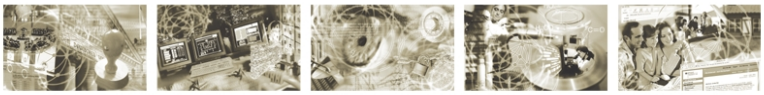
Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	De-Mail
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Die Technische Richtlinie (TR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit dem Titel „Technische Richtlinie De-Mail“ stellt das Rahmenwerk der Zertifizierung dar und beschreibt die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die De-Mail-Dienste erfüllen müssen, sowie die Anforderungen zur Prüfung dieser Eigenschaften.

Die TR ist modular aufgebaut entsprechend der in De-Mail enthaltenen Dienste und das vorliegende Dokument referenziert auf dienstspezifische Module.

2 Aufbau der Technischen Richtlinie De-Mail

Die TR De-Mail des BSI umfasst die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die De-Mail-Diensteanbieter erfüllen müssen, sowie die Anforderungen zur Prüfung dieser Eigenschaften.

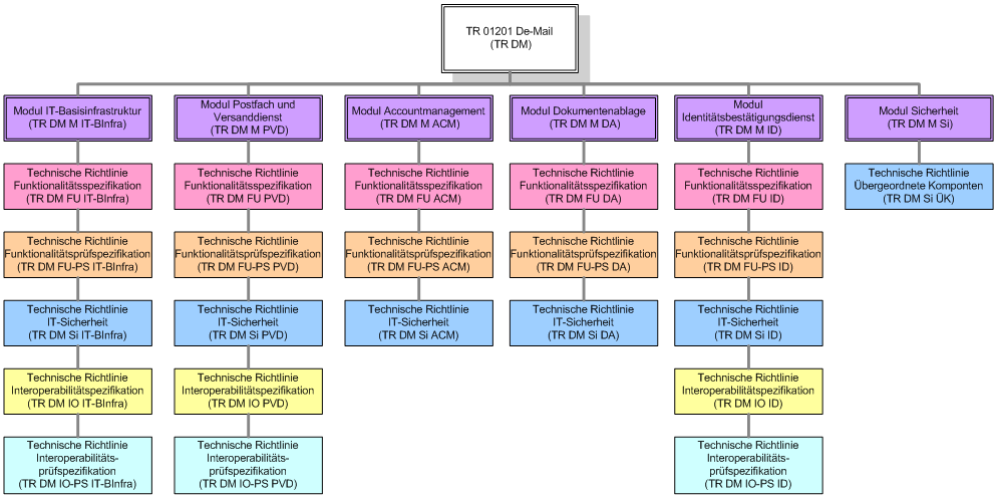


Abbildung 1: Dokumentenstruktur Technische Richtlinie De-Mail (TR DM) (vgl. Zuordnung der Bezeichnungen und der Modulnummern in Abschnitt 9)

Die TR De-Mail hat einen modularen Aufbau entsprechend der De-Mail-Dienste, die angeboten werden. Zu jedem De-Mail-Dienst gibt es ein Modul mit der Beschreibung der Anforderungen an die Funktionalität, Interoperabilität (soweit gegeben) und Sicherheit des De-Mail-Dienstes. Die Spezifikationen zur Interoperabilität beschränken sich auf die Kommunikation zwischen den DMDA und die Metadaten der Nachrichten. Bei der Implementierung der Dienste können Mehrwertdienste in den Ablauf der Verarbeitung integriert werden, insofern die Sicherheit und die Funktion nicht beeinträchtigt werden.

Weiterhin enthält jedes Modul Prüffälle. Für die De-Mail-Dienste, die eine Kommunikation zwischen verschiedenen De-Mail-Diensten umfassen, sind zu verwendende Datenstrukturen und Übertragungsprotokolle definiert.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

3 De-Mail-Dienste

3.1 Postfach- und Versanddienst (PVD)

Der PVD stellt Funktionen für das Erstellen, Versenden, Empfangen und Abrufen von Nachrichten zur Verfügung und wird im Modul [TR DM PVD M] beschrieben.

3.2 Dokumentenablage (DA)

Der DA stellt Funktionen für Upload, Download sowie zur Verwaltung und Suche von Dokumenten und Dateien zur Verfügung und wird im Modul [TR DM DA M] beschrieben.

Der Dienst ist optional und muss nicht angeboten werden.

3.3 Identitätsbestätigungsdienst (ID)

Der ID stellt Funktionen von der Erstellung eines Ident-Auftrages durch einen Nutzer bis zum Versenden einer Ident-Bestätigung an einen Service Provider über den Postfach- und Versanddienst von De-Mail zur Verfügung. Der Dienst wird im Modul [TR DM ID M] beschrieben.

Der Dienst ist optional und muss nicht angeboten werden.

3.4 Accountmanagement

Der zuverlässige Nachweis der Identität ist in der De-Mail-Konzeption unmittelbar mit dem Nutzerkonto verbunden. Das De-Mail-Konto ermöglicht den Zugang zu den De-Mail-Diensten. Sämtliches Handeln eines Nutzers in De-Mail ist unmittelbar mit dem De-Mail-Konto verbunden und lässt sich immer auf ihn zurück führen.

Das Konto Management (ACM) definiert, unter welchen Bedingungen das De-Mail-Konto eines Nutzers vom DMDA neu angelegt, freigeschaltet, gesperrt oder gelöscht werden darf. Weiterhin definiert das Konto Management, unter welchen Rahmenbedingungen ein Nutzer seine im De-Mail-Konto hinterlegten Identitätsdaten ergänzen oder ändern darf. Der Dienst wird im Modul [TR DM ACM M] beschrieben.

3.5 IT-Basisinfrastruktur

ÖVD, persönliches Adressbuch sowie IT-Basis-Dienste (Log-Informationen, Nutzung authentischer Zeitquellen und DNS) werden durch die sogenannte IT-Basisinfrastruktur den De-Mail-Diensten zur Verfügung gestellt. Der Dienst wird im Modul [TR DM IT-BInfra M] beschrieben.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

4 Interoperabilität der De-Mail-Dienste

Die Spezifikation der notwendigen Datenstrukturen, Datenformate und Transportprotokolle erfolgt für die Dienste PVD [TR DM PVD M], ID [TR DM ID M] und IT-Basisinfrastruktur [TR DM IT-BInfra M].

5 Modulübergreifende Sicherheit

Ziel des Moduls „ Sicherheit Modulübergreifend“ der TR De-Mail [TR DM Si M] ist es, die Basis für eine adäquate Absicherung der Einsatzumgebungen zu schaffen.

6 Prüfung der De-Mail-Dienste

6.1 Funktionsprüfung der De-Mail-Dienste

Nachfolgend sind Prüffälle spezifiziert, mit denen die Funktionalität von De-Mail geprüft werden kann.

Die Spezifikation der notwendigen Prüffälle erfolgt in den Modulen

- Post- und Versanddienst [TR DM PVD FU-PS],
- Identifizierungsdienst [TR DM ID FU-PS],
- IT-Basisinfrastruktur [TR DM IT-BInfra FU-PS],
- Accountmanagement [TR DM ACM FU-PS],
- Dokumentenablage [TR DM DA FU-PS].

6.2 Interoperabilitätsprüfung der De-Mail-Dienste

Die Spezifikation der notwendigen Prüffälle erfolgt in den Modulen

- Post- und Versanddienst [TR DM PVD IO-PS],
- Identifizierungsdienst [TR DM ID IO-PS],
- IT-Basisinfrastruktur [TR DM IT-BInfra IO-PS],
- Accountmanagement [TR DM ACM IO-PS],
- Dokumentenablage [TR DM DA IO-PS]

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

7 Rahmenbedingungen

In diesem Kapitel sind die Rahmenbedingungen beschrieben, die für alle Funktionen aller De-Mail-Dienste gelten.

7.1 Client-seitige Sicherheit

Im Allgemeinen kann De-Mail nur wenig Einfluss auf die Nutzerumgebung nehmen, da diese nicht im unmittelbaren Einflussbereich von De-Mail liegt. Der DMDA hat jedoch die Aufgabe, den Nutzer durch die folgenden beiden Bereichen zu unterstützen:

- Sensibilisierung und Beratung: Der Nutzer sollte wissen, welche Risiken bestehen und wie er diese Risiken vermeiden kann. Es sind sowohl technische als auch organisatorische Maßnahmen zu nennen und Hilfestellungen zur Umsetzung anzubieten.
- Technische Produktlösungen: Der De-Mail-Diensteanbieter hat für seine Nutzer entsprechende technische Komponenten zu empfehlen. Hierzu sind mindestens folgende Komponenten zu betrachten:
  - sichere Client-Lösungen,
    - Virenscanner-Produkte,
    - Personal-Firewall-Produkte,
    - Signaturerstellungs- bzw. -verifikationslösungen,
    - Ver-/Entschlüsselungslösungen,
    - Hardware-Token,
    - Chipkartenlesegeräte.

Die Anwendungskomponenten zur Nutzung der De-Mail-Dienste sollten derart gestaltet sein, dass

- eine Manipulation dieser,
- eine Nutzung durch unberechtigte Personen oder Anwendungen,
- ein Einsehen, Löschen oder Manipulation der Daten durch unberechtigte Personen oder
- das Ausführen von Schadcode über die Anwendung,

auch vom Client des Nutzers aus, möglichst nicht erfolgen kann oder durch den Nutzer selbst verhindert und bemerkt werden kann.

7.2 Unterstützung von Standard-Software

Der Zugriff auf die De-Mail soll für den Nutzer mit Standardsoftware möglich sein. Als Anwendungen bieten sich Web-Browser und E-Mail-Clients für den Postfach- und Versanddienst an. Eine Anbindung mittels einer Standardsoftware muss durch den DMDA unterstützt werden. Die Umsetzung einer Webanwendung sollte erfolgen.

7.3 Graphische Benutzeroberflächen

Die graphische Oberfläche von De-Mail-Webanwendungen ist so zu gestalten, dass sie sich durch eine einfache Bedienung auszeichnen und die Darstellung der Daten und Funktionen übersichtlich ist. Die Basisfunktionalität muss innerhalb der Darstellung der Anwendung deutlich erkennbar sein.

Die Gestaltung der Web-Oberflächen von De-Mail sollte entsprechend den Gesetzgebungen zur Barrierefreiheit (Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV)) vorgenommen werden.

7.4 Speicheranforderungen

Der DMDA hat jedem Nutzer für alle Dienste zusammen einen minimalen Speicherplatz zu gewährleisten. Welche Funktionalität trotz erschöpften Speicherplatzes unterstützt werden muss, ist in [TR DM PVD M] und [TR DM DA M] beschrieben.

Konto	***Minimaler Speicherplatz***
Natürliche Personen	100 MB
Institutionen	100 MB

Tabelle 1: Übersicht der Speicheranforderungen

7.5 Allgemeine Verfügbarkeit der Anwendung und Daten

Es ist ein Regelbetrieb von 7x24 Stunden mit hoher Verfügbarkeit vorzusehen. Die Verfügbarkeit aller Dienste darf den im Rahmen-Sicherheitskonzept (vgl. [TR DM Si M]) festgelegten Wert nicht unterschreiten.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

8 Abkürzungsverzeichnis

Es wird an dieser Stelle ein zentrales Abkürzungsverzeichnis geführt.

Abkürzung	*Beschreibung*
ACM	Accountmanagement
ALG	Application Level Gateway
BSI	Bundesamt für Sicherheit in der Informationstechnik
CSP	Crypto Service Provider
DA	Dokumentenablage
DBMS	Datenbankmanagementsystem
DM	De-Mail
DMDA	De-Mail-Diensteanbieter
DMZ	Demilitarisierte Zone
DN	Distinguished Name
DNS	Domain Name Service
Ende-zu-Ende	Ende-zu-Ende
HTTPS	Hypertext Transfer Protocol Secure
ID	Identitätsbestätigungsdienst
IT	Informationstechnik
LDAP	Lightweight Directory Access Protokoll
MESZ	Mitteleuropäische Sommerzeit
MEZ	Mitteleuropäische Zeit
nPA	neuer Personalausweis
NTP	Network Time Protocol
Ö-VD	Öffentlicher Verzeichnisdienst von De-Mail
OCSP	Online Certificate Status Protocoll
ÖVD	Öffentlicher Verzeichnisdienst des DMDA
PDF	Portable Document Format
PVD	Postfach- und Versanddienst
RZ	Rechenzentrum

SAK	(qualifizierte) Signaturanwendungskomponente
SMTP	Simple Mail Transfer Protocol
SP	Service Provider
SSEE	Sichere Signaturerstellungseinheit
SSL	Secure Socket Layer
TLS	Transport Layer Security
TR	Technische Richtlinie
URI	Universal Resource Identifier
UTC	Coordinated Universal Time
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

Tabelle 2: Abkürzungen

9 Übersicht TR-Dokumente

Nummer	*Bezeichnung*	*Titel*
BSI-TR 01201 Teil 1	TR DM IT-BInfra M	Technische Richtlinie IT-Basisinfrastruktur Modul
BSI-TR 01201 Teil 1.1	TR DM IT-BInfra FU	Technische Richtlinie IT-Basisinfrastruktur Funktionalitätsspezifikation
BSI-TR 01201 Teil 1.2	TR DM IT-BInfra FU-PS	Technische Richtlinie IT-Basisinfrastruktur Funktionalitätsprüfspezifikation
BSI-TR 01201 Teil 1.3	TR DM IT-BInfra Si	Technische Richtlinie IT-Basisinfrastruktur IT-Sicherheit
BSI-TR 01201 Teil 1.4	TR DM IT-BInfra IO	Technische Richtlinie IT-Basisinfrastruktur Interoperabilitätsspezifikation
BSI-TR 01201 Teil 1.5	TR DM IT-BInfra IO-PS	Technische Richtlinie IT-Basisinfrastruktur Interoperabilitätsprüfspezifikation
BSI-TR 01201 Teil 2	TR DM ACM M	Technische Richtlinie Accountmanagement Modul
BSI-TR 01201 Teil 2.1	TR DM ACM FU	Technische Richtlinie Accountmanagement Funktionalitätsspezifikation
BSI-TR 01201 Teil 2.2	TR DM ACM FU-PS	Technische Richtlinie Accountmanagement Funktionalitätsprüfspezifikation
BSI-TR 01201 Teil 2.3	TR DM ACM Si	Technische Richtlinie Accountmanagement IT-Sicherheit
BSI-TR 01201 Teil 3	TR DM PVD M	Technische Richtlinie Postfach- und Versanddienst Modul
BSI-TR 01201 Teil 3.1	TR DM PVD FU	Technische Richtlinie Postfach- und Versanddienst Funktionalitätsspezifikation
BSI-TR 01201 Teil 3.2	TR DM PVD FU-PS	Technische Richtlinie Postfach- und Versanddienst Funktionalitätsprüfspezifikation
BSI-TR 01201 Teil 3.3	TR DM PVD Si	Technische Richtlinie Postfach- und Versanddienst IT-Sicherheit
BSI-TR 01201 Teil 3.4	TR DM PVD IO	Technische Richtlinie Postfach- und Versanddienst Interoperabilitätsspezifikation
BSI-TR 01201 Teil 3.5	TR DM PVD IO-PS	Technische Richtlinie Postfach- und

Nummer	*Bezeichnung*	*Titel*
		Versanddienst Interoperabilitätsprüfspezifikation
BSI-TR 01201 Teil 4	TR DM ID M	Technische Richtlinie Identitätsbestätigungsdienst Modul
BSI-TR 01201 Teil 4.1	TR DM ID FU	Technische Richtlinie Identitätsbestätigungsdienst Funktionalitätsspezifikation
BSI-TR 01201 Teil 4.2	TR DM ID FU-PS	Technische Richtlinie Identitätsbestätigungsdienst Funktionalitätsprüfspezifikation
BSI-TR 01201 Teil 4.3	TR DM ID Si	Technische Richtlinie Identitätsbestätigungsdienst IT-Sicherheit
BSI-TR 01201 Teil 4.4	TR DM ID IO	Technische Richtlinie Identitätsbestätigungsdienst Interoperabilitätsspezifikation
BSI-TR 01201 Teil 4.5	TR DM ID IO-PS	Technische Richtlinie Identitätsbestätigungsdienst Interoperabilitätsprüfspezifikation
BSI-TR 01201 Teil 5	TR DM DA M	Technische Richtlinie Dokumentenablage Modul
BSI-TR 01201 Teil 5.1	TR DM DA FU	Technische Richtlinie Dokumentenablage Funktionalitätsspezifikation
BSI-TR 01201 Teil 5.2	TR DM DA FU-PS	Technische Richtlinie Dokumentenablage Funktionalitätsprüfspezifikation
BSI-TR 01201 Teil 5.3	TR DM DA Si	Technische Richtlinie Dokumentenablage IT-Sicherheit
BSI-TR 01201 Teil 6	TR DM Si M	Technische Richtlinie Sicherheit Modulübergreifend
BSI-TR 01201 Teil 6.1	TR DM Si ÜK	Technische Richtlinie Sicherheit Übergeordnete Komponenten

Tabelle 3: Übersicht TR-Dokumente

10 Literaturverzeichnis

Es wird an dieser Stelle ein zentrales Literaturverzeichnis geführt.

Bezeichnung	*Titel*
[BSI 100-1]	BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
[BSI 100-2]	BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
[BSI 100-3]	BSI-Standard 100-3: Risikoanalyse auf der Basis von IT Grundschutz
[BSI 7550]	BSI – Technische Leitlinie; Anforderungen an Zutrittskontrollanlagen
[BSI 7551]	BSI – Technische Leitlinie; Zutrittskontrollanlagen – Richtlinien für die Projektierung und Ausführung
[C-PKI]	Common PKI Specifications for interoperable Applications V1.1, 2004
[DSKritKat]	Kriterienkatalog für den Datenschutznachweis
[ETSI TS 102 231]	Electronic Signatures and Infrastructures (ESI) – Provision of harmonized Trust-service status information (Ref: RTS/ESI-000083)
[ICAO-MRTD]	ICAO – Doc 9303 Machine readable Travel Documents- Appendix 2 to Section IV 1 to Section III, Appendix 3 to Section III
[IS-Rev]	BSI, Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf der Basis von IT-Grundschutz, V2.0, Stand März 2010, www.bsi.bund.de/IS-Revision
[IT-GS Katalog]	IT-Grundschutz Katalog
[PenTest]	BSI, Durchführungskonzept für Penetrationstests, Studie, November 2003, www.bsi.bund.de/ContentBSI/Publikationen/Studien/pentest/index_htm
[Prog_Personen]	BSI, Programm zur Kompetenzfeststellung und Zertifizierung von Personen, V 2.0, 06. August 2010, www.bsi.bund.de/cln_183/ContentBSI/Themen/ZertifizierungundAnerkennung/Komformitaetsbestaetigung/Personen/personenallg.html
[Prog_Stellen]	BSI, Programm zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern, V 2.0, Stand 06. August 2010, www.bsi.bund.de/cln_174/DE/Themen/ZertifizierungundAkkreditierung/Konformitaetsbewertung/Konformitaetsbewertung_node.htm
[RFC-X509]	Internet X.509 Public Key Infrastructure Certificate and CRL Profile RFC 5280

Bezeichnung	*Titel*
[RFC1034]	P. Mockapetris RFC 1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
[RFC1035]	P. Mockapetris RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
[RFC2119]	S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, 1997
[RFC2487]	SMTP Service Extension for Secure SMTP over TLS
[RFC2782]	A. Gulbrandsen, P. Vixie, L. Esibov RFC 2782: A DNS RR for specifying the location of services (DNS SRV)
[RFC2822]	RFC 2822 Internet Message Format
[RFC3401]	M. Mealling RFC 3401: Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS
[RFC3402]	M. Mealling RCF 3402: Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm
[RFC3403]	M. Mealling RFC 3403: Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database
[RFC3404]	M. Mealling RFC 3404: Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application
[RFC3405]	M. Mealling RFC 3405: Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures
[RFC3958]	L. Daigle, A. Newton RFC 3958: Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)
[RFC4033]	DNSSEC Intro RFC (http://tools.ietf.org/html/rfc4033)
[RFC4398]	RFC 4398 „Storing Certificates in the Domain Name System (DNS)“
[RFC4871]	RFC 4871 Domain Keys Identified Mail
[RFCSMIME]	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1, RFC 3851
[SAML-CORE20]	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005

Bezeichnung	*Titel*
[TLS10]	The TLS Protocol Version 1.0, RFC 2246
[TLS11]	The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346
[TLS12]	The Transport Layer Security (TLS) Protocol Version 1.1, RFC 5246
[TR 02102]	BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
[VB_Personen]	BSI, Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen, V 2.0, Stand 06. August 2010, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Personen_V2_0.pdf?__blob=publicationFile
[VB_Stellen]	BSI, Verfahrensbeschreibung zur Anerkennung von Prüstellen und Zertifizierung von IT-Sicherheitsdienstleistern, V 2.0, 06. August 2010, www.bsi.bund.de/Shared.ocs/Downloads/DE/BSI/Zertifizierung/VB-Stellen_V2_0.pdf?__blob=publicationFile
[WebAppSec]	Sicherheit von Webanwendungen, Maßnahmenkatalog und Best Practices
[XAdES]	ETSI TS 101 903 XAdES
[XML Signatur]	XML-Signature Syntax and Processing, W3C, 2002, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/ sowie RFC3275
[Zert ISO 27001]	Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits

Tabelle 4: Literaturverzeichnis

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	IT-Basisinfrastruktur Modul
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 1
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

1 Einleitung

Dieses Modul beschreibt die Struktur der IT-Basisinfrastruktur. Das Modul ist Bestandteil der [TR DM].

