Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Accountmanagement Funktionalitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 2.1
Version:	1.6

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 beinhaltet die funktionalen Spezifikationen des Accountmanagements und ist Bestandteil von [TR DM ACM M].

2 Identitätskonzept

Es wird innerhalb der De-Mail-Dienste zwischen zwei Ausprägungen von Identitäten unterschieden:

- natürliche Personen
- Institutionen[1]

Für beide Ausprägungen muss jeweils ein minimales Set von hinreichend charakterisierenden Attributen durch den DMDA vor Eröffnung eines De-Mail-Kontos zuverlässig erfasst und registriert werden. Dieses minimale Set wird als Identitätsattribute bezeichnet.

Ein Identitätsbezeichner im De-Mail-Verbund ist die De-Mail-Adresse.

2.1 De-Mail-Adressen

Die De-Mail-Adresse setzt sich wie folgt zusammen: Nutzer-Teil@Domänen-Teil

2.1.1 Nutzerteil

Für natürliche Personen kann der Nutzerteil der Adresse auf folgende Arten gebildet werden:

- <Vorname(n)>.<Nachname>[.<Nummer>]
- <Künstlername / Ordensname>[.<Nummer>]

Der Nachname muss in der Adresse enthalten sein. Wenn der Nachname länger als 62 Zeichen ist, wird dieser nach dem 62. Zeichen abgeschnitten und das erste Zeichen des Vornamens inkl. Punkt vorangestellt. Soll eine Nummer angehängt werden, wird der Nachname um die notwendige Anzahl an Zeichen gekürzt.

Die Verwendung des Vornamens ist verpflichtend. Der Nutzer kann einen oder mehrere Vornamen wählen oder eine Abkürzung wählen. Die Abkürzungen sind beginnend mit dem Anfangsbuchstaben und in der äquivalenten Folge der Buchstaben des jeweiligen Vornamens zu wählen. Es muss sich um einen Vornamen bzw. Teil des Vornamens handeln, der in dem Identifikationsdokument ausgewiesen wurde. Wenn kein Vorname bei der Identifizierung festgestellt wurde, kann dieser entfallen. In diesem Fall wird das Feld mit dem Wert „---“ gefüllt. Dies wird nicht mit in die De-Mail-Adresse aufgenommen und auch nicht im ÖVD angezeigt. Alternativ kann das Feld für den Vornamen mit der leeren Zeichenkette „“ gefüllt werden, die dann als dem Wert „---“ gleichwertig gilt. In beiden Fällen besteht der Nutzerteil der Adresse ausschließlich aus dem erfassten Nachnamen, ggf. gefolgt von einer Nummer: <Nachname>[.<Nummer>].

Die Nummer ist optional. Die Nummer wird jedoch bei Mehrfachvergabe des gleichen Namens erforderlich und kann dann vom Nutzer frei wählbar sein.

Für Institutionen gibt es keine Vorgaben bei dem Nutzerteil, da diese selbst für die Verteilung der Adressen zuständig ist.

1 Unter dem Begriff „Institution“ werden hier juristische Personen, Personengesellschaften und öffentliche Stellen zusammengefasst.

Neben der vom DMDA zugeordneten primären De-Mail-Adresse kann der DMDA dem Nutzer die Möglichkeit geben, weitere sogenannte pseudonyme De-Mail-Adressen zu beantragen bzw. zu nutzen. Die Bildung einer pseudonymen De-Mail-Adresse erfolgt nach folgender Namenskonvention:

- pn_<Bezeichnung>

Es muss als Pseudonym jede Bezeichnung genutzt werden können, die bei dem entsprechenden DMDA noch nicht einer anderen Identität zugeordnet ist. Alle aus moralischen, ethischen oder politischen Gründen nicht akzeptablen Namen sind dabei auszuschließen. Auch dürfen die reservierten System-Adressen nicht als Bezeichnung von pseudonymen De-Mail-Adressen verwendet werden. Die entsprechende Black-List führt der DMDA. Des Weiteren darf das Zeichen „.“ innerhalb der Bezeichnung nicht vorkommen.

2.1.2 Domänenteil

Der Domänenteil besteht aus einer Domäne, die durch den DMDA ausschließlich für De-Mail genutzt wird.

Mehrere DMDA können sich auf die Verwendung einer DMDA-Domäne einigen und diese gemeinsam anmelden und verwenden. Diese wird als DMDA-Sammeldomäne bezeichnet.

Jeder DMDA muss seine DMDA-Domäne, DMDA-Sammeldomäne oder Unterdomäne der Sammeldomäne „de-mail.de“ bei der zuständigen Behörde im Rahmen der Akkreditierung anmelden. DMDAs mit eigener DMDA-Domäne oder DMDA-Sammeldomäne können daneben zusätzlich die Sammeldomäne „de-mail.de“ nutzen.

Es besteht die Möglichkeit Domänen unterhalb einer DMDA-Domäne, DMDA-Sammeldomäne oder Domänen unterhalb von „de-mail.de“ für verschiedene Marken anzumelden, wenn der DMDA den Nutzen begründet darlegen kann. Dies kann z. B. der Fall sein, wenn der DMDA unter verschiedenen Marken, unterschiedliche Nutzergruppen erreichen möchte. Die Zulassung, ein Angebot unter mehreren Domänen anzubieten, obliegt dem BSI.

Die DMDA sind für die Verwaltung ihrer eigenen DMDA-Domänen oder DMDA-Sammeldomäne verantwortlich. Die Berechtigungen zum Zugriff auf die Verwaltung der Sammeldomäne „de-mail.de“ erteilt das BSI.

Die DMDA dürfen die DMDA-Domäne oder DMDA-Sammeldomänen auch nach der Einstellung der Tätigkeit als DMDA nicht für andere Email-Dienste nutzen.

Es wird angestrebt, dass auch Institutionen und Privatpersonen eigene Second-Level-Domänen für De-Mail beantragen können, sofern diese ausschließlich für De-Mail genutzt werden. Gegenwärtig wird geprüft, ob und ggfs. wie diese Nutzung umgesetzt werden kann. Dafür sind zusätzliche Konzepte/Infrastrukturkomponenten erforderlich, die noch erarbeitet werden müssen. Sobald umsetzungsfähige Konzepte vorliegen, soll die Technische Richtlinie nach Anhörung des Ausschusses De-Mail-Standardisierung gem. § 18 De-Mail-Gesetz entsprechend erweitert werden.

Die Domäne setzt sich wie folgt zusammen:

<local-part>@<4th-Level>.<3rd-Level-Domain>.<2nd-Level-Domain>.<Top-Level-Domain>

Der <local-part> wird für natürliche Personen in Abschnitt 2.1.1. geregelt. Institutionen können den <local-part> in ihrem Verantwortungsbereich frei vergeben.

