Bundesanzeiger
Herausgegeben vom
Bundesministerium der Justiz
www.bundesanzeiger.de

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Postfach- und Versanddienst Interoperabilitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI – TR 01201 Teil 3.4
Version:	1.7

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: de-mail@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieses Modul ist Bestandteil von [TR DM PVD M]. Hier werden Datenstrukturen und Datenformate des Postfach- und Versanddienstes spezifiziert.

2 Datenstrukturen

Im PVD sind insbesondere „Nachrichten“, „Bestätigungsnachrichten“ und „Meldungsnachrichten“ zu unterscheiden. In diesem Dokument werden die Elemente dieser Datenstrukturen bestimmt und definiert. Diese Datenstrukturen dienen als Grundlage zur Bestimmung der Datenformate und deren Kodierungen.

Bestätigungsnachrichten sind Nachrichten, die die vom PVD erstellten Bestätigungen über den Zustand einer Nachricht, wie bspw. für den Versand oder die Zustellung von Nachrichten, im Nachrichten-Body beinhalten.

Meldungsnachrichten sind Nachrichten, die vom PVD erstellt werden, um den Nutzern Informationen über bestimmte Ereignisse zukommen zu lassen. Die zu übermittelnde Meldung ist im Nachrichten-Body der Nachricht enthalten. Meldungen können aber auch über andere Kommunikationsschnittstellen dem Nutzer bekannt gemacht werden, bspw. als Text auf einer Webseite, wenn ein Webbrowser verwendet wird.

2.1 Nachrichten

Nachrichten müssen aus Metadaten und dem Nachrichten-Body (siehe Abschnitte 2.1.1 und 2.1.2) bestehen. Nachrichten bzw. Teile der Nachrichten können vom Sender (clientseitig) elektronisch signiert und/oder verschlüsselt werden.

Von Nachrichten ist konzeptuell ein Nachrichtenentwurf als Vorstufe zu einer Nachricht zu unterscheiden. Eine Nachricht, die noch nicht vom Postfachdienst vollständig entgegengenommen und für den Versand vorbereitet worden ist, gilt als Nachrichtenentwurf. Eine Nachricht ist für den Versand vorbereitet, wenn die Metadaten in der Nachricht durch den Postfachdienst gesetzt worden sind.

De-Mail-Nachrichten müssen mindestens aus den nachfolgend beschriebenen Komponenten bestehen.

2.1.1 Metadaten

Die Metadaten müssen zusammen mit der Nachricht übermittelt und an entsprechender Stelle im Kontrollfluss des PVD ausgewertet werden. In Abhängigkeit der eingestellten Werte werden die dazu vorgesehenen Aktivitäten ausgeführt.

2.1.2 Nachrichten-Body

Innerhalb eines Nachrichten-Body können beliebig viele Abschnitte (multipart) enthalten sein.

2.1.3 Clientseitige Signatur und Verschlüsselung

Durch den Nutzer elektronisch signierte und / oder Ende-zu-Ende verschlüsselte Nachrichten oder Nachrichtenanhänge müssen bei De-Mail verlustfrei weitergeleitet werden.

3 Datenformate

Eine De-Mail-Nachricht ist eine Internet-E-Mail gemäß [RFC2822], die die im Folgenden genannte Strukturmerkmale besitzt. Insbesondere enthält sie die von der [TR DM PVD FU] geforderten Metadaten zur Steuerung des PVD.

3.1 Header

Die Verarbeitung der De-Mail-Nachrichten im PVD wird gesteuert mit Hilfe von zusätzlichen Metafeldern im Header der Nachricht. De-Mail-spezifische Metadaten müssen als X-Header-Zeilen kodiert werden. Es gelten alle allgemeinen Regeln des RFC 2822 für Header-Zeilen. Im Sinne des RFC sind X-Header-Zeilen „Optional fields“ (RFC 2822 Abschnitt 3.6.8). Durch die Kodierung der Metadaten als X-Header-Zeilen wird eine De-Mail-Nachricht zu einer speziellen Form einer RFC2822-Mail. Bereits vorhandene Header-Felder, die nicht De-Mail-spezifisch sind, sollten in der Nachricht belassen werden.

Bei der Verarbeitung der X-Header muss die Groß-/ Kleinschreibung der Namen ignoriert werden. Der X-Header-Name sollte klein geschrieben werden.

3.1.1 Übersicht über die Header von De-Mail-Nachrichten

Die Metadaten einer De-Mail-Nachricht müssen wie folgt durch X-Header-Zeilen und E-Mail-Header-Zeilen abgebildet werden:

Nr.	*Bezeichnung*	*Header-Name*	*Nachrichtentypen*[1][2]				
			N	*B*	*M*	*I*	*W/F*[3]
1	Versandbestätigung	X-de-mail-confirmation-of-dispatch	XX				wie original Bestätigung wird nicht beim Versand einer Weiterleitung oder Nachsendung erzeugt

1 N=Normale De-Mail-Nachricht, B=Bestätigungsnachricht, M=Meldungsnachricht, I=Ident-Bestätigungsnachricht, W/F weitergeleitete und nachgesendete Nachrichten
2 XX = muss vorhanden sein, X = kann vorhanden sein, leer = darf nicht vorhanden sein
3 Weitergeleitete und nachgesendete Nachrichten

