

DIN EN 14615

ICS 03.240

**Postalische Dienstleistungen –
Digitale Freimachungsvermerke –
Inhalte, Sicherheit und Gestaltung;
Deutsche Fassung EN 14615:2005**

Postal services –
Digital postage marks –
Applications, security and design;
German version EN 14615:2005

Services postaux –
Marques d'affranchissement digitales –
Applications, sécurité et design;
Version allemande EN 14615:2005

Gesamtumfang 141 Seiten

Normenausschuss Bürowesen (NBü) im DIN

Nationales Vorwort

Das vorliegende europäische Dokument wurde vom CEN/TC 331 „Postalische Dienstleistungen“ unter Beteiligung deutscher Experten erarbeitet.

Der für die deutsche Mitarbeit zuständige Arbeitsausschuss im DIN Deutsches Institut für Normung e. V. ist der NBü-1.6 „Postalische Dienstleistungen“.

Deutsche Fassung

**Postalische Deinstleistungen —
Digitale Freimachungsvermerke —
Inhalte, Sicherheit und Gestaltung**

Postal services —
Digital postage marks —
Applications, security and design

Services postaux —
Marques d'affranchissement digitales —
Applications, sécurité et design

Diese Europäische Norm wurde vom CEN am 26. August 2004 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: rue de Stassart, 36 B-1050 Brüssel

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	5
2 Normative Verweisungen.....	5
3 Begriffe	6
4 Symbole und Abkürzungen	9
5 Inhalte digitaler Freimachungsvermerke und Gestaltungsprozesse	9
5.1 Einleitung.....	9
5.2 Unternehmensplanung digitaler Freimachungsvermerke.....	12
5.3 Systemanalyse für digitale Freimachungsvermerke	13
5.4 Sicherheitsanalyse digitaler Freimachungsvermerke	14
5.5 Gestaltung digitaler Freimachungsvermerke	14
Anhang A (normativ) Spezifikations-Prüflisten	16
Anhang B (informativ) Überlegungen hinsichtlich der Unternehmensplanung	18
Anhang C (informativ) Überlegungen hinsichtlich der Sicherheitsanalyse	25
Anhang D (informativ) Überlegungen hinsichtlich der Systemanalyse.....	59
Anhang E (informativ) Überlegungen zu Inhalten digitaler Freimachungsvermerke.....	70
Anhang F (informativ) Statistische Analyse der Prüfung digitaler Freimachungsvermerke.....	77
Anhang G (informativ) Mitteilungssicherheitsalgorithmen.....	86
Anhang H (informativ) VGC-Erzeugungs- und Verifizierungsdaten.....	101
Anhang I (informativ) Architekturbeispiele.....	108
Anhang J (informativ) Beispiele digitaler Freimachungsvermerke (nicht maßstabsgetreu)	117
Anhang K (informativ) Relevante geistige Eigentumsrechte.....	122
Anhang L (informativ) Schaubilder über die Inhalte digitaler Freimachungsvermerke.....	125
Literaturhinweise	136

Vorwort

Dieses Dokument (EN 14615:2005) wurde vom Technischen Komitee CEN/TC 331 „Postalische Dienstleistungen“ erarbeitet, dessen Sekretariat vom NEN gehalten wird.

ANMERKUNG Dieses Dokument wurde von Fachleuten des CEN/TC 331/WG 3 und des WPV im Rahmen der Absichtserklärung zwischen CEN und dem WPV entwickelt.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juli 2005, und etwaige entgegenstehende nationale Normen müssen bis Juli 2005 zurückgezogen werden.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinie(n).

Dieses Dokument (EN 14615:2005) ist das CEN-Äquivalent der WPV¹⁾-Norm S36-4. Es darf nur nach vorheriger Rücksprache mit CEN/TC 331 und dem WPV-Normenausschuss nach der Absichtserklärung zwischen CEN und dem WPV ergänzt werden.

Der Beitrag des WPV zur Norm wurde von dem Normenausschuss des WPV und dessen Untergruppen geleistet²⁾, nach den in Teil V der „Allgemeinen Informationen über WPV-Normen“ enthaltenen Vorschriften.

Bei diesem Dokument handelt es sich um die erste Ausgabe von EN 14615, sie entspricht jedoch der vierten Ausgabe (S36-4) der WPV-Norm S36, deren Revisionshistorie im Vorwort der WPV-Fassung der Spezifikation enthalten ist.

Dieses Dokument enthält Literaturhinweise.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

1) Der Weltpostverein (WPV) ist eine spezialisierte Einrichtung der Vereinten Nationen, der den weltweiten Postdienst regelt. Die Postdienste seiner 189 Mitgliedsländer bilden das weltweit größte physikalische Verteilnetz. Etwa 5 Millionen Postbedienstete in mehr als 660 000 Postdienststellen auf der ganzen Welt bearbeiten jährlich insgesamt 425 Milliarden Postsendungen im inländischen Postverkehr und fast 6,7 Milliarden grenzüberschreitende Sendungen. Etwa 4,5 Milliarden Pakete werden jährlich per Post versendet. Um mit dem Wandel im Telekommunikationsmarkt Schritt halten zu können, verwenden die Postdienste zunehmend neue Kommunikations- und Informationstechnologien und gehen damit über das hinaus, was traditionell als ihr Kernpostgeschäft angesehen wird. Sie erfüllen die gestiegenen Erwartungen ihrer Kunden durch die Bereitstellung einer erweiterten Produktpalette und Mehrwertdiensten.

2) Der Normenausschuss des WPV entwickelt und unterhält eine steigende Zahl von Normen zur Verbesserung des Austauschs von postspezifischen Informationen zwischen den jeweiligen Postdiensten und fördert die Kompatibilität zwischen dem WPV und den internationalen Postinitiativen. Er arbeitet eng mit den Postdiensten, den Kunden, Lieferanten und den sonstigen Partnern, einschließlich den verschiedenen internationalen Organisationen zusammen. Der Normenausschuss stellt sicher, dass in den Bereichen wie beispielsweise dem elektronischen Datenaustausch, der Maillkodierung, Postformen und Frankiereinrichtungen kohärente Normen entwickelt werden. Die WPV-Normen werden nach den in Teil VII der Allgemeinen Informationen über WPV-Normen festgelegten Vorschriften veröffentlicht, die kostenlos über die Webseite des WPV herunter geladen werden können (www.upu.int).

Einleitung

Der Übergang vom Hochdruck zum Digitaldruck bietet Chancen für eine effektivere Übertragung der Informationen mit Hilfe von Postsendungen. Die aktuellen Freimachungsvermerke enthalten Angaben wie den Portowert, das Einlieferungsdatum oder die Gerätekennung, diese Angaben liegen jedoch nicht in maschinenlesbarer Form vor. Die wachsende Anwendung der Digitaldruck- und Bildverarbeitungstechnologien schafft Möglichkeiten zur Entschlüsselung wichtiger Daten in Form von digitalen Freimachungsvermerken, die für eine Datenerfassung per Computer geeigneter ist. Die Annahme dieser Technologien erfordert jedoch eine sorgfältige Untersuchung sowohl für die Maximierung der Vorteile aus ihrer Einführung als auch aufgrund der Tatsache, dass die digitale Drucktechnologie einen Bedarf an anderen Sicherheitsmaßnahmen mit sich bringt, verglichen mit denjenigen, die im Allgemeinen im Hochdruck angewendet werden.

Das Dokument beschreibt eine Reihe von Faktoren, die im Rahmen des Gestaltungsprozesses digitaler Freimachungsvermerke zu berücksichtigen sind. Es verfolgt drei Hauptziele. Es soll fungieren als:

- a) **Standardverfahren:** für die Gestaltung von Inhalten digitaler Freimachungsvermerke;
- b) **Richtlinie:** zur Unterstützung bei der Erstellung nationaler Normen für digitale Freimachungsvermerke;
- c) **Querverweis:** zum Verweisen auf andere Standards und Dokumente, die sich mit Inhalten digitaler Freimachungsvermerke befassen.

Es wird betont, dass diese Faktoren einen repräsentativen Charakter aufweisen sollen und keinen Anspruch auf Vollständigkeit erheben.

Das Dokument enthält außerdem zahlreiche Beispiele für mögliche Architekturen und Planungslösungen für die aufgeworfenen Fragen. Diese sind nicht normativ. Sie dienen lediglich der Veranschaulichung und es gibt sicherlich eine breite Palette anderer hierin nicht beschriebener Möglichkeiten. Es soll nicht vorgeschlagen werden, dass eine hierin beschriebene Architektur, Planung oder technische Lösung unbedingt erforderlich oder einer anderen überlegen ist, gleichgültig ob hierin beschrieben oder nicht.

Die Implementierung bestimmter in den informativen Abschnitten dieser Spezifikation beschriebener Techniken könnte die Verwendung geistiger Eigentumsrechte beinhalten, die Patentrechten unterliegen. Es liegt in der Verantwortung der Normenanwender, die erforderliche Patentrecherche vorzunehmen und sicherzustellen, dass alle einschlägigen Patente allgemein zugänglich, lizenziert³⁾ oder als ungültig angefochten sind. Weder CEN noch der WPV kann die Verantwortung im Falle eines Verstoßes von Seiten der Anwender dieses Dokuments gegen die geistigen Eigentumsrechte Dritter übernehmen. Dennoch sind die Anwender des Dokuments sowie die Eigentümer solcher Rechte gehalten, das Sekretariat des WPV-Normenausschusses bzw. des CEN/TC 331 über jede ausdrückliche Forderung in Kenntnis zu setzen, nach der eine hierin beschriebene Technik oder Lösung in einem Mitgliedsland des CEN oder des WPV patentrechtlich geschützt ist. Alle diesbezüglichen Forderungen werden ohne Schaden für die eigenen Rechte in die nächste aktualisierte Fassung dieser Norm bzw. nach Ermessen des Normenausschusses bzw. CEN/TC 331 aufgenommen. In Anhang K dieses Dokuments sind die geistigen Eigentumsrechte aufgeführt und vor der Genehmigung der Veröffentlichung dieser Version der Norm der CEN/TC 331 und des WPV-Normenausschusses zur Kenntnis gebracht.

ANMERKUNG Solche geistigen Eigentumsrechte werden in Anhang K auf der Grundlage „ohne Obligo“ erwähnt. Dies bedeutet, dass eine solche Erwähnung nur anzeigt, dass eine bestimmte Partei die Ansicht geäußert hat, dass durch die Verwendung der Norm in einigen Fällen die erwähnten geistigen Eigentumsrechte verletzt werden könnten. Es sollte nicht so ausgelegt werden, dass die Gültigkeit einer solchen Ansicht bestätigt wird und die Anwender ihre eigenen Nachforschungen anstellen sollten, um festzustellen, ob die erwähnte IPR tatsächlich auf ihren spezifischen Fall zutrifft.

3) Den Postdienstleistern wird nahegelegt, sich zu vergegenwärtigen, dass ein Vertrauen auf patentierte Ansätze nicht unbedingt die Schaffung eines effektiven Monopols nach sich zieht. Dies könnte selbst dann eintreten, wenn die Verwendung der jeweiligen Ansätze vom Postdienstleister lizenziert wird, sofern die Bedingungen der Lizenzvereinbarung den Patentinhaber dazu verpflichten, die Patente unter bestimmten Bedingungen den Postdienstleistern und Lieferanten, einschließlich den Wettbewerbern des Patentinhabers zur Verfügung zu stellen.

1 Anwendungsbereich

Dieses Dokument beschreibt ein empfohlenes Verfahren für die Entwicklung der Spezifikation digitaler Freimachungsvermerke (DPMs) — d. h. Inhalte, die mit den digitalen Druck- und Bilddatenerfassungstechnologien in der Postindustrie verknüpft sind, größtenteils für den Nachweis der Portoabrechnung bzw. — bezahlung. Es ist nicht beabsichtigt, bestimmte Architektur bzw. einen bestimmten Entwurf für solche Inhalte vorzuschreiben oder zu empfehlen, sondern nur den Prozess anzugeben, durch den eine Architektur oder ein Entwurf entwickelt werden sollte.

ANMERKUNG 1 Aus diesem Grund sind in dieser Norm sowohl ein normativer als auch ein informativer Inhalt berücksichtigt. Die Abschnitte 1 bis 5 sowie Anhang A weisen normativen Charakter auf, während die übrigen Anhänge informativer Art sind. Alle nicht normativen (informativen) Abschnitte sind als solche in der Überschrift gekennzeichnet.

Der Prozess beruht auf einem zyklischen Modell, welches die Geschäftsplanung, Systemanalyse, Sicherheitsanalyse sowie eine ausführliche Gestaltung der digitalen Freimachungsvermerke umfasst.

Bei dem festgelegten Verfahren handelt es sich lediglich um eine Empfehlung und die für die Gestaltung der Inhalte digitaler Freimachungsvermerke zuständigen Personen sind nicht verpflichtet, sich daran zu halten. Durch die Verwendung soll jedoch sichergestellt werden, dass alle relevanten Aspekte des Gestaltungsverfahrens berücksichtigt werden und dass die daraus folgende technische Beschreibung so aufgebaut ist, dass sie sich mit einer von Dritten erzeugten technischen Beschreibung vergleichen lässt. Es ist zu hoffen, dass die Anwendung dadurch besser verständlich und weniger zweideutig für die Anwender ist.

Es wird vorausgesetzt, dass die Anwender der Norm mit den normalen Verfahren für die Gestaltung computergestützter Inhalte vertraut sind, und die Norm beschränkt sich deshalb auf Aspekte, die spezifisch für die Gestaltung von Inhalten digitaler Freimachungsvermerke sind. Insbesondere enthält das Dokument lediglich Anforderungen und Überlegungen in Bezug auf Inhalte, die digitale Freimachungsvermerke auf einzelnen Postsendungen als Mittel zur Datenübermittlung (Mitteilungen) verwenden. Der Abschnitt „Design“ befasst sich lediglich mit der Gestaltung der digitalen Freimachungsvermerke selbst. Es werden keine Aspekte der Gestaltung, einschließlich der möglichen Verwendung anderer mit anderen Mitteln übertragener Mitteilungen (z. B. Einlieferungslisten) berücksichtigt, um zusätzliche Daten zu übertragen, auch wenn diese ebenso wichtig sein könnten.

Die Norm setzt voraus, ohne dies jedoch zu fordern, dass digitale Freimachungsvermerke eingeführt werden sollen, die den WPV-Normen S27, S28 und S25 entsprechen (siehe Literaturhinweise), und stellt eine Richtlinie für die Anwendung dieser Standards bereit. Viele der Richtlinien, Empfehlungen und Prüflisten gelten jedoch gleichermaßen für die Gestaltung von DPM-Inhalten unter Verwendung digitaler Freimachungsvermerke aufgrund anderer als den von S28 unterstützten Symbolen bzw. erfordern Daten, die von den nach S25 festgelegten Datenkonstrukten nicht aufgenommen werden können.

ANMERKUNG 2 Auch wenn S28 [7] nur für die Darstellung mit Hilfe zweidimensionaler Symbole gilt und sich der Umfang auf zwei davon beschränkt, ist Data Matrix und PDF417, seine Erweiterung um andere Symbole, einschließlich linearer Barcodes und OCR-Darstellung der Daten, für weitere Überlegungen offen. Anwender, die der Auffassung sind, dass ihre Anforderungen durch die festgelegten Einschränkungen nicht erfüllt werden können, werden deshalb dazu aufgefordert, sich an das Sekretariat des WPV-Normenausschusses zu wenden, damit von diesem eine entsprechende Erweiterung der Norm in Betracht gezogen werden kann.

ANMERKUNG 3 Auch wenn in S25 [5] ein erster Satz Datenkonstrukte festgelegt ist, soll dieser Satz auf einer Bedarfsbasis erweitert werden. Anwender, die der Auffassung sind, dass ihre Anforderungen durch die vorhandenen Datendefinitionen nicht erfüllt werden können, werden deshalb dazu aufgefordert, sich an das Sekretariat des WPV-Normenausschusses im Hinblick auf eine entsprechende Erweiterung der Norm zu wenden.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

WPV-Normenglossar⁴⁾

ANMERKUNG Auch wenn die Norm unter der Annahme entwickelt wurde, dass die Anwender ihre digitalen Freimachungsvermerke auf der Grundlage der WPV-Normen S28 [7] und S25 [5] realisieren möchten, handelt es sich hierbei um keine wirkliche Forderung. Diese beiden Standards werden aus diesem Grund zusammen mit zahlreichen anderen relevanten Normen, die für das Begriffsbestimmungsverfahren für digitale Freimachungsvermerke berücksichtigt werden sollten, in der (informativen) Literaturliste am Ende der Norm aufgeführt.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die im WPV-Normenglossar enthaltenen Begriffe und folgende Begriffe.

3.1

Änderung

absichtliches Ändern der in einem digitalen Freimachungsvermerk enthaltenen Angaben

3.2

Authentisierung

Nachweisverfahren, dass die auf einer Postsendung verschlüsselten Angaben, einschließlich in deren digitalem Freimachungsvermerk, intern übereinstimmen und von der auf der Sendung angegebenen Quelle stammen

3.3

Absprache

Kooperation zwischen zwei oder mehreren Parteien in betrügerischer Absicht

3.4

Kopieren (en: copying)

Duplizieren eines originalen digitalen Freimachungsvermerks zur Herstellung identischer Kopien und unbefugte Verwendung dieser Kopien auf Postsendungen, die in das Postsystem eingebracht werden

3.5

Fälschen

unbefugtes Erstellen eines Symbols, welches einem legitimen digitalen Freimachungsvermerk ähnelt oder gleicht, in betrügerischer Absicht

3.6

Gegenmaßnahme

Handlungen, Gesetze, Verfahren, Mechanismen oder kombinierte Maßnahmen davon, die ergriffen werden können, um gegnerische Angriffe auf ein oder unabsichtliche Fehler bei den Inhalten digitaler Freimachungsvermerke festzustellen, aufzuhalten, zu vereiteln und/oder zu vermeiden bzw. den aus dem Vorkommen solcher Angriffe oder Fehler entstehenden Schaden zu kontrollieren oder zu begrenzen

3.7

Kryptoanalyse

Verwendung von mathematischen Techniken beim Versuch, die Verwendung von Verschlüsselungsmethoden zu unterbinden, insbesondere im Zusammenhang mit Informationssicherheitsdiensten

4) Die WPV-Normen lassen sich vom International Bureau des WPV beziehen, dessen Kontaktangaben der Literaturliste entnommen werden können; das WPV-Normenglossar kann kostenlos über die Internet-Adresse <http://www.upu.int> heruntergeladen werden.

3.8**verschlüsselter Gültigkeitscode****VGC**

verschlüsselt aus ausgewählten Postsendungsdaten abgeleiteter Wert, der zur Überprüfung der Integrität solcher Daten und der Authentisierung ihrer Herkunft verwendet werden kann

ANMERKUNG Als ein VGC kann ein verkürzter MAC (basierend auf einem symmetrischen Chiffrieralgorithmus) oder eine digitale Signatur (auf der Basis eines asymmetrischen Algorithmus) verwendet werden. Siehe auch Austauschgültigkeitscode (AGC) sowie C.9.2 und C.9.3.

3.9**Daten erfassen****Daten lesen**

Erfassen und Dekodieren der maschinell dargestellten Angaben in einem digitalen Freimachungsvermerk

3.10**Daten lesen**

siehe unter „Daten erfassen“

3.11**Gültigkeitsprüfung digitaler Freimachungsvermerke**

Prozess einer kryptografischen oder anderweitigen Authentisierung der Herkunft und Integrität von Angaben digitaler Freimachungsvermerke

3.12**digitale Signatur**

kryptografisch von ausgewählten Daten mit Hilfe eines Public Key-Algorithmus abgeleiteter Wert, mit dem ein Datenempfänger in Kombination mit dem entsprechenden Public Key und dessen Inhaber die Herkunft der Daten authentisieren und deren Integrität prüfen kann

ANMERKUNG Siehe C.9.2. Die Verwendung von digitalen Signaturen schützt

- den Absender gegen Betrug durch Dritte oder den Empfänger und
- den Empfänger gegen Betrug durch Dritte und Erfüllungsverweigerung durch den Absender.

3.13**exchange validation code (Austauschgültigkeitscode)****EVC**

bekannter oder zwischen einem Absender und einer *lizenzierenden Post* vereinbarter Code, der bei Aufdruck auf einer Postsendung vom Absender von der *lizenzierenden Post* dazu verwendet werden kann, die Herkunft der Sendung zu authentisieren und unter bestimmten Bedingungen die Integrität der vereinbarten *DPM*-Daten zu prüfen

ANMERKUNG Siehe auch *verschlüsselter Gültigkeitscode* (VGC) sowie C.9.4.