Die De-Mail-Dienste PVD, DA sowie ID und auch die Funktionen des Accountmanagements rufen ihrerseits Funktionen der IT-Basisinfrastruktur auf, um ihre fachspezifischen Aufgaben zu erfüllen.

Zu den IT-Basisinfrastruktur-Diensten gehören:

- der ÖVD
- das persönliche Adressbuch,
- der DNS,
- der Zeitdienst,
- der Protokollierungsdienst

2 Dokumentenübersicht

2.1 Funktionale Anforderungen

Die funktionalen Anforderungen an die IT-Basisinfrastruktur werden in [TR DM IT-BInfra FU] beschrieben, sowie die besonderen nicht-funktionalen Anforderungen.

2.2 Interoperabilität

Die Datenstrukturen zur Gewährleistung der Interoperabilität der IT-Basisinfrastruktur in [TR DM IT-BInfra IO] beschrieben.

2.3 IT-Sicherheit

Die spezifischen Anforderungen an die Sicherheit der IT-Basisinfrastruktur werden in [TR DM IT-BInfra Si] beschrieben.

2.4 Funktionsprüfung

Die Spezifikation der Prüffälle für die Funktionsprüfung erfolgt in [TR DM IT-BInfra FU-PS].

2.5 Interoperabilitätsprüfung

Die Spezifikation der Prüffälle für die Interoperabilitätsprüfung erfolgt in [TR DM IT-BInfra FU-PS].

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	IT-Basisinfrastruktur Funktionalitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 1.1
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Tabellenverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die funktionalen Spezifikationen der IT-Basisinfrastruktur und ist Bestandteil von [TR DM ACM M].

In diesem Modul werden die zwingenden Anforderungen an die IT-Basisinfrastruktur von De-Mail technikneutral beschrieben,. Eine Spezifikation von Protokollen und zugehörigen Parametern erfolgt nur dort, wo dies aus funktionaler Sicht explizit erforderlich ist.

2 ÖVD

Im ÖVD können Daten eines Nutzers vom DMDA veröffentlicht werden, soweit der Nutzer dies ausdrücklich verlangt. Andere De-Mail-Nutzer können auf diese zugreifen und in dem Datenbestand suchen.

2.1 Allgemeine Anforderungen

Jeder DMDA betreibt notwendig einen eigenen ÖVD. Für die Nutzer ist eine Suche über die ÖVD aller DMDA möglich. Die Suche ist nur für authentisierte Nutzer möglich. Suchanfragen stellt der Nutzer dazu immer an den ÖVD seines eigenen DMDA. Dieser muss die Suchanfragen für den Nutzer an den zuständigen ÖVD des fremden DMDA weiterleiten.

Bei der Suche außerhalb des ÖVD des eigenen DMDA kann der zuständige DMDA und damit dessen ÖVD z. B. anhand einer angegebenen De-Mail-Adresse oder der De-Mail-Domain eindeutig bestimmt werden. Die Anfrage kann dann direkt nur an den zuständigen DMDA gestellt werden.

Die Suche muss erfolgen können für

- natürliche Personen anhand [Vorname, Name, Ort], [De-Mail-Domain],
- Institutionen anhand [Name, Ort, DMDA], [De-Mail-Domain],
- und jeweils anhand der [De-Mail-Adresse].

Weitere Suchmöglichkeiten können durch den DMDA angeboten werden.

Zur Durchführung der Suche übermittelt der ÖVD des Nutzers die Suchanfrage an den jeweils zuständigen ÖVD. Dieser führt die Suche aus und sendet das Ergebnis an den ÖVD des Nutzers zurück.

Es werden maximal 200 Einträge zurückgesendet. Der ÖVD des Nutzers präsentiert diesem schließlich das Ergebnis. Die Ergebnisse müssen diskriminierungsfrei sortiert werden, d.h. die Suchergebnisse müssen anhand objektiver Kriterien aufgelistet werden. Der Nutzer hat somit selbst keinen unmittelbaren Zugriff auf die ÖVD anderer DMDAs.

Das Ergebnis einer Abfrage ist spätestens nach einer Gesamtzeit von 20 Sekunden zu liefern. Jeder DMDA darf dabei maximal 10 Sekunden von der Anfrage bis einschließlich der Übermittlung des Ergebnisses benötigen.

Dem Nutzer ist nur die Suche und der lesende Zugriff auf die Informationen des ÖVD gestattet. Schreibenden bzw. löschenden Zugriff haben ausschließlich DMDA-interne Dienste, z. B. das Accountmanagement.

2.2 Informationsmodell

Das Informationsmodell beschreibt, welche Daten bei einer Veröffentlichung im ÖVD zu einem Nutzer veröffentlicht werden können oder müssen. Diese werden in einer Verzeichnis-Informationsstruktur gespeichert.

Für jede De-Mail-Adresse eines Nutzers kann ein Eintrag im ÖVD existieren. Dabei sind die nachfolgend aufgeführten Bedingungen zur Veröffentlichung zu berücksichtigen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Darüber hinaus gibt es für natürliche Personen und Institutionen die Möglichkeit, einen Eintrag über die Nutzung des Authentisierungsniveaus „hoch“ vorzunehmen. Ein weiteres Attribut für X.509-basierte Verschlüsselungszertifikate muss zur Verfügung gestellt werden.

Änderungen an Daten im Accountmanagement sind im ÖVD zu übernehmen. Dazu gehören:

- Neuer Eintrag (De-Mail-Konto freigeschaltet und Nutzer hat Attribute zur Veröffentlichung freigegeben)
- Eintrag löschen
- Attribute ändern (Nutzer hat Attribute geändert)
- Attribute löschen (Nutzer hat die Freigabe für ÖVD zurückgezogen)

2.2.1 Natürliche Personen

Natürliche Personen können die nachfolgend aufgeführte Teilmenge der in [TR DM ACM FU] definierten Attribute veröffentlichen:

Attribut	*KANN / MUSS veröffentlicht werden*
De-Mail-Adresse	MUSS
Maximales Authentisierungsniveau	MUSS
Titel	KANN
Vorname	KANN (nur in Verbindung mit Nachname)
Nachname	KANN
Straße und Hausnummer	KANN (nur in Verbindung mit Ort)
Ort	KANN
Staat	KANN
Zertifikat des Nutzers	KANN

Tabelle 1: Attribute im ÖVD für natürliche Personen

Wenn auf ausdrückliches Verlangen des Nutzers Daten über diesen im ÖVD veröffentlicht werden, müssen diese zwingend dessen De-Mail-Adresse und sein maximal mögliches Authentisierungsniveau enthalten.

Bei Eintrag eines Künstler- oder Ordensnamens in der primären De-Mail-Adresse darf anstelle von Vor- und Nachnamen nur der entsprechende Künstler- bzw. Ordensname veröffentlicht werden.

Bei Pseudonym-Adressen dürfen nur technische Informationen veröffentlicht werden:

- De-Mail-Adresse (MUSS),
- Unterstützung des hohen Authentisierungsniveaus (MUSS) und
- Verschlüsselungszertifikat (KANN).

Informationen, die eine Möglichkeit zur Auflösung des Pseudonyms bieten, d. h. Vor- und Nachname sowie Wohnsitz-Daten, dürfen somit in diesem Fall nicht veröffentlicht werden. Für die Inhalte des Verschlüsselungszertifikats (z.B. Common Name im Zertifikat) ist der Nutzer verantwortlich.

2.2.2 Institutionen

Nutzer eines Kontos für Institutionen können die nachfolgend aufgeführte Teilmenge der in [TR DM ACM FU] definierten Attribute veröffentlichen:

Attribut	*KANN / MUSS veröffentlicht werden*
De-Mail-Domain	MUSS
De-Mail-Adresse als Hauptadresse	MUSS
Maximales Authentisierungsniveau	MUSS
Langform des Namen	KANN
Straße und Hausnummer	KANN (nur in Verbindung mit Ort)
Ort	KANN
Staat	KANN
X.509-Zertifikat des Nutzers	KANN

Tabelle 2: Attribute im ÖVD für Institutionen

Wenn auf ausdrückliches Verlangen des Nutzers Daten über diesen im ÖVD veröffentlicht werden, müssen diese zwingend dessen De-Mail-Adresse, sein maximal mögliches Authentisierungsniveau und eine Hauptadresse enthalten.

Bei De-Mail-Konten von Institutionen können weitere Eintragungen für Mitarbeiter (Personen), Rollen und Organisationseinheiten vorgenommen werden. Dies ist durch den Nutzer festzulegen.

3 Persönliches Adressbuch

Das persönliche Adressbuch dient der dezentralen Speicherung von Kontakten bzw. Adressierungsinformationen, die innerhalb der einzelnen De-Mail-Dienste verwendet werden können. Das persönliche Adressbuch ist unabhängig von dem ÖVD. Mittels eines persönlichen Adressbuchs kann der Nutzer seine Kontakte verwalten und über die De-Mail-Dienste nutzen. Zur Verwaltung zählen

- neue Kontakte anlegen,
- bestehende Kontakte löschen und
- Attribute innerhalb eines bestehenden Kontaktes ändern.

Für jeden Nutzer muss ein persönliches Adressbuch mittels Web-Applikation zur Verfügung gestellt werden.

Es müssen mindestens alle Informationen die auch für den ÖVD definiert sind gespeichert werden können (vgl. 2.2). Zusätzliche Attribute können gespeichert werden. Es können Verteilerlisten angelegt werden und innerhalb der De-Mail-Dienste genutzt werden.

Im persönlichen Adressbuch muss wie im ÖVD gesucht werden können.

4 Nutzung von IT-Basisdiensten

Eine Manipulation von Diensten und deren Informationen und Daten, einschließlich der Meta-Informationen, muss von dem DMDA durch geeignete Maßnahmen verhindert werden.

4.1 Protokollierungsinformationen

Alle Informationen, die für die Dienste und die Nachweise benötigt werden, sind innerhalb der DMDA-Infrastruktur in Protokollierungsdatenbanken integer und authentisch zu speichern. Protokollierungsdaten müssen so gespeichert werden, dass sie für notwendige und berechtigte Auswertungen verfügbar sind. Lesenden Zugriff auf die Protokollierungsdaten erhalten die jeweiligen berechtigten Personen. Ein unberechtigtes teilweises oder komplettes Löschen ist durch geeignete Maßnahmen zu verhindern.

4.2 Nutzung von authentischen Zeitquellen

In allen Systemen innerhalb der zentralen DMDA-Infrastruktur ist die gesetzliche Zeit über authentische Zeitquellen zu nutzen (vgl. [TR DM IT-BInfra IO]). Die gesetzliche Zeit ist auch den Nutzern jederzeit darzustellen.

Jeder DMDA ist für die korrekte Zeitsynchronisation seiner IT-Systeme mit der gesetzlichen Zeit und deren Nutzung durch die einzelnen De-Mail-Dienste verantwortlich.

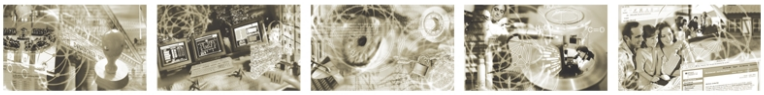
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

5 Zusammenwirken der DMDA

DMDA sind verpflichtet, untereinander zusammenzuarbeiten. Die technische Zusammenarbeit hinsichtlich der Funktionalität bezieht sich dabei auf folgende Aspekte:

- die Übermittlung von De-Mails an den jeweiligen DMDA, der innerhalb der Empfängeradresse referenziert ist;
- die Entgegennahme von De-Mails durch den DMDA, der innerhalb der Empfängeradresse referenziert ist;
- die Übermittlung von Eingangs- und Abholbestätigungen an den Absender einer De-Mail;
- die Übermittlung von Anfragen an den ÖVD des DMDAs, der innerhalb der Suchanfrage referenziert ist;
- die Entgegennahme von Anfragen von anderen DMDAs hinsichtlich des ÖVD und die Übermittlung der Antwort;
- die Übernahme von Antworten zu Anfragen an den ÖVD des DMDAs, wenn sich die Antwort auf die Anfrage bezieht;
- die Übermittlungen von Meldungen, die bei bestimmten Konstellationen des Prozessablaufes (z.B. ungültige De-Mail-Adresse) erzeugt werden können.

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	IT-Basisinfrastruktur IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 1.3
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: de-mail@bsi.bund.de
Internet: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die IT-Sicherheitsanforderungen, die über die generellen Anforderungen aus dem Modul [TR DM Si M] hinausgehen und speziell für die IT-Basisinfrastruktur anzuwenden sind, und ist Bestandteil von [TR DM IT-BInfra M].

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die angenommene Netzinfrastruktur eines typischen De-Mail-Dienstes.

Bei der Erstellung des realen IT-Sicherheitskonzepts sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der bereits in [TR DM Si ÜK] skizziert ist.

3 Bedrohungen

Es werden in diesem Abschnitt nur die Bedrohungen für die IT-Basisinfrastruktur betrachtet, die sich zusätzlich zu den Bedrohungen aus [TR DM Si ÜK] durch die Funktionalität der IT-Basisinfrastruktur ergeben.

3.1 Fehlerhafte Systemzeit

Die Basisinfrastruktur stellt die Zeit für die De-Mail-Dienste zur Verfügung. Dabei gilt, dass De-Mail die gesetzliche Zeit verwendet. Es ist denkbar, dass durch bewusste Manipulation oder durch technisches Versagen eine falsche Zeit verwendet wird. Dies kann dazu führen, dass fehlerhafte Bestätigungen über den Zustand einer De-Mail-Nachricht ausgestellt werden.

3.2 Fehlerhafte Eintragungen im ÖVD

Fehlerhafte Einträge im ÖVD können durch Fehleingabe, technisches Versagen oder bewusste Manipulation entstehen. Solche fehlerhaften Einträge können dazu führen, dass Nachrichten an einen anderen Benutzer adressiert bzw. versendet werden und es damit zu einem Verlust hinsichtlich der Vertraulichkeit kommt.

3.3 Automatisierte ÖVD-Abfrage

Durch automatisierte Abfrage besteht die Möglichkeit, den gesamten Datenbestand des ÖVD abzufragen und danach für unbekannte Zwecke zu verwenden.

3.4 Unberechtigter Zugriff auf den ÖVD

Es besteht die Gefahr, dass unberechtigte Personen versuchen, Zugriff auf die im ÖVD verfügbaren Daten zu erlangen.

3.5 Fehlerhafte Einträge im DNS

Fehlerhafte Einträge im DNS können durch Fehleingaben, technisches Versagen oder bewusste Manipulation entstehen. Solche fehlerhaften Einträge können dazu führen, dass Daten nicht zugestellt werden.

4 Sicherheitsziele

Im Folgenden werden weitergehende Sicherheitsziele der IT-Basisinfrastruktur beschrieben, die über die in [TR DM Si ÜK] Aufgeführten gelten.

4.1 Verwendung der korrekten Zeit

In den Systemen muss die korrekte Zeit eingesetzt werden, um den Zeitpunkt des Eingangs und der Weiterleitung von Nachrichten genau dokumentieren zu können.

4.2 Korrekte Einträge innerhalb des ÖVD

Die Inhalte des ÖVD müssen mit den Daten des Accountmanagements übereinstimmen.

4.3 Korrekte Authentisierung der Nutzer

Die Nutzung und Administration darf nur durch authentisierte und autorisierte Personen erfolgen.

4.4 Korrekte Einträge im DNS

Die Einträge im DNS des DMDA müssen korrekt sein.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

5 Anforderungen

5.1 Allgemeine Anforderungen

5.1.1 Zeitservice

Zeitquelle für den Zeitservice ist die gesetzliche Zeit (MEZ/MESZ), die von der Physikalisch-Technische Bundesanstalt (PTB) als UTC(PTB)+1(2) realisiert und verbreitet (DFC77, Telefonzeitdienst der PTB, NTP) wird.

Folgende Anforderungen werden an den Zeitservice bei De-Mail gestellt:

- Die Uhrzeiten aller im De-Mail-System eingesetzten Komponenten sind über einen dedizierten Zeitserver, der über die oben geforderte gesetzliche Zeit verfügt, zu synchronisieren.
- Die Synchronisierung muss über gesicherte Kanäle erfolgen.
- Die Zeit wird über das separate Management-Netz verbreitet. Das Management-Netz ist ein physikalisch getrenntes Netz und dient unabhängig vom Netz der Nutzdaten der Administration der Systeme. Die Administration darf nur über diese Netz möglich sein.
- Die Zeitinformation, die der Zeitserver zur Verfügung stellt, darf max. 1 Sekunde von der gesetzlichen Zeit abweichen.
- Durch geeignete technische Maßnahmen ist sicherzustellen, dass die Zeit des Zeitservers nicht manipuliert werden kann. Es ist auch sicherzustellen, dass Manipulationen am Zeitsignal sicher erkannt werden. Dies kann beispielsweise durch den Abgleich mit der Systemzeit eines Referenzsystems erfolgen.
- Die Betriebssysteme und die Anwendungssoftware der IT-Systeme, die den Zeitservice für die jeweilige De-Mail-Infrastruktur zur Verfügung stellen, sind durch den Administrator regelmäßig, mindestens einmal täglich, auf Integrität zu überprüfen.

5.1.2 ÖVD

Es darf ausschließlich der Applikationsserver Schreibrechte auf den ÖVD haben.

Es dürfen ausschließlich authentisierte De-Mail-Nutzer eine Verzeichnisdienstanfrage durchführen können.