3 Datenformate

Nr.	*Bezeichnung*	*Header-Name*	*Nachrichtentypen*				
			N	*B*	*M*	*I*	*W/F*
2	Eingangsbestätigung	X-de-mail-confirmation-of-receipt	XX				wie original Bestätigung wird nicht beim Eingang einer Weiterleitung, sondern nur beim Eingang einer Nachsendung erzeugt
3	Abholbestätigung	X-de-mail-confirmation-of-retrieve	XX				wie original Bestätigung wird nicht beim Eingang einer Weiterleitung, sondern nur beim Eingang einer Nachsendung erzeugt
4	Absenderbestätigt	X-de-mail-authoritative	XX				wie original
5	Persönlich	X-de-mail-private	XX	wie ori-gi-nal		XX	wie original
6	Absender-Adresse	X-de-mail-sender	XX	XX	XX	XX	wie original
7	Empfänger-Adresse(n) (auch für CC, BCC)	X-de-mail-chosen-recipient	XX	XX	XX	XX	wie original
8	Betreff	Subject	XX	XX	XX	XX	wie original
9	Nachrichten-Kennung des Absenders	X-de-mail-private-id	X	X	X		wie original
10	Antwort-Adresse	Reply-To	X	X	X	X	wie original
11	Authentisierungs-niveau	X-de-mail-auth-level	XX	X	X	X	wie original
12	Authentisierungs-Mechanismus	X-de-mail-auth-mechanism	XX	X	X	X	wie original
13	Versanddatum und -Zeit	Date	XX	XX	XX	XX	wie original
14	De-Mail-Message-ID	X-de-mail-message-id	XX	XX	XX	XX	wie original

Nr.	*Bezeichnung*	*Header-Name*	*Nachrichtentypen*				
			N	*B*	*M*	*I*	*W/F*
15	De-Mail-Server	X-de-mail-originator-provider	XX	XX	XX	XX	wie original
16	Nachrichten-Typ	X-de-mail-message-type	XX	XX	XX	XX	wie original
17	Hashwert / Signatur	X-de-mail-integrity	XX	XX	XX	XX	wie original
18	Signaturzertifikat des DMDA	X-de-mail-signature-certificate	X	XX	X	XX	wie original
19	Empfänger-Adressen für den Transport	X-de-mail-actual-recipient	XX	XX	XX	XX	XX
20	Weiterleitungs-Absender	Resent-To Resent-From Resent-Date Resent-Message-ID	X	X	X	X	
21	Weiterleitungs-nachrichten	Envelope-to	X	X	X	X	
22	Version der X-Header	X-de-mail-version	XX	XX	XX	XX	wie original
23	Vollständiger Name	X-de-mail-account-holder	XX				
24	Meldungs-nachrichtentyp	X-de-mail-notification-type			XX		
25	Absender	From	XX	XX	XX	XX	wie original
26	Message-ID	Message-ID	XX	XX	XX	XX	wie original

Tabelle 1: Übersicht der Header von De-Mail-Nachrichten

Wenn ein Header in der Nachricht doppelt vorkommt, muss der Wert des Header genommen werden, der in der Reihenfolge von oben als erstes steht.

3.1.2 X-de-mail-confirmation-of-dispatch

Dieses Feld zeigt an, ob die Versandoption „Versandbestätigung“ gesetzt wurde. Es muss auf „yes“ gesetzt werden, wenn diese Option ausgewählt wurde.

Wenn das Feld nicht gesetzt ist, wird der Wert standardmäßig auf „no“ gesetzt und entsprechend verarbeitet.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-confirmation-of-dispatch	Zeichenkette, case sensitive	„yes“, „no“

Tabelle 2: Felddefinition des Feld X-de-mail-confirmation-of-dispatch

3.1.3 X-de-mail-confirmation-of-receipt

Dieses Feld zeigt an, ob die Versandoption „Eingangsbestätigung“ gesetzt wurde. Es muss auf „yes“ gesetzt werden, wenn diese Option ausgewählt wurde.

Wenn das Feld nicht gesetzt ist, wird der Wert standardmäßig auf „no“ gesetzt und entsprechend verarbeitet.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-confirmation-of-receipt	Zeichenkette, case sensitive	„yes“, „no“

Tabelle 3: Felddefinition des Feld X-de-mail-confirmation-of-receipt

3.1.4 X-de-mail-confirmation-of-retrieve

Dieses Feld zeigt an, ob die Versandoption „Abholbestätigung“ gesetzt wurde. Es muss auf „yes“ gesetzt werden, wenn diese Option ausgewählt wurde.

Wenn das Feld nicht gesetzt ist, wird der Wert standardmäßig auf „no“ gesetzt und entsprechend verarbeitet.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-confirmation-of-retrieve	Zeichenkette, case sensitive	„yes“, „no“

Tabelle 4: Felddefinition des Feld X-de-mail-confirmation-of-retrieve

3.1.5 X-de-mail-authoritative

Dieses Feld zeigt an, ob die Versandoption „Absenderbestätigt“ gesetzt wurde. Es muss auf „yes“ gesetzt werden, wenn diese Option ausgewählt wurde.