Institutionen müssen und natürliche Personen können eine <3rd-Level-Domain> erhalten. Bei der Auswahl der Bezeichnung muss ein direkter Bezug zur natürlichen Person oder der Institution hergestellt werden können. Weitere Untergliederungen sind möglich.

2.1.2.1 Beispiele

DMDA-Domäne

Natürliche Personen	<vorname>.<nachname>@<Domäne des DMDA>
	Erika.mustermann@dmda-a.example
	<vorname>.<nachname>@<name>.<Domäne des DMDA>
	Erika.mustermann@mustermann.dmda-a.example
Institutionen	<local-part>@<Institution>.<Domäne des DMDA>
	poststelle@institution.dmda-a.example

DMDA-Sammeldomäne

Natürliche Personen	<vorname>.<nachname>@<DMDA>.<Sammeldomäne>
	Erika.mustermann@dmda-a.dmda-sammeldomäne.example
	<vorname>.<nachname>@<Name>.<Sammeldomäne>
	Erika.mustermann@mustermann.dmda-sammeldomäne.example
Institutionen	<local-part>@(<Abteilung/Standort>.)[2]<Institution>.<Sammeldomäne>
	poststelle@standort_A.institution.dmda-sammeldomäne.example

De-Mail-Domäne

Natürliche Personen	<vorname>.<nachname>@<DMDA>.< de-mail.de>
	Erika.mustermann@dmda-a.de-mail.de
	<vorname>.<nachname>@<Name>.< de-mail.de>
	Erika.mustermann@mustermann.de-mail.de
Institutionen	<local-part>@(<Abteilung/Standort>.)[3]<Institution>.< de-mail.de>

2 optional

3 optional

	poststelle@standort_A.institution.de-mail.de

2.1.3 Abbildungsregeln für De-Mail-Adressen

Folgende allgemeine Regelungen zur Bildung der De-Mail-Adresse für natürliche Personen einerseits und Institutionen andererseits sind zu beachten:

- Bei dem Nutzerteil von primären De-Mail-Adressen natürlicher Personen:

  Innerhalb eines Typs werden unterschiedliche Bestandteile, die im Identifikationsdokument mit einem Leerzeichen getrennt werden, mit „_“ (Unterstrich) getrennt, z.B. beim Vornamen „wilhelm_joachim“. Das Trennzeichen „-„(Hyphen) im Vor- oder Nachnamen wird auch in die Adresse übernommen.
- De-Mail-Adressen müssen im Format RFC 2822[4] gewählt werden.
- Es muss die Empfehlung gemäß RFC 5321[5] beachtet werden, dass der Nutzerteil maximal 64 Zeichen aufweisen darf.
- Der Domainname darf maximal 189 Zeichen lang sein.
- Die gesamte Adresse darf eine maximale Länge von 253 Zeichen nicht überschreiten
- Zeichen des Alphabets müssen als Kleinbuchstaben genutzt werden.

Die Übersetzungsregeln für Sonderzeichen in ASCII-Zeichen sind im Dokument [ICAO-MRTD] definiert. Die im ICAO-Dokument existierenden Empfehlungen sind verpflichtend zu nutzen und identisch auf Kleinbuchstaben anzuwenden.

2.1.4 System-Adressen des DMDA

Von den De-Mail-Adressen für natürliche Personen und Institutionen sind die System-Adressen abzugrenzen. System-Adressen sind spezielle für den Betrieb von De-Mail-Diensten unterhalb einer DM-Domain reservierte Adressen. Diese Adressen unterliegen nicht den besonderen Formatvorgaben einer De-Mail-Adresse für natürliche Personen oder Institutionen.

Die Adresse wird nach folgendem Format gebildet:

<Bezeichnung>@<De-Mail-Domäne>

Die zu nutzenden Bezeichnungen sind in den jeweiligen Funktionalitätsspezifikationen der De-Mail-Dienste definiert (siehe [TR DM ID FU], [TR DM IT-BInfra FU], [TR DM PVD FU], [TR DM DA FU]). Beispiele sind Absender-Adressen für vom DMDA erzeugte Nachrichten, wie z. B. für Versand-, Eingangs- oder Abholbestätigungen.

2.2 Identitäten natürlicher Personen und Institutionen

Jedes De-Mail-Konto wird genau einer Identität zugeordnet. Die Identität wird über Identitätsattribute beschrieben, die verpflichtend aufgenommen werden.

4 IETF-Standard
5 IETF-Standard

2.2.1 Identität natürlicher Personen

Im Folgenden werden die Identitätsattribute genannt, die durch den DMDA im Rahmen der Erstregistrierung aufgenommen und zuverlässig verifiziert werden müssen.

Attribut	*Bemerkungen*
Vorname	Ist ein Rufname innerhalb der Identifikationsdokumente definiert, kann auch ausschließlich dieser aufgenommen werden.
Nachname	inkl. Adelstitel, kann auch der Familienname oder Lebenspartnerschaftsname sein.
Geburtsdatum	
Geburtsort	
Straße und Hausnummer	Hauptwohnsitz[6]
Wohnort	Inkl. Ortsteil, wenn vorhanden (mit „–“ vom Ort abgetrennt)
Postleitzahl	
Staat	In dem sich der Wohnort befindet

Tabelle 1: Pflicht-Identitätsattribute natürlicher Personen

Neben den Pflichtattributen können folgende Attribute aufgenommen werden:

Attribut	*Bemerkung*
Titel	Akademischer Grad. Eine Verwendung des Titels in der De-Mail-Adresse ist nicht möglich.
Ordensname/Künstlername	Nur bei Nutzung des Ordensnamens bzw. Künstlernamens innerhalb der primären De-Mail-Adresse muss der Ordensname bzw. der Künstlername im Identifikationsdokument eingetragen sein..

Tabelle 2: Optionale Identitätsattribute natürlicher Personen

Die Verifikation der optionalen Identitätsattribute ist nur notwendig, sofern diese sich auf die primäre De-Mail-Adresse auswirken (Verwendung des Ordens- oder Künstlernamens).

Wenn die Attribute nicht zuverlässig ermittelt wurden, dürfen diese nicht in den De-Mail-Diensten verwendet werden.

2.2.2 Identität von Institutionen

Im Folgenden werden die Identitätsattribute genannt, die durch den DMDA im Rahmen der Erstregistrierung aufgenommen und verifiziert werden müssen.

Attribut	*Bemerkungen*
Name / Bezeichnung	Beinhaltet auch die Kurzform der Institution (z.B. GmbH, AG, GbR, AöR), wenn diese vorhanden ist.