3.14**Betrug**

betrügerisches Ausfüllen oder Ändern eines legitimen *digitalen Freimachungsvermerks*

3.15**lizenzierende Post**

Postdienstleister, welcher einen bestimmten Absender lizenziert, *digitale Freimachungsvermerke* auf Sendungen zu verwenden, die bei dem *Postdienstleister* eingeliefert werden

3.16

Message Authentication Code (Mitteilungsauthentisierungscode)

MAC

verschlüsselt aus ausgewählten Daten abgeleiteter Wert, mit dem sich die Datenintegrität und die implizite Datenherkunft nachweisen lassen

ANMERKUNG 1 Die vorstehende Definition weicht von dem WPV-Normenglossar ab.

ANMERKUNG 2 Mit MACs lässt sich die Herkunft von Daten weniger gut authentisieren als mit digitalen Signaturen, weil sie keinen Schutz gegen Betrug durch den Empfänger bzw. gegen eine Erfüllungsverweigerung durch den Absender bieten, sofern nicht der Chiffrierschlüssel nur einem vertrauenswürdigen Dritten bekannt ist und die Überprüfung von diesem vorgenommen wird.

ANMERKUNG 3 MACs beruhen auf geheimen zwischen dem Absender und dem Prüfer vereinbarten Angaben (privater Chiffrierschlüssel). Datenintegrität besteht, solange die geheimen Angaben nicht preisgegeben werden und unter der Voraussetzung, dass solche geheimen Angaben von Dritten ohne vorherige Kenntnis dieser nicht per Zufall korrekt erraten werden. Siehe C.9.3, G.4 und G.6.2 für weitere Informationen.

3.17

Beschädigung

Unkenntlichmachen eines digitalen Freimachungsvermerks in der Absicht einer Umgehung des Prüfprozesses und somit der Zahlung

3.18

Zahlungsprüfung

Prüfprozess, ob der korrekte Zahlungsbetrag für eine Postsendung und dessen Postdienst abgerechnet wurde

3.19

Postsendungsdaten

auf eine bestimmte Postsendung bezogene Angaben, die der *lizenzierenden Post* entweder bekannt sind oder zwischen ihr und dem Absender kommuniziert werden, oder die sich anhand der Postsendung selbst erfassen lassen

ANMERKUNG Das heißt, dass Postsendungsdaten folgende Angaben enthalten können:

- physikalisch messbare Kenndaten einer Sendung, wie beispielsweise das Gewicht;
- verschlüsselt oder unverschlüsselt auf der Sendung aufgedruckte Angaben, sei es in Klartextform, als Barcode oder in Form eines digitalen Freimachungsvermerks;
- Angaben, die mit Hilfe anderer Maßnahmen übertragen werden, z. B. in einer EDI-Mitteilung.

3.20

wieder verwenden bzw. erneut übertragen

Wiederverwendung oder erneute Übertragung einer *Mitteilung* (einschließlich eines digitalen Freimachungsvermerks) in betrügerischer Absicht

ANMERKUNG Das Kopieren eines digitalen Freimachungsvermerkes wird unter der Überschrift „Kopieren“ behandelt wird; „Wieder verwenden“ bezieht sich auf die Wiederverwendung eines originären digitalen Freimachungsvermerks (vergleiche Stempelreinigung).

3.21

Sicherheitsmerkmal

Sicherheitstechnik

Merkmal eines *digitalen Freimachungsvermerks*, durch das die Komplexität erhöht und eine unbemerkte Reproduktion oder Änderung des *digitalen Freimachungsvermerks* erschwert wird

ANMERKUNG Siehe C.9.5.

3.22**Bedrohung**

Angriffsmethode auf die Inhalte eines digitale Freimachungsvermerks, die bei erfolgreicher Anwendung einem Postdienstleister, dessen Agenten bzw. dessen Kunden Schaden zufügen würde

3.23**verkürzter MAC**

Sonderfall eines *Mitteilungsauthentisierungscode*s, der eine nicht-leere Untergruppe des Ergebnisses aus der Anwendung des für die MAC-Berechnung ausgewählten Chiffrieralgorithmus darstellt

ANMERKUNG Die Verkürzungsmethode wird zur Verkürzung des MAC (Platzeinsparung in digitalen Freimachungsvermerken) sowie zur weiteren Erschwerung von Schlüsselextraktionsversuchen verwendet. Die Verkürzung sollte jedoch nicht zu stark ausfallen (d. h., der MAC sollte nicht übermäßig verkürzt werden) — siehe C.9.3 und G.4.4.

3.24**Anfälligkeit**

Schwachstelle; schadensanfällig durch feindliche Angriffe oder unabsichtliche Fehler

4 Symbole und Abkürzungen

Im Sinne dieses Dokuments gelten die nachstehenden sowie die im WPV-Normenglossar enthaltenen Symbole und Abkürzungen.

CVC:	cryptographic validation code (verschlüsselter Gültigkeitscode)
EVC:	Austauschgültigkeitscode (AGC)
FIPS:	Federal Information Processing Standard (Bundesnorm für die Informationsverarbeitung)
FIPS PUB:	Verweis auf eine FIPS-Veröffentlichung, herausgegeben vom National Institute of Standards and Technology (nationalen Institut für Normung und Technologie). Die Zahl nach „PUB“ bezieht sich auf die Nummer der Veröffentlichung, auf die verwiesen wird.
NIST:	(Vereinigte Staaten von Amerika) National Institute of Standards and Technology (nationales Institut für Normung und Technologie)
 x _m:	Modulus m Wert von x, d. h. $x - m \times \text{INT}(x/m)$

5 Inhalte digitaler Freimachungsvermerke und Gestaltungsprozesse

5.1 Einleitung

Digitale Freimachungsvermerke sind Poststempel mit Angaben, die erfasst und von den Absendern, *Postbearbeitungsorganisationen* sowie den Postempfängern bearbeitet werden können und die über drei verschiedene Funktionsmerkmale verfügen:

- der Informationsgehalt wird als Mitteilung ausgedrückt, die international standardisierte Datenkonstrukte enthält;
- die *Mitteilung* wird auf der Postsendung in Form eines oder mehrerer maschinenlesbarer Symbole dargestellt;
- die Lesegeschwindigkeit und Genauigkeit der Datenerfassung auf den Symbolen werden durch die Aufnahme von Fehlerprüf- und Korrekturdaten erhöht.

Digitale Freimachungsvermerke können zur Unterstützung einer Reihe von computergestützten postalischen Anwendungen verwendet werden, die zu verschlüsselnde Angaben auf Postsendungen in einer Form erfordern, dass diese von automatischen Geräten leicht erfasst werden können. Zu solchen Anwendungen gehören der Nachweis einer Wertzeichenabrechnung bzw. -bezahlung, zusammen mit den Anwendungen, die Mehrwertdienste darstellen, wie beispielsweise Einlieferungsnachweise, Tracking und Tracing, zeitgenaue Zustellung usw.

Die Implementierung von digitalen Freimachungsvermerken sollte durch die Gesamtunternehmensziele und -strategien beschleunigt werden. Es wird vorausgesetzt, dass diese bereits bekannt sind und dass man sich darin einig ist, dass Inhalte digitaler Freimachungsvermerke einen wesentlichen Beitrag zu deren Realisierung leisten.

Die Gestaltung von Inhalten digitaler Freimachungsvermerke läuft als zyklischer Prozess in 4 einzeln abgeschlossenen Schritten ab: Unternehmensplanung, Systemanalyse, Sicherheitsanalyse und Gestaltung der Inhalte digitaler Freimachungsvermerke. Diese Zyklen sollten interaktiv und iterativ sein. In der nachstehenden Abbildung wird der Gesamtprozess veranschaulicht. Dieser beginnt mit der Unternehmensplanung, gefolgt von der gleichzeitigen Durchführung von Arbeiten an der Systemanalyse und der Sicherheitsanalyse und endet schließlich mit der Gestaltung der digitalen Freimachungsvermerke. Die ausführliche Planung der weiteren Systemaspekte erfordert ähnliche Planungsbemühungen, diese bleiben jedoch im Rahmen dieses Dokuments unberücksichtigt.

Der Unternehmensplanungszyklus ist nach 5.2 vorzunehmen und führt zu **digitalen Freimachungsvermerken** und (möglicherweise weiteren) **Inhaltsspezifikationen**, die sowohl die Anforderungen und die Einschränkungen des Unternehmens berücksichtigen. Die Angemessenheit des Umfangs dieser Spezifikationen ist durch Verweis auf die Prüfliste in A.1 nachzuweisen.

Als Eingabe in den Systemanalysezyklus digitaler Freimachungsvermerke ist die Inhaltsbeschreibung zu verwenden. Dies ist nach 5.3 vorzunehmen und führt zu der **Systemspezifikation**, die sowohl die Anforderungen und die Einschränkungen des Systems berücksichtigt. Die Angemessenheit des Umfangs dieser Spezifikationen ist durch Verweis auf die Prüfliste in A.3 nachzuweisen.

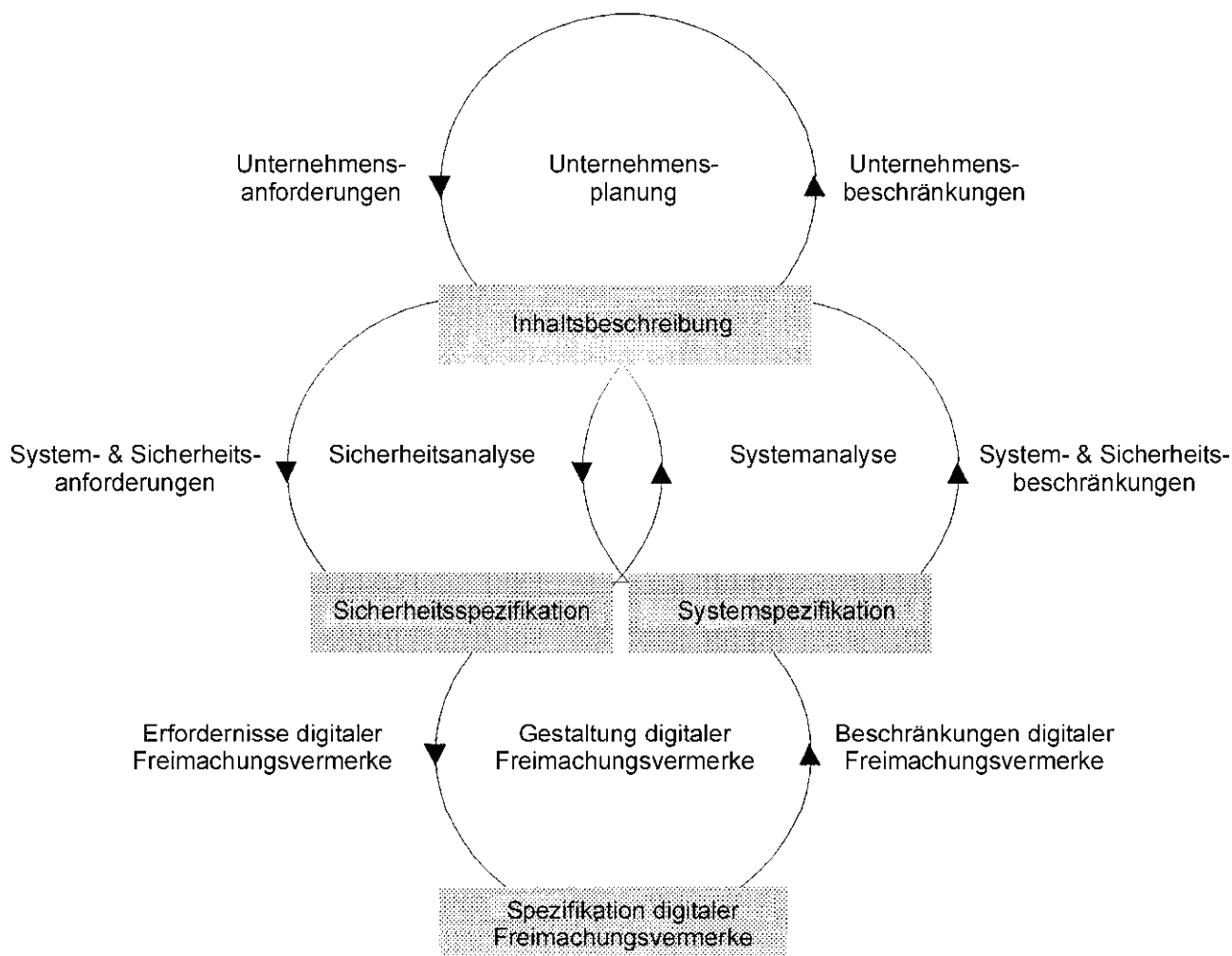


Bild 1 — Inhalte digitaler Freimachungsvermerke und Gestaltungsprozess

Bei den meisten Inhalten digitaler Freimachungsvermerke, jedoch nicht unbedingt bei allen, wird erwartet, dass sie einen Freimachungsnachweis oder eine eindeutige Kennung der Postsendungen beinhalten. Dieser Standard schließt deshalb die Sicherheitsanalyse und die Planung der Sicherheitsinfrastruktur mit ein, wobei er eine gesonderte Behandlung dieses Systemanalyseaspekts rechtfertigt. Dies ist nach 5.4 vorzunehmen, was eine separate **Sicherheitsbeschreibung** nach sich zieht. Die Angemessenheit des Umfangs dieser Spezifikationen ist durch Verweis auf die Prüfliste in A.2 nachzuweisen.

Die System- und Sicherheitsbeschreibung dienen als Eingabe für den vierten Schritt und umfassen den Entwurf des digitalen Freimachungsvermerks selbst. Dies ist nach 5.5 durchzuführen und führt zu einer **technischen Beschreibung der digitalen Freimachungsvermerke**, die sowohl den Inhalt der Mitteilung, als auch die Kodierung sowie weitere Aspekte berücksichtigt, wie die Einbeziehung von Klartextangaben, die allgemeine Aufmachung, die Platzierung und den Druck. Die Angemessenheit des Umfangs dieser Spezifikationen ist durch Verweis auf die Prüfliste in A.4 nachzuweisen. In allen Phasen sollte eine enge Zusammenarbeit zwischen Kunden (Sender und Empfänger), den Anbietern technischer Lösungen, wie z. B. Lieferanten von Postfertigstellungs- und Postbearbeitungssystemen, und Postdienstleistern stattfinden.

Es wird betont, dass der Prozess eventuell wiederholt werden muss: es ist gut möglich, dass in späteren Phasen möglicherweise Probleme auftreten, die im Rahmen der in der (den) vorhergehenden Phase(n) erstellten Beschreibung(en) nicht zufrieden stellend gelöst werden können. In diesem Fall ist es nötig, zurückzugehen und den Prozess zu wiederholen, um diese Probleme zu lösen.

5.2 Unternehmensplanung digitaler Freimachungsvermerke

Unternehmensplanung ist die notwendige Vorstufe zur erfolgreichen Einführung von Inhalten digitaler Freimachungsvermerke. Der erste Schritt im Unternehmensplanungszyklus besteht darin, das Ziel festzulegen: was soll mit den Inhalten digitaler Freimachungsvermerke erreicht werden und in welchem Zusammenhang steht dies mit den allgemeinen Unternehmenszielen und -strategien? Sowohl kurzfristige als auch langfristige Gesichtspunkte sind zu berücksichtigen.

Anhang B enthält informative Richtlinien bezüglich der Hauptthemen, die angesprochen werden sollen. Der Kernpunkt ist die Festlegung, welche Anwendungen für welche Marktsegmente (siehe B.1) unterstützt werden sollen (siehe B.2). Diesbezügliche Entscheidungen werden von den Unternehmenszielen und -prioritäten des Postdienstleisters sowie von den Merkmalen des bestehenden Geschäfts, einschließlich der technischen Infrastruktur beeinflusst. B.3 enthält einleitende Bemerkungen zu den Überlegungen, die im Laufe des Auswahlprozesses voraussichtlich angestellt werden.

Die Ergebnisse dieser Planung sind so zu dokumentieren, dass sie die Grundlage für die Genehmigung durch das Management bilden und als Definition höherer Ebene dienen können, von der ausgehend genauere Anforderungsbeschreibungen und -entwürfe entwickelt werden können. Das Ergebnis des Unternehmensplanungsprozesses besteht also in einem oder mehreren Dokumenten, die zusammen die **Inhaltsbeschreibung** ausmachen. Diese stellen die Unternehmensanforderungen an die Inhalte digitaler Freimachungsvermerke ausreichend detailliert dar, um Rahmenbedingungen festzulegen, innerhalb derer der Systementwurf erstellt werden kann.

Die Beschreibungen umreißen den Anwendungsbereich der zu implementierenden Inhalte digitaler Freimachungsvermerke, definieren die zu erreichenden Ziele und die Vorgaben, innerhalb derer diese implementiert und betrieben werden sollen. Die Mittel zur Ausstattung der Inhalte und zur Erreichung der Ziele und der erwarteten Vorteile sollen ebenfalls enthalten sein.

Die nachstehende Liste definiert den minimalen empfohlenen Bereich für die Anwendungsbeschreibung, eine entsprechende Prüfliste findet sich in Anhang A. Anwendern der Norm bleibt es unbenommen, diesen Bereich auszuweiten und/oder ihn auf die von ihnen bevorzugte Dokumentationsstruktur anzuwenden, es muss jedoch sichergestellt sein, dass das Ergebnis mindestens die angegebenen Themen umfasst.

- a) **Unternehmensumfeld und -ziele:** eine Beschreibung des allgemeinen Kontexts, innerhalb dessen die Inhalte digitaler Freimachungsvermerke implementiert werden sollen;
- b) **Funktion von Inhalten digitaler Freimachungsvermerke:** eine Beschreibung, welche Inhalte digitaler Freimachungsvermerke unterstützt werden sollen, für welche Marktsegmente, einschließlich einer Angabe, wie sie zum Erreichen der allgemeinen Unternehmensziele beitragen sollen;
- c) **Beschreibung ausgewählter Inhalte:** Eine Beschreibung der ausgewählten Inhalte digitaler Freimachungsvermerke, die ausreichend genau sein sollte, um als Grundlage für eine System- und Sicherheitsanalyse und eine Gestaltung digitaler Freimachungsvermerke zu dienen. Dazu sollte zählen:
 - wie die Abrechnung vorgenommen und kontrolliert werden soll;
 - wie die Sendungen in das Postsystem eingeliefert werden sollen;
 - wie digitale Freimachungsvermerke bei der Postbearbeitung verwendet werden;
 - die Hauptschnittstellen zu anderen Postsystemen, einschließlich derer für Abrechnung, Ertragskontrolle, Zahlungsmanagement und Postbearbeitungsabläufen.
- d) **Beschränkungen hinsichtlich Infrastruktur und Design:** Eine Beschreibung der technischen Infrastrukturmerkmale, in welche die geplanten Inhalte digitaler Freimachungsvermerke zu integrieren sind, und wie sich diese dadurch voraussichtlich ändern werden, sowie eine Beschreibung der entstehenden Beschränkungen bei der Gestaltung und Implementierung digitaler Freimachungsvermerke;
- e) **Verfahrensweisen und Prioritäten bei der Implementierung:** Eine Beschreibung des Zusammenhangs der geplanten Inhalte digitaler Freimachungsvermerke mit anderen laufenden und geplanten Projekten;

- f) **betriebliche Auswirkungen:** Eine Analyse der zu erwartenden Auswirkungen für die beteiligten Parteien,
d. h. für Kunden (sowohl Versender als auch Empfänger), den Postdienstleister selbst und Dritte, einschließlich Postbearbeitungsorganisationen, Diensteanbieter sowie Anbieter von Postversandsystemen und -anlagen;
- g) **Ausführungsplan, einschließlich zeitliche Planung, Hilfsmittel und Investitionen:** Ein Plan mit einer Beschreibung, wie die Inhalte implementiert werden sollen, einschließlich einer Liste von Hauptmeilensteinen und der Ablaufplan einer Beschreibung der erforderlichen Ressourcen und der entstehenden Kosten;
- h) **Vorteile und Rechtfertigung der Kosten:** Eine Analyse der erwarteten quantitativen und qualitativen Vorteile, in welchem Verhältnis stehen diese zu den Kosten und wie hoch ist der erwartete Gewinn sowohl für den Postdienstleister und für die anderen betroffenen Parteien. Es sollte berücksichtigt werden, dass ein ausreichender Anreiz für alle Parteien vorhanden ist;
- i) **entscheidende Faktoren für den Erfolg:** Eine Beschreibung der zentralen Faktoren für den Erfolg der Einführung und des anschließenden Betriebs sowie der Maßnahmen, die zur Kontrolle dieser Faktoren zu ergreifen sind;
- j) **Managementkontrolle und -bewertung:** Eine Beschreibung, wie die Implementierung und der anschließende Betrieb verwaltet und geregelt werden. Dabei sollten insbesondere die Schlüsselfaktoren angesprochen werden und welche quantitativen Maßnahmen für eine Unterstützung der Managemententscheidungsprozesse zur Verfügung stehen müssen.