Wenn das Feld nicht gesetzt ist, wird der Wert standardmäßig auf „no“ gesetzt und entsprechend verarbeitet.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-authoritative	Zeichenkette, case sensitive	„yes“, „no“

Tabelle 5: Felddefinition des Feld X-de-mail-authoritative

3.1.6 X-de-mail-private

Dieses Feld zeigt an, ob die Versandoption „Persönlich“ gesetzt wurde. Es muss auf „yes“ gesetzt werden, wenn diese Option ausgewählt wurde.

Wenn das Feld nicht gesetzt ist, wird der Wert standardmäßig auf „no“ gesetzt und entsprechend verarbeitet.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-private	Zeichenkette, case sensitive	„yes“, „no“

Tabelle 6: Felddefinition des Feld X-de-mail-private

3.1.7 X-de-mail-sender

Dieses Feld muss die vom Absender gewählte De-Mail-Adresse enthalten, von der die Nachricht versendet wird.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-sender	E-Mail-Adresse gemäß RFC 2822 „addr-spec“	De-Mail-Adresse gemäß [TR DM ACM FU]

Tabelle 7: Felddefinition des Feld X-de-mail-sender

3.1.8 X-de-mail-chosen-recipient

Dieses Feld muss die vom Absender gewählten Empfänger-Adressen, an die die Nachricht versendet wird, beinhalten. Mehr als die BCC-Adresse des jeweiligen BCC-Empfängers darf nicht auf der Empfänger-Seite in den Metadaten enthalten sein.

Dies ist ein strukturiertes Headerfeld mit der Syntax[4]

X-de-mail-chosen-recipient = [FWS] „to“ / „cc“ / „bcc“ [FWS] “=“ [FWS] address-list[5] [FWS] [“;” X-de-mail-chosen-recipient]

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-chosen-recipient	X-de-mail-chosen-recipient	Jedes Strukturelement „to“, „cc“ und „bcc“ darf nicht mehr als einmal verwendet werden.

Tabelle 8: Felddefinition des Feld X-de-mail-chosen-recipient

Falls keine Empfänger in der Nachricht für cc bzw. bcc vorhanden sind, dürfen diese nicht enthalten sein.

Bei der Verwendung von BCC-Empfängern müssen Sonderregeln beachtet werden:

Weil die unter „to” und „cc“ aufgeführten Empfänger der Nachricht keine Kenntnisse der BCC-Empfänger haben dürfen, muss die Nachricht mehrfach für den Versand erstellt werden. Dabei ist zu beachten, dass der Hashwert und die Signatur für die Nachrichten mehrfach berechnet und erstellt werden muss. Gleiches gilt auch für die Versandbestätigung, da dort der Hashwert der Nachricht festgehalten wird.

Die Empfänger können ebenfalls im Format der [RFC 2822] "name-addr" Notation genutzt und verarbeitet werden.

4 ABNF-Notation gemäß RFC 2234
5 Mehrfachbelegung mit „;“ getrennten De-Mail-Adresse

3.1.9 X-de-mail-auth-level

Dieses Feld bezeichnet das Authentisierungsniveau, dem der genutzte Authentisierungsmechanismus zum Zeitpunkt der Erstellung der Nachricht zugeordnet ist.

Feldname	*Feldwertsyntax*	*mögliche Werte*
X-de-mail-auth-level	RFC 2822 „unstructured“	[„normal“, „high“]

Tabelle 9: Felddefinition des Feld X-de-mail-auth-level

3.1.10 X-de-mail-auth-mechanism

Dieses Feld muss die Bezeichnung des Authentisierungsmechanismus beinhalten, mit dem der Absender sich zum Zeitpunkt des Versendens der Nachricht am De-Mail-Konto angemeldet hat.

Diese Spezifikation legt keine Werte für dieses Feld fest.

Feldname	*Feldwertsyntax*	*mögliche Werte*
X-de-mail-auth-mechanism	RFC 2822 „unstructured“	

Tabelle 10: Felddefinition des Feld X-de-mail-auth-mechanism

3.1.11 X-de-mail-originator-provider

Dieses Feld muss eine eindeutige Bezeichnung des De-Mail-Servers beinhalten, der diese Metadaten erstellt.

Feldname	*Feldwertsyntax*	*mögliche Werte*
X-de-mail-originator-provider	RFC 2822 „domain-part“	FQDN (Full qualified domain name) des DMDA-Servers

Tabelle 11: Felddefinition des Feld X-de-mail-originator-provider

3.1.12 X-de-mail-message-type

Dieses Feld muss den Nachrichtentyp einer Nachricht beinhalten. Innerhalb des PVD sind De-Mail-Nachrichten, Bestätigungs- und Meldungsnachrichten sowie Ident-Bestätigungsnachrichten vorgesehen.

Folgende Nachrichtentypen sind in dieser Fassung der Spezifikation definiert:

Typ	*Bedeutung*
normal	Normale De-Mail-Nachricht
confirmation of dispatch	Versandbestätigung
confirmation of receipt	Eingangsbestätigung
confirmation of retrieve	Abholbestätigung
malware-acknowledge	Bestätigungsnachricht im Falle von gefundener Schadsoftware

malware-notification	Meldungsnachricht im Falle von gefundener Schadsoftware
notification	Meldungsnachricht
identification	Ident-Bestätigungsnachricht (siehe [TR DM ID FU])

Tabelle 12: Wertdefinitionen des Feld X-de-mail-message-type

Feldname	***Feldwertsyntax***	***mögliche Werte***
X-de-mail-message-type	RFC 2822 unstructured	gemäß Tabelle 12, Spalte “Typ”

Tabelle 13: Felddefinition des Feld X-de-mail-message-type

3.1.13 X-de-mail-integrity

In diesem Feld sind die beiden logischen Header-Felder „Hashwert“ und „Signatur des DMDA“ abgebildet.