Alle Schreibzugriffe auf den ÖVD werden protokolliert. Bei Schreibzugriffen, die nicht durch den Server erfolgen, muss eine Alarmierung durch das Protokollierungssystem erfolgen.

Alle Berechtigungsänderungen auf dem ÖVD werden protokolliert. Bei Änderungen muss eine Alarmierung durch das Protokollierungssystem erfolgen.

Die Betriebssysteme und die Anwendungssoftware der IT-Systeme, die den öffentlichen Verzeichnisdienst für den jeweiligen De-Mail-Dienst zur Verfügung stellen, sind durch den Administrator regelmäßig, mindestens einmal täglich, auf Integrität zu überprüfen.

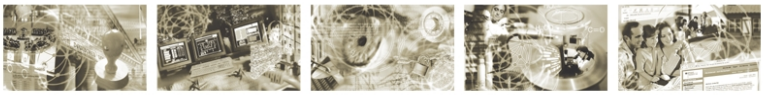
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

5.2 Administration des DNS

Die Einträge im DNS-Server sind regelmäßig auf ihre Korrektheit zu prüfen. Es sollte DNSSEC zum Einsatz kommen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	IT-Basisinfrastruktur Interoperabilitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 1.4
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul ist Bestandteil von [TR DM IT-BInfra M]. Hier werden Datenstrukturen und Datenformate der IT-Basisinfrastruktur spezifiziert.

2 Transportverschlüsselung

Alle Verbindungen zu einem DMDA müssen mittels Transport Layer Security (TLS) verschlüsselt erfolgen.

Die Verbindungen müssen TLS in der Version 1.0 [TLS10] und sollten die Versionen 1.1 [TLS11], 1.2 [TLS12] und ggf. folgende Versionen unterstützen. Ältere SSL-Versionen dürfen nicht unterstützt werden.

Folgende Cipher-Suites dürfen verwendet werden:

- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `TLS_RSA_WITH_AES_256_CBC_SHA`
- `TLS_DH_DSS_WITH_AES_128_CBC_SHA`
- `TLS_DH_DSS_WITH_AES_256_CBC_SHA`
- `TLS_DH_RSA_WITH_AES_128_CBC_SHA`
- `TLS_DH_RSA_WITH_AES_256_CBC_SHA`
- `TLS_DHE_DSS_WITH_AES_128_CBC_SHA`
- `TLS_DHE_DSS_WITH_AES_256_CBC_SHA`
- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA`
- `TLS_DHE_RSA_WITH_AES_256_CBC_SHA`

Bis auf weiteres dürfen auch diese Cipher-Suites verwendet werden:

- `TLS_RSA_WITH_3DES_EDE_CBC_SHA`
- `TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA`

Für andere Cipher-Suites müssen die Anforderungen aus der jeweils aktuellen Version des Kryptoalgorithmenkatalogs [TR 02102] des BSI gewählt werden.

Alle nicht empfohlenen Cipher-Suites müssen deaktiviert sein. Ein Verbindungsaufbau mit solchen Algorithmen muss stets abgelehnt werden.

Wenn eine Clientauthentisierung für die Verbindung gefordert wird, gelten die folgenden Anforderungen:

- Die Prüfung der verwendeten Zertifikate muss mittels LDAP oder OCSP erfolgen.Die Prüfung des Zertifikats, welches zur Authentisierung der Gegenseite verwendet wird, muss mindestens alle 24 Stunden erfolgen und kann bis zur nächsten Prüfung zwischengespeichert werden.
- Wenn die Prüfung des Zertifikats fehlschlägt, darf die Verbindung nicht aufgebaut werden.
- Die Verbindung kann nach der Übertragung offengehalten werden. Dies verhindert, dass bei häufiger Übertragung von Daten von einem DMDA zu einem anderen der aufwändige Verbindungsaufbau wiederholt stattfindet.Bei der nächsten Gültigkeitsprüfung muss ein erneuter Verbindungsaufbau erfolgen.

In der folgenden Tabelle werden alle möglichen Verbindungen, das dabei zu verwendende Protkoll und eine Kennzeichnung, ob eine Clientauthentisierung erforderlich ist, aufgelistet.

Quelle	***Ziel***	***Protokoll***	***Port***	***Clientauthentisierung***
Nutzer	DMDA	HTTPS	443	kann
Nutzer	DMDA	Alle weiteren Protokolle zur Anbindung		kann
PVD DMDA 1	PVD DMDA 2	SMTP über TLS	1465	muss
ÖVD DMDA 1	ÖVD DMDA 2	LDAPS	636	muss

Tabelle 1: Übersicht der Verbindungen, Protokolle sowie der Clientauthentisierung

Im Falle der Übertragung einer De-Mail-Nachricht von einem DMDA zu einem anderen wird die Verschlüsselung des Kanals mittels TLS initiiert (implizites TLS). Die Übertragung der Nachrichten muss dabei via SMTP über TLS auf Port 1465 stattfinden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

3 Domänenverschlüsselung

Die Domänenverschlüsselung dient dem Schutz jeder einzelnen De-Mail-Nachricht auf dem Transportweg von einem DMDA zu einem anderen. Dazu muss die De-Mail-Nachricht vor dem Versand verschlüsselt und beim Empfang entschlüsselt werden.

Die Verschlüsselung der De-Mail-Nachrichten muss mittels S/MIME [SMIME] realisiert werden. Um die Interoperabilität zu gewährleisten, sind die Anforderungen für S/MIME aus [C-PKI] zu erfüllen.

Bei der Domänenverschlüsselung müssen Verschlüsselungs- und Hash-Algorithmen aus [TR02102] verwendet werden.

– Seite 49 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

4 Zertifikate für die Inter-DMDA-Kommunikation

Im Folgenden werden die Inhalte der Zertifikate definiert, die für die Transport- und die Domänenverschlüsselung zwischen den DMDA verwendet werden. Sofern nicht explizit erwähnt, sind die Inhalte der Zertifikate für die Transport- und die Domänenverschlüsselung gleich.

Attribut	***Transportverschlüsselung***	***Domänenverschlüsselung***	***Clientauthentication***
CN	[Host].[DMDA-Domain]	[DMDA-Domain]	[DMDA-Domain]
OU	De-Mail		
O	Bund		
C	de		
Schlüssel-verwendung	keyEncipherment digitalSignature	keyEncipherment digitalSignature	KeyEncipherment, digitalSignature
Extended Key Usage	Serverauthentifizierung (Webserver) 1.3.6.1.5.5.7.3.1	Email Protection 1.3.6.1.5.5.7.3.4	Client authentication 1.3.6.1.5.5.7.3.2

Tabelle 2: Inhalte der Zertifikate

Die Qualität der verwendeten Schlüssel muss mindestens den Anforderungen aus [TR 02102] genügen.

Die Beantragung der Zertifikate erfolgt bei der zuständigen Behörde. Die Behörde, die die PKI verwaltet, sorgt für die Einhaltung der Namensgebung in den ausgestellten Zertifikaten.

Die von dem DMDA aktuell verwendeten Zertifikate für die Domänenverschlüsselung müssen im DNS-Record gemäß [RFC 4398] als PKIX-Typ hinterlegt werden.

Der Abruf der Zertifikate muss über den Eintrag im DNS-Record des DMDA erfolgen.

Ein Zertifikat muss direkt nach dem Abruf auf seine Authentizität und Gültigkeit hin überprüft werden. Die Prüfung beinhaltet eine Prüfung gegen eine Sperrlisten oder einen OCSP-Responder. Erst danach darf es für maximal 24 Stunden zwischengespeichert werden.

5 Domain Name Service

Jeder DMDA muss für seine, ausschließlich für De-Mail, verwendeten Domain(s) einen eigenen Name-Server (Domain Name System, [RFC 1034], [RFC 1035]) betreiben.

Die Auskünfte des DNS-Servers sollten mittels DNSSEC (siehe [RFC 4033]) gesichert werden. Die Sicherung sollte für alle Domänen des DMDA genutzt werden.

Es muss ein autoritativer DNS-Server für die Domäne definiert werden (NS) und ein Record für den Eingang externer Mails (MX). Diese externen Mails sind keine De-Mails, sondern normale E-Mails. Es darf nur der De-Mail-Dienst angeboten werden. Außerdem müssen die Einträge für die vom DMDA angebotenen De-Mail-Dienste definiert werden, damit diese gefunden werden können.

Für alle DM-Domains und Subdomains muss ein SRV-Record „_ldaps._tcp§ existieren, der auf den ÖVD des DMDA verweist.

Beispiel-Zonefile für den DNS-Server eines DMDA:

```
;zonefile for <De-Mail-Domäne>
$TTL 1D
@     IN    SOA  ns.<dmda>. hostmaster.<dmda>. (
      1     ; Serial
      8H    ; Refresh
      2H    ; Retry
      1W    ; Expire
      1D)   ; Minimum TTL
      NS    ns ;the authoritative name server
      MX 10      mail ;the external mail server
_smtp._tcp      IN SRV  10   0 1465  mail ;the SRV RR for the mail
server
_ldap._tcp      IN SRV  10   0 636   dir ; the SRV RR for the
directory service
ns         A X.Y.Z.A
mail       A X.Y.Z.B
dir        A X.Y.Z.C
;Zertifikat für Domänenverschlüsselung
hostmaster.<dmda> IN CERT PKIX [Zertifikat gemäß RFC 4398]
```

Beispiel-Zonefile für den DNS-Server. In diesem Beispiel wird die Institution Firma beim DMDA gehostet (die Domain firma.de muss ebenfalls ausschließlich für De-Mail verwendet werden):

```
;zonefile for <Institution>.<De-Mail-Domäne>
$TTL 1D
```

```
@     IN    SOA  ns.<Institution>.<De-Mail-Domäne>.
hostmaster.<Institution>.<De-Mail-Domäne>. (
      1     ; Serial
      8H    ; Refresh
      2H    ; Retry
      1W    ; Expire
      1D)   ; Minimum TTL
            IN    NS    ns.<dmda>.de
            IN    MX 10     mail

_smtp._tcp      IN SRV    0    0    25   mail
_ldap._tcp      IN SRV    0    0    636  dir
_demail._tcp    IN SRV    0    0    1465 de-mail

dns         A <ns.DMDA-IP-Adresse>
mail        A <mail.DMDA -IP-Adresse>
dir         A <dir.DMDA -IP-Adresse>
de-mail     A <de-mail.DMDA -IP-Adresse>
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

6 Verzeichnisdienst

Im Verzeichnisdienst muss auf ausdrückliches Verlangen eines Nutzers ein Eintrag angelegt werden, der freigegebene Informationen über diesen Nutzer und dessen Konto enthält.

6.1 LDAP-Schema

Als Objektklasse („`objectclass`“) muss für natürliche Personen `inetOrgPerson` verwendet werden. Neu definierte Attribute für De-Mail müssen `demail` als Präfix erhalten. Die benötigten neuen Objektklassen müssen zudem `Object` als Postfix erhalten. Zur Vereinfachung und zur Vermeidung von Fehlern wird im LDAP-Schema keine Beschränkung vorgenommen.

Für die Identitätsattribute und die vorgegebenen ergänzenden Attribute werden die zwei Objektklassen `demailPersonObject` und `demailLegalPersonObject` definiert. Diese nehmen die neu definierten Attribute sowie einige bereits vorhandene auf, aber keine der in `inetOrgPerson` enthaltenen Attribute (da es sich bei dem Attribut `mail` um ein Identitätsattribut handeln soll, reicht `inetOrgPerson` hier nicht aus). Beide Objektklassen sind Hilfsklassen (Typ `AUXILIARY`). Sollen später weitere Attribute definiert bzw. aufgenommen werden, so sind diese in neue Objektklassen aufzunehmen, welche ebenfalls als Hilfsklassen zu definieren sind. In den folgenden Tabellen zu natürlichen Personen und Institutionen werden die möglichen Angaben in Auflistungen zusammengefasst und das jeweils zu verwendende LDAP-Attribut definiert. Hierbei ist ebenfalls angegeben, ob es sich im LDAP um ein MUST- oder MAY-Attribut (Pflicht vs. Optional) handelt.

Es handelt sich bei den aufgeführten Attributen um Identitätsattribute bzgl. der Erfassung, die durch den DMDA verifiziert sein müssen. Es dürfen nur die genannten Attribute veröffentlicht werden.

6.1.1 Attribute

Sofern nicht anders angegeben, darf ein Attribut nur einmal verwendet werden, selbst wenn der entsprechende Attributtyp („`attributetype`“) im LDAP-Schema eine mehrfache Verwendung zulässt. Die Ausnahme hinsichtlich der Verzeichnisdienst-Einträge ist das Verschlüsselungs-Zertifikat („`userCertificate`“).

6.1.2 Natürliche Personen

Folgende Attribute können veröffentlicht werden. Es handelt sich bei den aufgeführten Attributen um Identitätsattribute, die durch den DMDA verifiziert sein müssen. Es dürfen nur die genannten Attribute veröffentlicht werden.

Attribut **Primär De-Mail-Adresse**	**Attribut** **Pseudonym De-Mail-Adresse**	**LDAP-Attribut**	**Objektklasse**
Vorname	[kein Eintrag][1]	`givenName (MAY)`	`inetOrgPerson`

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Attribut **Primär De-Mail-Adresse**	Attribut **Pseudonym De-Mail-Adresse**	LDAP-Attribut	Objektklasse
Nachname	Pseudonym-Bezeichner	`sn (MUST)`	`person`
Name[2]	Pseudonym-Bezeichner	`cn (MUST)`	`person`
Displayname[3]	Pseudonym-Bezeichner	`displayName (MAY)`	`inetOrgPerson`
Titel	[kein Eintrag]	`personalTitle (MAY)`	`demailPersonObject`
Hauptwohnsitz_Straße	[kein Eintrag]	`street (MAY)`	`organizationalPerson`
Hauptwohnsitz_Hausnummer	[kein Eintrag]		
Hauptwohnsitz_Ort	[kein Eintrag]	`l (MAY)`	`organizationalPerson`
Hauptwohnsitz_Staat	[kein Eintrag]	`c (MAY)`	`demailPersonObject`
Primär De-Mail-Adresse	Pseudonym De-Mail-Adresse	`mail (MUST)`	`demailPersonObject`
Höchstes Authentisierungsniveau	Höchstes Authentisierungsniveau	`demailMaxAuthLevel (MUST)`	`demailPersonObject`
Verschlüsselungs-Zertifikat	Verschlüsselungs-Zertifikat	`userCertificate (MAY)`	`inetOrgPerson`

Tabelle 3: LDAP-Attribute natürlicher Personen

Für die eindeutige Abbildung kann das Attribute `mail` verwendet werden.

Das Attribut `c` muss mit dem zweistelligen Country Code gemäß ISO 3166 gefüllt werden.

6.1.3 Institution

Das Feld `sn` ist ein Pflichtfeld, das bei Accounts von Institutionen genauso wie cn zu belegen ist.

Hinweis: das Attribut `c` in der Klasse `demailBaseObject` ist wegen der Nationalität einer Institution erforderlich.

1 „[kein Eintrag]“ stellt dar, dass das Feld nicht befüllt wird

2 Der Name besteht aus der Zusammensetzung aus [Vorname Nachname] oder bei Künstler-/Ordens-Name aus dem angegebenen Bezeichner.

3 Der Displayname besteht aus der Zusammensetzung aus [Nachname, Vorname] oder bei Künstler-/Ordens-Name aus dem angegebenen Bezeichner.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Attribut	LDAP-Attribut	Objektklasse
De-Mail-Domain der Institution	dc (MUST; Alias für domainComponent)	dcObject
Name - Langform	o (MUST) displayname (MUST)	Organization demailLegalPersonObject
Anschrift - Straße	street MAY)	organization
Anschrift - Hausnummer		
Anschrift - Ort	l (MAY)	organization
Anschrift - Staat	c (MAY)	demailLegalPersonObject
De-Mail-Adresse	mail (MUST)	demailLegalPersonObject
Höchstes Authentisierungsniveau	demailMaxAuthLevel (MUST)	demailLegalPersonObject
Verschlüsselungs-Zertifikat	userCertificate (MAY)	pkiUser

Tabelle 4: LDAP-Attribute von Institutionen

Nutzer der Institution können sowohl als Person als auch als Rolle abgebildet werden. Werden Anschriftsdaten oder Daten zu Geschäftsfeld/Gegenstand der Organisation bei Rollen oder Personen eingetragen, sind die Daten der entsprechenden Institution zu verwenden.

Attribut	LDAP-Attribut	Objektklasse
Vorname	givenName (MAY)	inetOrgPerson
Nachname	sn (MUST)	person
Name[= Vorname Nachname]	cn (MUST)	person
Displayname [Nachname, Vorname]	displayName (MUST)	inetOrgPerson
Name – Langform der Institution	o (MUST)	demailLegalPersonUserObject
Anschrift - Straße	street (MAY)	inetOrgPerson
Anschrift - Hausnummer		
Anschrift - Ort	l (MAY)	inetOrgPerson

Attribut	LDAP-Attribut	Objektklasse
Anschrift - Staat	c (MAY)	demailLegalPersonUserObject
De-Mail-Adresse	mail (MUST)	demailLegalPersonUserObject
Verschlüsselungszertifikat	userCertificate (MAY)	inetOrgPerson
Höchstes Authentisierungsniveau	demailMaxAuthLevel (MUST)	demailLegalPersonUserObject

Tabelle 5: LDAP-Attribute von Nutzern bei einer Institution: Personen

Attribut	LDAP-Attribut	Objektklasse
Bezeichner [= local-part der De-Mail-Adresse]	cn (MUST) displayName (MUST)	organizationalRole demailLegalPersonUserObject
Anschrift - Straße	street (MAY)	organizationalRole
Anschrift - Hausnummer		
Anschrift - Ort	l (MAY)	organizationalRole
Anschrift - Staat	c (MAY)	demailLegalPersonUserObject
Name – Langform der Institution	o (MUST)	demailLegalPersonUserObject
De-Mail-Adresse	mail (MUST)	demailLegalPersonUserObject
Verschlüsselungszertifikat	userCertificate (MAY)	pkiUser
Höchstes Authentisierungsniveau	demailMaxAuthLevel (MUST)	demailLegalPersonUserObject

Tabelle 6: LDAP-Attribute von Nutzern bei einer Institution : Rollen

Zur Strukturierung einer Institution in Organisationseinheiten kann der in der nachfolgenden Tabelle dargestellte Knoten verwendet werden. Werden Anschriftsdaten oder Daten zu Geschäftsfeld/Gegenstand der Organisation bei Rollen oder Personen eingetragen, sind die Daten der entsprechenden Institution zu verwenden.

Attribut	LDAP-Attribut	Objektklasse
Sub-Domain der De-Mail-Domain der Institution	`dc (MUST)`	`dcObject`
Name - Langform	`ou (MUST)` `displayname (MUST)`	`organizationalUnit` `demailLegalPersonUserObject`
Anschrift - Straße	`street (MAY)`	`organizationalUnit`
Anschrift - Hausnummer		
Anschrift - Ort	`l (MAY)`	`organizationalUnit`
Anschrift - Staat	`c (MAY)`	`demailLegalPersonUserObject`
Name – Langform der Institution	`o (MUST)`	`demailLegalPersonUserObject`
De-Mail-Adresse	`mail (MUST)`	`demailLegalPersonUserObject`
Verschlüsselungs-Zertifikat	`userCertificate (MAY)`	`pkiUser`
Höchstes Authentisierungsniveau	`demailMaxAuthLevel (MUST)`	`demailLegalPersonObject`

Tabelle 7: LDAP-Attribute von Nutzern bei einer Institution : Organisationseinheiten

Es muss durch den DMDA sichergestellt sein, dass jede De-Mail-Adresse im Attribut `mail` nur einmal im Verzeichnisdienst eingetragen wird.

Das Attribut `c` muss mit dem zweistelligen Country Code gemäß ISO 3166 gefüllt werden.

6.2 De-Mail-Schema

Das u.a. Schema muss verwendet werden.