6 im melderechtlichen Sinne

Attribut	*Bemerkungen*
Straße und Hausnummer und / oder Postfach	Sitz oder Hauptsitz
Ort	Sitz oder Hauptsitz
Staat	Sitz oder Hauptsitz
Rechtsform	Sitz oder Hauptsitz
Art des Registers	Soweit vorhanden
Registerort	Soweit vorhanden
Registernummer	Soweit vorhanden
Berechtigung zur Nutzung Versandoption „Abholbestätigung“	Bei öffentlichen Stellen, die formell zustellen dürfen.
Namen der Mitglieder des Vertretungsorgans oder der gesetzliche Vertreter	
Firma, Name oder Bezeichnung, Rechtsform, Art des Registers, Registerort, Registernummer (soweit vorhanden) und Anschrift des Sitzes oder Hauptsitzes	Falls ein Mitglied des Vertretungsorgans oder der gesetzlichen Vertreter eine juristische Person ist.

Tabelle 3: Identitätsattribute juristischer Personen

2.3 Verifikation von Identitätsattributen

Die verpflichtenden Identitätsattribute müssen zuverlässig festgestellt und verifiziert werden. Für jedes Identitätsattribut wird der Zeitpunkt der letzten Verifikation gespeichert.

Während der gesetzlichen Aufbewahrungsfristen müssen die Daten zur Verifikation der Identitätsattribute verfügbar sein. Der DMDA muss sicherstellen, dass Integrität und Authentizität der Daten mindestens während dieser Zeit sichergestellt sind.

Von einer zuverlässigen Feststellung der Identitätsattribute ist dann auszugehen, wenn:

- die Angaben des Nutzers im Antrag zur Identifizierung mit den Angaben in den anerkannten Dokumenten (vgl. 2.3.1 und 2.3.2) übereinstimmen und
- bei natürlichen Personen der Vergleich des Lichtbildes im Ausweisdokument mit der zu identifizierenden Person übereinstimmt.

Die Neuerfassung oder Änderung von Identitätsattributen muss durch den Nutzer beantragt werden. Die Änderungen dürfen nur durch den berechtigten Nutzer beantragt werden können und müssen dokumentiert werden.

Es muss durch den DMDA eine Prüfung bzw. ein Abgleich der Daten erfolgen, die einerseits bei der Identifizierung erfasst werden und andererseits den Daten, die im System gespeichert wurden. Bei einer manuellen Erfassung der Daten im System muss die Prüfung der Daten durch verschiedene Personen erfolgen (Vier-Augen-Prinzip). Bei einer Online-Erfassung (z. B. eID-

Funktion des neuen Personalausweises) darf eine automatische Prüfung stattfinden. Vorher darf keine Übernahme der Daten in bzw. Freigabe der Daten für De-Mail-Dienste erfolgen.

Identitätsattribute müssen anhand des Originaldokuments oder beglaubigter Abschriften durch den DMDA selbst oder durch im Unterauftrag stehende vertrauenswürdige Dritte überprüft worden sein, bevor sie freigeschaltet werden dürfen. Sofern elektronische Registerdaten verwendet werden, ist ebenfalls eine sorgfältige Verifikation und Dokumentation durch den DMDA sicherzustellen.

Die Feststellung kann erfolgen durch

- Mitarbeiter des DMDA,
- vertrauenswürdige Dritte (unter Einbindung in das Sicherheitskonzept),
- mittels der eID-Funktion des neuen Personalausweises.

2.3.1 Feststellung bei natürlichen Personen

Der DMDA muss sich vergewissern, dass die erhobenen Daten korrekt sind. Bei natürlichen Personen müssen die Identitätsattribute

a) anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, insbesondere anhand eines inländischen oder nach ausländerrechtlichen Bestimmungen anerkannten oder zugelassenen Passes, Personalausweises oder Pass- oder Ausweisersatzes,

b) anhand von Dokumenten, die bezüglich ihrer Sicherheit einem Dokument nach Buchstabe a gleichwertig sind,

c) anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes,

d) anhand einer qualifizierten elektronischen Signatur oder

e) anhand sonstiger geeigneter technischer Verfahren mit gleichwertiger Sicherheit zu einer Identifizierung anhand der Dokumente nach Buchstabe a

überprüft werden.[7]

In Fall c) ist sicherzustellen, dass die vom Zertifizierungsdiensteanbieter erfassten Identitätsdaten sicher an den DMDA übermittelt werden.

In Fall e) ist die gleichwertige Sicherheit durch den DMDA nachzuweisen. Dazu ist eine vollumfängliche Beschreibung des Verfahrens und eine ausführliche Risikobetrachtung zu erstellen.

2.3.2 Feststellung bei Institutionen

Bei Institutionen müssen die Identitätsattribute

a) anhand eines Auszugs aus dem Handels- oder Genossenschaftsregister oder aus einem vergleichbaren amtlichen Register oder Verzeichnis,

b) anhand der Gründungsdokumente,

c) anhand von Dokumenten, die bezüglich ihrer Beweiskraft den Dokumenten nach den Buchstaben a oder b gleichwertig sind, oder

d) durch Einsichtnahme in die Register- oder Verzeichnisdaten

7 Gemäß § 3 De-Mail-Gesetz

überprüft werden.[8]

Für die Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter gelten die Vorgaben aus Abschnitt 2.3.1 zur Identifikation einer natürlichen Personen entsprechend. Wenn ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine Institution ist, so gelten für diese ebenfalls die Regeln zur Feststellung aus diesem Abschnitt.

Bei Institutionen darf der zu erbringende Nachweis nicht älter als 1 Monat sein.

Als Identitätsbestätigungen können folgende Nachweise, die vom Antragsteller beizubringen sind, erbracht werden.