Dieses Feld muss in jeder Nachricht durch den DMDA gesetzt werden. Es muss ein Header nach DomainKeys Identified Mail (DKIM) Signatures [RFC 6376] enthalten sein.

Nachrichten mit der Versandoption „Absenderbestätigt“ müssen gemäß [RFC 6376] signiert werden. Alle anderen Nachrichten können signiert werden.

Die Metadaten, über die der Hashwert erstellt wurde, werden nach Versand durch den Postfachdienst des Absenders im Kontrollfluss des PVD nicht verändert. Über den Hashwert können Integritätsverletzungen erkannt werden.

Als Hashalgorithmus muss eine in [TR 02102] empfohlene Hashfunktion verwendet werden.

Die Erstellung und Prüfung des Hashwerts und der Signatur sind in Abschnitt 3.1.21 ausführlich beschrieben.

Feldname	***Feldwertsyntax***	***mögliche Werte***
X-de-mail-integrity	RFC 2822 unstructured	gemäß RFC 6376

Tabelle 14: Felddefinition des Feld X-de-mail-integrity

3.1.14 X-de-mail-signature-certificate

Dieses Feld muss durch den DMDA gesetzt werden, falls das Feld DKIM-Signature eine Signatur enthält (siehe Abschnitt 3.1.13).

Der Inhalt des Feldes muss das Zertifikat zur qualifizierten elektronischen Signatur der Metadaten enthalten. Das Zertifikat muss im Format X.509 [RFC 5280] als BASE64-Text eingetragen werden.

Feldname	*Feldwertsyntax*	*mögliche Werte*
X-de-mail-signature-certificate	RFC 2822 „unstructured“	Base64 kodiertes X.509-Zertifikat

Tabelle 15: Felddefinition des Feld X-de-mail-signature-certificate

3.1.15 X-de-mail-actual-recipient

Dieses Feld muss die tatsächlichen Empfänger-Adressen vom Postfach-Dienst beinhalten.

Bei Weiterleitungen und Nachsendungen müssen die Empfänger-Adressen umgeschrieben werden. Im Initial-Zustand müssen diese Adressen denen von X-de-mail-chosen-recipient entsprechen.

Feldname	*Feldwertsyntax*	*mögliche Werte*
X-de-mail-actual-recipient	x-de-mail-chosen-recipient	Jedes Strukturelement „to“, „cc“ und „bcc“ darf nicht mehr als einmal verwendet werden

Tabelle 16: Felddefinition des Feld X-de-mail-actual-recipient

3.1.16 X-de-mail-version

Dieses Feld muss mit derjenigen Version der Technischen Richtlinie gefüllt werden, nach der das System zertifiziert ist.. Es dient dazu, bei einer späteren Weiterentwicklung erkennen zu können, nach welchen Spezifikationen die Nachricht erstellt wurde.

Feldname	*Feldwertsyntax*	*mögliche Werte*
X-de-mail-version	RFC 2822 „unstructured“	1.0, 1.1, 1.2, 1.7

Tabelle 17: Felddefinition des Feld X-de-mail-version

3.1.17 X-de-mail-private-id

Dieses Feld dient dem Absender dazu, eine Zuordnung einer versendeten Nachricht zu einer Bestätigungsnachricht durchführen zu können.

Das Feld kann durch den Versender der Nachricht gesetzt werden. Der DMDA darf das Feld nicht verändern.

Wenn für die Nachricht eine Bestätigungsnachricht erstellt wird, muss das Feld in die Bestätigungsnachricht übernommen werden.

Diese Spezifikation legt keine Werte für dieses Feld fest.

Die Länge des Feldes beträgt maximal 1024 Zeichen.

Feldname	*Feldwertsyntax*	*mögliche Werte*
X-de-mail-private-id	RFC 2822 „unstructured“	

Tabelle 18: Felddefinition des Feld X-de-mail-private-id

3.1.18 X-de-mail-message-id

Dieses Feld enthält für jede Nachricht eine eindeutige Identifikationnummer. Der DMDA muss sicherstellen, dass diese eine Nachricht eindeutig identifizierbar macht.

Das Feld Message-ID aus [RFC 2822] kann mit dem gleichen Wert gefüllt werden.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-message-id	RFC 2822 „unstructured“	

Tabelle 19: Felddefinition des Feld X-de-mail-message-id

3.1.19 X-de-mail-account-holder

Das Feld enthält bei nat. Personen den Namen und die Vornamen bzw. nur das Pseudonym bei Pseudonymadressen und bei Institutionen den Namen oder die Bezeichnung des Kontoinhabers.

Das Feld ist bei allen normalen De-Mails zu setzen.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-account-holder	RFC 2822 „unstructured“	

Tabelle 20: Felddefinition des Feld X-de-mail-account-holder

3.1.20 X-de-mail-notification-type

Dieses Feld enthält eine Typbezeichnung für eine Meldungsnachricht. Das Feld wird nur in Meldungsnachrichten gefüllt.