```
# LDAP schema extension for citizen portal
#
# Prefix for OIDs: 1.3.6.1.4.1.7924.2.1
# Prefix for names: demail
# Postfix for object classes: Object

attributetype ( 1.3.6.1.4.1.7924.2.1.1.1
      NAME 'demailMaxAuthLevel'
```

```
      DESC 'describes the maximum authentification the person is capable of
(NORMAL/HIGH/VERY HIGH)'
      SUP name SINGLE-VALUE )


### objects ###


objectclass ( 1.3.6.1.4.1.7924.2.1.2.1 NAME 'demailBaseObject'
      DESC ''
      SUP top
      AUXILIARY
      MUST ( mail )
      MAY ( c ) )


objectclass ( 1.3.6.1.4.1.7924.2.1.2.2 NAME 'demailSecurityObject'
      DESC ''
      SUP (demailBaseObject)
      AUXILIARY
      MUST ( demailMaxAuthLevel ) )


objectclass ( 1.3.6.1.4.1.7924.2.1.2.3 NAME 'demailPersonObject'
      DESC ''
      SUP ( demailSecurityObject)
      AUXILIARY
      MAY ( personalTitle ) )


objectclass ( 1.3.6.1.4.1.7924.2.1.2.4 NAME 'demailLegalPersonObject'
      DESC ''
      SUP ( demailSecurityObject)
      AUXILIARY
      MUST (displayName))


objectclass ( 1.3.6.1.4.1.7924.2.1.2.5 NAME 'demailLegalPersonUserObject'
      DESC ''
      SUP ( demailSecurityObject)
      AUXILIARY
      MUST (displayName $ o))


