 69
D.2.11 Sicherheitsmanagement 69
D.2.12 Prüfung 69
D.2.13 Anwendungsdienste 69
D.3 Aufgabenzuweisung und Architekturplanung 69
D.4 Weitere ausführliche Planungsaspekte 70
D.4.1 Einleitung 70
D.4.2 Datenerfordernisse und Datenquellen 70
D.4.3 Drucken der digitalen Freimachungsvermerke 71
D.4.4 Datenerfassung digitaler Freimachungsvermerke 73
D.4.5 Anwendungsverarbeitung 75
D.4.6 Sicherheitsanalyse 75
D.4.7 Fehlerbehandlung 76

Anhang E (informativ) Überlegungen zu DPM-Gestaltung 77
E.1 Dateninhalt 77
E.2 Dateneintrag 78
E.3 Datenkonstruktabbildung 79
E.4 Symbologie 81
E.5 Klartextinformationen 82
E.6 Layout, Ausrichtung und Aussehen 83
E.7 Leistungs- und Prüfkriterien 84

Anhang F (informativ) Statistische Analyse der Prüfung digitaler Freimachungsvermerke 85
F.1 Einleitung 85
F.2 Ziel und Umfang der Überprüfung von Postsendungen 85
F.3 Erkennung von digitalen Freimachungsvermerken mit ungültigem Gültigkeitscode 86
F.3.1 Einleitung 86
F.3.2 Parameter 87

F.3.3 Mögliche Ergebnisse 88
F.3.4 Analyse der Ergebnisse 88
F.3.5 Berechnung der Häufigkeit von Betrugsfällen 89
F.4 Einfluss der Länge des VGC auf die Betrugserkennung 92
F.5 Erkennung von kopierten digitalen Freimachungsvermerken 93

Anhang G (informativ) Mitteilungssicherheitsalgorithmen 95
G.1 Einleitung 95
G.2 In Mitteilungssicherheitsdiensten verwendete Hash-Funktionen 95
G.3 Asymmetrische Verschlüsselungsalgorithmen (öffentliche Schlüssel) 96
G.3.1 DSA 96
G.3.2 RSA 96
G.3.3 ECDSA 97
G.3.4 Digitale Signaturen bei Hybridsendungen mit teilweiser Mitteilungsrückgewinnung 98
G.3.5 Sonstige digitale Signaturverfahren 100
G.4 Mitteilungsauthentisierungscode(MAC)-Algorithmen 100
G.4.1 Allgemeines 100
G.4.2 CBC DES 100
G.4.3 Advanced Encryption Standard (AES) 101
G.4.4 HMAC 101
G.4.5 MAC-Verkürzung und VGC-Länge 102
G.5 Erzeugung des Austauschgültigkeitscodes (AGC) 104
G.6 Algorithmusauswahl für die VGC-Implementierung 105
G.6.1 Einleitung 105
G.6.2 Kryptografische Wirkung der allgemein verwendeten Algorithmen 105
G.6.3 Länge des Gültigkeitscodes und Längenerweiterung 108
G.6.4 Erzeugungs- und Verifizierungskomplexität 108
G.6.5 Komplexität der Schlüsselerzeugung 109
G.6.6 Infrastruktur der Chiffrierschlüsselverwaltung 109
G.6.7 Geistige Eigentumsrechte 110
G.6.8 Rechtmäßige Anwendung, Ausfuhr- und Einfuhrgenehmigung 110

Anhang H (informativ) VGC-Erzeugungs- und Verifizierungsdaten 111
H.1 Einleitung 111
H.2 Datenquellen zur Verifizierung 111
H.2.1 Einleitung 111
H.2.2 Auf der Sendung verschlüsselte Daten 112
H.2.3 Datenbankzugriff durch Datenbankabfrage 112
H.3 Während des Verifizierungsprozesses verwendete Datenauswahl 113
H.3.1 Einleitung 113
H.3.2 Annahmekontrollcode 114
H.3.3 Stapelkennung und Sendungsnummer, Prüfplakette 114
H.3.4 VGC 115
H.3.5 Datum/Uhrzeit 115
H.3.6 Zustellsicherheitscode 116
H.3.7 Gerätekennung, Kundenkennung bzw. Prüfplakette 116
H.3.8 Portowert 117
H.3.9 Zertifikatskennung für den öffentlichen Schlüssel 117
H.3.10 Tarifparameter, einschließlich Dienstekennung 118

Anhang I (informativ) Architekturbeispiele 119
I.1 Einleitung 119
I.2 REMPI-Architektur 119
I.2.1 Einleitung 119
I.2.2 Versendersysteme 119
I.2.3 Postfertigstellungssystem 119
I.2.4 Postfertigstellungs-Drucksubsystem 120
I.2.5 Sicheres Abrechnungssystem 120
I.2.6 Ankündigungssystem 121

I.2.7 Annahmesystem **121**
I.2.8 Postsendungsprüfsystem **122**
I.2.9 Abstimmungs- und Supportsysteme **122**
I.2.10 Bank **122**
I.2.11 Postsysteme **122**
I.2.12 Postbearbeitungsinfrastruktur **123**
I.2.13 Kundeninformationssystem **123**
I.2.14 Abfrage- und Datensystem **123**
I.3 USPS IBIP-Konfigurationen **123**
I.3.1 Einleitung **123**
I.3.2 Systemkomponenten **124**
I.3.3 Konfiguration A **125**
I.3.4 Konfiguration B **127**

Anhang J (informativ) Beispiele digitaler Freimachungsvermerke (nicht maßstabsgetreu) **128**
J.1 Australia Post **128**
J.2 Canada Post **128**
J.3 Deutsche Post **129**
J.4 Die Post, Schweiz **130**
J.5 Royal Mail **131**
J.6 United States Postal Service (USPS) **132**

Anhang K (informativ) Relevante geistige Eigentumsrechte **133**
K.1 Einleitung **133**
K.2 Massachusetts Institute of Technology **133**
K.3 Neopost **133**
K.4 Pitney Bowes Inc **134**
K.5 Pitney Bowes Inc, zusammen mit der Certicom Corp **135**
K.6 Handelministerium der Vereinigten Staaten von Amerika **135**
K.7 United States Postal Service (Postdienst der Vereinigte Staaten von Amerika) **135**

Anhang L (informativ) Schaubilder über die DPM-Gestaltung **136**
L.1 Anwendbarkeit von Gegenmaßnahmen gegen festgestellte Bedrohungen **136**
L.2 Von typischen Anwendungen und Gegenmaßnahmen verwendete Datenelemente **139**
L.3 Abbilden von Datenelementen auf die Datenquelle und die Datenkonstrukte digitaler Freimachungsvermerke **143**

Literaturhinweise **145**