Feldname	*Feldwertsyntax*	*Werte*
X-de-mail-notification-type	RFC 2822 „unstructured“	

Tabelle 21: Felddefinition des Feld X-de-mail-notification-type

Jede Meldungsnachricht muss genau einen der folgenden Nachrichtentypen enthalten:

Typ	*Bedeutung*
unknown-recipient	Unbekannter Empfänger
closed-account	Geschlossenes Konto
invalid-format	Ungültiges Format der De-Mail
other	Sonstige Meldungsnachricht (der Anlass erschließt sich aus dem Text der Nachricht)

Tabelle 22: Wertdefinitionen des Feld X-de-mail-notification-type

3.1.21 Berechnung von Hashwert und Signaturen

Die Berechnung des Hashwerts und einer Signatur muss unmittelbar vor der Übergabe der Nachricht an den Versanddienst erfolgen. Die Nachricht muss zu diesem Zeitpunkt die folgenden Bedingungen erfüllen:

1. Alle Metadaten sind gesetzt.
2. Sofern die Nachricht nicht an einen BCC-Empfänger gesendet wird, sind alle BCC-Angaben aus den Metadaten X-de-mail-chosen-recipient entfernt, andernfalls enthält das Feld die BCC-Angabe des Empfängers dieser Blindkopie.
3. Alle Header-Zeilen sind gemäß der Längenbeschränkungen von [RFC 2822] „gefoldet".
4. Alle Zeilen enden mit CR LF.
5. Alle Header-Zeilen und der Nachrichten-Body sind gemäß [RFC 2045]-[RFC 2049] (MIME) bzw. [RFC 3851] (S/MIME) Encoding normalisiert.

Für die Erstellung der DKIM-Signatur müssen folgende Parameter verwendet werden:

- Der Parameter „c" (Kanonisierung) muss als Wert „simple/simple" verwenden.
- Der Parameter „l" (Body-Length) darf nicht verwendet werden. Falls dieser vorhanden ist, muss der Wert ignoriert werden.
- Der Parameter „a" (Hash- und Signaturalgorithmus) muss wie folgt gefüllt werden:
    - für Nachrichten, die signiert werden: [Hashalgorithmus]/[Signaturalgorithmus]
    - für Nachrichten, die gehasht werden: [Hashalgorithmus][6]
    - Für den Hashalgorithmus gem. [RFC 5754] müssen folgende Schreibweisen verwendet werden:
        - sha256
        - sha384
        - sha512
    - Für die Signaturalgorithmen müssen folgende Schreibweisen verwendet werden:
        - rsa für RSA gem. [RFC 5754] (RSASSA-PKCS1-v1_5)
        - ec-dsa für ECDSA gem. [RFC 5754]
        - rsassa-pss für RSASSA-PSS gem. [RFC 4056]
    - Der DMDA muss die Prüfung all dieser Algorithmen unterstützen. Es dürfen nur Algorithmen eingesetzt werden, die den Vorgaben aus [TR-03116-4] entsprechen.
- Der Parameter „q" muss mit dem Wert „x-header/x-de-mail-signature-certificate" gefüllt werden, wenn eine Signatur gebildet wird.
- Der Parameter „b" enthält, wenn die Nachricht signiert wird, den Wert der Signatur gemäß [RFC 6376]. Wenn die Nachricht nicht signiert wird, enthält der Parameter den Hashwert (vgl.

6 Dies soll die Unterscheidung, ob eine Nachricht signiert ist oder nur ein Hashwert berechnet wurde, insbesondere bei der Prüfung vereinfachen.

header-hash in [RFC 6376]), der in die Signaturberechnung gemäß [RFC 6376] eingegangen wäre.

- Die Hashwertberechnung muss über die Headerfelder (Parameter „h“) in der folgend beschriebenen Reihenfolge erfolgen:
    - From
    - Date
    - Message-ID
    - Subject
    - Reply-To
    - X-de-mail-confirmation-of-dispatch
    - X-de-mail-confirmation-of-receipt
    - X-de-mail-confirmation-of-retrieve
    - X-de-mail-authoritative
    - X-de-mail-private
    - X-de-mail-sender
    - X-de-mail-chosen-recipient
    - X-de-mail-auth-mechanism
    - X-de-mail-auth-level
    - X-de-mail-originator-provider
    - X-de-mail-message-type
    - X-de-mail-version
    - X-de-mail-private-id (falls vorhanden)
    - X-de-mail-message-id
    - X-de-mail-account-holder
- Wenn ein Header, der in die Signatur einfließt, doppelt vorhanden sein sollte, wird der erste von oben benutzt. Alle weiteren müssen ignoriert werden.

Der Ablauf der Hashwertberechnung muss, wie in [RFC 6376] beschrieben, mit den zuvor erwähnten Parametern erfolgen.

Die Prüfungen der DKIM-Signatur weicht von [RFC 6376] ab. Für die Prüfung des Signaturwerts muss das Zertifikat und der darin enthaltene öffentliche Schlüssel aus dem Feld X-de-mail-signature-certificate genutzt werden. Dieses Zertifikat muss auf Gültigkeit geprüft werden. Der Bezug des öffentlichen Schlüssels darf nicht wie in [RFC 6376] über das DNS erfolgen. Wenn das Feld X-de-mail-signature-certificate nicht vorhanden ist, muss lediglich der Hashwert verglichen werden (vgl. Beschreibung des Parameter „b“).