# end of schema
```

`personalTitle` ist im COSINE LDAP/X.500 Schema-Schema definiert (siehe RFC 4524).

6.2.1 De-Mail-LDAP-Modell

In der Abbildung 1 ist das Modell der Verzeichnisdienst-Struktur für einen DMDA dargestellt.

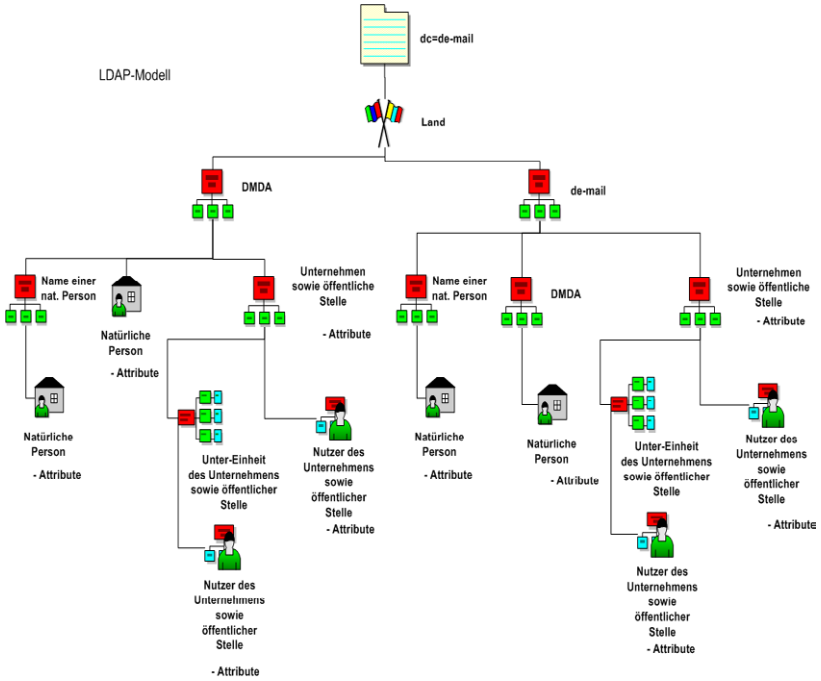


Abbildung 1: LDAP-Modell

In der Abbildung 2 ist eine beispielhafte Instanziierung des De-Mail-LDAP-Modelles dargestellt.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

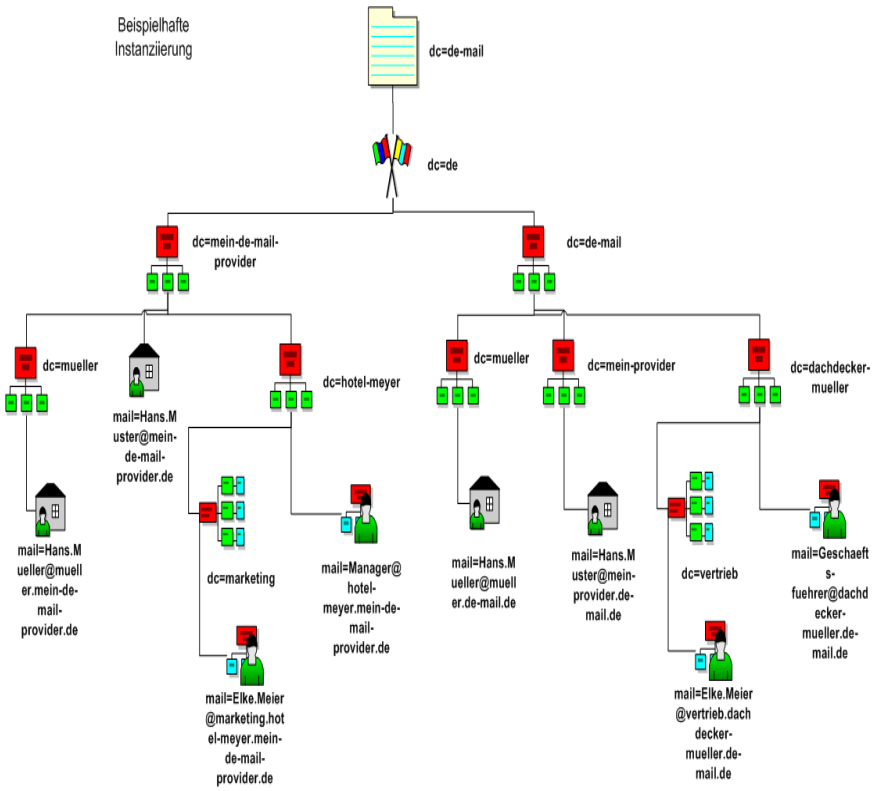


Abbildung 2: Beispielhafte Instanziierung des LDAP-Modells

6.3 Verzeichnisdienstabfragen

Für die Kommunikation der ÖVD untereinander (DMDA zu DMDA) muss LDAPv3 verwendet werden. Zur Übertragung muss der ÖVD implizites TLS (also LDAPS) über Port 636/tcp einsetzen (siehe Abschnitt 2).

Die Authentisierung zwischen den DMDA muss mittels TLS-ClientAuthentication erfolgen.

Der Zugriff auf den ÖVD eines DMDA muss allen anderen DMDA ermöglicht werden.

Die Suchbasis muss direkt aus der De-Mail-Adresse abgeleitet werden können. Jedem Level der Domain muss ein Verzeichnis der Suchbasis in entsprechender Reihenfolge gleichkommen.

Ein ÖVD muss einen namingContext „dc=de-mail“ bereitstellen. Die Suchbasis bei Suchoperationen muss „dc=de-mail“ oder spezifischer (z.b. „dc=institution,dc=de-mail,dc=de, dc=de-mail“) sein.

Beispiel:

De-Mail-Adresse: info@institution.de-mail.de

Suchbasis: dc=institution, dc=de-mail, dc=de, dc=de-mail

Bei allen DM-Domains und Subdomains kann der zugehörige Verzeichnisdienst, anhand von SRV-Records („_ldaps._tcp“) der entsprechenden Domain, ausfindig gemacht werden.

Beispiel:

DM-Domain: institution.de-mail.de

SRV-Record des ÖVD: _ldaps._tcp.institution.de-mail.de

7 Liste der vertrauenswürdigen DMDA-Domains

Um den DMDAs und auch den Nutzern eine Liste der vertrauenswürdigen De-Mail-Domains der DMDAs für das Routing von De-Mails zur Verfügung zu stellen, wird eine Trusted Service List (gemäß [ETSI TS 102 231] in der jeweils aktuellen Version) durch die zuständige Behörde erstellt und für alle Abfragenden zur Verfügung gestellt. Diese enthält die Domains aller akkreditierten DMDA.

Das Dokument muss durch den DMDA ausgewertet werden, um die gültigen De-Mail-Domains zu ermitteln.

Für jeden akkreditierten DMDA ist ein `<tsl:TrustServiceProviderList>`-Eintrag vorhanden.

Für jede Domäne des DMDAs gibt es einen `<tsl:TSPService>`-Eintrag.

Dort ist unter `<tsl:ServiceName>` die Domäne des DMDA hinterlegt.

Für den Dienst bei dem Status zu prüfen, ob dieser aktiv ist.

Der Zeitpunkt für das nächste Update ist im Eintrag `<tsl:NextUpdate>` enthalten.

Die URL zum Abruf teilt die zuständige Behörde mit.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Accountmanagement Modul
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 2
Version:	1.0

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beschreibt die Struktur des Accountmanagements. Das Modul ist Bestandteil der [TR DM].

Der zuverlässige Nachweis der Identität eines Nutzers ist in der De-Mail-Konzeption unmittelbar mit dessen Nutzerkonto verbunden. Das De-Mail-Konto ermöglicht den Zugang zu den De-Mail-Diensten eines DMDA. Sämtliches Handeln eines Nutzers im De-Mail-Verbund ist unmittelbar mit dem De-Mail-Konto verbunden und lässt sich immer auf dieses zurückführen.

In diesem Modul wird das Management von De-Mail-Konten beschrieben. Das Accountmanagement definiert, unter welchen Bedingungen das De-Mail-Konto eines Nutzers vom DMDA neu angelegt, freigeschaltet, gesperrt oder aufgelöst werden darf. Weiterhin definiert das Accountmanagement, unter welchen Bedingungen ein Nutzer seine im De-Mail-Konto hinterlegten Identitätsdaten und Einstellungen für das De-Mail-Konto ändern darf.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2 Dokumentenübersicht

2.1 Funktionale Anforderungen

Die funktionalen Anforderungen an das Accountmanagement werden in [TR DM ACM FU] beschrieben, sowie die besonderen nicht-funktionalen Anforderungen.

2.2 IT-Sicherheit

Die spezifischen Anforderungen an die Sicherheit des Accountmanagements werden in [TR DM ACM Si] beschrieben.

2.3 Funktionsprüfung

Die Spezifikation der Prüffälle für die Funktionsprüfung erfolgt in [TR DM ACM FU-PS].

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Accountmanagement Funktionalitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 2.1
Version:	1.0

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Tabellenverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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>]

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.

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.

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

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

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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. Jeder DMDA meldet genau eine Provider-Domäne bei der zuständigen Behörde an. Der DMDA ist für die Verwaltung der Domäne verantwortlich und stellt sicher, dass diese nur für De-Mail-Dienste verwendet wird.

Beispiele: @<mein-DMDA-x>.de, @<mein-DMDA-y>.de oder
@<mein-DMDA-z>.de-mail.de (sofern eine Sammeldomäne benutzt wird).

Der DMDA kann Unterdomänen an natürliche Personen oder Institutionen vergeben. Eine Unterdomäne kann nur einer natürlichen Person oder Institution zugeordnet werden.

Beispiele: @<unternehmen>.<mein-DMDA-x>.de oder @<unternehmen>.de-mail.de

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.

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 local-part 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[2] gewählt werden.
- Es muss die Empfehlung gemäß RFC 2821[3] beachtet werden, dass der local-part maximal 64 Zeichen aufweisen darf.
- Der Domainname darf maximal 220 Zeichen lang sein.
- 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 IETF-Standard

3 IETF-Standard

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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.

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 ausschließlich dieser aufgenommen werden.
Nachname	inkl. Adelstitel, kann auch der Familienname oder Lebenspartnerschaftsname sein.
Geburtsdatum	
Geburtsort	
Straße und Hausnummer	Hauptwohnsitz[4]
Wohnort	Inkl. Ortsteil, wenn vorhanden (mit „–“ vom Ort abgetrennt)
Staat	

Tabelle 1: Pflicht-Identitätsattribute natürlicher Personen

Neben den Pflichtattributen können folgende Attribute aufgenommen werden:

4 im melderechtlichen Sinne

Attribut	*Bemerkung*
Titel	Akademischer Grad (wenn im Identifikationsdokument erfasst)
Ordensname/Künstlername	Nur bei Nutzung des Ordensnamens bzw. Künstlernamens innerhalb der primären De-Mail-Adresse muss der Ordensname bzw. der Künstlername im Identifikationsdokument eingetragen und die amtliche Registrierung verifiziert worden sein.

Tabelle 2: Optionale Identitätsattribute natürlicher Personen

Die Verifikation der optionalen Identitätsattribute ist nur notwendig, wenn die zusätzlichen Attribute verwendet werden sollen (z.B. der Künstlername in der primären De-Mail-Adresse). Wenn die Attribute nicht zuverlässig ermittelt wurden, dürfen diese nicht in der primären De-Mail-Adresse 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.
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 Register, 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 positiv ist.

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. Vor der Freigabe dürfen die Daten nicht für die De-Mail-Dienste verwendet werden.

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, wobei in diesem Fall folgende Verfahren verwendet werden dürfen:
  - Identitätsfeststellung, die auch im Rahmen der Identifizierung gemäß Signaturgesetz bzw. -verordnung zugelassen ist,
  - Identitätsfeststellung im Rahmen eines Bankregistrierungsverfahrens (insbesondere nach § 4 Abs. 3 und 4 GwG) in einem deutschen Kreditinstitut, oder
  - der Feststellung der Identität durch Notare oder dafür zuständige kommunale Behörden (z.B. Personalausweisbehörden),
- 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 anhand

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

- „eines gültigen amtlichen Ausweises, der ein Lichtbild des Nutzers 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 oder anhand von Dokumenten mit gleichwertiger Sicherheit“,
- mittels des elektronischen Identitätsnachweises des neuen Personalausweises oder
- „einer qualifizierten elektronischen Signatur nach § 2 Nummer 3 des Signaturgesetzes“

erhoben werden.[5] Im letztgenannten Fall ist sicherzustellen, dass die vom Zertifizierungsdiensteanbieter erfassten Identitätsdaten sicher an den DMDA übermittelt werden.

2.3.2 Feststellung bei Institutionen

Bei Institutionen müssen die Identitätsattribute anhand

- „eines Auszuges aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis“,
- der Gründungsdokumente oder
- gleichwertiger beweiskräftiger Dokumente oder
- durch Einsichtnahme in die Register- oder Verzeichnisdaten.

erhoben werden.[6]

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 gesetzlichen Vertreter einer 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

5 Gemäß § 3 De-Mail-Gesetz

6 Gemäß § 3 De-Mail-Gesetz

Institutionen	*Art der Identitätsbestätigung*
	(Papierform oder wenn möglich elektronisch)

Tabelle 4: Identitätsbestätigungen bei Unternehmen

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 Unternehmen

Für öffentliche Stellen:

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

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.

In 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[7]

Das Authentisierungsniveau „normal“ entspricht der Benutzung von Benutzername und Passwort.

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

- Zwei-Faktor-Authentisierung (Wissen und Besitz)
- 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 möglichst 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 Si ÜK]).

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 Si ÜK]).

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

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.

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),
- die Auswahl des Standard-Authentisierungsniveaus,
  - standardmäßig „normal“,
  - kann auf „hoch“ 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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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 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.

Wenn der Nutzer das Authentisierungsniveau „normal“ nutzt, darf der DMDA das genutzte Passwort nicht in einem in Klartext wiederherstellbaren Format speichern.

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 Sperrart Zugangsperre „normal“, nachdem er sich mit dem Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet hat.

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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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 endgültigen Löschung 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.

Weiterhin muss dem Nutzer die Möglichkeit geboten werden, einen Nachsendeauftrag (vgl. [TR DM PVD FU] zu einem anderen De-Mail-Konto zu stellen. Alle empfangenen Nachrichten werden in diesem Fall während einer vom DMDA festgelegten Übergangszeit an die im Nachsendeauftrag genannte De-Mail-Adresse weitergeleitet.

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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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.

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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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 bei De-Mail-Kontos von Institutionen mit mindestens 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 Rücksetzen 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 Änderung des Passworts für normales Authentisierungsniveau

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.

Es wird geprüft,

- ob das alte Passwort ein gültiges Passwort ist,
- ob die zweifach erfassten neuen Passworte identisch sind,
- ob das angegebene neue Passwort den Passwort-Regeln des DMDA gemäß [TR DM Si M] 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 nach der Verifikation auch 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 02101]),
- 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.

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.

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 einschließlich der De-Mail-Domain haben, ist die De-Mail-Adresse neu zu vergeben. Eine geänderte De-Mail-Adresse bzw. eine kontobezogene De-Mail-Domain für natürliche Personen muss dem De-Mail-Konto für eine Übergangszeit zugeordnet bleiben.

Die geänderte De-Mail-Adresse muss für den Zeitraum der verbleibenden Zuordnung zum De-Mail-Konto für den Empfang von Nachrichten genutzt werden. Sie darf als Versandadresse jedoch nicht mehr verwendet werden können.

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 weitere Nutzerkonten 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[8] Nutzung des De-Mail-Kontos durch Mitarbeiter anzulegen. Die Unterkonten gehören zu einer oder mehreren 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 und die Zuordnung zu ihren Unterkonten erfolgen durch den Nutzer. Die Zuordnung einer natürlichen Person zu einem Unterkonto und einer De-Mail-Adresse, die anzeigt, dass er im Auftrag der Institution handelt, muss durch den Nutzer definiert, geändert und gelöscht werden können.

8 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 Dritten und insbesondere der aufsichtsführenden Behörde 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:

- 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 die 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 Nutzer hat sicherzustellen, dass der Nutzer von dem Auskunftsersuchen unverzüglich informiert werden kann.

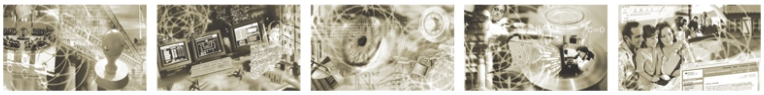
Die Inhalte der Dokumentation zur De-Mail-Konto-Eröffnung, bei Änderungen von Kontodaten und Kontozuständen sowie die Inhalte der Dokumentation zur Auskunftserteilung müssen entsprechende der Fristen gemäß Tabelle 7: Aufbewahrungsfristen der Dokumentation aufbewahrt werden.

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

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Accountmanagement IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 2.3
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die IT-Sicherheitsanforderungen, die sich speziell auf das Accountmanagement beziehen und über die generellen Anforderungen an die Sicherheit aus dem Modul [TR DM Si M] hinausgehen und ist Bestandteil von [TR DM ACM M].

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die in [TR DM IS ÜK] angenommene Netzinfrastruktur eines DMDA.

Bei der Erstellung des realen IT-Sicherheitskonzeptes sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der bereits in [TR DM Si ÜK] skizziert ist.

3 Bedrohungen

Folgende generische Bedrohungen werden für das Account Management angenommen:

3.1 Falsche Zuordnung eines De-Mail-Kontos zu einer natürlichen Person bzw. Institution

Bei einer falschen Zuordnung eines De-Mail-Kontos zu einer natürlichen Person bzw. Institution kann das Ziel, eine authentische Kommunikation, die insbesondere auf einer gesicherten Identifizierung, die gesicherte Erfassung der Identitätsdaten und der gesicherten und eindeutigen Zuordnung zum Konto basiert, nicht mehr erreicht werden. Eine falsche Zuordnung oder eine nicht nachvollziehbare Zuordnung kann etwa durch folgende Umstände erfolgen:

- Technisches Versagen
- Menschliches Versagen
- Fehlerhafte Identifizierung
- Manipulation der Zuordnung des De-Mail-Kontos
- Manipulation/Fälschung der Konto-Daten inkl. Dokumentation
- Löschung/Verlust von Konto-Daten inkl. Dokumentation

3.2 Missbräuchliche Nutzung eines Accounts

Gelingt es einem Angreifer, in den Besitz der Authentisierungsdaten zu gelangen oder eine Schwachstelle in den verwendeten IT-Verfahren und IT-Systemen auszunutzen, kann er mit der Identität des Kontoinhabers agieren und sich im Rechts- und Geschäftsverkehr als diesen ausgeben.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