5.3 Systemanalyse für digitale Freimachungsvermerke

Die zweite Phase des Anwendungs- und Planungsprozess digitaler Freimachungsvermerke ist die Systemanalyse. Diese sollte parallel zur Entwicklung der Sicherheitsbeschreibung ausgeführt werden (siehe 5.4), da die beiden Sachverhalte eng miteinander verknüpft sind: zumindest bei Inhalten, die in Zusammenhang mit Zahlungsanwendungen stehen, entsprechen viele Funktionen denen der sicherheitstechnischen Gegenmaßnahmen.

Es sollte die normale Abfolge der Systemanalyse und Gestaltungsprozesse eingehalten werden, allerdings ist es möglicherweise notwendig, der zeitlichen Abstimmung von Entwicklung und Einführung besondere Beachtung zukommen zu lassen. Es könnte gut möglich sein, dass langfristige Ziele im Kontext der bestehenden postalischen Infrastruktur nicht auf wirtschaftliche Art und Weise verwirklicht werden können, also sollten die Implementierungsentwürfe und -pläne eine stufenweise Weiterentwicklung der Infrastruktur in Betracht ziehen.

Am Ende dieser Phase muss ein Kontrolldokument, die so genannte Systemspezifikation, vorliegen, das die zur Unterstützung der ausgewählten Inhalte digitaler Freimachungsvermerke erforderliche Systemarchitektur beschreibt und den Systementwurf ausreichend genau beschreibt, um Rahmenbedingungen für die Erstellung einer detaillierten Gestaltung von Inhalten digitaler Freimachungsvermerke zu schaffen. Die Systembeschreibung muss alle zum Erreichen der Unternehmensziele erforderlichen zu erfüllenden Systemanforderungen enthalten. Es müssen mindestens die folgenden Sachverhalte behandelt werden, von denen die meisten im informativen Anhang D ausführlicher erörtert sind:

- a) Bedarfsanalyse;
- b) Funktionsbeschreibung;
- c) Aufgabenzuweisung und Architekturplanung;
- d) Leistungskriterien;
- e) Systemarchitektur;
- f) Anwendungsprozesse;
- g) Erfordernis zur Dateneingabe;

- h) Datenquelle;
- i) Datenerfassung digitaler Freimachungsvermerke;
- j) Abtastverfahren;
- k) Fehlerbehandlung;
- l) infrastrukturelle Anforderungen und Beschränkungen.

5.4 Sicherheitsanalyse digitaler Freimachungsvermerke

Die dritte Phase des Gestaltungs- und Planungsprozesses der Inhalte digitaler Freimachungsvermerke ist die Ausarbeitung einer Sicherheitsbeschreibung. Diese sollte parallel zu der in 5.3 beschriebenen Systemanalyse stattfinden.

Sicherheitsanforderungen müssen in Zusammenhang mit den allgemeinen Unternehmenszielen definiert werden. Das Sicherheitssystem sollte auf diese Anforderungen zugeschnitten sein und dabei auch die rapide technische Entwicklung auf dem Gebiet der Informationssicherheit berücksichtigen. Der kosteneffektivste Sicherheits-systementwurf unterliegt mit großer Wahrscheinlichkeit den Einflüssen der vorhandenen postalischen Infrastruktur, der Bewertungsgrundlage des Postbearbeitungssystems, dem Wert der digitalen Freimachungsvermerke und dem kulturellen und rechtlichen Rahmen, innerhalb dessen die DPM-Anwendungen eingeführt werden sollen. Anhang C enthält einen informativen Leitfaden betreffend einiger zentraler zu berücksichtigender Punkte.

Das Ergebnis der Untersuchung muss in einer Sicherheitsbeschreibung dokumentiert werden. Diese sollte mindestens folgende Aspekte umfassen:

- a) **Sicherheitstechnische Ziele, Verfahren und ökonomische Aspekte**, die die Rahmenbedingungen für die Durchführung der Sicherheitsanalyse festlegen.
- b) **Bedrohungen und Schwachstellen** des Systems, besonders derer, die den Ertrag des Postdienstleisters gefährden.
- c) **Gegenmaßnahmen** zur möglichen Anwendung bei der Verhinderung von Angriffen auf das System, zur Unterstützung bei der Erkennung von Sicherheitslöchern und der Feststellung ihrer Herkunft sowie bei der Sammlung von Beweisen für Betrugsversuche;

ANMERKUNG Wie in C.4 erklärt, werden diese Gegenmaßnahmen in 2 Klassen eingeteilt: Zum Schutz der Sicherheit des digitalen Freimachungsvermerks selbst entworfene Sicherheitsfunktionen auf Mitteilungsebene und Gegenmaßnahmen auf der Inhaltsebene, die anwendungsspezifische Probleme betreffen.

- d) **Sicherheitsökonomische Aspekte und Auswahl von Gegenmaßnahmen**, Bestimmung und Rechtfertigung des zur Implementierung ausgewählten Pakets von Gegenmaßnahmen.
- e) **Anwendung von Gegenmaßnahmen**, zur Bestimmung wann, wo und wie die verschiedenen Gegenmaßnahmen angewendet werden sollen.
- f) **Implementierungsoptionen**, besonders für Sicherheitsfunktionen auf der Mitteilungsebene, wo es eine große Auswahl an anwendbaren Methoden und Verfahren gibt.

5.5 Gestaltung digitaler Freimachungsvermerke

Die letzte Phase beinhaltet die Gestaltung der digitalen Freimachungsvermerke selbst, einige Beispiele davon sind im (informativen) Anhang J enthalten. Bei der Gestaltung sind möglicherweise Kompromisse bei widersprüchlichen Erfordernissen zu machen. Etwaige Kompromisse sollten sowohl inhaltliche Erfordernisse als auch umwelt-technische Einschränkungen berücksichtigen. Die in der Inhaltsbeschreibung dokumentierten Unternehmensziele, die aus der Unternehmensplanung digitaler Freimachungsvermerke (siehe 5.2) hervorgehen, sollten während dieses Prozesses im Auge behalten werden.

ANMERKUNG Anhang E enthält eine informative Einführung einiger zentraler voraussichtlich auftretender Probleme. Dieser Abschnitt enthält keine Information zum Entwurf von zusätzlichen für die Implementierung von Inhalten digitaler Freimachungsvermerke erforderlichen Systemteilen, da diese nicht in den Bereich dieses Dokuments fallen.

Nach diesem Zyklus muss ein Kontrolldokument vorliegen, die so genannte **Spezifikation digitaler Freimachungsvermerke**, in der der digitale Freimachungsvermerk ausreichend detailliert beschrieben wird, damit die Anlage bzw. die Software von den jeweiligen Anwendern entwickelt werden kann. Sie sollte mindestens enthalten:

- a) Dateninhalt;
- b) Dateneintrag;
- c) Darstellung und Abbildung des Datenkonstrukts;
- d) Symbologie;
- e) Klartextinformationen;
- f) Layout, ansprechendes Erscheinungsbild und Anordnung;
- g) Leistungs- und Prüfkriterien.

Anhang A (normativ)

Spezifikations-Prüflisten

A.1 Beschreibung der Inhalte digitaler Freimachungsvermerke

Die folgende Themenliste muss zur Überprüfung verwendet werden, ob der Umfang der nach 5.2 entwickelten Beschreibung der Inhalte digitaler Freimachungsvermerke angemessen ist.

- a) wirtschaftliches Umfeld und Aspekte
- b) Funktion von Inhalten digitaler Freimachungsvermerke;
- c) Beschreibung ausgewählter Inhalte;
- d) Beschränkungen hinsichtlich Infrastruktur und Design;
- e) Verfahrensweisen und Prioritäten bei der Implementierung;
- f) betriebliche Auswirkungen: Kunden/Postdienstleister/Dritte;
- g) Implementierungsplan: Zeitplanung, Ressourcen, Investitionen;
- h) Vorteile und Rechtfertigung der Kosten;
- i) entscheidende Faktoren für den Erfolg;
- j) Managementkontrolle und -bewertung, Faktoren, quantitative Maße.

A.2 Systembeschreibung

Die folgende Themenliste muss zur Überprüfung verwendet werden, ob der Umfang der nach 5.3 entwickelten Systembeschreibung angemessen ist.

- a) Anforderungsanalyse
- b) Funktionsbeschreibung;
- c) Aufgabenzuweisung und Architekturplanung;
- d) Leistungskriterien;
- e) Systemarchitektur;
- f) Anwendungsprozesse;
- g) Erfordernis zur Dateneingabe;
- h) Datenquelle;
- i) Datenerfassung der Inhalte digitaler Freimachungsvermerke;
- j) Abtastverfahren;
- k) Fehlerbehandlung;
- l) infrastrukturelle Anforderungen und Beschränkungen.

A.3 Sicherheitsbeschreibung

Die folgende Themenliste muss zur Überprüfung verwendet werden, ob der Umfang der nach 5.4 entwickelten Sicherheitsbeschreibung angemessen ist.

- a) Sicherheitsaspekte, Regelungen und Wirtschaftlichkeit
- b) Bedrohungen und Schwachstellen;
- c) Analyse der Sicherheitsdienste auf Mitteilungsebene;
- d) Analyse der Gegenmaßnahmen auf Inhaltsebene;
- e) Auswahl von Gegenmaßnahmen;
- f) Anwendung von Gegenmaßnahmen;
- g) Implementierung der Sicherheitsdienste auf Mitteilungsebene.

A.4 Beschreibung digitaler Freimachungsvermerke

Die folgende Themenliste muss zur Überprüfung verwendet werden, ob der Umfang der nach 5.5 entwickelten Beschreibung digitaler Freimachungsvermerke angemessen ist.

- a) Dateninhalt;
- b) Dateneintrag;
- c) Darstellung und Datenkonstrukte;
- d) Symbologie;
- e) Klartextinformationen;
- f) Layout, gefälliges Aussehen und Anordnung;
- g) Leistungs- und Prüfkriterien.

Anhang B (informativ)

Überlegungen hinsichtlich der Unternehmensplanung

B.1 Mögliche Anwendungen

Ein digitaler Freimachungsvermerk enthält eine Mitteilung, die eigenständig oder in Verbindung mit anderen Mitteilungen bzw. gespeicherten Daten für eine oder mehrere Postsendungsaufdrucke verwendet werden kann. Digitale Freimachungsvermerke lassen sich zur Unterstützung einer breiten Palette von postalischen Anwendungen verwenden und bieten daher einen Mehrwert sowohl für den *Postdienstleister* als auch den Absender. Mit digitalen Freimachungsvermerken lässt sich zunächst das erhobene Porto prüfen (Zahlungsprüfung), was nachstehend vorausgesetzt wird, obgleich ähnliche Überlegungen für Inhalte digitaler Freimachungsvermerke gelten würden, die keine Portoprüfung beinhalten.

Mögliche Anwendungen sind mindestens:

- a) **Bei der Abrechnung des Absenderentgelts führt der Absender bzw. das vom Absender verwendete Gerät** die Entgeltabrechnungsfunktion aus, wobei mit Hilfe des digitalen Freimachungsvermerks der Nachweis einer Abrechnung erbracht wird. In diesem Fall soll dem Postdienstunternehmen ein Prüfmittel bereitgestellt werden, dass die von den Absendern erzeugten und auf Postsendungen aufgebrachten digitalen Freimachungsvermerke richtig abgerechnet wurden und den Sendungseigenschaften wie beispielsweise Dienstart, Größe und Gewicht entsprechen. Dies erfordert die Validierung der in dem digitalen Freimachungsvermerk sowie in allen anderen vom Absender erzeugten zugehörigen Abrechnungsmitteilungen enthaltenen Informationen. Dies impliziert die Feststellung des Absenders, die Festlegung der erforderlichen Dienste sowie die Erfassung ausreichender Sendungsattribute, um den Portowert zu überprüfen. Die Ergebnisse können dann mit den Abrechnungsunterlagen und den entsprechenden Zahlungen so in Wechselbeziehung gebracht werden, dass ein angemessener Grad der Postentgeltsicherung sichergestellt ist.
- b) Bei der **Entgeltabrechnung des Postdienstleisters** führt der Postdienstleister die entsprechenden Abrechnungsfunktionen durch und erstellt die Rechnungen für die bearbeiteten Postsendungen mit Hilfe der aus den digitalen Freimachungsvermerken bzw. der entsprechenden Mitteilungen gewonnenen Daten wie beispielsweise der Empfangskontrollunterlagen oder der Einlieferungslisten. In diesem Fall sollten Möglichkeiten geschaffen werden, dass der Absender die bei ihm eingehenden Rechnungen prüfen kann. Die (automatische) Rechnungserstellung bei Geschäftsantwortsendungen ist ein gutes Beispiel für diese Abrechnungsart. Normale (gewerblich erzeugte) Postsendungen könnten – falls so gewünscht – ebenfalls auf diese Art abgerechnet werden, auch wenn hierbei Sicherheitsfragen und andere Überlegungen anzustellen sind, die in dieser Norm nicht enthalten sind.
- c) **Abrechnung und Kontrolle von Geschäftsantworten:** Im Falle von Geschäftsantwortsendungen kann der digitale Freimachungsvermerk die Lizenznummer der Geschäftsantwort bzw. eine sonstige Kennung über die Herkunft der Sendung enthalten. Diese kann sowohl für eine Überprüfung der Bestimmungsadresse als auch zur Kontrolle von statistischen Erhebungen und zur Rechnungserstellung verwendet werden.
- d) **Dienstkennung,** bei welcher der digitale Freimachungsvermerk vom Postbearbeitungssystem zur Festlegung der Absendertiming-, Bearbeitungs- und Zustellanforderungen für eine Postsendung verwendet werden kann.
- e) **Messung der Dienstgüte,** bei welcher der digitale Freimachungsvermerk eine eindeutige Kennung für die Postsendung enthält, die dazu verwendet wird, die Nachverfolgungsdaten beim Durchlaufen der Postsendung durch den Postbearbeitungsprozess zu erfassen, um die bereitgestellte Dienstgüte zu messen. Die Kennung kann zusammen mit der tatsächlichen Datums-/Zeitangabe an unterschiedlichen Punkten des Postsendungsstroms gelesen werden. Diese Angaben lassen sich zur Bereitstellung von rechtzeitigen Berichten über die erreichte Dienstgüte im Vergleich zu den Normen verwenden. Ausgewählte Angaben können den Kunden gegebenenfalls zugänglich gemacht werden. Diese Anwendung könnte sich auf den Dateninhalt und die Gestaltung des digitalen Freimachungsvermerks auswirken. Sind beispielsweise getrennte Berichte für unterschiedliche Produkte und Dienste

erforderlich, so könnte es erforderlich sein, Service-Daten (siehe WPV-Norm S25 [5]) in den digitalen Freimachungsvermerk aufzunehmen. Sollen beispielsweise Leistungsdaten bis zum Zustellpunkt aufgezeichnet werden, ist ein Mittel zur Datenerfassung am Zustellpunkt erforderlich. Dies könnte sich auf die Symbolauswahl und den Entwurf des digitalen Freimachungsvermerks auswirken.

ANMERKUNG Viele Postdienststellen verwenden zu diesem Zweck wahrscheinlich postseitig aufgebrachte Kennungen, so genannte ID-Tags. Die Angaben können sich jedoch noch auf die kundenseitig aufgebrachten Kennungen beziehen, sofern die Verknüpfung zwischen dem ID-Tag und dem digitalen Freimachungsvermerk am selben Punkt des Postbearbeitungsprozesses protokolliert wird.

- f) **Grenzüberschreitende Bearbeitung**, bei der die Angabe auf dem digitalen Freimachungsvermerk von den *Postbearbeitungsorganisationen* gemeinsam mit dem Ziel genutzt wird, die Effizienz der Verarbeitung einer Postsendung zu erhöhen. So könnte der digitale Freimachungsvermerk beispielsweise die Kennung von besonderen Sendungen enthalten und Abrechnungsdaten über fällige Dienst- und Endgeräteentgelte liefern. Dazu müssen die WPV-Normen bei der Gestaltung von digitalen Freimachungsvermerken eingehalten werden.
- g) **Bearbeitung von Kundenanfragen**, bei der Kennung und Service-Daten im digitalen Freimachungsvermerk zur Unterstützung der Bereitstellung von Dienstangaben an den Absender verwendet werden. Als Beispiele hierfür wären zu nennen: Einlieferungsnachweis; Bericht über den aktuellen Standort einer Postsendung im Postbearbeitungsprozess (Nachverfolgen); Benachrichtigung über nicht zustellbare Sendungen; Bereitstellung von Zeit- und Zustellnachweisberichten usw.
- h) **Absenderdefinierte Inhalte**: Die Absender können ihre eigenen Inhalte festlegen, wie beispielsweise Vorklassifizierung von Antwortsendungen, durch Zuweisung bestimmter Angaben im Feld Kundendaten des digitalen Freimachungsvermerks. Es lassen sich drei Kategorien von absenderspezifischen Inhalten unterscheiden:
 - i) Absender an Post; dabei besteht zwischen Absender und Postdienstleister ein Vertrag zur Unterstützung einer spezifischen Anwendung;
 - ii) Absender an Empfänger; z. B. durch Verwendung der Daten im digitalen Freimachungsvermerk als Unterstützung der internen Sortierung beim Empfänger;
 - iii) Absender an sich selbst; für Geschäftsantworten oder im Falle einer Rücksendung nicht zustellbarer Sendungen.

Diese Inhalte werden von einem Datenfeld im digitalen Freimachungsvermerk unterstützt und können vom Absender verwendet werden: Das Feld „Customer Data Field“ (*Kundendatenfeld*). Der Absender legt die Anwendung und deren Dateninhalte fest. Die Daten im Kundendatenfeld werden im Allgemeinen vom Postsystem ignoriert, sofern keine spezifische gemeinsame Anwendung – wie in dem vorstehenden Fall (i) – vorliegt. Wird eine gemeinsame Anwendung festgelegt, sollte die Qualität der Quellenangabe im Kundendatenfeld kontrolliert werden.

B.2 Marktsegmentierung

B.2.1 Ansatz

Die Implementierung der Technologie digitaler Freimachungsvermerke sollte getrennt für jedes Marktsegment in Betracht gezogen werden. Diese Segmente werden im Allgemeinen durch Verweis auf die Absenderereigenschaften, durch das Verfahren der Posteinlieferung und die Zahlungsmittel festgelegt.

B.2.2 Absendersegmentierung

Eine Absendersegmentierung könnte auf folgenden Faktoren beruhen:

- a) Art der Absenderorganisation (risikobezogen);
- b) Postsendungsvolumen;
- c) zur Erzeugung der Postsendung verwendete Methode/Technologie: Erstellung, Zusammenstellung und Fertigstellung;

- d) dem Absender zur Verfügung stehende Informationsverarbeitungstools;
- e) Posteinlieferungs- und Annahmeverfahren.

Jedes Segment hat spezifische Bedürfnisse und Möglichkeiten. Eine mögliche Segmentierung aufgrund des von den Absendern bearbeiteten Postsendungsvolumens wird nachstehend vorgestellt, wobei die einzelnen Postdienstleister auch andere Parameter verwenden können:

- **Postzentrum:** Massenversender mit mehreren fest angestellten Beschäftigten und hoch spezialisierten Postbearbeitungssystemen. Die Postaktivitäten werden häufig auf interne Kostenzentren zurück verlagert;
- **Postraum:** Versender mit durchschnittlichem Sendungsvolumen mit fest angestellten Beschäftigten und spezialisierten Versendungsanlagen;
- **Poststelle:** Versender mit geringem Sendungsvolumen ohne fest angestellte Bediener und einer gemeinsam genutzten Versendungsanlage;
- **Desktop:** Im Allgemeinen ein einzelner Absender oder eine kleine Absendergruppe mit einem PC und einem Drucker, die Postsendungen mit Hilfe einer Standardbürosoftware oder einer Desktop Publishing-Software erstellen. Eine kleine Postversendungsanlage wie beispielsweise eine Frankiermaschine könnte dazu auch verwendet werden. Gruppen von PC-Anwendern innerhalb derselben Organisation könnten vernetzt werden.