Für eingetragene Gesellschaften:

Institutionen	*Art der Identitätsbestätigung*
GmbH, AG, oHG, KG, etc.	Handelsregisterauszug (Papierform oder wenn möglich elektronisch)
Partnerschaftsgesellschaft	Partnerschaftsregisterauszug (Papierform oder wenn möglich elektronisch)
eG	Genossenschaftsregisterauszug (Papierform oder wenn möglich elektronisch)
eV	Vereinsregisterauszug (Papierform oder wenn möglich elektronisch)

Tabelle 4: Identitätsbestätigungen bei eingetragenen Gesellschaften

Für nicht eingetragene Gesellschaften:

Institutionen	*Art der Identitätsbestätigung*
Freiberuflich Selbstständige	Selbstauskunft oder Steuerbescheinigung über freiberufliche/Selbständige Einkünfte
GbR	Selbstauskunft oder Vertrag
Gewerbetreibende	Selbstauskunft oder Gewerbeanmeldung des Gewerbetreibenden
Rechtsanwälte, Architekten etc.	Selbstauskunft oder Verbands- oder Kammerbestätigung
Handwerker	Selbstauskunft oder Bestätigung der relevanten berufsständigen wirtschaftspolitischen Vereinigung (z.B. Handwerkskammer)

Tabelle 5: Identitätsbestätigungen bei nicht eingetragenen Gesellschaften

Für öffentliche Stellen:

8 Gemäß § 3 De-Mail-Gesetz

Institutionen	*Art der Identitätsbestätigung*
Ministerien des Bundes und der Länder	Richtet sich nach der jeweiligen Gemeinsamen Geschäftsordnung der Bundes- bzw. jeweiligen Landesministerien (GGO der Bundesministerien z.B. §§ 6, 17 und 18; Zeichnungsvollmacht zur analogen Anwendung der Vertretungsvollmacht); ggf. mit Vorlage einer Urkunde mit Siegel
Sonstige Behörden des Bundes und der Länder	Analog GGO
Gemeinden, Kommunen etc.	Gemeindeordnung für Gebietskörperschaften bzw. entsprechende zur Identifizierung geeignete Dokumente

Tabelle 6: Identitätsbestätigungen bei öffentlichen Stellen

3 De-Mail-Konto

Ein De-Mail-Konto ist genau einer Identität zugeordnet. Die Identität wird im Rahmen des Registrierungsprozesses zuverlässig erfasst.

Zu einem De-Mail-Konto werden unter anderem folgende Daten gespeichert:

- Identitätsdaten des Nutzers
- Informationen zur Authentifizierung
- De-Mail-Adresse
- De-Mail-Domain (bei Institutionen verpflichtend/bei natürlichen Personen optional)
- Pseudonym-Adressen (nur bei natürlichen Personen)

3.1 An- und Abmeldung am De-Mail-Konto

Bei der Anmeldung an dem De-Mail-Konto muss sich der Nutzer authentisieren. Der DMDA muss hierfür zwei Authentisierungsniveaus anbieten:

- Normal
- Hoch[9]

Das Authentisierungsniveau „normal“ entspricht der Benutzung von Benutzername und Passwort. Die Speicherung des Passwortes beim DMDA darf dabei nicht in einem in Klartext wiederherstellbaren Format erfolgen.

Das Authentisierungsniveau „hoch“ setzt Verfahren voraus, die folgende Anforderungen erfüllen:

- Zwei-Faktor-Authentisierung (Besitz und Wissen)
- Schutz vor unberechtigter Kopie des Wissens
- Einmaligkeit der zur Authentisierung eingesetzten Daten (z.B. Einmal-Passwort)

Der DMDA ist verpflichtet, mindestens zwei Verfahren für das Authentisierungsniveau „hoch“ anzubieten. Ein Verfahren muss dabei die eID-Funktion des neuen Personalausweises sein.

Sollte durch den DMDA ein Authentisierungstoken für das Authentisierungsniveau „hoch“ zur Verfügung gestellt werden, hat dessen Übergabe so zu erfolgen, dass ein Missbrauch ausgeschlossen werden kann.

Bei der Authentifizierung wird durch den DMDA geprüft, ob:

- die Authentisierungsdaten korrekt sind,
- das Authentisierungstoken nicht gesperrt ist,
- das Konto nicht (temporär) gesperrt ist (vgl. 3.6.1 und 3.6.2) und
- bei der Verwendung des Authentisierungsniveaus „normal“ die Anforderungen an das Passwort eingehalten werden (vgl. [TR DM ACM Si]).

9 entspricht der „sicheren Anmeldung“ gemäß § 4 De-Mail-Gesetz

Der DMDA muss sich gegenüber dem Nutzer authentisieren, bevor dieser vom DMDA authentifiziert werden kann. Die Authentisierungen erfolgen ausschließlich über vertrauenswürdige Verbindungen (gemäß [TR DM IS GS] bzw. [TR DM IS 27001]).

Nach einer erfolgreichen Authentisierung des Nutzers wird der Nutzer zum Zugriff auf die von ihm gewählten De-Mail-Dienste und Daten durch den DMDA autorisiert.

Für den Fall, dass für eine Nachricht im Postfach des Nutzers durch eine öffentliche Stelle eine Abholbestätigung verlangt wurde, ist sicherzustellen, dass diese ausschließlich versendet wird, wenn der Nutzer sich erfolgreich mit dem Authentisierungsniveau „hoch“ angemeldet hat [TR DM PVD FU].

Der Nutzer muss sich jederzeit von der Nutzung des De-Mail-Kontos abmelden können. Dabei werden die Autorisierungen zur Nutzung der Dienste und der Daten durch den DMDA entzogen.

3.2 Übersicht zu den Zuständen eines Kontos

Das Einrichten eines De-Mail-Kontos umfasst

- die Beantragung in Form einer Antragstellung,
- die Reservierung einer gewünschten De-Mail-Adresse,
- die Erfassung in Form einer Registrierung mit Identitätsfeststellung und
- die Freigabe zur Nutzung des De-Mail-Kontos.

Diese Schritte werden auch als Erstregistrierung bzw. initiale Registrierung eines De-Mail-Kontos bezeichnet. Nachdem das De-Mail-Konto freigeschaltet ist, kann es durch seinen Nutzer genutzt werden. Im weiteren Verlauf muss das De-Mail-Konto gesperrt oder aufgelöst werden können.

3.3 Beantragung eines De-Mail-Kontos

3.3.1 Antrag auf Eröffnung eines De-Mail-Kontos

Bei der Antragstellung werden in einem Antrag die folgenden Daten erfasst:

- die Identitätsattribute für die natürliche Person oder die Institution,
- die gewünschte De-Mail-Adresse,
- der gewünschte De-Mail-Konto-Name (Benutzername für die Anmeldung – kann automatisch vergeben werden),
- die Auswahl des Standard-Authentisierungsniveaus,
  - standardmäßig „hoch“,
  - kann auf „normal“ durch den Nutzer geändert werden,
- optional: die pseudonyme De-Mail-Adressen (nur für natürliche Personen),
- optional: ein Entsperrpasswort,
- optional: die Einwillung zur Veröffentlichung von De-Mail-Kontodaten im ÖVD. Der DMDA darf den Nutzer nicht verpflichten, seine Daten in den ÖVD einzutragen,

- optional: Zugangseröffnung im Sinne von §3a Verwaltungsverfahrensgesetz, §36a Absatz 1 des Ersten Buches Sozialgesetzbuch und des §87a Absatz 1 Satz 1 der Abgabenordnung.