4 Sicherheitsziele

Dieses Modul enthält die Sicherheitsziele in Bezug auf das Account Management und ergänzt insoweit das [TR DM Si ÜK].

4.1 Zuverlässige Identifizierung und Erfassung der Teilnehmer

Die Erfassung der Identitätsdaten und die Identifizierung des Kontoinhabers muss zuverlässig erfolgen. Die Identitätsattribute der natürlichen Personen und Institution müssen eindeutig festgestellt und in die Systeme unverfälscht übernommen werden.

4.2 Nachvollziehbarkeit der Identitätsdaten und der Zuordnung zum De-Mail-Konto

Die Dokumentation der Identitätsdaten und der Zuordnung zwischen Identität und De-Mail-Konto muss zu jeder Zeit vollständig, authentisch und unverfälscht verfügbar sein.

4.3 Verhinderung des unbefugten Zugriffs auf die Authentisierungsinformationen

Der unbefugte Zugriff auf die geheimen und nicht kopierbaren Teile der Authentisierungsinformationen muss ausgeschlossen sein.

4.4 Verhinderung der unbefugten Veränderung von Authentisierungs- und Identifizierungsinformationen

Die unbefugte Veränderung von Authentisierungs- und Identifizierungsinformationen muss ausgeschlossen sein.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

5 Anforderungen

5.1 Verifikation von Identitätsattributen

Im Sicherheitskonzept muss mindestens festgehalten werden:

- wie die Identitätsattribute erfasst werden,
- wie die Verifikation durchgeführt wird und
- wie die Übermittlung der Identitätsattribute sowie der Verifikationergebnisse erfolgt.

Bei der Übermittlung muss sichergestellt sein, dass:

- die Identitätsattribute korrekt sind und
- vertraulich übermittelt werden.

Sofern sich der DMDA zur Identifizierung der Nutzer vertrauenswürdiger Dritter bedient, hat er sicherzustellen, dass die Qualität des Gesamtprozesses einschließlich dessen Zuverlässigkeit und Fachkunde auch in diesem Fall gewährleistet wird.

5.2 Erfassung

Die Daten zur Identität sind zuverlässig im System zu hinterlegen und dem De-Mail-Konto zuzuordnen. Die Anbindung des Kontoadministrators an das Accountmanagement muss verschlüsselt, integer und authentisiert erfolgen. Für die Authentisierung sind Mechanismen wie bei dem Authentisierungsniveau „hoch“ einzusetzen.

5.3 Authentisierungsniveaus

Für die Authentisierung des Nutzers sind folgende Authentisierungsmethoden für die beiden zugelassenen Authentisierungsniveaus vorzusehen:

- Normal
  - Die Authentisierung erfolgt mittels Konto-Name und Passwort. Es ist insbesondere die Maßnahme „2.11 Regelung des Passwortgebrauchs“ aus dem IT-Grundschutz zu beachten. Des Weiteren ist die maximale Gültigkeitsdauer für ein Passwort ein Jahr.
- Hoch
  - Die Authentisierung muss mit zwei von einander unabhängigen Sicherungsmitteln z. B. Mit Besitz und Wissen erfolgen. Das Authentisierungstoken muss sicherstellen, dass das Geheimnis nicht kopiert und ausgelesen werden kann. Des Weiteren muss die Einmaligkeit der Authentisierungsinformationen, die innerhalb eines Anmeldeprozesses übertragen werden, gewährleistet sein. Die Authentisierung muss gleichen Anforderungen bei falscher Authentisierung und den Freischaltprozess erfüllen, wie das Authentisierungsniveau „normal“. Es sind die Anforderungen an die kryptographischen Verfahren und Schlüssellängen aus der TR 02101 zu beachten.

5.4 Authentisierung des Nutzers

Es ist sicherzustellen, dass der Nutzer keinen Zugriff auf sein De-Mail-Konto hat, bevor sich ordnungsgemäß authentisiert hat. Der Nutzer hat sich jeweils vor Zugriff auf sein Konto gegenüber dem Dienst des DMDA mit Authentisierungsniveau „normal“ oder „hoch“ zu authentisieren.

Die Authentisierungsinformationen des Nutzers werden auf Gültigkeit geprüft. Im Erfolgsfall wird der Nutzer zur Nutzung der gestatteten Funktionen autorisiert. Im Fehlerfall wird eine Fehlermeldung ausgegeben.

Sofern für die Authentisierung der Nutzer der Mechanismus Benutzername/Passwort zugelassen wird, hat der DMDA eine dem Schutzbedarf angemessene Passwortrichtlinie zu erstellen (vgl. [IT-GS Katalog].

Der DMDA hat sich davon zu überzeugen, dass die bei der Erzeugung des Tokens für das Authentisierungsniveau „hoch“ eingesetzten Prozesse eine hinreichende Qualität und Vertrauenswürdigkeit in Bezug auf das angestrebte Authentisierungsniveau aufweisen. Wenn als Authentisierungstoken für das Authentisierungsniveau „hoch“ der elektronische Personalausweis zum Einsatz kommt, darf der DMDA ohne weiteres von der Eignung des Tokens und der Ordnungsmäßigkeit der diesbezüglichen Prozesse ausgehen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Postfach- und Versanddienst Modul
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 3
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beschreibt die Struktur des Postfach- und Versanddienstes. Das Modul ist Bestandteil der [TR DM].

Die Kommunikation mit der heute gängigen E-Mail kann die Sicherheit in der Papierwelt nicht nachbilden. Authentizität der Kommunikationspartner, Vertraulichkeit sowie Rechtsverbindlichkeit sind nicht gewährleistet und der Empfang bzw. die Zustellung einer Nachricht kaum nachweisbar. Ziel des Postfach- und Versanddienstes von De-Mail ist es, das Versenden und Empfangen von Nachrichten und Dokumenten im Internet so einfach, sicher und verbindlich zu machen wie heute die Papierpost.

Während der Postfachdienst von De-Mail dem Nutzer die Möglichkeit zur Verfügung stellt, elektronische Nachrichten unter einer elektronischen De-Mail-Adresse zu empfangen, zu speichern und zu verwalten, ermöglicht der Versanddienst das verbindliche und nachvollziehbare Versenden von elektronischen Nachrichten.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2 Dokumentenübersicht

2.1 Funktionale Anforderungen

Die funktionalen Anforderungen an den PVD werden in [TR DM PVD FU] beschrieben, sowie die besonderen nicht-funktionalen Anforderungen.

2.2 Interoperabilität

Die Datenstrukturen zur Gewährleistung der Interoperabilität des PVD werden in [TR DM PVD IO] beschrieben.

2.3 IT-Sicherheit

Die spezifischen Anforderungen an die Sicherheit des PVD werden in [TR DM PVD Si] beschrieben.

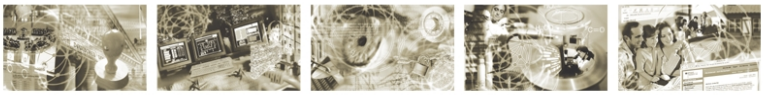
2.4 Funktionsprüfung

Die Spezifikation der Prüffälle für die Funktionsprüfung erfolgt in [TR DM PVD FU-PS].

2.5 Interoperabilitätsprüfung

Die Spezifikation der Prüffälle für die Interoperabilitätsprüfung erfolgt in [TR DM PVD FU-PS].

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Postfach- und Versanddienst Funktionalitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 3.1
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Abbildungsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Tabellenverzeichnis

1 Einleitung

Dieses Modul beinhaltet die funktionalen Spezifikationen des Postfach- und Versanddienstes und ist Bestandteil von [TR DM PVD M].

In diesem Modul werden die zwingenden Anforderungen an den PVD von De-Mail technikneutral beschrieben, sofern dieser angeboten wird. Eine Spezifikation von Protokollen und zugehörigen Parametern erfolgt nur dort, wo dies aus funktionaler Sicht explizit erforderlich ist.

2 Gesamtüberblick

Der Postfachdienst von De-Mail ermöglicht dem Nutzer als elektronischer Briefkasten, elektronische Nachrichten sowohl zu versenden als auch zu empfangen. Der Versanddienst ist für das verbindliche Versenden der Nachrichten verantwortlich. Beide Dienste sind eng miteinander verknüpft. Einerseits kann ein Nutzer ohne Postfachdienst keine an ihn adressierten Nachrichten empfangen, und andererseits wird der Versanddienst benötigt, um Nachrichten von einem Nutzer an einen anderen zu versenden. Die Abbildung 1 gibt einen Überblick über die Architektur des PVD. Die Bestandteile der Architektur und deren Zusammenwirken werden in den nachfolgenden Abschnitten beschrieben.

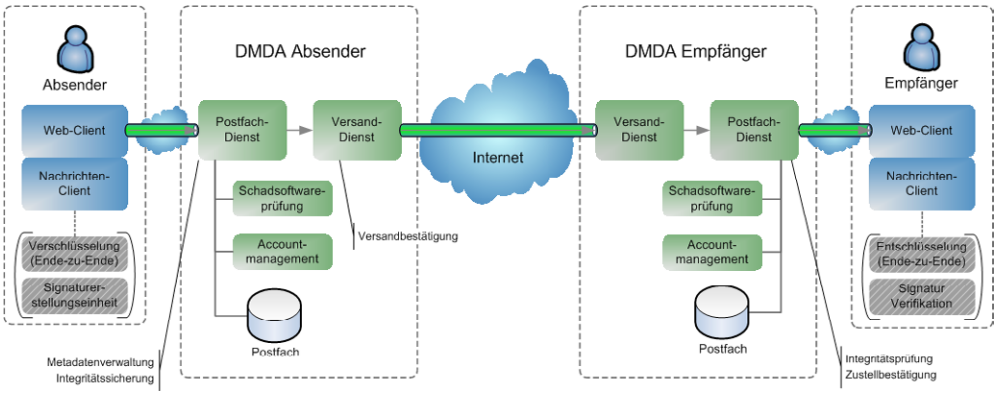


Abbildung 1: Architekturüberblick über den PVD

Absender und Empfänger von Nachrichten greifen über einen lokalen Web- oder Nachrichten-Client auf ihren Postfachdienst zu.

Der Postfachdienst erlaubt dem Nutzer, elektronische Nachrichten sowohl zu versenden als auch zu empfangen (siehe Abschnitt 3.1). Er sichert vor dem Versand von Nachrichten deren Integrität und schützt die Nachrichten durch Verschlüsselung vor dem Einblick unberechtigter Dritter. Beim Empfang entschlüsselt der Dienst die Nachrichten und prüft deren Integrität vor Abruf durch den Empfänger.

Empfangene und versendete Nachrichten werden im Postfach des Nutzers gespeichert und können dort von diesem verwaltet werden. Mit dem Postfach werden die De-Mail-Adressen des De-Mail-Kontos des Nutzers verbunden (primäre und pseudonyme Adressen, vgl. [TR DM ACM FU]). Unter dieser Adresse ist er einerseits als Empfänger erreichbar, andererseits kann er Nachrichten darunter als Absender versenden.

Zugriff erhält ein Nutzer auf sein Postfach über den Postfachdienst, wenn er sich an seinem De-Mail-Konto erfolgreich angemeldet hat (s. a. [TR DM ACM FU]). Das Authentisierungsniveau, mit dem der Nutzer sich am De-Mail-Konto anmeldet, wird sowohl beim Versand einer Nachricht als auch beim Lesen von empfangenen Nachrichten berücksichtigt.

Möchte der Absender die Nachricht zusätzlich elektronisch signieren und/oder Ende-zu-Ende-verschlüsseln, so kann er dies mit einer lokalen Signaturanwendungskomponente (SAK) bzw. mit einer lokalen Verschlüsselungskomponente durchführen. Diese Komponenten können auch in dem

lokalen Web- oder Nachrichten-Client, mit dem er die Nachrichten erstellt, integriert sein und können auch unabhängig von De-Mail genutzt werden. Auf diese Weise signierte und/oder verschlüsselte Nachrichten kann der Empfänger ebenfalls mit lokalen Komponenten entschlüsseln und vorhandene Signaturen prüfen. Darüber hinaus gewährleistet der DMDA die transparente Weiterleitung von bereits auf Nutzerseite verschlüsselten und/oder signierten Nachrichten.

Für das zuverlässige Versenden von elektronischen Nachrichten steht dem Nutzer der Versanddienst zur Verfügung (siehe Abschnitt 3.2). Dieser ermöglicht es, Nachrichten zu versenden und vom DMDA entsprechende Bestätigungen darüber zu erlangen, ob die Nachrichten versendet oder im Postfach des Empfängers eingegangen sind.

Nachrichten, die innerhalb des De-Mail-Verbundes versendet oder empfangen werden, werden obligatorisch auf Schadsoftware geprüft. Für qualifiziert signierte Nachrichtenanhänge kann der DMDA des Empfängers optional eine Signaturprüfung durchführen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

3 Funktionale Anforderungen

Die funktionalen Anforderungen an den PVD von De-Mail werden in diesem Abschnitt beschrieben.

3.1 Postfachdienst und Postfach

Jeder Nutzer von De-Mail besitzt mindestens ein Postfach. Auf dieses erhält er über den Postfachdienst Zugriff, wenn er sich an seinem De-Mail-Konto erfolgreich angemeldet hat (vgl. [TR DM ACM FU]). Das Authentisierungsniveau, mit dem der Nutzer sich am De-Mail-Konto angemeldet hat, wird sowohl beim Versand einer Nachricht als auch beim Abruf von Nachrichten (siehe Abschnitt 3.1.2.3) berücksichtigt.

In dem Postfach werden vom Nutzer versendete und an ihn übermittelte Nachrichten abgelegt. Zusätzlich können in dem Postfach z. B. Entwürfe von Nachrichten gespeichert werden.

Nachrichten werden an den Versanddienst für den zuverlässigen Transport an den oder die Empfänger übergeben und wenn gefordert Bestätigungen für den Versand, Eingang oder Abholung ausgestellt.

3.1.1 Erstellen und Versenden von Nachrichten

Bei der Erstellung der Nachrichten kann der Nutzer mindestens auswählen

- Versandoptionen (vgl. Abschnitt 3.3)
- Absenderadresse
  Der Nutzer hat die Auswahl zwischen der primären und einer ggf. gewählten pseudonymen De-Mail-Adresse, die dem De-Mail-Konto zugeordnet ist. Andere Adressen können nicht genutzt werden.
- Empfängeradresse
  Die Adressen können aus dem persönlichen Adressbuch, dem ÖVD oder manuell eingegeben werden. Es werden die Adressierungsarten „To:“ (Primärer Adressat), „CC:“ (*Carbon Copy*, Kopie) und „BCC:“ (*Blind Carbon Copy*, Blindkopie) unterstützt.
- Nachrichtentext
- Anhänge
  Die Anhänge können von dem lokalen Dateisystem des Nutzers oder aus der DA (optional) ausgewählt werden.

Des Weiteren kann die Nachricht optional durch den Nutzer mit einer (qualifizierten) Signatur versehen oder zusätzlich Ende-zu-Ende-verschlüsselt werden. Dies hat der DMDA in geeigneter Weise zu ermöglichen.

3.1.1.1 Übergabe einer Nachricht an den Postfachdienst

Die erstellte Nachricht wird vom lokalen Web- oder Nachrichten-Client mitsamt den ausgewählten Versandoptionen an den Postfachdienst des DMDA des Absenders übergeben.

Hat der Absender sich mit dem Authentisierungsniveau „normal“ am Postfachdienst angemeldet, so darf dieser pro Tag höchstens 100 Nachrichten versenden, wobei insgesamt (d.h. für alle 100 Nachrichten zusammen) höchstens 300 Empfänger adressiert werden dürfen. Dies soll verhindern, dass über eine kompromittierte De-Mail-Adresse Massensendungen verteilt werden.

Nach Entgegennahme der Nachricht durch den Postfachdienst prüft dieser die Nachricht auf Schadsoftware (vgl. Abschnitt 3.1.3.1), sofern die Nachricht nicht Ende-zu-Ende verschlüsselt ist. Wenn keine Schadsoftware gefunden worden ist, werden notwendige Metadaten der Nachricht, wie z. B. die korrekte Absender-Adresse oder die aktuelle Zeit, kontrolliert und ggf. ergänzt. Falls Schadsoftware gefunden worden ist, wird der Nutzer über das weitere Vorgehen informiert.

Der Postfachdienst versieht die Nachricht unter Einbeziehung der Metadaten mit einer Integritätssicherung. Die Nachricht wird über einen sicheren Kommunikationskanal an den Versanddienst übertragen und verschlüsselt im Postfach abgelegt (s. a. Abschnitt 3.2.2). Falls vom Absender eine Versandbestätigung angefordert wurde, wird ihm diese von seinem Versanddienst ausgestellt und in Form einer Nachricht in sein Postfach abgelegt.

3.1.2 Empfang und Abruf von Nachrichten

3.1.2.1 Ablage von Nachrichten im Postfach des Empfängers

Der Postfachdienst des Empfängers nimmt von seinem Versanddienst die übermittelten Nachrichten entgegen, legt diese im Postfach des Empfängers ab und erstellt eine Eingangsbestätigung, falls dies der Absender der Nachricht angefordert hat. Diese wird in einer separaten Nachricht an den Absender übermittelt. Der Empfänger der ursprünglichen Nachricht erhält eine Kopie der Eingangsbestätigung.

3.1.2.2 Darstellung der Nachrichten im Postfach

Im Postfach des Nutzers gespeicherte Nachrichten werden durch den Postfachdienst zu einer Liste zusammengefasst und entsprechend im lokalen Web- oder Nachrichten-Client dargestellt. Neu empfangene und noch nicht gelesene Nachrichten werden besonders gekennzeichnet. Weiterhin werden verschiedene Merkmale der Nachricht kenntlich gemacht. Der Nutzer hat die Möglichkeit, die Nachrichten nach diesen Merkmalen zu sortieren oder anzeigen zu lassen.

Nach folgenden Merkmalen muss in der Übersicht der eingegangenen Nachrichten mindestens differenziert werden können:

- Betreff der Nachricht,
- Absendezeitpunkt der Nachricht,
- Name des Absenders bzw. seine Adresse,

- Vorhandensein von Nachrichtenanhängen,
- Hinweis, ob vom Absender die Versandoptionen „Persönlich“ und/oder „Absenderbestätigt“ gewählt worden sind.

Folgende Informationen können optional in der Übersichtsansicht, müssen obligatorisch jedenfalls in der Einzelansicht einer Nachricht ersichtlich sein:

- Name des Empfängers bzw. seine Adresse,
- Authentisierungsniveau des Absenders,
- Vorhandensein einer Verschlüsselung,
- Vorhandensein von Signaturen (ggf. inkl. Prüfergebnisse),
- Hinweis, ob vom Absender eine Versand-, Eingangs- und/oder Abholbestätigung angefordert worden ist.

Nachrichten mit Schadsoftware müssen automatisch erkannt und in einen dafür vorgesehenen Ordner verschoben werden.

3.1.2.3 Abruf der Nachrichten

Der Postfachdienst muss sicherstellen, dass der Nutzer mit Authentisierungsniveau „normal“ nicht auf Nachrichten zugreifen kann, falls für die Nachricht die Versandoption „persönlich“ oder die Versandoption „Abholbestätigung“ gewählt wurde.