B.2.3 Postzugang und Einlieferung

Die Inhalte digitaler Freimachungsvermerke müssen die vorhandenen Zugangsmethoden enthalten und den Absendern den Zugang zu den Postdiensten noch weiter erleichtern. Die vorhandenen Zugangsmethoden, die zu berücksichtigen sind, umfassen:

- a) **nicht kontrollierter Eingang — Sendungen aus Kastenleerung**, einschließlich:
 - i) über einen öffentlich zugänglichen Briefkasten/Straßenbriefkasten in den Sendungsstrom eingebrachte Postsendungen;
 - ii) Einzelhandelsstellen mit Selbstbedienung;
- b) **kontrollierter Eingang**, einschließlich:
 - i) Sendungen, die über einen Postschalterangestellten eingeliefert werden;
 - ii) Sendungen, die über einen kontrollierten Annahmepunkt angenommen werden;
 - iii) frankierte Sendungen aus Sonderbriefkästen;
 - iv) Sendungen, die in besonderen Taschen oder Umschlägen eingehen;
 - v) von den Absendern direkt abgeholte Sendungen.

Es wird betont, dass die Inhalte nicht unbedingt alle Zugangsmethoden behandeln müssen. Je nach den Prioritäten und Zielsetzungen des Postdienstleisters kann entschieden werden, digitale Freimachungsvermerke zunächst nur für eine Zugangsmethode zu implementieren. Der erste Vorstoß bezüglich digitaler Freimachungsvermerke⁵⁾ durch USPS war auf kleine und Heimanwender ausgerichtet, die in einer nicht kontrollierten Annahmumgebung arbeiten, wohingegen die Deutsche Post AG und Royal Mail⁶⁾ mit Versendern mit mittlerem und hohem Sendungsvolumen begannen, die bei kontrollierten Annahmebedingungen arbeiten, in denen Details der Aussendungen vor der Einlieferung elektronisch übermittelt werden.

5) Dies bezieht sich auf IBIP: Abkürzung für: Information-Based Indicum Programme (informationsbasiertes Freimachungsvermerkprogramm).

6) Dies bezieht sich auf REMPI: Abkürzung für: Re-Engineering the Mailer-Post Interface

B.2.4 Zahlungsweise

Unterschiedliche Zahlungsmethoden und Zahlungssysteme werden angewendet. Bei vielen handelt es sich um automatisierte computerbasierte Systeme und überwiegend werden Systeme verwendet, die eine Fernrücksetzung der zulässigen Posteinrichtungen oder -anlagen unterstützen. In solchen Fällen ist es zu Zwecken der Zahlungsvalidierung vorteilhaft, dass die von diesen computerisierten Zahlungssystemen erhältlichen Angaben zusammen mit den aus der Datenerfassung über die digitalen Freimachungsvermerke gewonnenen Angaben verwendet werden.

Was die Bezahlung angeht, sind drei Punkte zu berücksichtigen: Zahlungsablauf, -mittel und -kontrolle.

a) **Zahlungsablauf.** Kann beruhen auf:

- i) Vorauszahlung: Vor der Versendung geleistete Zahlung. Diese Methode gilt für einen vorzeitigen Erwerb und die Verwendung von Briefmarken und wird häufig für Frankiersysteme eingesetzt. Die geleisteten Zahlungen können – müssen jedoch nicht unbedingt – einer oder mehreren Einlieferungen von Postsendungen direkt entsprechen;
- ii) nachträgliche Zahlung: Nach dem Eingang von Postsendungen geleistete Zahlung. Rechnungen für spezifische Aussendungen, monatliche Zahlungsweisen und auf Zahlungsobergrenzen basierende Systeme sind gebräuchlich. Auch hier werden häufig Frankiergeräte für die Abrechnungs- und Gutschriftenkontrolle eingesetzt;
- iii) zeitgleiche Zahlung oder Zahlung bei Inanspruchnahme: Zahlung nach einer spezifischen Einlieferung von Postsendungen, die zum Zeitpunkt der oder unmittelbar vor der Aufgabe geleistet wird. Dies entspricht u. a. Zahlungen, die an einem Postschalter zum Zeitpunkt der Posteinlieferung geleistet werden.

b) **Zahlungsmittel.** Eine Reihe von Zahlungsmitteln sind längst erprobt; einige davon sind nachstehend aufgeführt:

- i) Bargeld: im Allgemeinen zur Bezahlung am Postschalter verwendet;
- ii) Scheck: im Allgemeinen über die Post geleistete Zahlung;
- iii) EFT Abk. für „Electronic Funds Transfer“ (elektronische Überweisung): elektronische Alternative zu einer Scheckzahlung;
- iv) Einzugsermächtigung: eine direkte Abbuchung vom Bankkonto eines Kunden mit dessen vorheriger Zustimmung. Im Allgemeinen wird eine Zahlungstransaktion elektronisch vorgenommen;
- v) Kreditkarten⁷⁾: wird eher von Kleinkunden akzeptiert, z. B. von SOHO (Small Office/Home Office)-Versendern.

c) **Zahlungskontrollen.** Bei dem Ansatz der Gültigkeitsprüfung von digitalen Freimachungsvermerken sollten die Abrechnungsmethode, einschließlich aller Guthabenbedingungen sowie die Datenkonsolidierung für das gekaufte oder erworbene Entgelt berücksichtigt werden. Zu den Kontrollmethoden zählen:

- i) Frankierung: Die Guthaben- und Verbrauchsobergrenzen werden von den Versandanlagen des Kunden kontrolliert. Die Frankierung könnte vor Ort oder ferngesteuert erfolgen;
- ii) kontrollierte Annahme: Durch die Annahmeverfahren wird sichergestellt, dass die Kunden zum Zeitpunkt der Sendungseinlieferung ihre Porto-Kontingente nicht überschreiten (bzw. eine angemessene Zahlung leisten).

7) Einschließlich Kredit- und Guthabekarten sowie elektronische Geldbörsen.

B.3 Auswahl der Inhalte

B.3.1 Ansatz

Für jeden Postdienstleister stellen die Prioritäten und die praktischen Einschränkungen die Kriterien dar, auf denen die Auswahl der Inhalte beruht. Für jeden vorgeschlagene Inhalt sollte ein systematischer Bewertungsprozess befolgt werden, wobei eine enge Zusammenarbeit zwischen den unterschiedlichen Parteien (intern und extern) für den Erfolg des Inhalts verantwortlich ist. Die Wahl zwischen zwei möglichen Optionen kann sich an den traditionellen Entscheidungsfindungsprozessen⁸⁾ orientieren. Die relative Bedeutung der verschiedenen Kriterien sollte dabei berücksichtigt werden.

Einer der ausschlaggebenden Faktoren bezieht sich wahrscheinlich auf die Tatsache, dass sich die unterschiedlichen Inhalte unterschiedlich auf die Bearbeitung und Infrastruktur auswirken.

B.3.2 Infrastrukturelle Anforderungen und Beschränkungen

Die Postdienstleister leisten stets einen erheblichen Investitionsaufwand in die Infrastruktur ihrer automatischen Bearbeitungsanlagen. Die Möglichkeiten und die Leistung dieser Infrastruktur sind von einem Betreiber zum anderen unterschiedlich. Auch der Grad der Automatisierung könnte sich geografisch gesehen für die einzelnen Betreiber unterscheiden.

Die Zielsetzung von Inhalten digitaler Freimachungsvermerke ist möglicherweise innerhalb der Beschränkungen der vorhandenen postalischen Infrastruktur nicht immer zu verwirklichen und Kompromisse zwischen den Anwendungszielen und den erforderlichen Investitionen in die Infrastrukturverbesserungen müssen möglicherweise eingegangen werden. Pläne zur Änderung oder Aufrüstung der technischen Infrastruktur stellen stets einen bedeutsamen Faktor bei der Implementierung der meisten Inhalte digitaler Freimachungsvermerke dar.

Die zur Realisierung einer notwendigen Änderung der postalischen Infrastruktur erforderlichen finanziellen und personellen Ressourcen sollten vor der Erstellung des Geschäftsplanungszyklus erfasst und genehmigt werden. Die Anwendung eines phasenweisen Ansatzes kann möglicherweise wünschenswert sein, mit dem die rasche Implementierung von eingeschränkten und später erweiterbaren Inhalten ermöglicht wird, damit die angestrebten Inhalte vollständig unterstützt werden. So könnte es beispielsweise sinnvoll sein, einige Anwendungen durch die Verwendung von tragbaren oder Handheld-Scannern zu unterstützen, um die Inhalte digitaler Freimachungsvermerke lediglich von ausgewählten Stichproben von Postsendungen zu erfassen und andere Anwendungen so lange aufzuschieben, bis ein vollständiges Online-Lesen von digitalen Freimachungsvermerken unterstützt wird.

In jedem Fall sollte die Kluft zwischen dem, was zur Datenerfassung und Datenverarbeitung erforderlich ist, und den gegenwärtigen Möglichkeiten festgelegt und der Ansatz für eine Lösung dieser Unterschiede definiert werden.

- a) Datenquelle: Wie bereits in D.4.2 angesprochen, können die für die Inhalte digitaler Freimachungsvermerke erforderlichen Daten von verschiedenen Quellen stammen, von denen der digitale Freimachungsvermerk lediglich eine ist. Weitere wichtige Quellen sind Datenbanken, Online-Mitteilungen vom Kunden, Sendungsattributangaben und Prozessdaten aus der Verarbeitung von Postsendungen. Woher die Daten auch stammen, es könnte immer zu Implikationen auf die Postbearbeitungsinfrastruktur führen:
 - i) **digitaler Freimachungsvermerk:** beeinflusst den Bedarf an entsprechenden Datenerfassungsgeräten, insbesondere dort, wo Daten auf Postsendungen mit digitalen Freimachungsvermerken zu erfassen sind;
 - ii) **Datenbanken:** Der Zugang zu den postalischen Datenbanken setzt das Vorliegen einer geeigneten Infrastruktur voraus, die in der Lage ist, die Daten bereitzustellen und auf diese zuzugreifen, die für die Inhaltsprozesse digitaler Freimachungsvermerke innerhalb des erforderlichen Zeitrahmens benötigt werden;

8) So kann beispielsweise eine klar definierte Option als Verweis verwendet werden, wobei die Optionen durch einen entsprechenden Vergleich mit diesem Verweis bewertet werden können. Der Vergleich kann entweder subjektiv und qualitativ sein (gleich, besser oder schlechter) oder muss u. U. objektiv und quantitativ sein, abhängig von der Bedeutung des betrachteten Faktors.

- iii) **Online-Mitteilungen:** Die Gewinnung von Daten aus Versender/Post-Schnittstellenmitteilungen setzt das Vorhandensein von entsprechenden elektronischen Datenaustausch- und Weiterleitungs- und -speicherfunktionen für Mitteilungen voraus;
 - iv) **Sendungsattribute:** was die Erfassung von Daten aus den digitalen Freimachungsvermerken betrifft, so setzt die Erfassung anderer Postsendungsattribute wie beispielsweise der Zieladresse, der Sendungsabmessungen oder des Sendungsgewichts voraus, dass entsprechende Datenerfassungs-einrichtungen vorhanden sind;
 - v) **Prozessdaten:** ein Zugriff auf frühere Ergebnisse der Bearbeitung einer bestimmten Postsendung erfordert (a), dass die Sendung eine frei zugängliche Kennung trägt, wie beispielsweise ein ID-Tag und (b), dass eine integrierte Bearbeitungsinfrastruktur vorliegt, die in der Lage ist, die erforderlichen Daten innerhalb des erforderlichen Zeitrahmens bereitzustellen.
- b) **Datenerfassung der Inhalte digitaler Freimachungsvermerke:** Eine Datenerfassung kann während des gesamten Postbearbeitungssystems von der Einlieferung bis zur Zustellung erforderlich sein. Der Punkt und die Häufigkeit der Datenerfassung hängen vom erforderlichen Validierungsgrad sowie der Service- und Managementkontrolle ab. Daten lassen sich entweder mit Hilfe der verfügbaren automatischen Postbearbeitungsgeräte (dafür kann eine Aufrüstung sowohl der Hardware als auch der Software erforderlich sein) oder mit so genannten Handhelds bzw. tragbaren Geräten erfassen.
- c) **Datenverarbeitung:** Die Datenverarbeitung lässt sich online oder offline sowie entweder lokal oder zentral ausführen. Die lokale Verarbeitung hat möglicherweise den Vorteil schnellerer Antwortzeiten, während eine zentrale Verarbeitung die Datenkorrelation und Datenkonsolidierung vereinfachen könnte, beispielsweise um eine Datenkorrelation von Inhalten digitaler Freimachungsvermerke, Rücksetzungsdaten und statistischen Daten zu ermöglichen. Lokale und zentrale Datenverarbeitungssysteme verfügen außerdem über unterschiedliche Managementeigenschaften; zentrale Systeme lassen sich leichter kontrollieren als lokale oder dezentrale Systeme. Selbstverständlich können auch Hybridlösungen verwendet werden, bei denen einige Daten lokal und andere wiederum zentral verarbeitet werden. So könnte beispielsweise die Gültigkeit der Inhalte digitaler Freimachungsvermerke lokal in Echtzeit geprüft werden, während gleichzeitig ein doppeltes Auftreten zentral auf Zustellungsbasis festgestellt wird. Durch die getroffene Auswahl werden die Kommunikationsanfordernisse erheblich beeinflusst und der mögliche Aktualisierungsbedarf der Fernmeldeinfrastruktur sollte ebenfalls in Betracht gezogen werden.

Die Entscheidung zur Verarbeitung der Daten auf Online- oder Offlinebasis hängt von der verfügbaren Verarbeitungsleistung, den Ablaufferfordernissen sowie dem Zeitaufwand ab. In diesem Zusammenhang ist es sinnvoll, die Ablaufferfordernisse in Relation zu drei unterschiedlichen Zeitintervallen zu setzen: Zustellung in Echtzeit, zurückgestellte Zustellung und nachträgliche Zustellung:

- i) **Verarbeitung in Echtzeit:** bei der die Reaktionszeit schnell genug ist, um den Betrieb des laufenden Postbearbeitungsprozesses zu beeinflussen, beispielsweise durch Beeinflussung der Auswahl des Sortierbehälters während des Durchlaufens einer Postsendung einer Sortiermaschine.
- ii) **Zurückgestellte Verarbeitung:** bei der die Reaktionszeit schnell genug ist, um den Betrieb eines späteren Postbearbeitungsschrittes zu beeinflussen – beispielsweise durch Verwendung der während der Abgangssortierung einer Postsendung erfassten Angaben, um diese während der Eingangssortierung oder der Zustellfolge abzufangen.
- iii) **Nachträgliche Zustellung:** wo das Ergebnis der Bearbeitung von Informationen, die von einer Postsendung erfasst wurden, erst vorliegt, nachdem die Sendung sich außerhalb der Kontrolle des Postsystems befindet. Diese Informationen lassen sich zu statistischen Zwecken, zur Einleitung von Untersuchungsmaßnahmen oder zur Beeinflussung der Bearbeitung der nachfolgenden Postsendungen von derselben Quelle verwenden. Die Bearbeitungsergebnisse einer nachträglichen Zustellung können auch dazu verwendet werden, um über das Zeitintervall zu entscheiden, welches für die Bearbeitung zukünftiger Aussendungen verwendet wird, beispielsweise zur Kennzeichnung einer verdächtigen Sendung und zur Durchführung einer Bearbeitung der ausgewählten Sendung in Echtzeit.

B.3.3 Sonstige Faktoren

Die Auswahl der Inhalte könnte auch von anderen Faktoren beeinflusst werden, einschließlich der Antworten auf die folgenden Fragen:

- a) **Ziele/Prioritäten:** worauf ist die Aufmerksamkeit zu richten: Verbesserung oder Bereitstellung neuer Dienste und Produkte; leichter Kundenzugang zu Postdiensten und -produkten; Verbesserung der Managementinformationen oder Bereitstellung einer verbesserten Postentgeltsicherung?
- b) **Kundeneinfluss und Annahme:** welche Auswirkungen haben die vorgeschlagenen Inhalte auf die Kunden, welche Kosten entstehen und welcher Nutzen lässt sich daraus ziehen? Besteht für die Kunden die Notwendigkeit, ihre Betriebsabläufe umzustellen oder neue Technologien einzuführen? Wie lange wird dies in Anspruch nehmen und welche Anreize sind zur Beschleunigung des Prozesses erforderlich?
- c) **Rechtliche Fragen:** werden die Vorschläge vom Gesetz beeinflusst hinsichtlich des Datenschutzes und der Verwendung von Verschlüsselungstechnologien, gibt es Beschränkungen durch Freihandelsbestimmungen oder durch die Bestimmungen eines etwaigen vorbehaltenen Bereichsmonopols?
- d) **Rechtsfragen zum geistigen Eigentum Dritter:** sind die vorgeschlagenen Inhalte und Entwürfe abhängig von der Verwendung des geistigen Eigentums Dritter, was sind die diesbezüglichen Auswirkungen auf mögliche Anbieter von Zubehör und Technologie und welchen Grundsätzen folgt die Organisation bezüglich Lizenzierung oder wird die Verwendung geistigen Eigentums Dritter vermieden?
- e) **Auswirkungen auf die Organisation:** welche Auswirkungen haben die vorgeschlagenen Anwendungen auf die Organisation des Postdienstleisters und auf die Rolle und den Verantwortungsbereich verschiedener organisatorischer Funktionen, einschließlich der entsprechenden technologischen Voraussetzungen, Datenerfassung und -verarbeitung, Sicherheit, Prüfung/Untersuchung, betriebliches Management, Qualitätskontrolle usw.?
- f) **Investitionen und Finanzierung:** welche Investitionen von welchen Parteien und in welchem Zeitraum sind erforderlich, wie hoch ist der erwartete Ertrag und wie lassen sich Investitionen finanzieren?
- g) **Stand der Technik und Standards:** wie robust sind die vorgesehenen Technologien, wurden sie schon anderweitig vollständig erprobt und können die Entwicklungen auf der Basis weithin akzeptierter Standards durchgeführt werden?
- h) **Zeitliche Planung:** wie lange wird es dauern, die vorgeschlagenen Inhalte einzuführen und ihr gesamtes Potential auszunutzen; wie passt dies zu den Marktanforderungen?
- i) **Konkurrenzfähigkeit:** welche Auswirkungen haben mögliche Anwendungen auf die Wettbewerbsfähigkeit des Postdienstleisters?

Anhang C (informativ)

Überlegungen hinsichtlich der Sicherheitsanalyse

C.1 Kontext

Jedes System hat Schwachstellen, die es möglicherweise anfällig für Störungen – gleichgültig, ob zufällig oder konstruktionsbedingt – oder Missbrauch machen. Eine solche Störung bzw. ein solcher Missbrauch kann, wenn sie/er in der Praxis eintritt, schädliche wirtschaftliche oder betriebliche Auswirkungen oder Folgen für die Sicherheit des Menschen nach sich ziehen. Böswillige Parteien können versuchen, diese Folgen durch Angriffe auf das System herbeizuführen.

Die Sicherheitsanalyse befasst sich mit der Feststellung der Schwachstellen des Systems, den potentiellen Bedrohungen oder Angriffsmethoden, die möglicherweise verwendet werden können, sowie mit den Maßnahmen, die ergriffen werden können, um einen Schutz gegen solche Bedrohungen zu bieten und die Folgen jeder dennoch eintretenden Störung oder jeden Falls des Missbrauchs zu reduzieren.

Dieser informative Anhang soll dem Leser als Richtlinie über die Sicherheitsanalyse für Anwendungssysteme digitaler Freimachungsvermerke dienen. Er beschreibt das Erfordernis, dies in den Kontext einer Sicherheitsstrategie zu stellen (C.2), stellt einige der möglicherweise zu berücksichtigenden Bedrohungen und Schwachstellen heraus (C.3), legt unterschiedliche Ebenen fest, auf denen Schutzmaßnahmen (Gegenmaßnahmen) getroffen werden können (C.4), enthält einige der spezifischen Gegenmaßnahmen, die wahrscheinlich zu treffen sind (C.5 und C.6), erörtert die Auswahl der zu treffenden Gegenmaßnahmen (C.7), geht auf das Ausmaß ein, bis zu dem die ausgewählten Gegenmaßnahmen angewendet werden sollten (C.8), und stellt eine Richtlinie über die Optionen zu Implementierung der Sicherheit auf Mitteilungsebene bereit (C.9).

Die grundsätzliche Sicherheitsanforderung sieht vor, dass die Inhalte digitaler Freimachungsvermerke unter Berücksichtigung der als Folge dieser Analyse ausgewählten Sicherheitsmaßnahmen

- die Postentgelte genau abrechnen,
- sämtliche Informationen bereitstellen, die zu Prüfung der Portozahlung erforderlich sind,
- Angriffe auf das System abschrecken, indem sie diesen entgegenwirken, sie für Betrugsversuche höchst riskant bzw. wirtschaftlich unrentabel machen,
- versuchten oder tatsächlichen Postbetrug aufdecken, die Betrüger namentlich machen und die Sammlung von gesetzlich zulässigen Nachweisen zur Verwendung bei der Strafverfolgung unterstützen.