3.1.22 Envelope-to

Beim Empfang einer Nachricht müssen alle bereits vorhandenen envelope-to-Header entfernt werden. Danach muss der Header Envelope-to erneut gesetzt werden und mit der SMTP-Informationen rcpt-to, der die eigentliche Empfangsadresse des Postfachs enthält, gefüllt werden.

3.2 Automatische Weiterleitung von Nachrichten

Es müssen die folgenden weiteren Headerfelder nach RFC 2822 hinzugefügt werden, um den Empfänger über die Weiterleitung zu informieren:

- Resent-To
- Resent-From
- Resent-Date
- Resent-Message-ID

Das Feld X-de-mail-Actual-Recipient muss die neue Empfangsadresse enthalten. Der Inhalt der Nachricht und die in der Signatur enthaltenen Header dürfen nicht verändert werden.

Das Feld „To" der Nachricht, die weitergeleitet wird, darf nicht verändert werden.

3.3 Nachsendung von Nachrichten

Bei der Nachsendung einer Nachricht muss in das Feld X-de-mail-Actual-Recipient die neue Empfangsadresse eingetragen werden. Der Inhalt der Nachricht und die in der Signatur enthaltenen Header dürfen nicht verändert werden.

3.4 Body

Der Content eines Nachrichten-Bodys muss MIME-konform (RFC 2045-2049) sein. Besondere strukturelle Anforderungen bestehen für:

- Bestätigungsnachrichten (siehe Abschnitt 3.5)
- Meldungsnachrichten (siehe Abschnitt 3.5)
- Ident-Bestätigungsnachrichten (vgl. [TR DM ID IO])

3.4.1 Präsentation und Signatur besonderer Nachrichtentypen

Für die folgenden Nachrichtentypen gelten besondere Vorschriften zum Nachrichtenbody:

- Bestätigungsnachrichten (siehe Abschnitt 3.5)
- Meldungsnachrichten (siehe Abschnitt 3.5)
- Ident-Bestätigungsnachrichten (vgl. [TR DM ID IO]),

Inhaltlich muss die Nachricht zum einen als XML-Struktur gemäß den spezifischen Vorgaben dieses Moduls verfasst werden. Zum anderen muss eine PDF-Datei mit einer inhaltsgleichen Darstellung der in den XML-Strukturen enthaltenen Informationen erzeugt werden. Beide

Darstellungsformen der Nachricht müssen in einer MIME-Entity vom Typ „multipart/mixed“ zusammengefasst werden, die schließlich gemäß Abschnitt 3.1.21 signiert werden muss.

Ident-Bestätigungsnachrichten müssen darüber hinaus in der XML-Darstellung eine weitere qualifizierte Signatur gemäß XML-DSig-Standard enthalten, die erhalten bleibt, wenn diese XML-Strukturen zur automatisierten Weiterbearbeitung extrahiert werden.

3.5 Bestätigungs- und Meldungsnachrichten

Bestätigungs- und Meldungsnachrichten müssen in der nachfolgend beschriebenen XML-Struktur erzeugt werden.

3.5.1 Bestätigungsnachricht

Bestätigungsnachrichten müssen durch den ausstellenden DMDA qualifiziert elektronisch signiert werden.

Das Header-Feld `x-de-mail-messagetype` muss mit dem für die Bestätigungsnachricht entsprechenden Nachrichtentyp gefüllt werden.

Die Absender-Adresse der Bestätigungsnachricht muss die entsprechende System-Adresse (vgl. [TR DM ACM FU]) sein.

Der Betreff der Nachricht muss für Versandbestätigungen wie folgt lauten:

```
*Versandbestätigung* [Betreff der zu bestätigenden Nachricht]
```

Der Betreff der Nachricht muss für Eingangsbestätigungen wie folgt lauten:

```
*Eingangsbestätigung* [Betreff der zu bestätigenden Nachricht]
```

Der Betreff der Nachricht muss für eine Abholbestätigung wie folgt lauten:

```
*Abholbestätigung* [Betreff der zu bestätigenden Nachricht]
```

Die Versand- und Eingangsbestätigung müssen folgende Daten enthalten:

- Adresse des Absenders
- Adresse des Empfängers
- Datum und Zeit des Versands oder des Eingangs
- Name des DMDAs
- Hashwert der versendeten Nachricht (vollständiger Inhalt des Header-Feld x-de-mail-integrity)

Die Abholbestätigung muss folgende Daten enthalten:

- Adresse des Absenders
- Adresse des Empfängers
- Datum und Zeit des Eingangs (Zeitpunkt, an dem die Nachricht im Postfach eingegangen ist)
- Datum und Zeit der Anmeldung (Zeitpunkt, an die Abholbestätigung erzeugt wird)
- Name des DMDAs

- Hashwert der versendeten Nachricht (vollständiger Inhalt des Header-Feld x-de-mail-integrity)

Die Versand- und Eingangsbestätigungsnachricht selbst kann folgenden Text enthalten:

```
Hiermit wird bestätigt, dass die Nachricht mit den folgenden Angaben [an
den Empfänger versandt / im Postfach des Empfängers abgelegt] wurde.


Absender:       [Adresse des Absenders]
Empfänger:      [Adresse des Empfängers]
Datum:          [[Tag].[Monat].[Jahr] [Stunde]:[Minute]]
Betreff:        [Betreff]
Nachrichten-ID: [X-de-mail-message-id]
Prüfsumme:      [X-de-mail-integrity]


Die Bestätigung erfolgte durch [Name des Provider] [Link auf Seite des
Provider]
```

Für Versand- und Eingangsbestätigungen ist jeweils der entsprechende Text auszuwählen. Bei den Adressen ist die verwendete De-Mail-Adresse des Absenders und des Empfängers einzutragen.