Sofern ein ausreichendes Authentisierungsniveau gegeben ist, entschlüsselt der Postfachdienst die Nachricht und überträgt diese an den Nutzer.

3.1.2.4 Entschlüsselung der Nachrichten und Überprüfung von Signaturen

Bei Ende-zu-Ende verschlüsselten Nachrichten oder Nachrichtenanhängen kann eine lokale Entschlüsselungskomponente dem Nutzer ermöglichen, diese auf seinem System zu entschlüsseln. Unabhängig von einer Signaturprüfung (s. a. Abschnitt 3.2.2) durch den DMDA, die optional durchgeführt werden kann, kann der Empfänger auch eine eigene, auf seinem lokalen System installierte Verifikationskomponente zur Prüfung der Signaturen nutzen.

Der DMDA hat den Einsatz derartiger Komponenten in geeigneter Weise zu unterstützen.

3.1.3 Weitere Funktionen des Postfachdienstes und des Postfaches

Neben Erstellung, Versand und Empfang von Nachrichten unterstützt der Postfachdienst von De-Mail in diesem Zusammenhang relevante Funktionen, die in den nachfolgenden Abschnitten aufgeführt werden.

3.1.3.1 Prüfung auf Schadsoftware

Der Postfachdienst überprüft Nachrichten vom Absender, die er an diesen für den Versand übergeben hat, auf Schadsoftware. Nachrichten, die Schadsoftware enthalten, dürfen nicht weiterversendet werden, der Absender ist entsprechend zu informieren.

Nachrichten, die der Postfachdienst des Empfängers entgegen nimmt, werden ebenfalls auf Schadsoftware geprüft. Nachrichten, die durch Schadsoftware infiziert sind, dürfen dem Empfänger nicht übermittelt werden. Sowohl der Absender als auch der Empfänger der Nachricht erhalten eine entsprechende Information.

Wurde vom DMDA des Empfängers keine Schadsoftware gefunden, wird die Nachricht zugestellt. Beim Abruf der Nachricht darf der Nutzer diese erneut auf Schadsoftware untersuchen lassen. Wird nun eine solche gefunden, darf der Nutzer erst nach einem expliziten Warnhinweis auf diese Nachricht zugreifen.

3.1.3.2 Automatisierte Weiterleitung an eine andere De-Mail-Adresse

Der Nutzer muss die Möglichkeit haben an sein De-Mail-Konto gesendete Nachrichten automatisch an eine andere De-Mail-Adresse weiterleiten zu lassen. Bei der automatisierten Weiterleitung wird die Nachricht im Postfach des Nutzers abgelegt, bevor eine Kopie an die Weiterleitungs-Adresse gesendet wird. Die Weiterleitung an eine Adresse, die keine De-Mail-Adresse ist, ist unzulässig.

Bei Nachrichten, für die eine Abholbestätigung angefordert wurde, erfolgt keine Weiterleitung, sondern nur eine Benachrichtigung an die Weiterleitungsadresse über den Eingang dieser Nachricht.

3.1.3.3 Nachsendeauftrag an eine andere De-Mail-Adresse

Von der automatisierten Weiterleitung ist der Nachsendeauftrag an eine andere De-Mail-Adresse abzugrenzen. Innerhalb eines Auflösungsantrags zu seinem De-Mail-Konto (vgl. [TR DM ACM FU]) kann der DMDA dem Nutzer die Möglichkeit anbieten, einen Nachsendeauftrag an eine andere De-Mail-Adresse zu stellen. Alle empfangenen Nachrichten werden während einer festgelegten Übergangszeit an diese weitergeleitet. Bei einem Nachsendeauftrag wird keine Kopie im Postfach des Nutzers abgelegt. Eine ggf. angeforderte Eingangsbestätigung oder Abholbestätigung wird erst durch den Postfachdienst erzeugt, an den die Nachricht nachgesendet worden ist.

3.1.3.4 Export und Import von Nachrichten

Der Nutzer muss die Möglichkeit haben, empfangene und versendete Nachrichten und deren Anhänge auf sein lokales System zu exportieren. Der Export erfolgt durch den Postfachdienst auf Anforderung des Nutzers, inkl. des Integritätsschutzes (vgl. Abschnitt 3.2.2).

3.1.3.5 Zugriff auf Adressbuch und ÖVD

Über den Postfachdienst kann der Nutzer auf die Kontaktdaten zugreifen, die in dem Adressbuch seines De-Mail-Kontos hinterlegt sind.

Zusätzlich zu dem persönlichen Adressbuch kann der Nutzer auch den ÖVD von De-Mail (siehe [TR DM IT-BInfra FU]) nutzen, in dem die freigegebenen Kontaktdaten der De-Mail-Nutzer veröffentlicht sind.

3.1.3.6 Weiterleiten und Beantworten von Nachrichten

Der Nutzer hat die Möglichkeit, eine Nachricht an andere De-Mail-Empfänger weiterzuleiten und diese zu beantworten. Standardmäßig wird die ursprüngliche Nachricht als Anhang einer neuen Nachricht weitergeleitet, sodass die Metadaten der ursprünglichen Nachricht erhalten bleiben. Andere Weiterleitungsformate (z. B. ein „>“ vor jeder Zeile der ursprünglichen Nachricht) kann der Nutzer konfigurieren. Es ergeben sich die gleichen Anforderungen wie für eine neue Nachricht (vgl. Abschnitt 3.1.1).

3.1.3.7 Ablage von Nachrichten in Kategorien

Nachrichten können vom Nutzer in eigene Kategorien sortiert werden. Eine Kategorie entspricht einem Ordner, in dem die Nachricht abgelegt werden kann. Die Möglichkeit einer Zuordnung zu mehreren Kategorien kann optional durch den DMDA angeboten werden.

Es ist auch möglich, Nachrichten automatisch bei Empfang im Postfach entsprechenden Kategorien zuzuordnen. Eine Administration dieser Regeln erfolgt durch den Nutzer selbst.

3.1.3.8 Suchfunktionen für Nachrichten

Der Nutzer muss eine Suchfunktion des Postfachdienstes nutzen können, um Nachrichten innerhalb seines Postfaches aufzufinden. Optional können Anhänge von Nachrichten mit Office- und PDF-Dokumenten durchsucht werden, sofern diese nicht Ende-zu-Ende-verschlüsselt sind.

3.1.3.9 Löschen von Nachrichten

Nachrichten dürfen durch den Nutzer nur in einem 2-Stufen-Prozess gelöscht werden können:

1. Stufe: Verschieben der zu löschenden Nachricht in einen Papierkorb, in dem zu löschende Dokumente abgelegt werden.
2. Stufe: Endgültiges und unwiederbringliches Löschen von allen bzw. einzelnen Nachrichten aus dem Papierkorb.

Nachrichten, bei denen sich der Empfänger mit Authentisierungsniveau „hoch“ anmelden muss, um auf die Nachrichten zugreifen zu können, dürfen nur gelöscht werden, wenn sich der Empfänger auf diesem Authentisierungsniveau angemeldet hat. Eine Nachricht, für die eine Eingangs- oder Abholbestätigung erteilt worden ist, darf durch den Empfänger mit Authentisierungsniveau „normal“ erst 90 Tage nach ihrem Eingang gelöscht werden können. Bei der Abholbestätigung beginnt diese Frist erst, wenn sie ausgestellt wurde, dass heißt, wenn sich der Empfänger einmal mit Authentisierungsniveau „hoch“ angemeldet hat. Wenn der Empfänger sich mit

Authentisierungsniveau „hoch“ anmeldet, darf die Nachricht auch vor Ablauf der 90 Tage gelöscht werden können.

3.2 Versanddienst

Der Versanddienst stellt zusammen mit dem Postfachdienst sicher, dass Nachrichten von einem De-Mail-Nutzer zu einem anderen De-Mail-Nutzer vertraulich und verbindlich übermittelt werden. Weiterhin ermöglichen beide Dienste, Bestätigungen darüber zu erlangen, ob die Nachricht versendet wurde oder im Postfach des Empfängers eingegangen ist (siehe Abschnitte 3.2.2).

3.2.1 Benachrichtigung bei falscher Adressierung oder vollständiger Sperrung

Bei Empfang einer Nachricht an

- eine nicht existierende De-Mail-Adresse oder
- an ein vollständig gesperrtes De-Mail-Konto (vgl. [TR DM ACM FU]),

sendet der Versanddienst eine Fehlermeldung an den Absender. Es darf keine Eingangsbestätigung ausgestellt werden.

3.2.2 Transport von Nachrichten innerhalb von De-Mail

Die Übermittlung der Nachrichten vom Postfachdienst des Absenders zum Postfachdienst des Empfängers erfolgt innerhalb von De-Mail ausschließlich über sichere Transportkanäle (vgl. [TR DM Si ÜK].

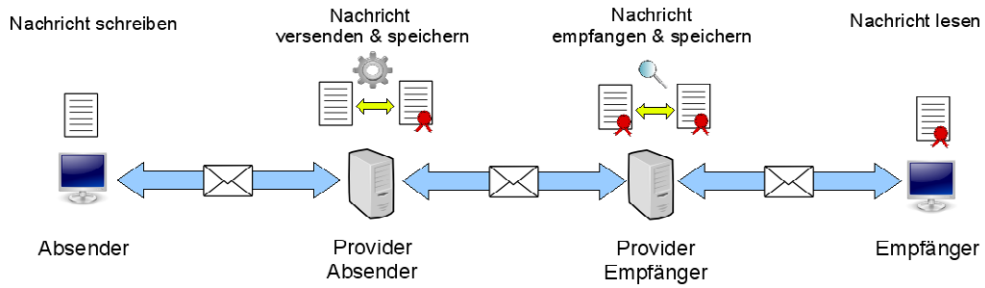


Abbildung 2: Transport von Nachrichten innerhalb von De-Mail

Unmittelbar nach Entgegennahme der Nachricht vom Sender überprüft der Postfachdienst die Nachricht auf Schadsoftware und die übermittelten Metadaten auf Validität. Der DMDA ergänzt weitere Metadaten wie z. B. die aktuelle Zeit und versieht die Nachricht inklusive der Metadaten mit einer Integritätssicherung. Die Metadaten sind der Nachricht eindeutig zugeordnet. Anschließend wird die Nachricht sowohl für den Postfachdienst des Empfängers als auch für den Postfachdienst des Absenders verschlüsselt. Die so gesicherte Nachricht wird vom Postfachdienst sowohl in das Postfach des Absenders als auch an den Versanddienst des Absenders übertragen.

Der Versanddienst des Absenders übermittelt die gesicherte Nachricht anschließend an den Versanddienst des Empfängers, der prüft, ob er die Nachricht zustellen kann. Im positiven Fall leitet er die Nachricht an den Postfachdienst weiter. Nach Entgegennahme durch den Postfachdienst wird die Nachricht wiederum temporär entschlüsselt und auf Schadsoftware geprüft. Die Nachricht wird im Postfach des Empfängers verschlüsselt abgelegt.

Ein Abruf von Nachrichten durch den Empfänger erfolgt über einen sicheren Transportkanal. Der Postfachdienst prüft hierbei, ob das aktuelle Authentisierungsniveau des Empfängers für den Zugriff auf die konkrete Nachricht ausreicht. Nachfolgend entschlüsselt der Postfachdienst die abgerufene Nachricht, kontrolliert die Integritätssicherung und übermittelt sie an den lokalen Web- oder Nachrichten-Client.

3.3 Versandoptionen

Die Einführung elektronischer Versandoptionen mit einer definierten und standardisierten Anzahl von Produktausprägungen ist eine wesentliche Aufgabe von De-Mail.

Bei dem Versand von Nachrichten innerhalb von De-Mail sind die folgenden Merkmale von wesentlicher Bedeutung:

- Authentizität des Empfängers einer Nachricht
- Authentizität des Absenders einer Nachricht
- Bestätigungen über den jeweiligen Zustand einer Nachricht
- Integritätssicherung von Nachrichten

Die oben aufgeführten Merkmale sind in den nachfolgend beschriebenen Versandoptionen abgebildet.

Alle Versandoptionen müssen vom DMDA angeboten werden. Die Versandoptionen können einzeln auswählbar sein. Der DMDA kann Kombinationen der Versandoptionen anbieten.

In der Bezeichnung muss sichergestellt sein, dass alle Versandoptionen für den Nutzer klar erkennbar sind. Der Nutzer ist bei Kombinationen darüber zu informieren, welche Versandoptionen in diesen enthalten sind.

3.3.1 Persönlich

Hiermit kann der Absender zum Ausdruck bringen, dass er besonderen Wert auf den sicheren Zugang seiner Nachricht beim Empfänger selbst legt. Hier muss das erforderliche Authentisierungsniveau des Empfängers „hoch“ sein, um die Nachricht lesen zu können. Um diese Option wählen zu können, muss das Authentisierungsniveau des Absenders ebenfalls „hoch“ sein.Verfügt der Empfänger nicht über das Authentisierungsniveau "hoch", wird die Nachricht von seinem Postfachdienst mit einer Fehlermeldung an den Absender zurückgeschickt.

3.3.2 Absenderbestätigt

Hiermit kann der Absender gegenüber dem Empfänger zum Ausdruck bringen, dass er sich zum Absenden der Nachricht sicher angemeldet hat. Um diese Option wählen zu können, muss das Authentisierungsniveau des Absenders „hoch“ sein. Der DMDA des Absenders versieht die Nachricht und die Metadaten mit einer qualifizierten Signatur.

3.3.3 Versandbestätigung

Hiermit erhält der Absender einen Nachweis über den ordnungsgemäßen Versand seiner Nachricht. Die Versandbestätigung wird vom Versanddienst des Absenders erzeugt und diesem per Nachricht übermittelt.

3.3.4 Eingangsbestätigung

Hiermit erhalten Absender und Empfänger einen Nachweis darüber, wann der DMDA des Empfängers die Nachricht im Postfach des Empfängers abgelegt hat. Die Eingangsbestätigung wird vom Postfachdienst des Empfängers erzeugt und dem Absender sowie dem Empfänger der ursprünglichen Nachricht per Nachricht übermittelt.

3.3.5 Abholbestätigung

Hiermit erhalten Absender und Empfänger einen Nachweis darüber, wann der DMDA die Nachricht im Postfach des Empfängers abgelegt hat und dass sich der Empfänger nach dem Eingang der Nachricht an seinem De-Mail-Konto mit Authentisierungsniveau „hoch“ angemeldet hat. Die Abholbestätigung wird vom Postfachdienst des Empfängers erzeugt, wenn sich der Empfänger das erste Mal nach dem Ablegen der Nachricht in seinem Postfach mit Authentisierungsniveau „hoch“ anmeldet. Die Abholbestätigung wird dem Absender sowie dem Empfänger der ursprünglichen Nachricht per Nachricht übermittelt. Diese Option steht beim Versand nur berechtigten öffentlichen Stellen zur Verfügung.

4 Besondere nicht-funktionale Anforderungen

4.1 Speicherplatz

Jeder Nutzer eines De-Mail-Kontos hat einen Mindest-Speicherplatz (vgl. [TR DM]) zur Verfügung. Die Größenbegrenzung einer Nachricht darf nicht unter 10 MByte liegen.

Der Nutzer muss gewarnt werden, sobald der freie Speicherplatz seines Postfaches nur noch über weniger als 10% des maximalen Speicherplatzes verfügt.

Wenn der Speicherplatz belegt ist, kann der DMDA den Versand weiterer Nachrichten unterbinden. Der Empfang von Nachrichten muss weiterhin möglich sein.

4.2 Transportzeiten

Nachrichten, die über den PVD versendet werden, müssen spätestens acht Stunden nach Absendung beim DMDA des Empfängers im Postfach liegen und durch den Empfänger abgerufen werden können. Erfolgt der Versand von Nachrichten an einen Empfänger eines anderen DMDAs, muss der DMDA des Absenders die Nachricht spätestens nach 4 Stunden dem DMDA des Empfängers übermittelt haben.

4.3 System-Adressen

In der nachfolgenden Tabelle werden die System-Adressen (siehe [TR DM ACM FU]) aufgelistet, die innerhalb des PVD verwendet werden müssen.

Verwendungszweck	***De-Mail-Adresse***
Versandbestätigung	Versandbestaetigung@<DMDA>
Eingangsbestätigung	Eingangsbestaetigung@<DMDA>
Abholbestätigung	Abholbestaetigung@<DMDA>
Warnung vor Schadsoftware	Schadsoftware-Warnung@<DMDA>
Meldung	Meldung@<DMDA>

Tabelle 1: Liste der in dem PVD verwendeten System-Adressen

Weitere Adressen können durch den DMDA für eigene Verwendungszwecke selbst definiert werden.

5 Datenstrukturen

Im PVD sind insbesondere „Nachrichten“, „Bestätigungsnachrichten“ und „Meldungsnachrichten“ zu unterscheiden.

5.1 Nachrichten

Konzeptuell ist von einer Nachricht 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 (siehe Abschnitt 7, Schritt 27) gesetzt worden sind.

Nachrichten bestehen aus Metadaten und dem Nachrichtentext.

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

Nr.	Bezeichnung	Werte	Beschreibung
1	Versandbestätigung	ja / nein	Dieses Feld entspricht der Versandoption „Versandbestätigung“. Es ist auf „ja“ gesetzt, falls diese Option in Schritt 1 ausgewählt wurde. In diesem Fall generiert der PVD des Absenders eine Versandbestätigung, sobald diese Nachricht versendet worden ist (Schritt 34 ff.).
2	Eingangsbestätigung	ja / nein	Dieses Feld entspricht der Versandoption „Eingangsbestätigung“. Es ist auf „ja“ gesetzt, falls diese Option in Schritt 1 ausgewählt wurde. In diesem Fall generiert der PVD des Empfängers eine Eingangsbestätigung, sobald diese Nachricht im Postfach des Empfängers abgelegt worden ist (Schritt 65 ff.).
3	Abholbestätigung	ja / nein	Dieses Feld entspricht der Versandoption „Abholbestätigung“. Es ist auf „ja“ gesetzt, falls diese Option in Schritt 1 ausgewählt wurde. Der Absender muss zum Zeitpunkt des Versendens mit Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet sein (Prüfung erfolgt in Schritt 19). Eine Abholbestätigung darf nur durch berechtigte öffentliche Stellen angefordert werden (Prüfung erfolgt in Schritt 22). Ist diese Versandoption gesetzt, generiert der PVD

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Nr.	Bezeichnung	Werte	Beschreibung
			des Empfängers eine Abholbestätigung, nachdem diese Nachricht in dessen Postfach abgelegt worden ist und der Nutzer sich das nächste Mal an seinem De-Mail-Konto mit Authentisierungsniveau „hoch“ anmeldet.
4	Absenderbestätigt	ja / nein	Dieses Feld entspricht der Versandoption „Absenderbestätigt“. Es ist auf „ja“ gesetzt, falls diese Option ausgewählt wurde. Der Absender muss zum Zeitpunkt des Versendens mit Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet sein (Prüfung erfolgt in Schritt 19).
5	Persönlich	ja / nein	Dieses Feld entspricht der Versandoption „Persönlich“. Es ist auf „ja“ gesetzt, falls diese Option ausgewählt wurde. Der Empfänger muss zum Zeitpunkt des Abrufs mit Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet sein (Prüfung erfolgt in Schritt 76). Der Absender muss zum Zeitpunkt des Versendens mit Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet sein (Prüfung erfolgt in Schritt 19).