Es wird hervorgehoben, dass es sich bei der Sicherheit um ein wirtschaftliches und betriebliches Thema handelt: Kein Sicherheitssystem kann das Vorkommen von Fehlern oder Systemangriffe verhindern und es ist unmöglich, die Wahrscheinlichkeit solcher Fehler oder Angriffe mit der Folge einer Störung auszuschließen. Durch eine erhöhte Sicherheit lässt sich jedoch das Vorkommen von Fehlern und Angriffen reduzieren und die negativen Folgen ihres Auftretens vermeiden oder mindern. Dies lässt sich jedoch nur auf Kosten einer erhöhten Systemkomplexität sowie eines verminderten Betriebskomforts erreichen, was beides wirtschaftliche Kosten nach sich zieht, die gegenüber den Vorteilen abzuwägen sind. Die Aufgabe der Sicherheitsanalyse besteht demzufolge in der Anzahl von Gegenmaßnahmen, die zu einem optimalen Systemschutz führt. Idealerweise sollte das Ergebnis der Anwendung dieser Gegenmaßnahmen so sein, dass

- keine Partei einen Nutzen aus einem erfolgreichen Angriff auf das System ziehen können sollte, ohne zusätzlichen Zeit- und Ressourcenaufwand, um einen Angriff zu starten, der im Vergleich zu den erzielten Vorteilen unverhältnismäßig groß ist,

ANMERKUNG 1 Der Begriff Nutzen wird hier im weitest möglichen Sinn und nicht im rein wirtschaftlichen Sinn verwendet: böswillige Parteien können davon profitieren, indem sie Unterbrechungen herbeiführen und dem Systembetreiber oder den Nutzern einen wirtschaftlichen Schaden beifügen, ohne dabei unbedingt einen direkten wirtschaftlichen Nutzen für sich selbst daraus zu ziehen. Angriffe zur 'Verweigerung der Rechenleistung' im Internetbetrieb stellen ein Beispiel hierfür dar.

- für einen Angreifer – gleichgültig ob erfolgreich oder nicht – sollte ein hohes Abschreckungspotential in Relation zu dem aus einem erfolgreichen Angriff zu erwartenden Nutzen vorliegen,

ANMERKUNG 2 Selbst wenn der erste vorstehende Punkt richtig ist, sind sich potentielle Angreifer möglicherweise nicht bewusst, dass der Aufwand für einen Erfolg den zu erwartenden Nutzen übersteigt bzw. sich einfach auf ihr Glück verlassen (wie bei der Teilnahme an Lotterien). Maßnahmen zur Feststellung solcher Angreifer, so dass andere (systemexterne) Mittel verwendet werden können, damit diese keine weiteren Angriffe starten können, sind deshalb wünschenswert.

- das Sicherheitsniveau sollte in dem Sinne optimal sein, dass die wirtschaftlichen und operationalen Kosten einer erhöhten Sicherheit höher sein sollten als die möglichen Vorteile, die durch die entstehende geringere Anfälligkeit des Systems erreicht werden, während die Einsparungen durch weniger Sicherheit geringer sein sollten als die möglichen Kosten für die daraus resultierende höhere Anfälligkeit des Systems.

C.2 Sicherheitstechnische Ziele, Verfahren und ökonomische Aspekte

Jede sicherheitstechnische Überlegung sollte im Kontext der gesamten Sicherheitsstrategie gesehen werden und die zutreffenden Ziele und Beschränkungen definieren. Die zu berücksichtigenden Themen umfassen:

- a) Unternehmensziele: die Absicherung zielt auf einen kostengünstigen Schutz des Systems gegen feindliche Angriffe und/oder unvorhergesehene Fehler ab, aber dieses Ziel kann auf verschiedene Art und Weise verfolgt werden: besteht das Ziel beispielsweise darin, durch Betrug und Fehler entstehende Verluste einfach zu minimieren oder muss auch die Auswirkung der Sicherheitsmaßnahmen auf die Anwendung des Dienstes sowie Erträge berücksichtigt werden?

ANMERKUNG 1 Manche Maßnahmen können – was die Sicherheit anbetrifft – sehr effektiv sein, allerdings zu Lasten des Geschäfts, das das Sicherheitssystem schützen soll. Die Überprüfung handschriftlicher Signaturen, zum Beispiel, wird in einem Umfeld mit persönlichem Kontakt zum Kunden traditionell zur Bestätigung von Zahlungsvorgängen. Allerdings haben Untersuchungen gezeigt, dass eine strenge Signaturenüberprüfung am Verkaufsort, zumindest im Falle von Zahlungsvorgängen mit Kreditkarte, die Anzahl der eindeutig gültigen Zahlungsvorgänge um 24 % reduzieren könnte.

- b) Sicherheitspolitik: es ist nicht praktikabel, jede Möglichkeit eines Angriffs auszuschließen, also sollte sich die Sicherheitspolitik darauf konzentrieren, welches Maß an Sicherheit um welchen Preis erreicht werden soll. Es müssen hierbei klare Richtlinien erstellt werden: wie wichtig ist Vorbeugung im Vergleich zur Erkennung, liegt der Schwerpunkt bei der Abschreckung auf der Erhöhung der Kosten, die für einen Angriff aufgewendet werden müssen, oder auf der Erhöhung der Kosten und der Wahrscheinlichkeit, gefasst zu werden?
- c) Wirtschaftliche Aspekte: das wirtschaftliche Gesamtziel der Sicherheitsanalyse ist die Minimierung der möglichen Schwachstellen des Systems im Rahmen annehmbarer Kompromisse, was Kosten/Nutzen und Qualität anbelangt. Die Herangehensweise zielt nicht darauf ab, die Möglichkeit eines Fehlers oder eines Angriffs gänzlich auszuschließen, sondern die Fehlerwahrscheinlichkeit zu minimieren und dafür zu sorgen, dass sich Angriffe nicht lohnen. Wenn beispielsweise der für den Angriff nötige Aufwand für den Eindringling bedeutend höher ist als der mögliche Gewinn, dann lohnt es sich nicht, in das System einzudringen. Umgekehrt ist es wahrscheinlich wirtschaftlich nicht lohnenswert, eine bestimmte Gegenmaßnahme oder Sicherheitstechnik zu implementieren, wenn die Kosten dafür hoch sind und nur geringer Schaden entstehen kann, wenn diese nicht vorhanden ist. Gleichzeitig sollten die Auswirkungen eines bestimmten Sicherheitssystems in betrieblicher Hinsicht und im Hinblick auf den Markt berücksichtigt werden. Das im Hinblick auf seine direkte Auswirkung optimale Sicherheitsniveau könnte möglicherweise alles andere als optimal aus gesamtbetriebswirtschaftlicher Sicht sein. Wenn die Sicherheitsmaßnahmen zu streng sind, kann das den Ablauf für die Kunden derart erschweren, dass sie zu einem anderen Anbieter abwandern, werden die Sicherheitsmaßnahmen als zu locker wahrgenommen, sind die Kunden möglicherweise misstrauisch und wandern ebenfalls zu einem anderen Anbieter ab.

ANMERKUNG 2 Beachten Sie, dass die Art und Weise, wie etwas wahrgenommen wird, so wichtig sein kann wie die Realität. Benutzer in einer Internetumgebung vermeiden es, Geschäftsvorgänge über eine Seite abzuwickeln, die den Ruf hat, unsicher zu sein, ganz egal, ob dieser Ruf gerechtfertigt ist oder nicht. Man kann sich leicht vorstellen, welche Auswirkungen auch nur ein weithin veröffentlichter Bericht darüber, „wie ich es geschafft habe, 1 000 Postsendungen zu verschicken, ohne dafür zu bezahlen“ in einer auf der Verwendung digitaler Freimachungsvermerke basierenden Postumgebung hat.

- d) **Architektur:** Sicherheitsmaßnahmen sind dann am effektivsten, wenn sie von vornherein für ein bestimmtes System entworfen werden. Mit anderen Worten, wenn ein Sicherheitsplan auf ein fertig entworfenen System angewendet wird, so führt dies im Allgemeinen zu einer geringeren Effektivität im Sicherheitsbereich. Des Weiteren ist es, wenn man die Sicherheit beim Erstentwurf des Systems mit einbezieht, aus wirtschaftlicher Sicht meistens am besten, eine Sicherheitsgrenze innerhalb des Gesamtsystems festzulegen und alle Sicherheitstechniken innerhalb dieser Grenze einzubinden. Beispielsweise können die physikalischen Mittel (wie z. B. Schutz gegen Manipulationen und/oder Mechanismen zur Erkennung von Manipulationen), die erforderlich sind, um der Gefahr eines physikalischen Eindringens in das System entgegenzuwirken, kostengünstiger gestaltet werden, wenn sie nur auf eine genau bestimmte eingeschränkte Menge von Systemelementen angewendet werden (d. h. auf diejenigen innerhalb der Grenze) und nicht auf das gesamte System. Außerdem spielt die Systemarchitektur eine Rolle, wenn es darum geht, welche Sicherheitstechniken erforderlich sind. Die in Anhang I beschriebenen Beispielarchitekturen stellen beispielsweise unterschiedliche architekturabhängige Sicherheitsanforderungen. In der REMPI (I.2) und der USPS-Konfiguration A (I.3.3) Architektur wird ein Sicherheitsmodul (PSD, postal security device) beim Kunden deponiert. Dies ist nicht der Fall bei der USPS-Konfiguration B (I.3.4), aus der sich andere Sicherheitsanforderungen ergeben.
- e) **Infrastrukturelle Beschränkungen:** welche Beschränkungen ergeben sich aus der vorhandenen Infrastruktur und den Möglichkeiten des Postdienstleisters, diese weiterzuentwickeln und zu erweitern? Zum Beispiel:
 - i) Sind die automatischen Postbearbeitungsgeräte in der Lage, die digitale Freimachungsvermerke betreffenden Daten online zu erfassen (oder können sie aufgerüstet werden, so dass sie diese erfassen können)?
 - ii) Gibt es betriebliche oder zeitliche Bedingungen für den Zugriff auf Daten in firmeninternen Datenbanken oder in Postbearbeitungssystemen?
 - iii) In welchem Maße unterstützt die bestehende Infrastruktur den elektronischen Datenaustausch mit den Kunden?
- f) **Rechtliche Rahmenbedingungen:** die gesetzlichen Rahmenbedingungen haben möglicherweise beträchtlichen Einfluss auf die Sicherheitsmaßnahmen, die verwendet werden können. Von besonderer Wichtigkeit sind vor allem Datenschutzanforderungen und die vertrauliche Behandlung von Daten, rechtliche Beschränkungen bei der Verwendung und/oder beim Export von Verschlüsselungssystemen und die rechtlichen Möglichkeiten, Regressansprüche gegenüber Tätern bei Betrug mit Postwertzeichen geltend zu machen. In manchen Ländern sind solche Entschädigungsmöglichkeiten begrenzt und der abschreckende Effekt, zur Verantwortung gezogen zu werden, kann dementsprechend geringer sein.

C.3 Bedrohungen und Schwachstellen

C.3.1 Einleitung

Bedrohungen umfassen alle Methoden, mit denen ein Angriff auf ein System in der Absicht, dem System selbst, seinen Betreibern oder seinen Benutzern Schaden zuzufügen, möglich ist. Bei tatsächlichen Angriffen könnten mehrere solcher Methoden kombiniert werden. Der verursachte Schaden muss nicht direkt finanziell messbar sein (d. h., er muss nicht unbedingt zu Umsatzbußen auf Seiten des Postdienstleisters führen) und für den Angreifer muss dabei kein direkter Vorteil entstehen. Schaden kann auch eintreten durch verminderte Produktivität, durch Geschäftsrückgang aufgrund von fehlendem Kundenvertrauen und durch die gesetzliche Haftpflicht für Schäden, die Kunden, Lieferanten oder Dritten entstehen. So könnte beispielsweise jemand, der sich eigentlich vertrauliche Informationen verschafft und offen legt das System in Verruf bringen, was eher zu indirektem Geschäftsverlust führen würden, als dass es dem Systembetreiber oder dem Eigentümer der betroffenen Informationen unmittelbaren Schaden zufügen würde.

Im Allgemeinen zielen Bedrohungen darauf ab, Schwachstellen oder Anfälligkeiten im System auszunutzen. Solche Schwachstellen können auch dazu führen, dass Schaden durch versehentliche Fehler entsteht.

Der erste Schritt jeder Analyse der Systemsicherheit ist die Erkennung und Bewertung potentieller Bedrohungen des Systems und seiner Anfälligkeiten. Im Verlauf dieses Verfahrens kann es dienlich sein zu berücksichtigen, dass es eine Vielzahl von Möglichkeiten gibt, wie Bedrohungen aus verschiedenen Anfälligkeiten und aufgrund einer Reihe von Ursachen entstehen können. Zu den möglichen Ursachen gehören:

- a) unlautere Systembenutzer mit einer Neigung zu Betrugsversuchen;
- b) unlautere Lieferanten, die ihnen bekannte Anfälligkeiten des Systems zu ihrem Vorteil ausnutzen;
- c) verärgerte oder unlautere Angestellte des Postdienstleisters, die ihre Systemzugangsprivilegien ausnutzen können;
- d) unbeteiligte Dritte (z. B. Netzwerk-Hacker bei einer netzwerkbasierter Architektur).

Für jede erkannte Bedrohung oder Kombination von Bedrohungen ist eine Bewertung vorzunehmen betreffend:

- a) die Relevanz der Bedrohung im Kontext des jeweiligen in der Entwicklung befindlichen Systems für digitale Freimachungsvermerke;
- b) die Anfälligkeiten des Systems hinsichtlich der besagten Bedrohung oder der Kombination von Bedrohungen (wie groß ist die Wahrscheinlichkeit, dass ein Schaden eintritt);
- c) das Ausmaß des wahrscheinlichen Schadens und
- d) die Notwendigkeit, Gegenmaßnahmen zu ergreifen (siehe C.4 bis C.8).

C.3.2 Umgebungskontext

Die Frage nach dem Kontext ist von besonderer Wichtigkeit. Im Wesentlichen bezieht sich die Analyse von Bedrohungen in einem Portoentgeltzahlungen betreffenden Kontext auf die Erkennung aller Angriffsmöglichkeiten jeder Stufe oder jeder Verknüpfung im Zahlungsprozess und auf die Analyse der geschäftlichen Konsequenzen solcher Attacken. Zu den grundlegenden Punkten dieser Analyse gehören die Frage nach der Haftung im Falle eines Sicherheitsverstößes und die Frage, wer die Kosten für die Bereitstellung der notwendigen Sicherheitsmaßnahmen trägt. Diese Fragen können nur im Zusammenhang des jeweiligen Geschäftsmodells, in dem die betriebliche Verantwortung und die unternehmerische Haftung festgelegt sind, angesprochen werden. So trägt in einigen Fällen möglicherweise der Anbieter des Geräts zum Erzeugen digitaler Freimachungsvermerke die Verantwortung für die Überprüfung und übernimmt die Haftung für die Folgen von Fehlern in diesem Prozess, in anderen Fällen trägt möglicherweise der Postdienstleister die Verantwortung und muss deshalb selbst Maßnahmen zum Schutz gegen Betrugsversuche ergreifen.

Bei der Analyse muss außerdem die Umgebung berücksichtigt werden, die aus der vorgeschlagenen Systemarchitektur entsteht. Dies beinhaltet fast sicher einige Komponenten, die unter der direkten physikalischen Kontrolle des Postdienstleisters stehen; andere, die der Kontrolle der Lieferanten und Unterauftragnehmer unterliegen, sowie wiederum andere, die vom Anwender kontrolliert werden. Bedrohungen, die mit Anlagen- oder Systemkomponenten zusammenhängen, welche sich am Standort des Absenders befinden (bzw. an einem anderen nicht von einer vertrauenswürdigen Partei kontrollierten Standort) erwecken besondere Besorgnis, weil solche Anlagen sich in einer Umgebung befinden, zu der ein Angreifer im Wesentlichen ungehinderten Zugang hat. Besondere Sorgfalt ist erforderlich, wenn die betreffenden Anlagen von Dritten geliefert werden und Genehmigungsverfahren durch den Postdienstleister unterliegen, wie in WPV-Norm S30 beschrieben. Bei Inhalten digitaler Freimachungsvermerke ist dies sehr wahrscheinlich der Fall für Druckgeräte und die Sicherheitsanalyse sollte diesen Geräten und deren Schnittstelle zu Abrechnungssystemen und kryptografischen Untersystemen demzufolge besondere Aufmerksamkeit widmen.

C.3.3 Allgemeine Bedrohungen für Systeme digitaler Freimachungsvermerke

Der nachstehende Text enthält eine Reihe von Bedrohungen, die für Systeme digitaler Freimachungsvermerke allgemein gültig sind. Es wird ausdrücklich darauf hingewiesen, dass die nachstehend angeführte Liste keinen Anspruch auf Vollständigkeit erhebt. Die Mehrzahl der aufgeführten Bedrohungen betreffen die Preisgabe, Veränderung, Kopie oder Ersetzung von Daten, allerdings sollten auch andere Arten von Bedrohungen, einschließlich physikalischer Angriffe und Versuche, einen zuverlässigen Betriebsablauf zu verhindern, nicht außer Acht gelassen werden.

Jeder Postdienstleister hat ein eindeutiges Umfeld, das möglicherweise einige der im Folgenden aufgeführten Bedrohungen von vornherein ausschließt, aber was noch wichtiger ist, für nicht genannte Bedrohungen anfällig sein kann. Eine gründliche Analyse muss durchgeführt werden, um die Liste gegebener Bedrohungen zu vervollständigen und jede dieser Bedrohungen angemessen zu berücksichtigen. Die Analyse muss sich mindestens mit den folgenden Punkte befassen:

- a) **Veränderung:** im Kontext dieser Norm, beinhaltet der Begriff Veränderung die absichtliche Veränderung von in digitalen Freimachungsvermerken enthaltenen Informationen. Ein digitaler Freimachungsvermerk mit einem niedrigen Frankierwert könnte beispielsweise geändert werden und einen wesentlich höheren Portowert anzeigen oder die Kenndaten könnten geändert werden, wodurch der digitale Freimachungsvermerk einer anderen Partei zuzuordnen wäre. Hierbei ist zu beachten, dass diese Abänderungen an den computerlesbaren Daten des digitalen Freimachungsvermerks oder den Klartextangaben oder an beiden vorgenommen werden können.
- b) **Geheime Absprachen:** der Begriff geheime Absprachen betrifft die Kooperation zwischen zwei oder mehr Parteien in betrügerischer Absicht. Diese könnten zwischen Kunden untereinander, zwischen Kunden und einem Lieferanten oder zwischen einer dieser Parteien und einem korrupten Angestellten des Postdienstleisters getroffen werden. So könnte zum Beispiel eine bei einem Postversender angestellte Person eine bei einem anderen Postversender angestellte Person bei der Erstellung von Post unterstützen, die angeblich von ersterer Organisation stammt, oder ein Postversender könnte einen Postangestellten bestechen, so dass dieser Kontrollverfahren zur Annahme von Postwurfsendungen umgeht (siehe nachstehenden Abschnitt unsachgemäße Einlieferung). Angriffe durch geheime Absprachen können nicht völlig verhindert werden, allerdings sind mit Sorgfalt entworfene Systeme lediglich anfällig für geheime Absprachen zwischen mehreren (d. h. mehr als zwei oder drei) Personen und verfügen außerdem über mehrfache Prüfverfahren, die die Aufdeckung von geheimen Absprachen unterstützen.
- c) **Erstellung von Kopien:** unter Erstellung einer Kopie fällt das Duplizieren eines originalen digitalen Freimachungsvermerks zur Herstellung (unbezahlter) identischer Kopien und die Verwendung dieser Kopien auf Postsendungen, die in das Postsystem eingebracht werden. Im Gegensatz zur Fälschung erfordert dies den Zugriff auf echte digitale Freimachungsvermerke oder genaue diesbezügliche Kenntnisse. Der jeweilige Schwierigkeitsgrad könnte davon abhängen, ob für die Herstellung des digitalen Freimachungsvermerks spezielle Geräte oder Lieferungen erforderlich sind (siehe C.6.5 a)).
- d) **Fälschung:** unter Fälschung fällt die in betrügerischer Absicht unternommene unbefugte Erstellung eines Symbols, welches in seinem Aussehen einem echten digitalen Freimachungsvermerk ähnelt oder entspricht. Darunter fällt auch die Erstellung von originalen, scheinbar legitimen, jedoch nicht autorisierten digitalen Freimachungsvermerken, die geschätzte oder vermutete verschlüsselte Gültigkeitscode- oder Austauschgültigkeitscode-Werte enthalten. Ein unbefugter Zugriff auf Geräte zur Authentisierung digitaler Freimachungsvermerke (Prüfgeräte) könnte zum Erzeugen gefälschter digitaler Freimachungsvermerke genutzt werden, bei denen bekannt ist, dass der geschätzte Gültigkeitscode oder Austauschgültigkeitscode korrekt ist, was den Nachweis des unbefugten Zugriffs erschwert oder unmöglich macht. Aus diesem Grund sollte der Zugriff auf die Prüfgeräte geschützt werden.
- e) **Kryptoanalyse:** unter Kryptoanalyse versteht man die Verwendung von mathematischen Techniken beim Versuch, die Verwendung von Verschlüsselungsmethoden zu unterbinden, insbesondere im Zusammenhang mit Informationssicherheitsdiensten. Das Ziel besteht für gewöhnlich darin, durch Ausnutzung von Wissen über Verschlüsselungsalgorithmen, Eingabedaten und/oder Ausgabedaten des Algorithmus Chiffrierschlüssel wiederherzustellen. Da bekannte kryptografische Algorithmen nur nach ausführlichen Untersuchungen durch Experten zugelassen werden, ist die Bedrohung durch Kryptoanalyse bei der Verwendung solcher zugelassener Algorithmen als gering einzuschätzen. Dennoch sollten die für die Verwendung in Systemen zum Erzeugen digitaler Freimachungsvermerke bestimmten Algorithmen und Parameterwerte sorgfältig ausgewählt werden. In Anhang G werden die gebräuchlichsten Algorithmen beschrieben und die mindestens einzuhaltenden Werte der relevanten Parameter angegeben.