3.3.2 Aufklärungs- und Informationspflichten

Der DMDA hat den Nutzer vor der erstmaligen Nutzung des De-Mail-Kontos entsprechend der gesetzlichen Aufklärungs- und Informationspflichten zu unterrichten.

Dabei sind diesem die erforderlichen Informationen in Textform mitzuteilen, deren Erhalt und Kenntnisnahme wiederum in Textform zu bestätigen sind.

3.4 Reservierung

Durch den DMDA erfolgt die Prüfung, ob der gewünschte De-Mail-Konto-Name und die gewünschte De-Mail-Adresse/De-Mail-Domain verfügbar sind.

Eine beantragte **De-Mail-Adresse** ist verfügbar, wenn

- sie nicht temporär für einen anderen Antragsteller reserviert wurde,
- sie nicht in einem Zeitraum von 30 Jahren – bei Pseudonym-Adressen 1 Jahr – für eine andere natürliche Person in der Vergangenheit freigeschaltet war und
- sie nicht zum aktuellen Zeitpunkt verwendet wird. Dies betrifft primäre und pseudonyme De-Mail-Adressen bei dem DMDA.

Eine beantragte **De-Mail-Domain** ist verfügbar, wenn

- sie nicht temporär für einen anderen Antragsteller reserviert wurde,
- sie nicht in einem Zeitraum von 30 Jahren für eine andere natürliche Personen bzw. von einem Jahr für eine andere Institution in der Vergangenheit freigeschaltet war und
- sie nicht zum aktuellen Zeitpunkt verwendet wird.

Sind der De-Mail-Konto-Name und die De-Mail-Adresse verfügbar, erfolgt die Reservierung des De-Mail-Kontos mit dem gewählten De-Mail-Konto-Namen und der De-Mail-Adresse, mit der Folge, dass kein anderer Antragsteller diese reservieren kann.

Die Reservierung des De-Mail-Konto-Namens, der De-Mail-Adresse oder der De-Mail-Domain kann durch den DMDA gelöscht werden, wenn

- der Antragsteller die Reservierung zurückzieht oder
- 6 Kalenderwochen nach der Reservierung die Anforderungen an die Freischaltung nicht erfüllt wurden.

Der De-Mail-Konto-Name, die De-Mail-Adresse oder die De-Mail-Domäne ist danach wieder frei verfügbar und kann dann auch durch einen anderen Nutzer reserviert werden.

Bei der Erstellung der De-Mail-Adressen beim DMDA ist darauf zu achten, dass die Konventionen für die Namensbildungen eingehalten werden (vgl. 2.1)

3.5 Freischaltung

Eine Nutzung der De-Mail-Dienste ist erst nach Freischaltung des De-Mail-Kontos durch den DMDA möglich.

Nach der Freigabe muss das De-Mail-Konto uneingeschränkt genutzt werden können.

3.6 Sperrung

Es können drei unterschiedliche Sperrarten für ein De-Mail-Konto definiert werden:

- vollständige Sperrung
- Zugangssperre
- Nutzungseinschränkung

Der DMDA muss eine telefonisch jederzeit erreichbare Sperrhotline zur Annahme von Sperranträgen, deren Prüfung und Veranlassung der Sperrung vorhalten, bei der eine unverzügliche Sperrung möglich ist.

3.6.1 Vollständige Sperrung

Im Falle einer vollständigen Sperrung sind das De-Mail-Konto und die Dienste nicht nutzbar. Eine Anmeldung am De-Mail-Konto ist nicht möglich.

Der Empfang von Nachrichten ist nicht möglich. Eintragungen im ÖVD sind mit Sperrung zu löschen.

3.6.2 Zugangssperre

Die Zugangssperre schränkt den Zugang für ein Authentisierungsniveau ein. Dabei ist nur die Authentisierung in Bezug auf das in der Sperrung definierte Authentisierungsniveau eingeschränkt.

Der Empfang von Nachrichten ist weiterhin möglich.

Bei mehrfacher Falscheingabe der Authentisierungsdaten durch den Nutzer ist eine Zugangssperre vorzunehmen. In diesem Fall kann die Zugangssperre auch temporär erfolgen. Nach spätestens drei nacheinander erfolgten Eingaben eines falschen Authentisierungsdatums erfolgt mindestens eine temporäre Zugangssperre. Während einer temporären Zugangssperre wird der Nutzer - auch mit den korrekten Authentisierungsinformationen - nicht zum Zugriff auf das De-Mail-Konto autorisiert. Die Entsperrung einer temporären Zugangssperre erfolgt nach einer vom DMDA festzulegenden Zeitspanne automatisch. Die Zeitspanne der temporären Zugangssperre ist mit jeder weiteren Zugangssperre zu erhöhen. Eine Überführung einer temporären Zugangssperre in eine nicht-temporäre Zugangssperre kann nach mehreren aufeinanderfolgenden temporären Zugangssperren vorgenommen werden.

Ein weiteres Beispiel für eine Zugangssperre liegt beim Authentisierungsniveau „hoch“ dann vor, wenn das Authentisierungstoken verloren geht oder das Authentisierungsverfahren insgesamt Mängel aufweist, die eine unbemerkte Fälschung oder Kompromittierung ermöglicht.

3.6.3 Nutzungseinschränkung

Der Nutzer wird in der Auswahl der verfügbaren Funktionen der Dienste eingeschränkt.

Das De-Mail-Konto kann nur zum Abrufen von Nachrichten oder zum Herunterladen von Dokumenten in der Dokumentenablage durch den Nutzer verwendet werden. Ein aktives Versenden von Nachrichten, die Beauftragung einer Ident-Karte oder das Ändern bzw. Hinzufügen von Dokumenten in der Dokumentenablage ist nicht möglich. Das De-Mail-Konto des Nutzers ist hierbei durch die De-Mail-Dienste weiterhin adressierbar.

Diese Sperrart kann bei einer Vertragsverletzung durch den Nutzer vorgesehen werden, z.B. bei Verzug mit der Zahlung des Nutzungsentgeltes.

3.7 Entsperrung

Eine Sperrung des De-Mail-Kontos kann durch eine Entsperrung wieder aufgehoben werden. Vor einer Entsperrung müssen die Gründe für die Sperrung beseitigt worden sein. Die Entsperrung ist mit der erneuten Freischaltung des De-Mail-Kontos abgeschlossen. Der DMDA hat dem Nutzer nach Wegfall des Sperrgrundes den Zugang zum De-Mail-Konto erneut zu gewähren.