Die Abholbestätigungsnachricht selbst kann folgenden Text enthalten:

```
Hiermit wird bestätigt, dass sich der Empfänger der Nachricht mit den
folgenden Angaben an seinem De-Mail-Konto sicher angemeldet hat.


Zeitpunkt des Eingangs der Nachricht:      [Tag].[Monat].[Jahr] [Stunde]:
[Minute] Uhr
Absender:       [Adresse des Absenders]
Empfänger:      [Adresse des Empfängers]
Datum:          [[Tag].[Monat].[Jahr] [Stunde]:[Minute]] Uhr
Betreff:        [Betreff]
Nachrichten-ID: [X-de-mail-message-id]
Prüfsumme:      [X-de-mail-integrity]


Die Bestätigung erfolgte durch [Name des Provider] [Link auf Seite des
Provider]
```

Für die Abholbestätigungen ist jeweils der entsprechende Text auszuwählen. Bei den Adressen ist die verwendete De-Mail-Adresse des Absenders und des Empfängers einzutragen.

Eine Bestätigungsnachricht muss einen XML-Anhang mit den folgenden Elementen beinhalten:

Elementname	***Datentyp***	***Länge***	***Bedeutung***
Subject	xs:string	unbegrenzt	Gemäß [TR DM PVD FU] ist der Betreff aus dem

Elementname	*Datentyp*	*Länge*	*Bedeutung*
			Text: [Bestätigungsart]: Betreff der ursprünglichen Nachricht zu bilden.
Text	xs:string	unbegrenzt	Dieser Text enthält Informationen über die Bestätigung.
Metadata			Die Metadaten der Nachricht, auf die sich die Bestätigungsnachricht bezieht, sind gemäß [TR DM PVD FU] in der Bestätigungsnachricht wiederzugeben (Details siehe unten).
Hash	xs:string	unbegrenzt	Hash-Wert der Nachricht (Metadatum Nr. 14), so wie er in der Originalnachricht enthalten gewesen ist.
Time	xs:dateTime		Zeitpunkt der Erstellung der Bestätigungsnachricht.
DeliveryTime	xs:dateTime		Optional: Nur bei der Abholbestätigung zu setzen. Enthält den Zeitpunkt, in dem die Nachricht im Postfach eingegangen ist.
Sender	xs:string	unbegrenzt	Aussteller der Bestätigungsnachricht (De-Mail-Adresse).
Signature	ds:signature		Bestätigungsnachrichten sind gemäß [TR DM PVD FU] qualifiziert zu signieren. Dazu wird abermals eine XML-Signatur angebracht, die sich in diesem Fall auf das Nachrichtenelement „Bestätigungsnachricht“ bezieht, das das Signaturfeld enthält.

Tabelle 23: Elemente der Bestätigungsnachricht

Die Metadaten der ursprünglichen Nachricht werden übernommen. Dieses Element enthält die Elemente des Typs „Metadate“, der alle Metadaten-Headerzeilen der Originalnachricht (s. Tabelle 1, also insbesondere alle für die Hashwertberechnung gemäß Abschnitt 3.1.21 benötigten Header) wie folgt wiedergibt:

Elementname	*Datentyp*	*Länge*	*Bedeutung*
Name	xs:string	unbegrenzt	Header-Feldname (siehe Abschnitt 3.1)
Value	xs:string	unbegrenzt	Wert des Header-Feldes in der Orginalnachricht, in normalisierter Darstellung (folding white space entfernt)
OriginalHeader	xs:string	unbegrenzt	Die original Header-Zeile der Originalnachricht in der Form, wie sie empfangen wurde. Folding white space ist noch enthalten. Dieser String war Grundlage der Hashwert- und der Signatur-Berechnung für die Originalnachricht.

Tabelle 24: Metadaten der Bestätigungsnachricht

3.5.2 Meldungsnachrichten

Das Header-Feld `x-de-mail-notification-type` muss mit dem für die Meldungsnachricht entsprechenden Nachrichtentyp gefüllt werden.

Die Absender-Adresse der Meldungsnachricht muss die entsprechende System-Adresse (vgl. [TR DM ACM FU]) sein.