- f) **Gerätemanipulation:** dies beinhaltet das unbefugte Manipulieren von Originalgeräten zur Herstellung digitaler Freimachungsvermerke in betrügerischer Absicht. Die unberechtigte Manipulation des aufsteigenden bzw. absteigenden Zählwerks eines Messgerätes könnte beispielsweise dazu führen, dass Portozahlungen umgangen werden.
- g) **Direktantrieb:** Dies beinhaltet die Datenübertragung auf ein Untersystem von einer nicht genehmigten Quelle mit dem Ziel der Herstellung eines manipulierten digitalen Freimachungsvermerks, entweder durch Verwendung von Wiwderverwendung (siehe q)) oder Fälschen (siehe d)).
- h) **Unberechtigter Zugriff auf Chiffrierschlüssel:** dies umfasst den Zugriff auf den/die geheime/n Chiffrierschlüssel eines legitimen Geräts oder eines berechtigten Nutzers von Seiten nicht autorisierter Dritter, denen dadurch ermöglicht wird, sich als legitimes Gerät oder als berechtigter Nutzer auszugeben, indem sie diese (kryptografische) Identifikation missbrauchen. Ein unbefugter Zugang zu Chiffrierschlüsseln würde alle kryptografisch geschützten Einrichtungen des Systems gefährden. Um solch einen unbefugten Zugang zu verhindern, muss bei der Gestaltung von Systemen zur Verwaltung und zum Schutz der Schlüssel mit besonderer Sorgfalt vorgegangen werden. Dabei muss auch darauf eingegangen werden, wie verfahren werden soll, wenn ein Fall von unberechtigtem Zugriff auf Schlüssel entdeckt wird.
- i) **Unbefugte Nutzung des Geräts:** hierunter versteht man das Betreiben oder die Manipulation eines echten Geräts in betrügerischer Absicht. Die Verwendung eines auf Vorauszahlung basierenden Zählers durch Unberechtigte könnte dazu führen, dass dem berechtigten Nutzer ein Schaden entsteht, da das von dem Betrüger verbrauchte und vom Zähler erfasste Porto dem berechtigten Nutzer nicht mehr zur Verfügung steht. Unter gewissen Umständen könnte auch der Gerätelieferant und/oder der Postdienstleister betroffen sein (z. B. kann bei einem auf Kredit basierenden System der Versender, dessen Messgerät gestohlen wurde, die Zahlung des danach von dem Gerät abgerechneten Portos verweigern).
- j) **Betrügerisches Auftreten:** von betrügerischem Auftreten spricht man, wenn ein Versender Postsendungen in das Postsystem einbringt, von denen er behauptet, dass sie von einem anderen Versender stammen. Zum Beispiel könnten in einer Situation, in der die Abrechnung vom Postdienstleister vorgenommen wird, digitale Freimachungsvermerke so verändert werden, dass sie die Geräte- oder Lizenzkennung eines anderen Versenders enthalten. Die betroffenen Postsendungen würden dann als von dem Versender stammend gedeutet, dessen Gerätekennung oder Lizenznummer in den digitalen Freimachungsvermerken erscheint, und würden ihm anstatt dem tatsächlichen Absender berechnet. Es wird darauf hingewiesen, dass betrügerisches Auftreten abhängig von den spezifischen Charakteristika des Anwendungssystems und des Entwurfs der digitalen Freimachungsvermerke ein Sonderfall von Veränderung, Gerätemanipulation bzw. unbefugte Nutzung des Geräts sein kann. Es kann auch mit einer unsachgemäßen Einlieferung zusammenhängen.
- k) **Unsachgemäße Einlieferung:** Die Einlieferung von Postsendungen in das Postsystem auf eine unsachgemäße Art kann zu einer Umgehung der normalen Einlieferungskontrollen führen. Ein unehrlicher Massensender könnte z. B. möglicherweise seine Sendungen über ein Auswechslungsamt einliefern, wodurch diese Sendungen als Sendungen zwischen zwei Postverwaltungen behandelt werden würden. Diese Bedrohung würde im Allgemeinen mit einer Absprache (siehe vorstehend) zwischen dem Versender und einem Beschäftigten des Postsystems zusammenhängen.
- l) **Induzierte Fehlfunktion:** Bei Betrieb eines Systems außerhalb des vorgesehenen Betriebsbereichs können Informationen wie beispielsweise kryptografische Schlüssel offen gelegt werden oder das Gerät kann einen unbefugten Zugriff auf Betriebsabläufe oder Dienste gewähren (z. B. Ändern der in einem Register gespeicherten Entgelte). Fehlfunktionen können zielgerichtet oder zufallsbedingt eingeleitet werden. Weitere Informationen können FIPS 140 [23] und WPV-Norm S30 [8] entnommen werden.
- m) **Unterwanderung des IT-Systems:** dies umfasst eine Reihe von für IT-Systeme typische Bedrohungen. Ein betrügerischer Postangestellter mit Zugang zur Finanzdatenbank, in der die von den Versendern/Anbietern eingezahlten Beträge erfasst werden, könnte die Datensätze zum Vorteil des Senders auf Kosten des Postdienstleisters manipulieren. Jeder Bestandteil des IT-Systems sollte untersucht werden, um die Wahrscheinlichkeit zu minimieren, dass ein unbefugter Zugriff auf Daten sowie deren Veränderung oder Löschung unentdeckt bleiben.

- n) **Missbrauch:** dies umfasst alle Fälle der Erzeugung digitaler Freimachungsvermerke für eine Postsendung, der jedoch für eine andere Sendung verwendet wird, oder bei dem die für die Erzeugung des digitalen Freimachungsvermerks verwendeten Parameter nicht mit den Eigenschaften der Postsendung übereinstimmen, für die der Freimachungsvermerk verwendet wird. Dies führt zu Einnahmeverlusten auf Seiten des Postdienstes, wenn das abgerechnete Porto für die mit dem Freimachungsvermerk versehene Sendung geringer ist als das eigentlich für diese Sendung erforderliche Porto, zum Beispiel, weil für eine geringere Gewichtsklasse bezahlt oder ein Rabattsatz unkorrekt angewendet wurde. Es kann jedoch schwierig sein, den Betrug nachzuweisen, da ein Missbrauch sowohl versehentlich als auch absichtlich erfolgen kann.
- o) **Beschädigung/Manipulation der Erkennungsrate:** unter den Begriff Beschädigung fällt, wenn ein digitaler Freimachungsvermerk in einem solchen Maße unkenntlich gemacht wird, dass er nicht von automatischen Lesegeräten und/oder mit dem menschlichen Auge zugeordnet werden kann und dies in der Absicht geschieht, den Verifikationsprozess zu umgehen und so die Bezahlung zu vermeiden. Es gibt viele Möglichkeiten, einen digitalen Freimachungsvermerk unleserlich zu machen, einschließlich Falzen, Verfälschen, Verschmieren usw. Der Nachweis von Beschädigungen kann schwierig sein, da die Erkennungsraten nie perfekt sind und durch ungünstige Zufälle oder Fehlfunktionen von Geräten beeinträchtigt werden können.
- p) **Erstattungsanträge:** die Verfahrensweisen in Bezug auf Rückerstattungsanträge und die damit verbundenen Gefahren unterscheiden sich von Postdienstleister zu Postdienstleister. Hier sollte der Erstattung von nicht genutztem im Voraus bezahltem Porto und dem Ersetzen beschädigter Sendungen und digitaler Freimachungsvermerke besondere Beachtung geschenkt werden.
- q) **Wiederverwendung bzw. erneute Übertragung:** dazu gehört die Wiederverwendung oder erneute Übertragung einer Mitteilung (einschließlich eines digitalen Freimachungsvermerks) in betrügerischer Absicht. Als Beispiele ließen sich die Wiederverwendung von Umschlägen mit digitalen Freimachungsvermerken und – möglicherweise noch bedeutsamer – wiederholte Kommunikationen (Übertragungen), wie beispielsweise Download von Porto-Kontingenten, zwischen den Subsystemen anführen. Im Gegensatz zu „Fälschen“ ist bei „Wiederverwendung bzw. erneute Übertragung“ ein Zugriff auf bzw. detaillierte Kenntnisse über eine legitime Originalmitteilung erforderlich. Eine solche Wiederverwendung könnte zum Erstellen von Kopien verwendet werden, die sich forensisch nicht von den Originalen unterscheiden lassen, wodurch möglicherweise imagespezifische Gegenmaßnahmen wie die in C.6.5 erörterten vermieden werden können. Zusätzlich zu einer Wiederverwendung von Briefumschlägen gibt es zwei grundlegende Methoden für die Wiederverwendung von Daten:
- 1) Aufzeichnen und wieder verwenden: dazu gehören die Aufzeichnung einer Datenübertragung und die spätere Wiederverwendung entweder mit demselben oder einem anderen Drucksubsystem.
 - 2) Wiederverwendung in Echtzeit: dazu gehört die gleichzeitige Weiterleitung einer Datenübertragung an mehrere Drucksubsysteme (beispielsweise durch Verwendung eines speziell konzipierten Kabel- oder Software-Spoolingprogramms).
- ANMERKUNG Das Kopieren eines digitalen Freimachungsvermerkes wird unter der Überschrift „Kopieren“ behandelt; „Wieder verwenden“ bezieht sich auf die Wiederverwendung eines originären digitalen Freimachungsvermerks (vergleiche Stempelreinigung).
- r) **Verweigerung:** Eine Verweigerung findet statt, wenn eine der beiden Parteien an einer Transaktion seine oder ihre Beteiligung daran verweigert. Das Herunterladen von Porto-Kontingenten in einem Frankiersystem auf die Frankiereinrichtung des Kunden stellt einen Geldtransfer dar. Behauptet der Kunde nachher, der Download habe nicht stattgefunden, so könnte der Postdienstleister eine Umsatzeinbuße erleiden, wenn er nicht in der Lage ist, den Downloadvorgang auf das Subsystem des Kunden nachzuweisen (z. B. durch einen unwiderlegbaren Prüfnachweis oder eine Transaktionshistorie). Ebenso könnte bei einem System, welches auf der Entgeltabrechnung des Postdienstleisters beruht (siehe 5.4), ein Versender die Verantwortung für die Herkunft von Sendungen nicht übernehmen.
- s) **Wiederverwendung:** siehe „erneute Übertragung“

- t) **Unterwanderung des Sicherheitssystems:** Unterwanderung des Sicherheitssystems wird definiert als das Eindringen in ein Sicherheitssystem in der Absicht, dieses außer Kraft zu setzen oder dessen Wirksamkeit zu beeinträchtigen. Wenn das Sicherheitssystem durchdrungen und außer Kraft gesetzt werden kann, könnten die durch das System geschützten anfälligen Stellen offen gelegt und ausgenutzt werden. Eine Schlüsseingabe in betrügerischer Absicht, bei der ein unzulässiger Schlüsselwert in die vom Sicherheitssystem unterstützte Schlüsselgruppe eingegeben wird, stellt ein anderes Beispiel hierfür dar.
- u) **Angriffe durch die Hintertür:** Bei Angriffen durch die Hintertür handelt es sich um nicht-invasive Angriffe, die sich der physikalischen Natur des Berechnungsprozesses bedienen, um Informationen über den geheimen Schlüssel zu erlangen. Die Ausführung von Verschlüsselungsvorgängen beinhaltet energieaufwändige und zeitraubende physikalische Prozesse. Durch eine Auswertung der Zeit- bzw. Energieaufwandsdaten können beispielsweise Informationen über den Wert des verwendeten Schlüssels gewonnen werden, selbst in Situationen, in denen die betreffende Anlage vor Manipulationen geschützt ist. Weitere Informationen können FIPS 140 [23] und WPV-Norm S30 [8] entnommen werden.
- v) **Ersatz:** Ersatz beinhaltet das Abfangen einer legitimen Postsendung und deren Ersetzen durch eine andere Sendung. In einer auf digitalen Freimachungsvermerken beruhenden Umgebung müsste die Ersatzsendung mit einer von der ursprünglichen Sendung genommenen Kopie des digitalen Freimachungsvermerks versehen werden, wodurch Missbrauch Vorschub geleistet wird (siehe vorstehend). Ist die nicht der Fall, hat ein Ersatz zwar keine direkten Auswirkungen auf die Entgelte des Postdienstleisters, es beeinträchtigt jedoch offensichtlich den Versender der ursprünglichen Sendung, welche nicht zugestellt wird, und könnte Forderungen nach sich ziehen, dass die Sendung durch den Postdienst verloren gegangen ist.
- w) **Unterzahlung:** siehe Missbrauch.

C.4 Sicherheit auf Inhalts- und Mitteilungsebene

Mit jedem Sicherheitssystem soll die Anfälligkeit eines geschützten Systems gegen mögliche Bedrohungen so weit verringert werden, wie dies wirtschaftlich, organisatorisch und technisch vertretbar ist. Selbstverständlich wäre es erstrebenswert, wenn solche Anfälligkeiten gänzlich ausgeschaltet werden könnten, nahezu alle praktischen Systeme leiden jedoch an Schwachstellen und eine vollständige Vermeidung dieser lässt sich höchstwahrscheinlich nicht realisieren, schon gar nicht auf eine kosteneffektive Art und Weise. Die Planung von Sicherheitssystemen beruht daher im Allgemeinen auf 2 prinzipiellen Faktoren:

- Schadenskontrolle;
- Abschreckung.

Schadenskontrolle befasst sich mit der Kostenminimierung und den Folgen aus Angriffen auf das und Fehlern im System. Dies erfordert eine hohe Erkennungsrate von Sicherheitsverstößen und die entsprechende Reaktion. Diese Reaktion kann sich entweder auf einen bestimmten Sicherheitsverstoß beziehen oder sich gegen die Möglichkeit ähnlicher Verstöße in der Zukunft richten. Somit kann die Reaktion auf die Feststellung durch Stichprobennahme, dass eine Postsendung einen unzureichenden oder unleserlichen digitalen Freimachungsvermerk trägt, beispielsweise entweder dazu führen, dass die Postsendung für eine Untersuchung abgefangen oder zugestellt wird und der Absender näher untersucht wird, um die Herkunft solcher Sendungen zu ermitteln.

Das Problem bei einem reinen Schadenskontrollansatz besteht darin, dass er für mögliche Angreifer keine abschreckende Wirkung darstellt. Abschreckungsmaßnahmen befassen sich aus diesem Grund mit einem erhöhten Kostenaufwand für einen Angriff auf das System, mit einer geringeren Erfolgswahrscheinlichkeit eines solchen Angriffs sowie mit einem verminderten Nutzen für den Angreifer. Solch ein Ansatz erfordert eine besseres und konsistenteres Feststellungsvermögen von Sicherheitsverstößen sowie verbesserte Abwehrmaßnahmen gegen den Eindringling anstelle einer Minimierung des unmittelbaren Einflusses auf das System. Somit sind folgende Abwehrmaßnahmen vorstellbar, sollten Postsendungen mit falschen digitalen Freimachungsvermerken festgestellt werden:

- Rücksendung anstelle einer Zustellung;
- Zustellung der Sendung, jedoch Durchführung einer Untersuchung des Absenders;

- Zustellung zusammen mit einem entsprechenden Vermerk an den Empfänger;
- Abfangen und Öffnen der Sendung (in einer für diesen Zweck zulässigen Einrichtung) zur Feststellung der Identität des Verursachers und Beschaffung eines gesetzlich zulässigen Betrugsnachweises (siehe nachstehender Absatz).

Die stärksten, jedoch schwierig zu realisierenden Abschreckungsmittel zielen auf die Besorgnis und Bestrafung von Angreifern ab. Zusätzlich zu einer hohen Abschreckungsrate ist dazu die Feststellung des Verursachers eines Angriffs und die Auferlegung einer geeigneten Strafe erforderlich. Der Abschreckungseffekt erfordert eine Ausgewogenheit zwischen dem Grad der Besorgnis und der Strafe für die überführten Täter, so dass der Angreifer ein hohes Gesamtrisiko trägt in Bezug auf den Gewinn, der erzielt wird, wenn der Sicherheitsverstoß bzw. der Täter unentdeckt bleibt. Es bedarf eines eindeutigen Regelwerks über Zusatzentgelte bei vermeidbaren Fehlern sowie strengen gesetzlichen Strafen im Falle von erfolgreich durchgeführten Betrugsversuchen. Letzteres bedingt, dass vom Sicherheitssystem der gesetzlich zulässige Nachweis zu erbringen ist. In einigen Kulturen könnten selbst geringe Verfolgungsraten eine ausreichende Abschreckungswirkung aufweisen, wenn die Strafen hoch genug ausfallen. Dadurch kann sich die Aufdeckung und Abschreckung durch Stichprobennahme als funktionierende Strategie erweisen, wenn die Stichprobenanzahl so gewählt wird, dass mit dem entsprechenden Wahrscheinlichkeitsgrad ein Angreifer gefasst werden kann.

Gegenmaßnahmen sind Techniken, mit denen feindliche Angriffe abgeschreckt, solche Angriffe und unvermeidbare Fehler festgestellt werden und, sofern möglich, die Anfälligkeit für mögliche Bedrohungen verringert oder ausgeschlossen wird. Dies lässt sich erreichen durch:

- a) Bereitstellung von Kontrollen, mit denen Fehler oder mögliche Angriffe festgestellt bzw. darauf reagiert werden kann, wodurch die Systemanfälligkeit durch die damit zusammenhängenden Bedrohungen verringert wird.
- b) Erhöhung der Kosten für die Durchführung feindlicher Angriffe bzw. Verringerung des zu erwartenden Nutzens für einen Angreifer, wodurch die Angriffe weniger lohnenswert erscheinen.
- c) Erhöhung der Erkennungswahrscheinlichkeit eines Angreifers bzw. Erhöhung der „Kosten“ für die Ergreifung, was ein Risiko birgt, durch welches sich die meisten Angreifer abschrecken lassen.

Beim Einsatz und der Durchführung von Gegenmaßnahmen ist Vorsicht walten zu lassen: wenn sie nicht korrekt und von entsprechend geschultem Personal eingesetzt bzw. durchgeführt werden, kann dies weitere Anfälligkeiten nach sich ziehen.

Gegenmaßnahmen können aus Mechanismen, Verfahren, Gesetzen usw. oder aus Kombinationen daraus bestehen. In dieser Norm werden sie ebenso wie in WPV-Norm S27 [6] in zwei Kategorien behandelt, entsprechend der Begriffe in S27 Mitteilungssicherheit und Anwendungssicherheit.