Zum Entsperren eines De-Mail-Kontos sind die folgenden Möglichkeiten zu schaffen:

- Entsperren durch DMDA nach Wegfall des Sperrgrunds (z. B. neuer Authentisierungstoken)
- Entsperren durch den Nutzer selbst bei der Zugangsperre „normal“, nachdem er sich mit dem Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet und die Sperre aktiv aufgehoben hat, z. B. durch Ändern des Authentisierungsmerkmals für das Authentisierungsniveau „normal“.

Weiterhin können folgenden Möglichkeiten geschaffen werden:

- Entsperren durch den Nutzer selbst bei der Zugangssperre, nachdem er ein vom DMDA definiertes Entsperrpasswort korrekt angegeben hat. Die Nutzung eines Entsperrpasswortes muss eingeschränkt sein (z.B. Anzahl der Fehlversuche). Das Entsperrpasswort kann bei der Registrierung oder zu einem späteren Zeitpunkt festgelegt werden.
- Entsperrung durch den DMDA nach Beendigung einer temporären Sperrung bei der Zugangssperre für das Authentisierungsniveau „normal“. Der Fehlbedienungszähler wird dabei nur dann zurückgesetzt, wenn nach Auflösung der temporären Sperrung eine erfolgreiche Authentifizierung des Nutzers erfolgte.

3.8 Vertragsbeendigung und Auflösung

3.8.1 Einstellen der Tätigkeit

Der DMDA muss die betroffenen Nutzer unverzüglich über die Einstellung seiner Tätigkeit benachrichtigen und über die Folgen aufklären. Zusätzlich ist die Zustimmung der Nutzer zur Übernahme des De-Mail-Kontos einschließlich Dokumentation durch einen anderen DMDA einzuholen. Übernimmt kein anderer DMDA das De-Mail-Konto, ist sicherzustellen, dass die im Postfach und in der Dokumentenablage gespeicherten Daten für mindestens drei Monate ab dem Zeitpunkt der Benachrichtigung des Nutzers abrufbar bleiben.

3.8.2 Vertragsbeendigung

Mit der Vertragsbeendigung unterliegt das De-Mail-Konto einer Sonderform der Nutzungseinschränkung.

Dem Nutzer ist für einen Zeitraum von drei Monaten nach Vertragsende ein eingeschränkter Zugang zu seinem De-Mail-Konto zu ermöglichen in der Form, dass er seine im Postfach und in der Dokumentenablage gespeicherten Daten herunterladen kann. Mindestens einen Monat vor der Auflösung des De-Mail-Kontos hat der DMDA den Nutzer auf diesen Sachverhalt in Textform hinzuweisen.

Ab dem Zeitpunkt der Vertragsbeendigung ist die aktive Nutzung des De-Mail-Kontos und der Dienste nicht mehr möglich. Dies betrifft sowohl den Versand und den Empfang von De-Mails, Ident-Nachweisen als auch das Hinzufügen von Daten in der Dokumentenablage.

Daten des De-Mail-Kontos, die im ÖVD eingetragen sind, müssen zum Zeitpunkt der Vertragsbeendigung entfernt werden.

3.8.3 Auflösung eines De-Mail-Kontos

Bei der Auflösung eines De-Mail-Kontos sind alle Daten, die in dem De-Mail-Konto gespeichert sind sowie dessen Daten im ÖVD zu löschen.

In jedem Fall muss sich der DMDA von der Identität des zur Auflösung berechtigten Nutzers überzeugen.

Ein aufgelöstes De-Mail-Konto kann nicht wieder freigeschaltet werden.

Wenn derselbe Nutzer ein neues De-Mail-Konto bei demselben DMDA eröffnen möchte, kann der DMDA dem Nutzer die alte De-Mail-Adresse erneut zuordnen. Hierbei kann der DMDA eine Frist, bis zu der dies möglich ist, vertraglich vereinbaren. Nach Ablauf dieser Frist ist eine erneute Nutzung der De-Mail-Adresse erst nach Ablauf der Sperrfrist möglich.

4 Accountmanagement durch den Nutzer

Nach der Freischaltung eines De-Mail-Kontos steht dieses in vertraglichem Umfang dem Nutzer bereit.

Änderungen an den Einstellungen und Identitätsdaten des De-Mail-Kontos dürfen nur nach Anmeldung mit dem Authentisierungsniveau „hoch“ durch den Nutzer realisiert werden. Bei Anmeldung mit Authentisierungsniveau „normal“ darf weder lesender noch schreibender Zugriff auf die Identitätsdaten erfolgen können. Ausgenommen hiervon ist die Anzeige von Vorname und Name des Kontoinhabers, da diese bereits in der De-Mail Adresse abgebildet sind.

Die Änderung von Adressdaten (Straße, Hausnummer, Postfach, Ort, Staat) kann durch den Nutzer durchgeführt werden. Eine erneute Verifikation ist nicht notwendig.

Die Änderung des Namens, der Bezeichnung, des Ordensnamens oder des Künstlernamens kann ebenfalls durch den Nutzer erfolgen. Hier ist eine erneute Verifikation der geänderten Identitätsattribute zwingend erforderlich. Dazu müssen die in Abschnitt 2.3 beschriebenen Verfahren zur Verifikation verwendet werden.

Änderungen an den De-Mail-Kontodaten können Einfluss auf Daten des ÖVD haben (vgl. [TR DM IT-BInfra FU]) und müssen nachgehalten und ggf. korrigiert werden.

4.1 Zugriff auf das De-Mail-Konto

4.1.1 Änderung des Authentisierungsverfahrens

Der Nutzer muss die Möglichkeit haben, das zur Authentisierung genutzte Verfahren jederzeit zu wechseln.

Der Nutzer kann in seinem De-Mail-Konto wählen, welches Verfahren er verwenden möchte, sowie die für das Verfahren notwendigen Einstellungen vornehmen.

Wenn ein Verfahren deaktiviert wird, darf eine Authentisierung mit diesem Verfahren nicht mehr möglich sein.

Wenn keine zwei voneinander unabhängigen Sicherungsmittel mehr verwendet werden können, um das Authentisierungsniveau „hoch“ zu nutzen, ist dies in der Konfiguration des De-Mail-Kontos zu hinterlegen. Außerdem ist bei einem Eintrag im ÖVD dieser mit dem Hinweis zu versehen, dass keine Nachrichten mit der Versandoption „Persönlich“ empfangen werden können (vgl. [TR DM PVD FU] und [TR DM IT-BInfra FU]).

4.1.2 Sperrung von Authentisierungsmechanismen

Der DMDA muss die Sperrung der Verwendung von Token unterstützen, die für das Authentisierungsniveau „hoch“ genutzt werden.