Eine Meldungsnachricht muss die folgenden Elemente beinhalten:

Elementname	*Datentyp*	*Länge*	*Bedeutung*
Subject	xs:string	unbegrenzt	Text, der die Art der Meldung widerspiegelt und den Bezug zum auslösenden Ereignis ermöglicht
Text	xs:string	unbegrenzt	Weitergehende Erläuterungen der Meldung
Time	xs:dateTime		Sekundengenauer Zeitpunkt der Erstellung der Meldung
Sender	xs:string	unbegrenzt	Eindeutiger Name des ausstellenden DMDA

Tabelle 25: Elemente der Meldungsnachricht

3.5.3 XML-Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema

  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  targetNamespace="urn:de-mail"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">
  <xs:import
```

```
    namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-
schema.xsd" />
  <xs:element name="Acknowledge-Message">
    <xs:annotation>
      <xs:documentation></xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Sender" type="xs:string" />
        <xs:element name="Metadata">
          <xs:complexType>
            <xs:sequence maxOccurs="unbounded">
              <xs:element name="Metadate">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="Name" type="xs:string"/>
                    <xs:element name="Value" type="xs:string"/>
                    <xs:element name="OriginalHeader"
type="xs:string" />
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="Subject">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:string" />
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
        <xs:element name="Text">
          <xs:complexType>
            <xs:simpleContent>
```

```
                <xs:extension base="xs:string" />
              </xs:simpleContent>
            </xs:complexType>
          </xs:element>
          <xs:element name="Hash" type="xs:string" />
          <xs:element name="Time" type="xs:dateTime" />
          <xs:element name="DeliveryTime" type="xs:dateTime" minOccurs="0"
/>
          <xs:element ref="ds:Signature" />
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="Notification-Message">
      <xs:annotation>
        <xs:documentation></xs:documentation>
      </xs:annotation>
      <xs:complexType>
        <xs:sequence>
          <xs:element name="Subject" type="xs:string" />
          <xs:element name="Text" type="xs:string" />
          <xs:element name="Time" type="xs:dateTime" />
          <xs:element name="Sender" type="xs:string" />
        </xs:sequence>
      </xs:complexType>
    </xs:element>
</xs:schema>
```

3.6 Export und Import

Zur Übertragung von Nachrichten von einem De-Mail-Konto in ein anderes De-Mail-Konto muss der Nutzer die Möglichkeit haben, Nachrichten zu exportieren und wieder zu importieren. Dabei müssen die Nachrichten beim Export in einer Textdatei im mbox-Format exportiert werden können.

Das mbox-Format ist grundlegend im Appendix 1 des [RFC 4155] definiert. Der Import und Export mit dem Ersetzen von `From_`muss nach der QMAIL-Spezifikation[7] erfolgen.

Neben dem Export im mbox-Format ist der Export für einzelne Nachrichten im plain-text-Format gemäß RFC 2822 mit allen Headern, Nachrichten-Body und Anhängen zu ermöglichen. Eine Prüfung der Integrität muss möglich sein.

7 http://web.archive.org/web/20080213071326/http://www.qmail.org/man/man5/mbox.html

Beim Import der Nachricht ist die `From` Zeile nicht auf inhaltliche Übereinstimmung mit dem Nachrichten-Header zu prüfen, deshalb sind die enthaltenen Daten beim Export beliebig zu belegen, sie müssen nur der Spezifikation entsprechen. Beim Import werden alle in dieser Datei enthaltenen Nachrichten wieder als einzelne De-Mail-Nachrichten im Postfach des Nutzers zur Verfügung gestellt.

Die enthaltenen Nachrichten müssen [RFC 2822] entsprechen und gültige De-Mail-Nachrichten sein, damit sie wieder importiert werden können. Ansonsten ist ein Fehler auszugeben.

In einer Textdatei im mbox-Format können 0 bis *n* Nachrichten sein.

4 Versionsübersicht

Der folgende Abschnitt enthält eine Übersicht der De-Mail-Header und deren Einsatz in den bisher erstellten Versionen

Header-Feld	*1.0*	*1.1*	*1.2*	*1.7*
X-de-mail-confirmation-of-dispatch	x	x	x	x
X-de-mail-confirmation-of-receipt	x	x	x	x
X-de-mail-confirmation-of-retrieve	x	x	x	x
X-de-mail-authoritative	x	x	x	x
X-de-mail-private	x	x	x	x
X-de-mail-sender	x	x	x	x
X-de-mail-chosen-recipient	x	x	x	x
Subject	x	x	x	x
X-de-mail-private-id	x	x	x (Längenbegrenzung eingeführt)	x
Reply-To	x	x	x	x
X-de-mail-auth-level	x	x	x	x
X-de-mail-auth-mechanism	x	x	x	x
Date	x	x	x	x
X-de-mail-message-id	x	x	x	x
X-de-mail-originator-provider	x	x	x	x
X-de-mail-message-type	x	x	x	x

Bundesanzeiger
Herausgegeben vom Bundesministerium der Justiz
www.bundesanzeiger.de
Bekanntmachung
Veröffentlicht am Dienstag, 29. März 2022
BAnz AT 29.03.2022 B3
Seite 25 von 26

Header-Feld	*1.0*	*1.1*	*1.2*	*1.7*
X-de-mail-integrity	x	x	x	x
X-de-mail-signature-certificate	x	x	x	x
X-de-mail-actual-recipient	x	x	x	x
Resent-To Resent-From Resent-Date Resent-Message-ID	x	x	x	x
Envelope-to	x	x	x	x
X-de-mail-version	1.0	1.1	1.2	1.7
X-de-mail-account-holder		x	x	x
X-de-mail-notification-type			x	x
From	x	x	x	x
Message-ID	x	x	x	x

Tabelle 26: Versionsübersicht

Bundesanzeiger
Herausgegeben vom Bundesministerium der Justiz
www.bundesanzeiger.de
Bekanntmachung
Veröffentlicht am Dienstag, 29. März 2022
BAnz AT 29.03.2022 B3
Seite 26 von 26