Mitteilungssicherheit befasst sich mit den Gegenmaßnahmen zum Schutz gegen Übertragungsfehler; Abfangen bzw. Ändern von Mitteilungen durch Dritte; betrügerisches Auftreten durch Dritte von autorisierten Absendern sowie Verweigerung von Mitteilungen durch deren Absender oder Empfänger. Die Mitteilungssicherheit kann umfassen:

- a) Schutz der Vertraulichkeit, d. h. Maßnahmen, um zu verhindern, dass Mitteilungen von Unbefugten abgefangen bzw. private Inhalte in Mitteilungen von Dritten gelesen werden, zu denen sie Zugang haben (ob befugt oder nicht);
- b) Schutz der Integrität, d. h. Maßnahmen, die getroffen werden, um zufällige (z. B. durch Übertragungsfehler) bzw. absichtliche Änderungen an Mitteilungen während der Übermittlung vom Absender zum Empfänger zu vermeiden;
- c) Authentisierung, d. h. Prüfverfahren, ob eine Mitteilung von einem spezifischen autorisierten Absender und nicht von einer anderen Partei stammt;
- d) Nicht-Verweigerung, d. h. Verfahren, die zur Sicherstellung verwendet werden, dass ein Absender einer Mitteilung es nicht zurückweisen kann, diese versendet zu haben, bzw. um sicherzustellen, dass der (die) Empfänger einer Mitteilung deren Eingang nicht zurückweisen kann (können).

Auch wenn digitale Freimachungsvermerke nach ihrer Definition Mitteilungen enthalten und demzufolge Sicherheitsmaßnahmen auf Mitteilungsebene unterliegen, es sich dabei nicht um die einzigen Mitteilungen handelt, für die dies gilt. Viele, wenn nicht sogar alle digitale Freimachungsvermerke enthalten andere Mitteilungen, wie beispielsweise elektronische Mitteilungen, die zur Guthabentrücksetzungszwecken verwendet werden, elektronische Belege oder Belege in Druckform (Einlieferungslisten und Einlieferungsbescheinigungen) sowie von Chiffrierschlüssel-Managementsystemen verwendete Mitteilungen. Auch wenn diese in dieser Norm nicht behandelt werden, unterliegen solche Mitteilungen der Sicherheit auf Mitteilungsebene und sollten während der Sicherheitsanalyse berücksichtigt werden. Von größter Bedeutung ist die Sicherstellung der Integrität aller Informationsströme, die mit den Inhalten digitaler Freimachungsvermerke zusammenhängen.

Anwendungssicherheit befasst sich mit Gegenmaßnahmen, die nicht auf der Ebene einzelner Mitteilungen behandelt werden können, einschließlich der Datenkorrelation zwischen unterschiedlichen Mitteilungen sowie zwischen Mitteilungen und Daten, die in postalischen Computersystemen unterhalten werden. Dazu lassen sich folgende Beispiele anführen:

- a) Gültigkeitsprüfung der Informationen in einem digitalen Freimachungsvermerk gegenüber den Zustell- oder Rückanschriftdaten;
- b) Gültigkeitsprüfung der Informationen in einem digitalen Freimachungsvermerk gegenüber den Klartextangaben derselben Daten (z. B. Freimachung oder Datum der beabsichtigten Aufgabe);
- c) Überprüfung der gesamten von einem Frankiergerät aufgetragenen Frankierung gegenüber den Unterlagen der Neufüllungen des Frankiergeräts sowie dem Sendungsaufkommen.

C.5 Sicherheitsfunktionen und Gegenmaßnahmen auf Mitteilungsebene

Postdienstleistern, die ein auf digitalen Freimachungsvermerken basierendes Portozahlungssystem einführen möchten, wird dringend empfohlen, die Sicherheit der in einem digitalen Freimachungsvermerk verschlüsselten Mitteilungen durch Verwendung einer entsprechenden Kombination aus vier Sicherheitsfunktionen zu schützen: Authentisierung, Vertraulichkeit, Datenintegrität und Nicht-Verweigerung.

Unter **Authentisierung** ist eine Sicherheitsfunktion zu verstehen, mit der die Identität einer an einer Transaktion beteiligten Einheit sichergestellt werden kann. Durch die Verwendung von Informationen, die im Allgemeinen nur einem bestimmten autorisierten Absender einer Mitteilung bekannt sind, wird damit vor allem sichergestellt, dass die Quelle einer eingegangenen Mitteilung echt ist, d. h., dass die Mitteilung tatsächlich von der Partei erstellt und versendet wurde, von der sie stammen soll.

Die Authentisierung fungiert vorwiegend als Gegenmaßnahme für Bedrohungen wie Fälschung und betrügerisches Auftreten, sie kann jedoch in einigen Fällen auch als Schutz gegen die Bedrohung *rechtswidrige Geräteverwendung* eingesetzt werden. Mit der Anwendung einer Authentisierungsfunktion für digitale Freimachungsvermerke soll aus diesem Grund sichergestellt werden, dass digitale Freimachungsvermerke nur von autorisierten Geräten bzw. Anwendern erzeugt werden und dass die Erkennung der jeweiligen Anwender erleichtert wird. Die Einführung einer Authentisierungsfunktion wird empfohlen. Bei einer solchen Implementierung sollte die Funktion für alle digitalen Freimachungsvermerke gelten, deren verschlüsselte Daten in der Praxis erfasst werden.

Eine Authentisierung wird im Allgemeinen durch Verwendung von Verschlüsselungstechniken wie beispielsweise digitalen Signaturen und Mitteilungsauthentisierungs-codes erreicht, auch wenn andere Ansätze möglich sind. Richtlinien über mögliche Implementierungsansätze sind in C.9 enthalten.

Vertraulichkeit ist eine Sicherheitsfunktion, mit der unbefugte Einheiten daran gehindert werden, die (geschützten Teile der) Inhalte einer Mitteilung auszulegen. Folglich kann die Mitteilung gespeichert oder übertragen werden, ohne Bedenken, dass der geschützte Informationsgehalt Dritten preisgegeben wird.

Vertraulichkeit richtet sich gegen eine Bedrohung durch Unterwandern von IT-Systemen. Die Anwendbarkeit auf die Mitteilungsinhalte von digitalen Freimachungsvermerken ist jedoch vermutlich auf Fälle beschränkt, bei denen

- Austauschgültigkeitscodes verwendet werden (siehe C.9.4);
- die Identität des Absenders oder des Geräts zum Erzeugen digitaler Freimachungsvermerke geschützt werden muss, damit sie nicht von Dritten (wie beispielsweise einem anderen die Postsendung rechtmäßig bearbeitenden Postdienstleister) zur Einschätzung des Sendungsaufkommens des Absenders verwendet werden, bzw.
- der digitale Freimachungsvermerk Angaben enthält, die der Absender vertraulich behandelt haben möchte.

Die Vertraulichkeitsfunktion gilt eindeutig auch in Fällen, in denen die Erstellung und das Drucken des digitalen Freimachungsvermerks getrennt vorgenommen werden – auch wenn dies eher ein Beispiel für die Anwendung der Funktion bei elektronischen Mitteilungen mit digitalen Freimachungsvermerksdaten als für den Schutz der verschlüsselt auf einer Postsendung aufgetragenen digitalen Freimachungsvermerksmitteilung darstellt. Insbesondere kann mit der Funktion verhindert werden, dass die Sendung von Unbefugten abgefangen und der digitale Freimachungsvermerk von einem Eindringling im Netz anschließend gedruckt wird. Wären die digitalen Freimachungsvermerke nicht geschützt und würden von einem Eindringling abgefangen und verwendet, könnte einer solchen unzulässigen Verwendung sicher mit Hilfe einer Dublettendatenbank (siehe C.6.3) begegnet werden; die den Postinspektoren zur Verfügung stehenden Angaben würden jedoch zum autorisierten Absender und nicht zu dem Eindringling führen.

Sofern erforderlich, wird Vertraulichkeit im Allgemeinen durch Verschlüsselung (kryptografische Umwandlung) der zu schützenden Daten erreicht, entweder mit Hilfe des öffentlichen Schlüssels eines ergänzenden öffentlichen/privaten Paares von Schlüsseln, von dem nur der private Schlüssel dem Empfänger der Mitteilung bekannt ist, bzw. durch Verwendung eines geheimen Schlüssels, der nur dem Absender und dem Empfänger bekannt ist.

Datenintegrität ist eine Sicherheitsfunktion, mit der sichergestellt wird, dass die geschützten Daten weder absichtlich noch zufällig geändert wurden. Somit wird verhindert, dass ungültige oder inkorrekte Daten heimlich durch rechtmäßige, geschützte Daten ersetzt werden.

Datenintegrität fungiert in erster Linie als Gegenmaßnahme für die Bedrohung durch Änderung, sie kann aber auch zum Schutz gegen *Missbrauch* angewendet werden, wenn der Integritätsschutz auf Daten erweitert wird, die intrinsisch in einer korrekten Postsendung enthalten sind. In diesem Fall führt das Aufbringen eines digitalen Freimachungsvermerks auf eine falsche Postsendung zu veränderten intrinsischen Daten, was wiederum zu einer Änderung führt.

Die Einführung einer Datenintegritätsfunktion wird empfohlen. Ferner sollte die Funktion für alle digitalen Freimachungsvermerke gelten, deren verschlüsselte Daten in der Praxis erfasst werden. Für den Schutz elektronischer Mitteilungen, wie beispielsweise Einlieferungslisten und Kontingentrücksetzungsmitteilungen, die mit vielen Inhalten digitaler Freimachungsvermerke zusammenhängen könnten, ist dies ebenfalls von Bedeutung.

Ebenso wie die Authentisierung wird auch die Datenintegrität im Allgemeinen durch Verwendung von Verschlüsselungstechniken wie beispielsweise digitalen Signaturen und Authentisierungs-codes erreicht. Andere nicht-verschlüsselte Techniken können in Fällen verwendet werden, bei denen eher ein Schutz gegen Übertragungsfehler als gegen eine absichtliche Manipulation eines Mitteilungsinhalts erforderlich ist. Richtlinien über mögliche Implementierungsansätze sind in C.9 enthalten.

Nicht-Verweigerung ist eine Sicherheitsfunktion, die eine Einheit an eine Transaktion knüpft, an der sie teilnimmt, d. h., sie erbringt den (gesetzlich zulässigen) Nachweis der Teilnahme an einer bestimmten Partei an der Transaktion und fungiert als Gegenmaßnahme gegen die Bedrohung Verweigerung. Der Zweck der Nicht-Verweigerungsfunktion besteht darin, den Absender einer Mitteilung daran zu hindern, deren Versand (Nicht-Verweigerung durch den Absender) bzw. den Empfänger daran zu hindern, deren Empfang erfolgreich zu verleugnen (Nicht-Verweigerung des Empfängers). Dies könnte insbesondere bei der Strafverfolgung eines Betrugs(versuchs) von Bedeutung sein, wenn die Identität eines Verursachers nachgewiesen werden muss.

Eine Nicht-Verweigerung des Versenders gilt insbesondere bei elektronischen und anderen Mitteilungen ohne digitale Freimachungsvermerke, die zwischen dem Absender, dem Postdienstleister und deren Agenten ausgetauscht werden. Aufgrund der Bedrohung des Kopierens sowie der Möglichkeit, dass ein bestimmter digitaler Freimachungsvermerk möglicherweise nicht tatsächlich vom Postbearbeitungssystem gelesen wird, hat sie lediglich beschränkte Gültigkeit für die Mitteilungen digitaler Freimachungsvermerke selbst.

Das Ergebnis der auf eine Mitteilung digitaler Freimachungsvermerke angewandten Nicht-Verweigerung durch den Absender kann eine angemessene Garantie dafür bieten (mit Ausnahme von Fälschungen), dass der auf einem digitalen Freimachungsvermerk angegebene Absender bzw. das angegebene Frankiergerät tatsächlich einen digitalen Freimachungsvermerk mit dem entsprechenden Inhalt erzeugt hat. Die Beförderung von Postsendungen ist jedoch im Allgemeinen unsicher und die Postsendung könnte im Prinzip während ihrer Erstellung und Bearbeitung von mehreren Parteien gesehen werden. Jede dieser Parteien könnte theoretisch eine Kopie des digitalen Freimachungsvermerks anfertigen und diese auf eine andere Postsendung aufbringen. Somit kann der Absender behaupten, sofern nicht alle kopierten digitalen Freimachungsvermerke nachweislich zu Missbrauch führen, dass die Sendung mit einem bestimmten digitalen Freimachungsvermerk nicht von ihm erstellt wurde, sondern eine Kopie einer seiner digitalen Freimachungsvermerke trägt. Um Gegenforderungen zu vermeiden, dass dies vom Postsystem als Dublette festgestellt werden könnte, kann er/sie weiterhin entweder behaupten, dass die echte Sendung bereits zugestellt wurde, ohne dass sein digitaler Freimachungsvermerk erfasst wurde oder dass eine tatsächliche Versendung der betreffenden Sendung nie vorgenommen wurde. Angesichts dieser Tatsache kann eine auf einem digitalen Freimachungsvermerk aufgebrachte Nicht-Verweigerung durch den Absender bestenfalls als Unterstützung für einen sonstigen Nachweis (z. B. Inhalt) der Herkunft einer Postsendung dienen.

Die Nicht-Verweigerung durch den Absender gilt auch für die Einheit, welche die in der Bereitstellung der Nicht-Verweigerungsfunktion verwendeten Angaben erstellt hat. Je nach Unternehmens- und Anwendungsszenarium, muss dies nicht unbedingt der Absender sein: beispielsweise könnte es auch das Frankiergerät des Absenders sein (welches möglicherweise unbefugt verwendet wurde) oder ein im Namen des Versenders arbeitender Versandarbeiter, der absichtlich oder versehentlich Sendungen erstellt, die tatsächlich nicht dem Versender gehören. Ist das von der Schlüsselbescheinigungsstelle verwendete Kennungsprüfverfahren fehlerhaft, könnte dies selbst eine dritte den Absender zum Zeitpunkt der Schlüsselausgabe oder –registrierung in betrügerischer Absicht auftretende Person sein.

Der Schutz gegen Verweigerung durch den Absender ist eng mit dem Thema Authentisierung verknüpft (siehe oben), wenn der hierfür unternommene Ansatz sicher ist und lediglich die dem Absender bekannten Angaben verwendet werden (beispielsweise der privaten Schlüssel eines öffentlich-privaten Schlüsselpaares), so ist eine Verweigerung durch den Absender sehr wahrscheinlich erfolglos; wenn der Ansatz fehlerhaft ist, kann der Absender wahrscheinlich eher behaupten, die Mitteilung wäre von einem Dritten erstellt worden.

Wie bei der Authentisierung wird die Nicht-Verweigerung durch den Absender im Allgemeinen mit Hilfe von Verschlüsselungstechniken realisiert. Sowohl digitale Signaturen als auch Mitteilungsauthentisierungs-codes können diese Funktion ausüben. Während digitale Signaturen eine explizite Nicht-Verweigerung durch den Absender erfordern, ist dies bei Mitteilungsauthentisierungs-codes implizit erforderlich, da mindestens zwei an einer durch einen Mitteilungsauthentisierungscode gesicherten Transaktion beteiligte Parteien unbedingt Zugriff auf den geschützten geheimen Schlüssel haben müssen. Folglich kann der Absender stets versuchen zu behaupten, dass eine strittige Mitteilung vom Empfänger erzeugt wurde bzw. dass die Schlüsselsicherheit des Empfängers preisgegeben wurde. Aus diesem Grund beschränkt sich die Verwendung von geheimen Verschlüsselungs-algorithmen für Nicht-Verweigerungszwecke auf Situationen, in denen entweder dem Empfänger keine Vorwürfe gemacht werden können oder Ansprüche gegen Dritte erhoben werden, die sowohl von der Absender- als auch von der Empfängerseite als vertrauenswürdig anerkannt werden.

Verweigerung durch den Empfänger — die Behauptung eines Empfängers, eine Mitteilung nicht oder zu einem anderen als dem tatsächlichen Zeitpunkt empfangen zu haben — stellt in bestimmten Fällen ebenfalls ein Risiko dar, insbesondere bei Mitteilungen, die sich auf besondere Sendungsklassen beziehen. Ein Schutz gegen diese Eventualitäten wird üblicherweise dadurch gewährt, dass der Empfänger den Empfang zu bestätigen hat. Solche Bestätigungen können gegebenenfalls mit Hilfe der Authentisierungs- und Nicht-Verweigerungsfunktionen des Absenders geschützt werden.

Die Zugriffssicherheit auf den Mitteilungskommunikationskanal kann ebenfalls eine Rolle für den Schutz der Verweigerung sowohl durch den Absender als auch durch den Empfänger spielen: beispielsweise können im Falle von Mitteilungen, die auf physikalischem Wege vorgelegt werden, Annahmekontrollverfahren dazu verwendet werden, die Absenderidentität am Übergabepunkt der Mitteilung zu überprüfen; als Empfangsbestätigung werden traditionell Signaturenverfahren verwendet (siehe auch Einschreibesendungen). Diese Überlegung kann jedoch für digitale Freimachungsvermerke selbst nicht angestellt werden, da diese für alle Parteien mit Zugang zur Postsendung zugänglich sind.

C.6 Gegenmaßnahmen auf Anwendungsebene

C.6.1 Einleitung

In Folgenden werden einige der Gegenmaßnahmen auf Anwendungsebene erläutert, die ergriffen werden können. Es wird betont, dass die Beschreibung nicht so ausgelegt werden sollte, dass sie eine vollständige Liste an Möglichkeiten darstellt, und die Postdienstleister werden dazu aufgefordert, auch andere Techniken zu berücksichtigen.

Angesichts des Umfangs dieser Norm befassen sich die folgenden Abschnitte hauptsächlich mit Gegenmaßnahmen, die sich in bestimmter Weise auf digitale Freimachungsvermerke beziehen, welche vorrangig als Nachweis bzw. Grundlage der Portoabrechnung dienen. Mit diesem Nachweis sollen die Postdienstleister (oder deren Agenten) in die Lage versetzt werden, Betrugsversuche besser feststellen zu können. Wird eine (mögliche) betrügerische Handlung festgestellt, sollte mit Hilfe der Angaben des digitalen Freimachungsvermerks und der anderen auf (oder in besonderen Fällen in) der Postsendung vorhandenen Angaben die verantwortliche Partei festgestellt und der gesetzlich zulässig Nachweis erbracht werden können. Dies ist nur möglich, wenn der digitale Freimachungsvermerk die entsprechenden Datenelemente enthält (siehe Anhang E), die gegen eine Manipulation geschützt sind (siehe Datenintegrität in C.5) und mit anderen (geprüften) Informationen übereinstimmen, die innerhalb des postalischen Zahlungssystems verfügbar sind.

C.6.2 Zugangs- und Anwendungskontrollen

Einer Vielzahl von Bedrohungen kann durch Zugangsbeschränkungen oder Anwendungskontrollen von sensiblen Teilen des Systems begegnet werden. Bei Frankiersystemen ohne digitale Freimachungsvermerke sind eine Anwendungskontrolle durch Guthabenrücksetzungsverfahren und Überwachungstimer sowie ein Schutz gegen Gerätemanipulation durch Kontrolle des physikalischen Zugangs mit Hilfe von Manipulationsfeststellungstechniken üblich. Solche Ansätze sind wahrscheinlich auch in einer Umgebung mit Inhalten digitaler Freimachungsvermerke erforderlich, insbesondere zum Schutz von kryptografischen Schlüsseln und entgeltbezogene Daten. FIPS PUB 140-2 [23] und WPV-Norm S30 [8] enthalten eine Richtlinie für die Sicherstellung, dass kryptografische Schlüssel innerhalb eines Moduls sicher verwaltet werden. Ähnliche Grundsätze sollten für den Schutz von entgeltbezogenen Daten angewendet werden. Es sollte angemerkt werden, dass die bestimmten angewendeten Gegenmaßnahmen [siehe insbesondere die nachstehenden Absätze b), d), f) und g)] von der Systemtopologie und dem Standort der Abrechnungssysteme und der kryptografischen Subsysteme abhängen könnten.

Die zu berücksichtigenden Ansätze umfassen:

- a) **Guthabenkontrolle:** Guthabenkontrollen sind Wertezähler, die — im Falle von Abrechnungsanwendungen — den Portobetrag begrenzen, der mit einem entsprechenden Gerät abgerechnet werden kann. Im Allgemeinen kann der Grenzwert durch Guthabenrücksetzungsverfahren zurückgesetzt werden, die entweder mit der Geräteprüfung oder mit einem Guthabenrücksetzungssystem verknüpft sind. Zwei Fälle können dabei berücksichtigt werden. Im ersten Fall wird die Kontrolle im Gerät selbst vorgenommen. Dazu ist eine Kontrolle des physikalischen Zugangs zum Gerät oder ein Manipulationsschutz im Gerät erforderlich, da es sonst einer unbefugten Partei möglich ist, die Guthabengrenze zurückzustellen. Im zweiten Fall wird die Kontrolle entfernt vom Gerät vorgenommen (z. B. im Managementsystem) und funktioniert durch logische Kontrolle des Gerätebetriebs, z. B. durch Verweigerung des Anschlusses an ein Netzwerk oder (im Falle von digitalen Freimachungsvermerken) dadurch, dass digitale Freimachungsvermerke, die von den Geräten erzeugt wurden, deren Guthabengrenze erreicht ist, für ungültig erklärt und somit nicht akzeptiert werden.