Es muss bei jeder Anmeldung eine Prüfung auf Gültigkeit des Tokens erfolgen. Ein Token ist ungültig, wenn es abgelaufen oder gesperrt ist oder der Nutzer es von der weiteren Verwendung im Rahmen seines De-Mail-Kontos ausgeschlossen hat.

4.1.3 Zugriffsbeschränkung für das De-Mail-Konto

Der Nutzer muss selbst Beschränkungen für den Zugriff seines De-Mail-Kontos vornehmen können. Die Beschränkungen gelten hierbei für das gesamte De-Mail-Konto einschließlich aller

Nutzer bei einem De-Mail-Konto für Institutionen. Bei Institution gelten die Beschränkungen, die in dem De-Mail-Konto festgelegt werden, für alle Unterkonten.

Für die Auswahl, Änderung oder Löschung einer Beschränkung muss sich der Nutzer mit dem Authentisierungsniveau „hoch“ angemeldet haben.

Der Nutzer kann definieren, mit welchen Authentisierungsniveaus ein Zugriff auf sein De-Mail-Konto möglich ist. Die Beschränkung des Zugangs auf ein bestimmtes Mindestauthentisierungsniveau entspricht den Regelungen zur Zugangssperre aus dem Abschnitt 3.6.2. In diesem Fall wird die Beschränkung jedoch durch den Nutzer veranlasst.

Ein Löschen der Beschränkungen muss erfolgen können

- durch den Nutzer selbst oder
- bei technischen Problemen auf Basis eines Antrages des Nutzers auch durch den DMDA,

wobei der Nutzer erfolgreich mit Authentisierungsniveau „hoch“ authentifiziert worden sein muss.

4.1.4 Setzen und Ändern des Passworts der Authentisierungsniveaus

Der Nutzer gibt ein neues Passwort an. Dabei hat das neue Passwort identisch wiederholt erfasst zu werden, um fehlerhafte Eingaben zu vermeiden. Das alte Passwort muss ebenfalls zur Verifikation angegeben werden; bei einer Änderung des Passwortes für das Authentisierungsniveau „normal“ ist die erneute Eingabe des bestehenden Passworts entbehrlich, wenn der Nutzer mit dem Authentisierungsniveau „hoch“ angemeldet ist.

Es wird geprüft,

- ob das alte Passwort korrekt eingegeben wurde,
- ob die zweifach erfassten neuen Passworte identisch sind,
- ob das angegebene neue Passwort den Passwort-Regeln des DMDA gemäß [TR DM ACM Si] entspricht.

Der DMDA darf das genutzte Passwort nicht in einem in Klartext wiederherstellbaren Format speichern. Außer dem Nutzer darf keiner weiteren Partei das Passwort in seiner ursprünglichen Textform bekannt sein.

4.1.5 Änderung des De-Mail-Konto-Namens

Der DMDA kann dem Nutzer die Möglichkeit geben, den De-Mail-Konto-Namen, der zur Authentisierung genutzt wird, zu ändern. Bei der Änderung muss geprüft werden, ob der De-Mail-Konto-Name bereits für ein anderes De-Mail-Konto genutzt wird. Ist dies nicht der Fall, wird der De-Mail-Konto-Name dem De-Mail-Konto zugeordnet. Eine Authentisierung mit dem alten De-Mail-Konto-Namen darf danach nicht mehr möglich sein.

4.2 ÖVD

Der DMDA muss sicherstellen, dass Informationen im ÖVD ausschließlich auf ausdrückliches Verlangen des Nutzers veröffentlicht werden können (vgl. [TR DM IT-BInfra FU]).

Änderungen an den Daten im Accountmanagement müssen im ÖVD übernommen werden, wenn vorher eine Freigabe zur Veröffentlichung der geänderten Daten im ÖVD vorlag und diese nicht zurückgezogen wurde.

Der Nutzer muss im ÖVD für eine De-Mail-Adresse ein Verschlüsselungszertifikat veröffentlichen können. Bei natürlichen Personen müssen der primären Adresse und der Pseudonymadresse unterschiedliche Zertifikate zugeordnet werden können.

Bei der Veröffentlichung des Zertifikats prüft der DMDA:

- Verwendbarkeit hinsichtlich der Schlüssellänge des öffentlichen Schlüssels (vgl. [TR 02102]),
- Verwendbarkeit für die Funktion E-Mail-Verschlüsselung im Rahmen des De-Mail-Dienstes,
- Verwendbarkeit für die zum De-Mail-Konto zugeordnete De-Mail-Adresse oder Pseudonym-De-Mail-Adresse,
- Verwendbarkeit hinsichtlich Gültigkeit.

Die Verwendung selbstsignierter öffentlicher Schlüssel durch den Nutzer ist gestattet.

Der Nutzer ist darauf hinzuweisen, wenn der Gültigkeitszeitraum seines Zertifikats abgelaufen ist. Der DMDA kann das Zertifikat in einem solchen Fall aus dem ÖVD entfernen. Darüber ist der Nutzer zu informieren.

Der Nutzer kann gem. §7 Abs. 3 S. 2 ff. De-Mail-Gesetz vom Diensteanbieter verlangen, die Zustimmung für die Zugangseröffnung im Sinne von §3a Verwaltungsverfahrensgesetz, §36a Absatz 1 des Ersten Buches Sozialgesetzbuches und des §87a Absatz 1 Satz 1 der Abgabenordnung durch eine entsprechende Kennzeichnung im ÖVD zu veröffentlichen und dieses auch widerrufen.

Beim Einstellen der öffentlichen Schlüssel sollten dem Nutzer bei Fehlern oder Abweichungen von den Vorgaben sinnvolle Hinweise gegeben werden, um diese zu beheben.

4.3 Besonderheiten bei natürlichen Personen und Institutionen

4.3.1 Natürliche Personen

4.3.1.1 Änderung von primären De-Mail-Adressen

Bei Namensänderungen, die Einfluss auf die De-Mail-Adresse haben, ist eine neue De-Mail-Adresse zu vergeben. Die vorhandene Adresse kann weiterhin für den Empfang genutzt werden. Die Nachrichten können in einem gemeinsamen Postfach abgelegt werden. Der Versand von Nachrichten mit der Adresse ist nicht mehr gestattet. Der Zeitraum für den weiteren Empfang über die alte Adresse kann eingeschränkt werden.

4.3.1.2 Änderung von Pseudonym-De-Mail-Adressen

Für natürliche Personen können Pseudonym-De-Mail-Adressen angeboten werden.

Eine Pseudonym-De-Mail-Adresse darf nur einem De-Mail-Konto zugewiesen sein.