- b) **Elektronische Zugangskontrolle:** Dies beinhaltet die Verwendung von logischen Mitteln zur Einschränkung des Zugangs zu sensiblen Funktionen oder Dienste auf befugte Einheiten (einzelne Benutzer, Programme, Prozesse oder Systeme). Dies erfordert eine Authentisierung (d. h. Überprüfung, ob die zugreifende Einheit tatsächlich die Einheit ist, die zu sein sie vorgibt). Wie in FIPS 140-2 [23], 4.3 beschrieben, kann die Authentisierung auf der Verwendung von logischen Schlüsseln (Passwörtern oder PIN-Nummern), physikalischen Schlüsseln wie beispielsweise Smartcards und intrinsischen Attributen wie beispielsweise Fingerabdrücken oder anderen biometrischen Eigenschaften beruhen.

Die Anwendung einer elektronischen Zugangskontrolle innerhalb eines Systems digitaler Freimachungsvermerke kann zwei Zielsetzungen haben: um sicherzustellen, dass spezifische Einheiten Zugang zu den betreffenden sensiblen Funktionen haben bzw. um eine Einheit an eine Funktion zu koppeln und damit einer Verweigerung vorzubeugen.

Es wird empfohlen, mindestens die Portoabrechnungs-, Guthabenrücksetzungs-, Überwachungs- und Sicherheitsfunktionen mit Hilfe der elektronischen Zugangskontrolle zu schützen. Die sensiblen Systeme sollten mit mehreren Zugangskontrollebenen realisiert werden, so dass die zugreifenden Einheiten mit unterschiedlichen betrieblichen Rollen und Ebenen der Sicherheitsfreigabe über verschiedene Zugangsrechte verfügen können. Sofern erforderlich, sollten solche Zugangsrechte die Erfordernisse für mehrere unabhängige Einheiten verstärken, die an der Inbetriebnahme wichtiger Funktionen beteiligt sind. Eine manuelle Eingabe eines Chiffrierschlüssels sollte beispielsweise so realisiert werden, dass unterschiedliche Personen unterschiedliche Schlüsselkomponenten eingeben müssen, damit niemand (ohne Einverständnis) den vollständigen Schlüssel in Erfahrung bringen kann. Ebenso sollten für die Rücksetzung wichtiger Systeme, wie beispielsweise des Prüfsystems für digitale Freimachungsvermerke, mindestens zwei getrennte und unabhängige Betriebsabläufe erforderlich sein.

Wird eine elektronische Zugangskontrolle mit Hilfe von Passwörtern oder PIN-Nummern realisiert, sollten Maßnahmen ergriffen werden, um sicherzustellen, dass

- diese regelmäßig geändert werden,
- sie nicht auf der Betriebsplattform der Anwendung gespeichert, sondern von der Einheit eingegeben werden, die auf die Anwendung zugreifen möchte,
- sich die einzelnen Benutzer und Systemplaner der Sicherheitserfordernisse vollständig bewusst sind.

Eine elektronische Zugangskontrolle kann bidirektional sein müssen. D. h., eine Einheit (eine Person oder ein Anwendungsprozess), die ihre Identität einem Anwendungsdienst oder einer Funktion gegenüber nachweisen muss, kann auch einen Identitätsnachweis der jeweiligen Anwendung verlangen.

Dieses Erfordernis einer bidirektionalen elektronischen Zugangskontrolle wird besonders offenkundig bei zwei Anwendungsprozessen, die sich gegenseitig ihrer Software- und Versionsnummer versichern müssen.

Die Verwendung eines Konfigurationsmanagementsystems wird empfohlen, damit sichergestellt ist, dass die Anwendungssoftwarekomponenten

- vor der Inbetriebnahme korrekt installiert und konfiguriert sind und
- ihre Konfiguration, Versionsnummer und Integrität (d. h., dass sie nicht verändert wurden) regelmäßig überprüft werden.

ANMERKUNG 1 Dies kann auf verschiedene Arten erreicht werden: Jeder Prozess könnte beispielsweise eine (variable) Prüfsummenberechnung vom anderen anfordern.

ANMERKUNG 2 Es sollte betont werden, dass mit dem Konfigurationsmanagement den legitimen Benutzern ein Werkzeug für die bidirektionale elektronische Zugangskontrolle zur Verfügung gestellt wird, womit die Verwendung von illegitimer Software festgestellt werden kann.

- c) **Management verlorener und gestohlener Geräte:** Verlorene und gestohlene Geräte sind Geräte, die sich nicht mehr im Besitz der autorisierten Einheit befinden. Dies kann für hoch sensitive Anlagen gelten, die von autorisierten Anbietern elektronischer Prüfgeräte für Porto und digitale Freimachungsvermerke verwendet werden. Es eignet sich sicherlich für sensitive eindeutig feststellbare Anlagen, wobei Unterlagen über die zulässige Nutzung erstellt werden. Transaktionen, an denen ein bestimmtes Gerät beteiligt ist, sollten eine Gerätekennung enthalten oder einen Zugriff darauf ermöglichen, so dass Abhilfemaßnahmen (wie beispielsweise die Verweigerung aller digitalen Freimachungsvermerke) ergriffen werden können, falls ein Gerät als verloren oder gestohlen gemeldet wird. Im Idealfall sollte es möglich sein, Geräte per Fernsteuerung außer Betrieb nehmen zu können, wenn diese sich an das Managementsystem wenden, beispielsweise aufgrund einer Guthabenrückstellung oder einer Rückstellung des Überwachungstimers.
- d) **Physikalische Zugangskontrolle:** Der physikalische Zugang zu einem sensitiven Gerät lässt sich kontrollieren, indem das Gerät in einer Einrichtung untergebracht wird, zu dem lediglich befugte Personen Zutritt haben. Die Anforderungen für solche physikalischen Zugangskontrollsysteme sind vergleichbar mit denjenigen, die im Falle von anderen sensitiven computer-basierten Systemen gelten und werden in dieser Norm nicht weiter berücksichtigt.

Physikalische Zugangskontrollen sind auf jeder Ebene anwendbar, vom Grundstück, über das Gebäude und die Räume bis hin zum einzelnen Gehäuse. Die Zugangskontrollsysteme selbst sollten mit einem Manipulationsschutz versehen werden (siehe nachfolgend). Vorbehaltlich diesen Ausführungen können physikalische Zugangskontrollen ohne weiteren Manipulationsschutz angemessen sein bei in Postsystemeinrichtungen befindlichen Geräten und selbst bei Geräten, die von bewährten Anbietern betrieben werden (z. B. Ausgabegeräte für elektronische Portowerte) und einer Postsicherheitsprüfung unterliegen. Sie eignen sich jedoch nicht in solchen Fällen, bei denen die sensitiven Anlagen auf kundeneigenem Gelände untergebracht sind. In solchen Fällen sollte erwogen werden, die Geräte mit einem Manipulationsschutz zu versehen (siehe nachstehend).

- e) **Sichere Verknüpfung von Ausdruck und Abrechnung:** Eines der möglichen Hauptprobleme bei der Verwendung der digitalen Drucktechnologie besteht in der problemlosen Kopierbarkeit der Druckbilder. Wenigstens in den Fällen, in denen es keine andere angemessene Möglichkeit gibt festzustellen, ob solche Duplikate verwendet werden (siehe C.6.3), kann es wünschenswert sein, dies durch sichere Verknüpfung des Druckers digitaler Freimachungsvermerke an ein Portoabrechnungsmodul zu erschweren und damit die Verwendung des Druckers für eine (nicht abgerechnete) Reproduktion von digitalen Freimachungsvermerken zu verhindern. Auch wenn mit dieser Gegenmaßnahme das Kopieren von digitalen Freimachungsvermerken nicht verhindert wird (beispielsweise durch Einscannen und Drucken des Bildes auf einem anderen Drucker), kann damit eher sichergestellt werden, dass die entstandenen Drucke sich forensisch von den von einem autorisierten Drucker erzeugten Originalausdrucken unterscheiden lassen. Die Effektivität dieser Maßnahme kann durch Verwendung von Druckern für digitale Freimachungsvermerke mit unverwechselbaren Leistungsmerkmalen noch gesteigert werden.
- f) **Schutz gegen Angriffe durch die Hintertür:** Angriffe durch die Hintertür hängen von den aus der kryptografischen Funktionsanalyse des Zeitaufwands bzw. des Energieaufwands gewonnenen Informationen ab. Gegen solche Angriffe kann man sich durch die Verwendung von Techniken schützen, die so konzipiert sind, dass Änderungen dieser physikalischen Parameter verhindert werden. Der Bedarf an sowie die Komplexität solcher Gegenmaßnahmen hängen von der Art des enthaltenen Computerchips und Algorithmus ab — einige Algorithmen und Chips sind anfälliger für solche Angriffe durch die Hintertür als andere — und kein eindeutiger Standard wurde bis jetzt auf diesem Gebiet erarbeitet. Als Mindestmaßnahme wird empfohlen, die Sicherheitsgeräte, welche die Verschlüsselungsalgorithmen für die Berechnung der verschlüsselten Gültigkeitscodes ausführen, auf deren Anfälligkeit für Angriffe durch die Hintertür zu überprüfen.
- g) **Manipulationsschutz:** Wie im Allgemeinen bei herkömmlichen Frankiermaschinen können die sensitiven Geräte mit physikalischen Sicherheitseinrichtungen versehen werden, durch die mit hoher Wahrscheinlichkeit ein unbefugter Zugriff, eine Verwendung oder eine Manipulation des Geräts entweder nach dem Versuch festgestellt werden kann, indem sichtbare Zeichen hinterlassen werden (d. h. offensichtliche Manipulation), oder während des Versuchs (d. h. Feststellung einer Manipulation), so dass die entsprechenden Maßnahmen für einen Selbstschutz des Geräts getroffen werden können (d. h. Reaktion auf Manipulationsversuche). FIPS PUB 140-2 [23] und WPV-Norm S30 – International postage meter approval requirements (IPMAR) (Erfordernisse für die Genehmigung von Frankiergeräten) [8] enthalten die Erfordernisse hinsichtlich der Manipulationsschutzmechanismen für Frankiergeräte.

Ein Gerät, welches lediglich offensichtliche Manipulationsversuche anzeigt, bietet keinen ausreichenden Eigenschutz. Bei Verwendung in Verbindung mit einer regelmäßigen physikalischen Geräteprüfung kann dies jedoch eine effektive Gegenmaßnahme darstellen.

Die Reaktion auf eine Manipulation kann der Bericht an ein Gerätemanagementsystem, eine Änderung der wichtigen Gerätedaten oder die Deaktivierung des Geräts sein. Als Schutz gegen die Bedrohungen eines illegitimen Schlüsselzugangs und der Infiltration des Sicherheitssystems kann es wünschenswert sein, dass die Manipulationsreaktion eine Zerstörung (z. B. auf null setzen) beliebiger Schlüsselparmeter im Gerät beinhaltet. Bei digitale Freimachungsvermerke erzeugenden Geräten ist eine Deaktivierung möglicherweise nicht immer die beste Lösung: angesichts der Daten enthaltenden Eigenschaften von digitalen Freimachungsvermerken sollte das Gerät stattdessen weiterhin digitale Freimachungsvermerke erzeugen, diese jedoch aufgrund der Manipulation als ungültig kennzeichnen (siehe auch das Prinzip stiller Alarme für die physikalische Zugangskontrolle).

- h) **Betriebszählerkontrolle:** Betriebszählerkontrollen sind Betriebszähler, mit denen die Anzahl der Verwendungen eines Geräts oder dessen Dienste begrenzt wird. Sie gelten insbesondere für Prüfgeräte digitaler Freimachungsvermerke, die frei zugänglich verwendet (missbraucht) werden können, um die Gültigkeit von gefälschten digitalen Freimachungsvermerken mit zufälligen Sicherheitsdaten zu überprüfen.

Mehrere Kontrollebenen können wünschenswert sein. Zum Beispiel:

- i) eine begrenzte Anzahl von Versuchen für die Überprüfung einer bestimmten Transaktion (z. B. Überprüfung eines digitalen Freimachungsvermerks oder Überprüfung eines Zugangskontrollpassworts) innerhalb einer bestimmten Zeitperiode (bzw. aufeinander folgend);
- ii) eine Begrenzung der Gesamtverwendung des Prüfgeräts bzw. der Prüffunktion (z. B. für die Gesamtzahl der an einem Tag vorgenommenen Überprüfungen oder bis zur Rücksetzung des Geräts durch einen autorisierten Benutzer);
- iii) eine Begrenzung der Gesamtzahl oder Gesamtrate der entweder aufeinander folgenden, innerhalb einer bestimmten Zeitperiode bzw. bis zur Rücksetzung des Geräts durch einen autorisierten Benutzer zulässigen Überprüfungsfehler.

ANMERKUNG 3 Dies ist wahrscheinlich effektiver als eine Beschränkung der Gesamtverwendung. Mit einer schnellen Online-Überprüfung lassen sich etwa 30 Überprüfungsvorgänge je Sekunde durchführen. Das sind fast 2,6 Millionen je Tag, in der Praxis ist jedoch (im Normalfall) lediglich die Hälfte davon erforderlich. Könnte ein Angreifer auf eine solche Überprüfung zugreifen und sie dazu benutzen, die Gültigkeit der erratenen gefälschten und von einem 10-Bit-Schlüsselcode geschützten digitalen Freimachungsvermerk zu überprüfen, wäre der Fälscher mit einer Wahrscheinlichkeit von 1 zu 1 024 eines richtigen Ratens in der Lage, ohne bestehende Kontrolle 2 531 offensichtlich richtige (jedoch tatsächlich gefälschte) digitale Freimachungsvermerke täglich zu erzeugen und immer noch 1465 je Tag, wenn die Verwendung des Prüfgeräts auf 1,5 Millionen Prüfvorgänge je Tag beschränkt wäre. Werden jedoch im Normalfall mindestens 95 % der überprüften digitalen Freimachungsvermerke als gültig vorausgesetzt, könnte eine „Prüflehrgrenze“ von vielleicht 100 000 je Tag festgesetzt werden. Mit einer solchen Obergrenze könnte der Fälscher lediglich 100 098 Ratevorgänge mit dem Resultat von 97 gültigen Fälschungen durchführen, bevor sich das Gerät selbst deaktiviert. Mit einer normalen Erfolgsrate von 95 % beträgt die Wahrscheinlichkeit einer Anzahl von 20 aufeinander folgenden Fehlern etwa 1 von 10^{26} . Für einen Fälscher mit einer Erfolgsrate von lediglich 1 von 1 024 beträgt die Wahrscheinlichkeit etwa 0,98. Somit wird die Einrichtung einer Obergrenze von 20 aufeinander folgenden Fehlern dem normalen Betrieb eines Fälschers kaum Einhalt gebieten (obwohl die Möglichkeit eines schlechten „Stapels“ digitaler Freimachungsvermerke besteht), es besteht jedoch eine gute Möglichkeit, den Fälscher an seiner Tätigkeit zu hindern, bevor ein einziger gültiger digitaler Freimachungsvermerk erlangt werden kann.

- i) **Überwachungstimer:** Überwachungstimer sind Timer, die regelmäßig von einem autorisierten Prüftechniker oder über den Kontakt mit einem Gerätemanagementsystem zurückgestellt werden müssen. Ohne eine solche Rücksetzung würde das an sie angeschlossene Gerät deaktiviert. Eine solche Deaktivierung kann von Dauer oder vorübergehender Natur sein (d. h. bis zur nächsten Wartung oder dem nächsten Kontakt). Zwei Fälle können dabei berücksichtigt werden. Im ersten Fall ist der Timer im Gerät selbst implementiert. Dazu ist eine Kontrolle des physikalischen Zugangs zum Gerät oder ein Manipulationsschutz im Gerät erforderlich, da es sonst einer unbefugten Partei möglich ist, den Timer zurückzustellen. Im zweiten Fall ist der Timer vom Gerät abgesetzt (z. B. im Managementsystem) und funktioniert durch logische Kontrolle des Gerätebetriebs, z. B. durch Verweigerung des Anschlusses an ein Netzwerk oder (im Falle von digitalen Freimachungsvermerken) durch Ablehnung von digitalen Freimachungsvermerken als ungültig, die von den Geräten erzeugt wurden und ihr Zeitlimit überschritten haben.

Zugangs- und Verwendungskontrollen können kombiniert und zusammen mit anderen Arten von Gegenmaßnahmen verwendet werden. Die Implementierung exzessiver Kontrollen ist jedoch von begrenztem Wert.

C.6.3 Dublettenerkennung

Betrügerisches Kopieren (bzw. Replizieren) von digitalen Freimachungsvermerken stellt eine potentiell signifikante Verlustquelle an postalischen Erträgen dar. Mit der Dublettenerkennung wird versucht, dieser Bedrohung durch Feststellung solcher Dubletten zu begegnen, damit die entsprechenden Maßnahmen ergriffen werden können.

Um Dubletten ohne jeden Zweifel nachzuweisen, ist es erforderlich, dass bei einer aktuell vorliegenden Sendung nachgewiesen werden kann, dass eine frühere Sendung bereits mit demselben digitalen Freimachungsvermerk versehen war. Im Allgemeinen lässt sich dies durch Verwendung einer Dublettendatenbank erreichen:

- während der Überprüfung einer Postsendung werden die Daten digitaler Freimachungsvermerke erfasst und mit den früheren verarbeiteten Daten digitaler Freimachungsvermerke verglichen, die in der Datenbank gespeichert sind;
- ist der vorliegende digitale Freimachungsvermerk nicht auf einer früheren Sendung vorhanden, wird er in die Datenbank aufgenommen und kann für zukünftige Vergleiche herangezogen werden;
- wurde der digitale Freimachungsvermerk bereits früher verwendet, werden sowohl die entsprechende Postsendung als auch die frühere Postsendung mit dem identischen digitalen Freimachungsvermerk als mögliche Dubletten gekennzeichnet;
- andere Daten werden herangezogen (siehe nachstehende Beschreibung) oder eine Untersuchung wird durchgeführt, um festzustellen, welche der beiden Postsendungen echt ist und welche einen kopierten digitalen Freimachungsvermerk trägt.

Damit dieser Ansatz funktioniert, muss jeder legitime digitale Freimachungsvermerk eindeutig sein⁹⁾. Dies lässt sich auf verschiedene Art und Weise erreichen, einschließlich der Aufnahme eines (nicht rücksetzbaren) stetig ansteigenden Zählers, des Werts des aufsteigenden Register eines Frankiergeräts oder eines Datums-/Zeitstempels mit der entsprechenden Körnung in den digitalen Freimachungsvermerk.

Gleichgültig welche Methode verwendet wird, um einen digitalen Freimachungsvermerk eindeutig zu machen, der Ansatz erfordert einen Zugriff auf eine Datenbank mit „gebrauchten“ digitalen Freimachungsvermerken während des Sendungsprüfprozesses. Aufgrund ihrer Art kann die Datenbank sehr umfangreich werden: in einem „Worst Case“-Szenarium könnte dies bei einem unzureichend aufgebauten Sicherheitssystem dazu führen, dass **alle jemals** verwendeten digitalen Freimachungsvermerke beibehalten und durchsucht werden müssten. Selbst bei der bestehenden Computer- und Datenbanktechnologie hätte dies schwerwiegende Auswirkungen auf die Kosten und die Verarbeitung.

Eine Methode bezüglich einer Kostensenkung wäre der Versuch einer Dublettenerkennung nur für eine Probenauswahl von Postsendungen (siehe Anhang F). Dadurch würden sowohl die Datenbankgröße als auch der zu deren Durchsuchung erforderliche Verarbeitungsaufwand verringert. Dies reduziert jedoch auch die Wahrscheinlichkeit, eine Übereinstimmung zu finden, denn selbst wenn die untersuchte Postsendung einen kopierten digitalen Freimachungsvermerk trägt, besteht eine hohe Wahrscheinlichkeit, dass das Original nie geprüft wird.

9) Streng genommen ist es **nicht** erforderlich, dass digitale Freimachungsvermerke eindeutig sind. Bei einigen Anwendungen (wie beispielsweise PPI-Post) kann es wünschenswert sein, dass derselbe digitale Freimachungsvermerk auf einen ganzen Sendungsstapel aufgebracht werden darf. In diesem Fall soll dadurch kein unerlaubtes Kopieren vermieden, sondern sichergestellt werden, dass ein gegebener digitaler Freimachungsvermerk nicht öfter verwendet als für ihn abgerechnet wurde. Die Datenbank müsste einen Datensatz der zulässigen Verwendungshäufigkeit enthalten und einen Vergleich zwischen dieser und der tatsächlichen Anzahl von verwendeten digitalen Freimachungsvermerken zulassen.