Eine Pseudonym-De-Mail-Adresse ist, nachdem sie einem De-Mail-Konto zugeordnet war und die Zuordnung aufgehoben wurde, für eine Verwendung durch eine andere natürliche Person blockiert (vgl. 3.4). Während die Adresse für eine Wiederverwendung blockiert ist, darf sie keinem anderen De-Mail-Konto zugeordnet werden können. Der Nutzer kann die Pseudonym-De-Mail-Adresse jedoch zur sofortigen Wiederverwendung durch andere natürliche Personen freigeben.

4.3.2 Institutionen

Jeder Institution wird ein De-Mail-Konto zugeordnet. Dem De-Mail-Konto müssen Unterkonten zugeordnet werden können.

Die vertretungsberechtigten natürlichen Personen einer Institution müssen weitere natürliche Personen im Rahmen der Registrierung oder auch zu einem späteren Zeitpunkt als beauftragte Personen (im Folgenden „Administratoren“ genannt) eintragen lassen können. Ein Administrator verfügt über die Rechte, das De-Mail-Konto der Institution zu verwalten, um bspw. Unterkonten für die differenzierte[10] Nutzung des De-Mail-Kontos durch Mitarbeiter anzulegen. Die Unterkonten gehören zu einer De-Mail-Adressen der Institution. Die Zuordnung der Unterkonten zu den Mitarbeitern erfolgt durch den Administrator der Institution.

Online darf die Eintragung und Löschung eines Administrators nur erfolgen, wenn sich die vertretungsberechtigte Person mit dem Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet hat. Wenn dies nicht möglich ist, müssen die Eintragung und die Freischaltung durch den DMDA erfolgen.

Die Belehrung der Mitarbeiter erfolgt durch den Kontoinhaber.

10 Die Rechte zur Nutzung der einzelnen Dienste können innerhalb der Institution eigenverantwortlich vergeben werden.

5 Dokumentationspflicht

Bei allen Funktionen im Accountmanagement, die zu Änderungen der im Rahmen einer Beantragung eines De-Mail-Kontos erfassten Attribute führen (siehe Abschnitt 3.3), müssen entsprechende Dokumentationen vorgenommen werden, um die Daten und deren Unverfälschtheit gegenüber Beteiligten darstellen zu können.

Hierbei ist sowohl eine Dokumentation hinsichtlich der De-Mail-Kontoeröffnung als auch eine Dokumentation bei der Änderung von De-Mail-Kontodaten bzw. Kontozuständen vorzunehmen.

5.1 Natürliche Personen

Die Dokumentation für die De-Mail-Kontoeröffnung beinhaltet bei natürlichen Personen mindestens folgende Angaben:

- Nachweis über die Identität des Nutzers gemäß den gesetzlichen Vorgaben, z. B. das Protokoll der Identifizierung, einschließlich ggf. vorhandener und notwendiger Prüfprotokolle,
- die beantragte De-Mail-Adresse / De-Mail-Domäne,
- ggf. die beantragte(n) Pseudonym-Adresse(n),
- das Datum der Beantragung,
- Nachweis über die gesetzlich notwendige Aufklärung und Information des Nutzers,
- die Identifizierungsdaten zum bearbeitenden Mitarbeiter des DMDA (wenn eine manuelle Bearbeitung erfolgt),
- die erfassten Antragsdaten hinsichtlich aller Identitätsattribute.

5.2 Institutionen

Die Dokumentation für die Eröffnung eines De-Mail-Kontos beinhaltet bei Institutionen mindestens folgende Angaben:

- Nachweis über die Identität des Unternehmens oder der öffentlichen Stelle
- die beantragte De-Mail-Domain,
- das Datum der Beantragung,
- der Nachweis über die gesetzlich notwendige Aufklärung und Information des Nutzers,
- die Identifizierungsdaten zum bearbeitenden Mitarbeiter des DMDA (wenn eine manuelle Bearbeitung erfolgt),
- die erfassten Antragsdaten hinsichtlich aller Identitätsattribute.

5.3 Änderungen

Die Dokumentation bei Änderungen von De-Mail-Kontodaten und Kontozuständen muss mindestens folgende Angaben enthalten:

- das betroffene De-Mail-Konto,
- die jeweilige gesetzliche Zeit der Änderung,
- die Identifizierungsdaten des Nutzers,
- die Art der Verarbeitung (automatisiert, manuell),
- die Identifizierungsdaten zum bearbeitenden Mitarbeiter des DMDA (wenn eine manuelle Bearbeitung erfolgt),
- die Art der Verwaltung (z.B. Änderung, Vertragsbeendigung, Beantragung und Aktivierung bzw. Deaktivierung eines Nachsendeauftrages, Auflösung, Hinzufügen und Ändern von Authentisierungsdaten, Identifizierung, Verifizierung, Freischaltung, Sperrung inkl. Sperrart, Entsperrung) und
- die erfassten Daten hinsichtlich der geänderten Identitätsattribute, zugeordneter De-Mail-Adressen.

5.4 Auskunftserteilung

Der Prozess zur Auskunftserteilung ist ebenfalls zu dokumentieren. Diese Dokumentation enthält:

- den Antrag zur Auskunftserteilung einschließlich des Auskunftersuchenden,
- die Entscheidung des DMDA über den Antrag zur Auskunftserteilung,
- die Identifizierungsdaten des bearbeitenden Mitarbeiters des DMDA,
- die Mitteilung des Ergebnisses an den Auskunftsersuchenden,
- die Mitteilung über die Auskunftserteilung an den betroffenen Nutzer,
- die jeweilige gesetzliche Zeit bei einzelnen Prozessen innerhalb der Auskunftserteilung.

Der DMDA hat sicherzustellen, dass der Nutzer von dem Auskunftsersuchen unverzüglich informiert werden kann.

Die Inhalte der Dokumentation zur De-Mail-Konto-Eröffnung, bei Änderungen von Kontodaten und Kontozuständen sowie die Inhalte der Dokumentation zur Auskunftserteilung müssen entsprechende der Fristen gemäß Tabelle 7: Aufbewahrungsfristen der Dokumentation aufbewahrt werden.

Der Nutzer muss jederzeit Einsicht in die ihn betreffenden Daten erhalten können.

Bereich	*Aufbewahrungsfrist*
Daten der De-Mail-Kontoeröffnung	10 Jahre nach Vertragsbeendigung
Änderungen der Identitätsdaten	10 Jahre nach Vertragsbeendigung
Daten zur Auskunftserteilung	3 Jahre nach Auskunftserteilung

Tabelle 7: Aufbewahrungsfristen der Dokumentation