6	Absender-Adresse	De-Mail-Adresse	Die vom Absender in Schritt 2 gewählte De-Mail-Adresse, unter der die Nachricht versendet werden soll (Prüfung der Gültigkeit erfolgt in Schritt 12).
7	Empfänger-Adresse(n) (auch für CC, BCC)	De-Mail-Adresse	Die vom Absender in Schritt 3 gewählten Empfänger-Adressen, an die die Nachricht versendet werden soll (Prüfung auf Validität in Schritt 15). Hinweis: Nur die eigene BCC-Adresse wird für den jeweiligen BCC-Empfänger innerhalb der Metadaten auf der Empfänger-Seite belassen.
8	Betreff	Text	Der vom Absender in Schritt 4 angegebene „Betreff“ zur Nachricht.
9	Nachrichten-Kennung des Absenders	Text	Die vom Absender in Schritt 4 angegebene „Nachrichten-Kennung“ ermöglicht dem Absender, einer Nachricht zusätzlich zum Betreff eine Information mitzugeben. Anhand dieser Kennung kann er andere Nachrichten, die die Nachrichten-Kennung referenzieren, wie z. B.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Nr.	Bezeichnung	Werte	Beschreibung
			Bestätigungsnachrichten, einem internen Vorgang zuordnen.
10	Antwort-Adresse	De-Mail-Adresse	Optionale Angabe, an welche De-Mail-Adresse eine Antwort auf diese Nachricht adressiert werden soll (wird in Schritt 3 gesetzt). An diese Adresse werden auch eventuell angeforderte Bestätigungsnachrichten gesendet (Prüfung auf Validität in Schritt 12).
11	Authentisierungs-niveau	normal/hoch	Das Authentisierungsniveau, mit dem der Absender zum Zeitpunkt des Versendens der Nachricht am De-Mail-Konto angemeldet war (wird in Schritt 27 gesetzt).
12	Authentisierungs-Mechanismus	Text	Bezeichnung des Authentisierungsmechanismus, mit dem der Absender sich zum Zeitpunkt des Versendens der Nachricht am De-Mail-Konto angemeldet hatte (wird in Schritt 27 gesetzt). Hinweis: Dieses Feld wird im PVD nicht weiter ausgewertet. Es soll jedoch Absendern und Empfängern ermöglichen, sich bilateral auf einen für ein bestimmtes Fachverfahren notwendigen Authentisierungsmechanismus zu verständigen.
13	Versanddatum und -zeit	Datum & Zeit	Datum und sekundengenau Zeitangabe für den Zeitpunkt, an dem der Postfachdienst die Nachricht an den Versanddienst weiterleitet (wird in Schritt 27 gesetzt).
14	Message-ID	Text	Eindeutige Kennung der Nachricht, die vom Postfachdienst generiert wird. Mit dieser Kennung soll es möglich sein, Nachrichten im Rahmen einer Postfach-internen Verwaltung schnell zu referenzieren (wird in Schritt 27 gesetzt).
15	De-Mail-Server	Text	Eindeutige Bezeichnung des DMDA-Servers, der diese Metadaten erstellt (wird in Schritt 27 gesetzt).
16	Nachrichten-Typ	Bestätigungs-nachricht/ Meldungs-nachricht/ nicht weiter spezifizierte	In diesem Feld können spezielle Nachrichten, die automatisiert vom Empfänger-System behandelt werden sollen, als solche gekennzeichnet werden (siehe z. B. Schritt 27, Schritt 36, Schritt 54 und Schritt 67). Damit soll verhindert werden, dass der Inhalt aller Nachrichten aufwändig analysiert

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Nr.	Bezeichnung	Werte	Beschreibung
		De-Mail-Nachricht	werden muss, um die entsprechenden Nachrichten zu identifizieren. Innerhalb des PVD sind als spezielle Nachrichten Bestätigungs- und Meldungsnachrichten vorgesehen.
17	Hash-Wert / Signatur	Message Digest / Signatur	Message Digest, der über die Metadaten-Felder 1 bis 16, sowie über alle Abschnitte des Nachrichtentexts berechnet wird. Der Message Digest wird vom Postfachdienst des Absenders in Schritt 27 erstellt. Falls die Versandoption „Absenderbestätigt“ vom Nutzer gewählt wurde und dieser auch mit Authentisierungsniveau „hoch“ am De-Mail-Konto zum Zeitpunkt des Nachrichtenversandes angemeldet war, wird in Schritt 29 eine qualifizierte Signatur erzeugt und in dem Feld gespeichert. Die Metadaten werden nach Versand durch den Postfachdienst des Absenders im Kontrollfluss des PVD nicht verändert.
18	Signaturzertifikat des DMDA	Signatur	Dieses Feld wird durch den DMDA nur gesetzt (Schritt 29), falls die Versandoption „Absenderbestätigt„ vom Nutzer gewählt wurde und dieser auch mit Authentisierungsniveau „hoch“ am De-Mail-Konto zum Zeitpunkt des Nachrichtenversandes angemeldet war. Dieses Feld enthält das für die Signatur verwendete Zertifikat des DMDA.
19	Empfänger-Adressen für den Transport	De-Mail-Adresse	Hinweis: Beim Transport können die Empfänger-Adressen bei Weiterleitungen umgeschrieben werden (vgl. Schritt 48 und Schritt 70). Im Initial-Zustand müssen diese Adressen denen von Nr. 7 entsprechen (erfolgt in Schritt 27).
20	Weiterleitungs-Absender	De-Mail-Adresse	Dieses Feld wird durch den Postfachdienst des Empfängers nur gesetzt (Schritt 70), falls eine automatische Weiterleitung eingerichtet wurde. Das Feld wird auf die De-Mail-Adresse gesetzt, von der die Nachricht weitergeleitet wird.

Tabelle 2: Metadaten einer Nachricht

Die Metadaten 1 bis 5 („Versandoptionen“) entsprechen den vom Absender einer Nachricht ausgewählten Versandoptionen (vgl. Abschnitt 3.3). Falls ein Nutzer eine Nachricht oder Nachrichtenanhänge (qualifiziert) signiert oder Ende-zu-Ende-verschlüsselt, so werden in diesem Fall die ausgewählten Nachrichten-Teile direkt signiert und/oder verschlüsselt, ohne dies in den Metadaten explizit zu speichern.

Die Metadaten 6 bis 10 („Adressen und Betreff“) werden bei der Erstellung des Nachrichtenentwurfs (vgl. Abschnitt 7.1) durch den Nutzer spezifiziert. Die Metadaten 11 bis 19 („interne Verwaltungsdaten“) werden vom Postfachdienst des Absenders erstellt bzw. vordefiniert, wenn aus dem Nachrichtenentwurf eine Nachricht geworden ist (Schritt 27 und Schritt 29). Das Metadatum „Weiterleitungs-Absender“ (Feld 20) wird erst vom PVD des jeweiligen Empfängers gesetzt, von dem die Nachricht weitergeleitet wird.

5.2 Bestätigungen und Bestätigungsnachrichten

Bestätigungsnachrichten sind Nachrichten, die die vom PVD erstellten Bestätigungen, wie bspw. für den Versand oder die Zustellung von Nachrichten, im Nachrichtentext beinhalten. Die Bestätigung enthält mindestens folgende Informationen, die von der referenzierten Nachricht stammen:

Nr.	Bezeichnung	Wert	Bemerkung
1.	Betreff	[Bestätigungsart]: Betreff aus der ursprünglichen Nachricht	Text, der die Art der Bestätigung widerspiegelt und für den Nutzer eine einfache Verknüpfung zur ursprünglichen Nachricht ermöglichen soll, über deren Betreff.
2.	Bestätigungstext	Text	Weitergehende Erläuterungen zur Bestätigung.
3.	Metadaten	Metadaten der ursprünglichen Nachricht, über die der Hash-Wert berechnet wird (Felder 1 bis 16)	Die Metadaten ermöglichen eine Verknüpfung der Bestätigungsnachricht mit der ursprünglich versendeten Nachricht.
4.	Hash-Wert	Message-Digest	Hash-Wert der ursprünglichen Nachricht (Feld 17).
5.	Zeit	Datum und Uhrzeit	Zeitpunkt (sekundengenau) des Versandes (bei Versandbestätigung), der Ablage der Nachricht (bei Eingangsbestätigung) bzw. ersten Anmeldung nach der Ablage der Nachricht durch den Nutzer (Abholbestätigung)
6.	Aussteller	Kennung des DMDA	Eindeutiger Name des ausstellenden DMDA

Tabelle 3: Inhalt einer Bestätigung

Die Bestätigung ist durch den ausstellenden DMDA mit einer qualifizierten elektronischen Signatur zu signieren.

Das Feld Nachrichten-Typ in den Metadaten ist auf den Wert „Bestätigungsnachricht“ gesetzt. Absender einer Bestätigungsnachricht ist jeweils der DMDA von einer System-Adresse (vgl. [TR DM ACM FU]).

Bestätigungsnachrichen müssen einen Hinweis zur Verwendung oder Interpretation der Anhänge in Textform enthalten. Des Weiteren sollten diese Hinweise auch einige wesentliche Informationen aus den signierten Bestätigungen referenzieren, wie z. B. den Betreff der ursprünglichen Nachricht.

5.3 Meldungen und Meldungsnachrichten

Meldungen sind Informationen des DMDA an den Nutzer, um ihn über bestimmte Ereignisse zu informieren. In Abhängigkeit der Benutzerschnittstelle, die der Nutzer zur Interaktion mit dem PVD verwendet, können Meldungen unterschiedlich dargestellt oder bekannt gemacht werden. Alternativ können sie auch als Nachricht über den PVD an den Nutzer verschickt werden. Es muss sichergestellt werden, dass der Nutzer Meldungen, über die von ihm verwendete Benutzerschnittstelle unmittelbar zur Kenntnis nehmen kann.

Meldungen beinhalten mindestens folgende Informationen:

Nr.	Bezeichnung	Wert	Bemerkung
1	Betreff	Text	Text, der die Art der Meldung widerspiegelt und den Bezug zum auslösenden Ereignis ermöglicht
2	Meldungstext	Text	Weitergehende Erläuterungen
3	Zeit	Datum und Uhrzeit	Sekundengenauer Zeitpunkt der Erstellung der Meldung
4	Aussteller	Kennung des DMDA	Eindeutiger Name des ausstellenden DMDA

Tabelle 4: Inhalt einer Meldung

Werden Meldungen in Form von Nachrichten verschickt, so werden diese Nachrichten Meldungsnachrichten genannt.

Das Feld Nachrichten-Typ in den Metadaten einer Nachricht wird auf den Wert „Meldungsnachricht“ gesetzt. Der Betreff der Nachricht ist gleich dem Betreff der Meldung.

Wenn in diesem Dokument von einer „Meldungsnachricht“ gesprochen wird, so ist die Meldung in Form einer Meldungsnachricht zu verschicken. Ist hingegen nur von „Meldung“ die Rede, so kann diese in Abhängigkeit von der Benutzerschnittstelle auch anders verschickt bzw. dargestellt werden.

Werden Meldungen als Meldungsnachrichten verschickt und bezieht sich eine solche Meldungsnachricht auf eine andere vom Nutzer versendeten Nachricht, so sollte zur besseren

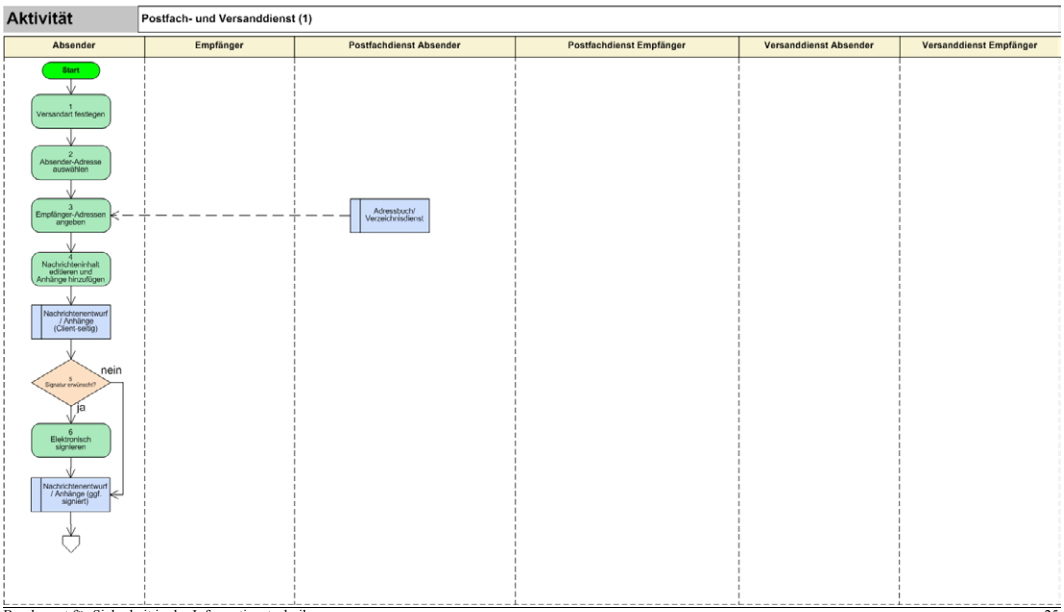
Zuordnung auf Nutzerseite der Wert des Metadatums „Nachrichten-Kennung des Absenders“ der ursprünglichen Nachricht in die Meldungsnachricht übernommen werden.

6 Aktivitätsdiagramm

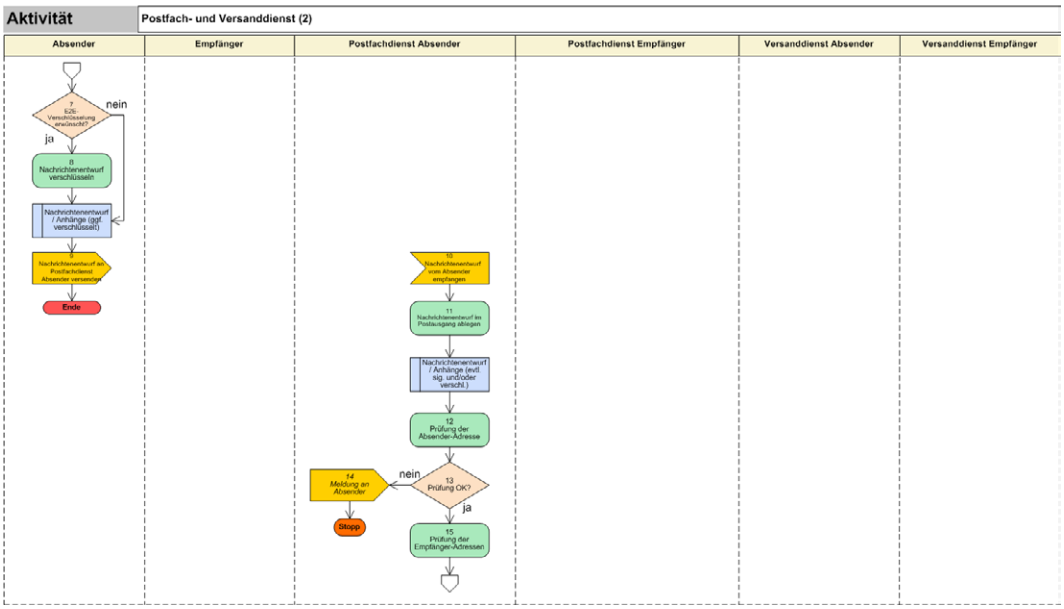
In Fehler: Referenz nicht gefunden wird der funktionale Ablauf des PVD für das Erstellen, Versenden, Empfangen und Abrufen von Nachrichten in einem Aktivitätsdiagramm dargestellt. Eine Legende zu den Symbolen des Aktivitätsdiagramms findet sich in Abschnitt 10. Eine detaillierte technisch-funktionale Beschreibung der einzelnen Aktionen und Schritte des Aktivitätsdiagramms erfolgt im Abschnitt 7.

Die im Aktivitätsdiagramm referenzierte „Transportsicherung“ entspricht dem in Abschnitt 3.2.2 beschriebenen Verfahren, nachdem eine zu versendende Nachricht durch den DMDA des Absenders integritätsgesichert und an den DMDA des Empfängers versendet wird.

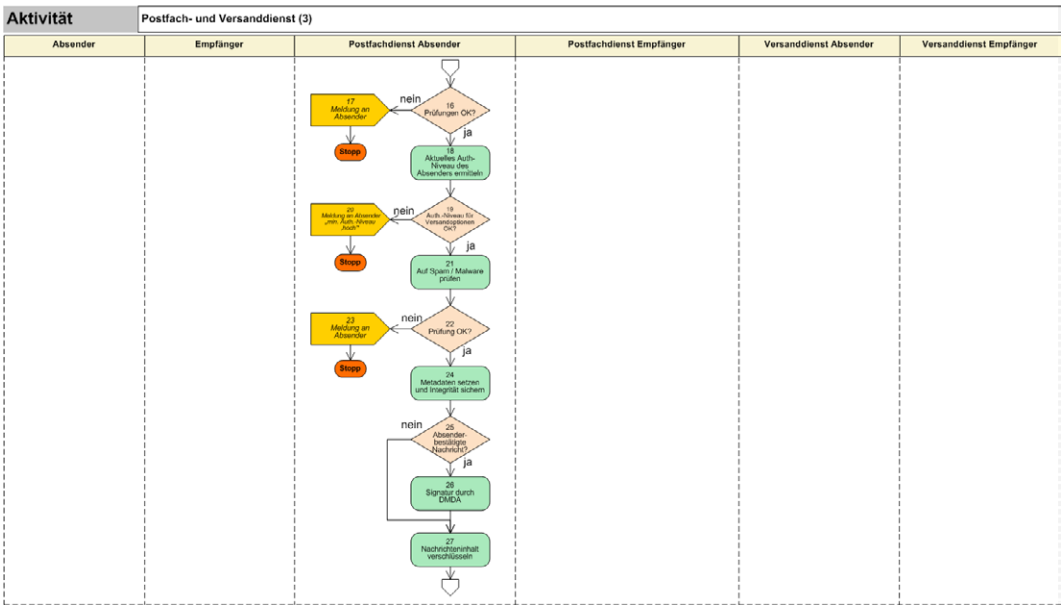
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger



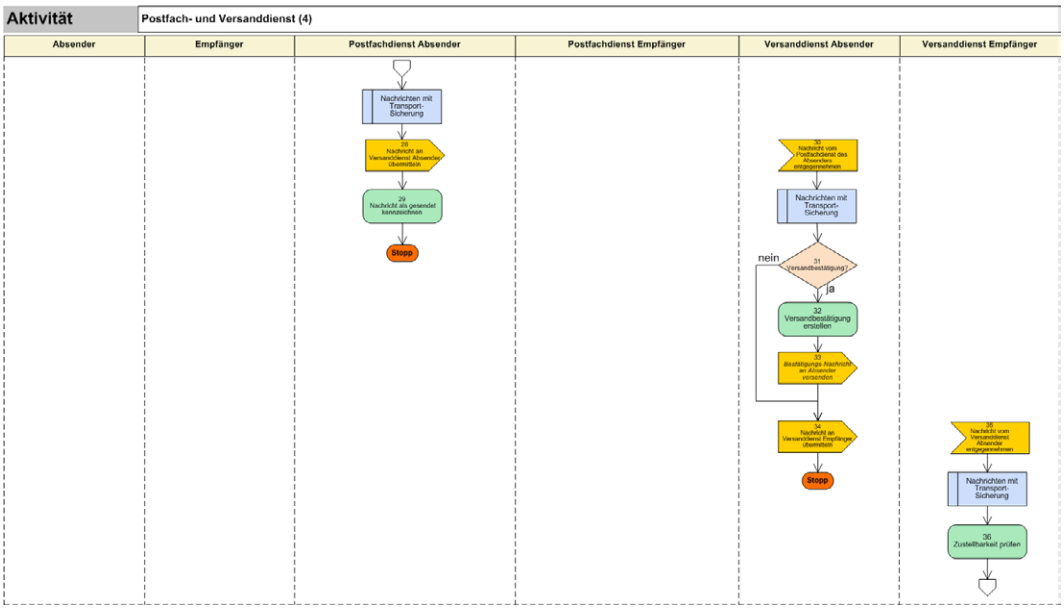
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger



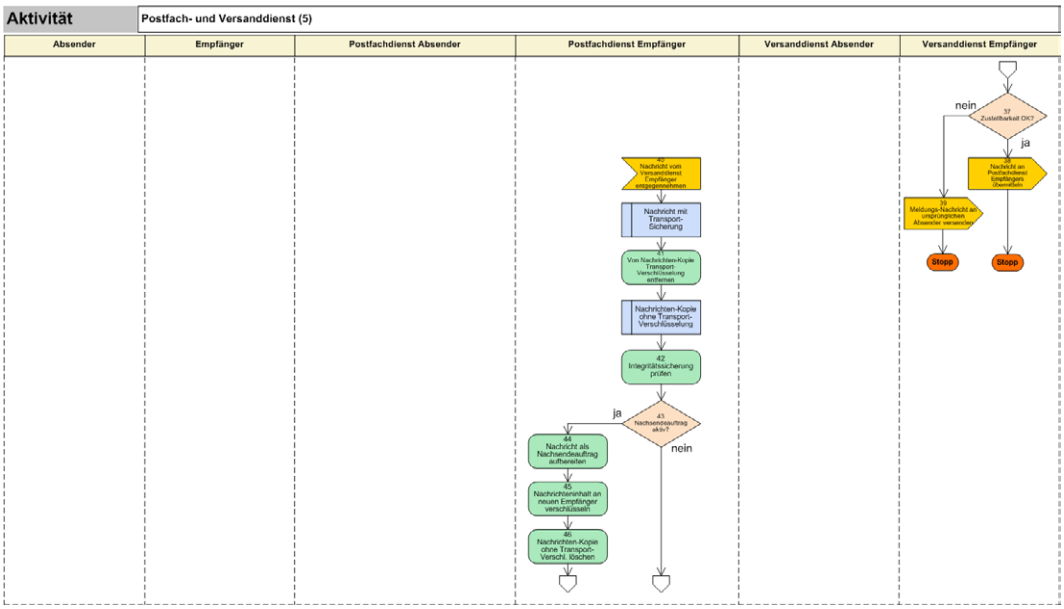
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

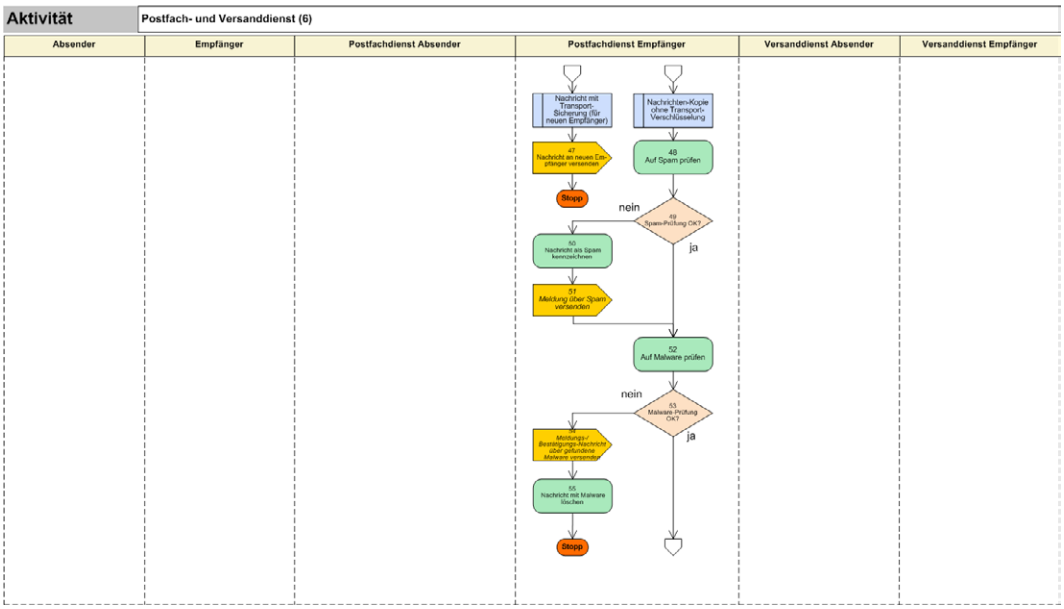


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

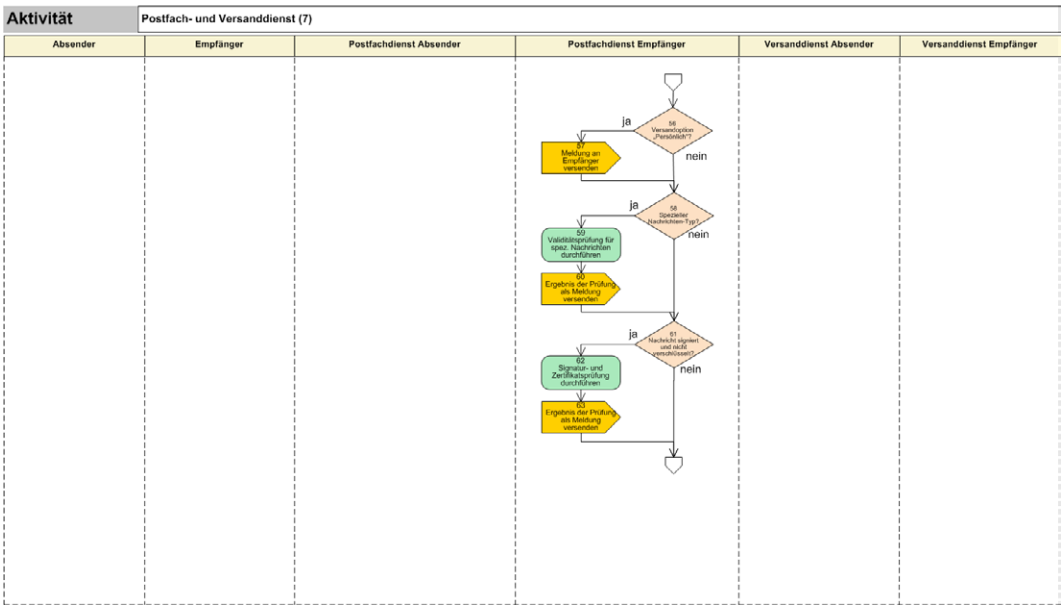


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

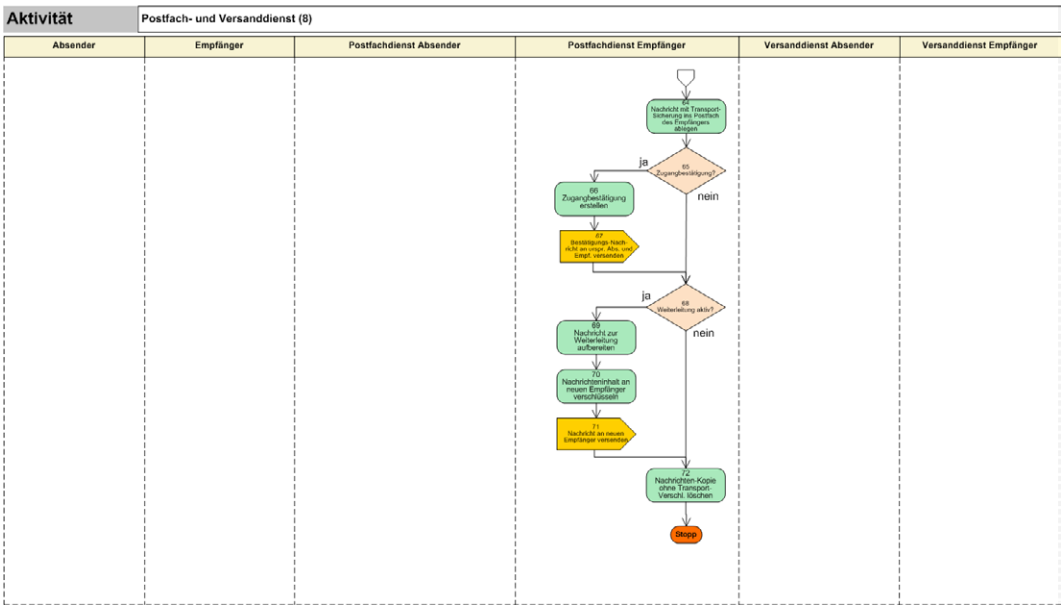




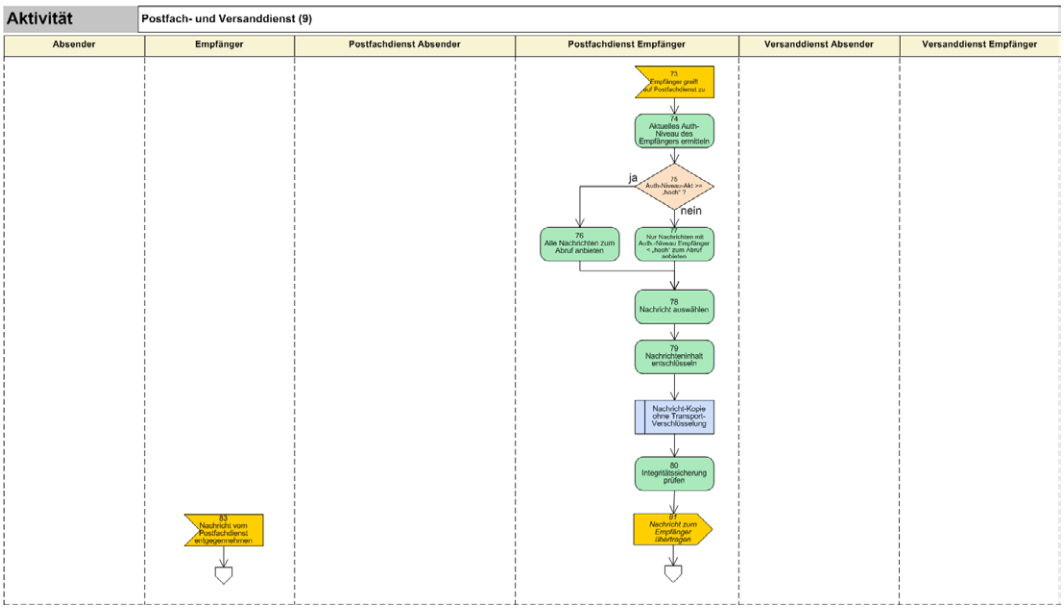
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger



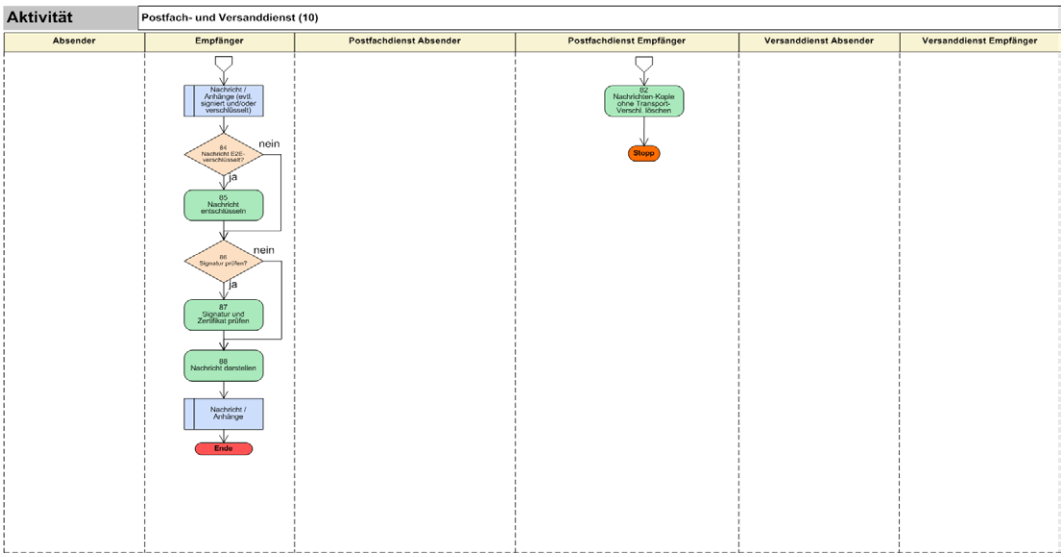
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger



Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger



Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger



7 Funktionale Beschreibung

Im Folgenden werden die einzelnen Schritte des Aktivitätsdiagramms aus Abschnitt 6 für das Erstellen, Versenden, Empfangen und Abrufen von Nachrichten mit dem PVD von De-Mail beschrieben. Funktionen, die der Nutzer interaktiv aufrufen kann, wenn er an seinem Postfach angemeldet ist, werden in Abschnitt 8 dargestellt. Die referenzierten Funktionen des Accountmanagements, der Schadsoftwareprüfung und des Zeitdienstes werden in [TR DM ACM FU] und [TR DM IT-BInfra FU] erläutert.

Im Kontrollfluss des PVD werden an verschiedenen Stellen neue Nachrichten, wie z. B. Bestätigungsnachrichten, automatisch erzeugt und an den Empfänger versendet. In diesen Fällen werden die in diesem Abschnitt beschriebenen Schritte für das Erstellen und Versenden von Nachrichten rekursiv durchlaufen. Die die Nachricht erzeugende Stelle wird damit zum Absender einer Nachricht.

Es werden in den nachfolgenden Tabellen die wichtigsten Fehlerfälle dargestellt, die vom DMDA bei dem von ihm angebotenen PVD mindestens zu berücksichtigen sind. Weitere können durch den DMDA hinzugefügt werden. Die Darstellung der Fehlerfälle für den Nutzer kann durch den DMDA gewählt werden.

7.1 Erstellen von Nachrichten durch den Absender

Die vorgegebene Reihenfolge für das Erstellen einer Nachricht (Schritt 1 bis Schritt 4) ist beispielhaft zu verstehen.

Schritt 1	**Versandoption festlegen**
Kurzbeschreibung	Der Absender erstellt einen neuen Nachrichtenentwurf und legt die Versandoptionen der Nachricht fest (vgl. Abschnitt 3.3).
Akteure	Absender
Auslöser	Absender
Vorbedingung	Fall a) Der Absender ist am De-Mail-Konto über Web-Schnittstelle angemeldet. Fall b) Der Absender verwendet einen lokalen Nachrichten-Client.
Input	Werte der Versandoptionen (ja/nein) • Versand-, Eingangs- und/oder Abholbestätigungen • Persönlich • Absenderbestätigt
Ergebnis	Versandoptionen für den entsprechenden Nachrichtenentwurf festgelegt
Nachbedingung	
Ablauf	• Absender erstellt einen neuen Nachrichtenentwurf durch die Funktionen „Neue Nachricht“, „Beantworten“ oder „Weiterleiten“

	• Absender legt die Versandoptionen fest
Fehlerfälle	
Schritt 2	**Absender-Adresse auswählen**
Kurzbeschreibung	Der Absender wählt aus, unter welcher zur Verfügung stehenden Absender-Adresse die Nachricht versendet werden soll.
Akteure	Absender
Auslöser	Absender
Vorbedingung	Fall a) Der Absender ist am De-Mail-Konto über Web-Schnittstelle angemeldet. Fall b) Der Absender verwendet einen lokalen Nachrichten-Client.
Input	Default-Absender-Adresse oder Auswahl der ihm zur Verfügung stehenden Absender-Adressen (primäre De-Mail-Adresse bzw. zum De-Mail-Konto zugehörige und gültige Pseudonym-Adressen).
Ergebnis	Absender-Adresse festgelegt
Nachbedingung	
Ablauf	Für Fall a) • Absender übernimmt die durch die Applikation angezeigte Default-Absender-Adresse ohne Änderung, oder • Absender wählt aus den zur Verfügung stehenden Kennungen eine Absender-Adresse aus. Für Fall b) • Absender übernimmt die durch die Applikation angezeigte Default-Absender-Adresse ohne Änderung, oder • Absender wählt aus den zur Verfügung stehenden Kennungen eine Absender-Adresse aus, oder • Absender editiert die Absender-Adresse frei. Hinweis: Nutzt der Absender einen lokalen Nachrichten-Client, hängt es von diesem ab, ob die Absender-Adresse frei editiert werden kann oder nur vorgegebene ausgewählt werden können. • Die ausgewählte Absender-Adresse wird in den Metadaten des Nachrichtenentwurfs gespeichert.
Fehlerfälle	FC-01: Ungültiges Adressformat FC-02: Keine De-Mail-Adresse
Schritt 3	**Empfänger-Adressen und optionale Antwort-Adresse angeben**
Kurzbeschreibung	Der Absender legt die Empfänger der Nachricht durch Angabe der Empfänger-Adressen fest. Weiterhin kann er optional auch eine Antwort-Adresse angeben.
Akteure	Absender

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Auslöser	Absender
Vorbedingung	
Input	Empfänger-Adressen (De-Mail-Adresse) und Antwort-Adresse (De-Mail-Adresse)
Ergebnis	Empfänger-Adressen angegeben
Nachbedingung	
Ablauf	• Absender editiert die Empfängeradressen frei oder wählt sie aus seinem persönlichen Adressbuch oder dem ÖVD (vgl. Funktion 7, Abschnitt 8) aus • Empfänger-Adressen und Antwort-Adresse werden in den Metadaten des Nachrichtenentwurfes gespeichert.
Fehlerfälle	FC-01: Ungültiges Adressformat
Schritt 4	**Nachrichteninhalt editieren und Anhänge hinzufügen**
Kurzbeschreibung	Der Absender editiert den Betreff der Nachricht, den Nachrichteninhalt und fügt ggf. Dateianhänge hinzu.
Akteure	Absender, DA (optional)
Auslöser	Absender
Vorbedingung	
Input	Nachrichtentext, Dateianhänge
Ergebnis	Nachricht editiert und ggf. Dateianhänge hinzugefügt
Nachbedingung	
Ablauf	• Absender editiert ◦ den Betreff ◦ Nachrichten-Kennung (optional) ◦ Nachrichtentext • Absender fügt Anhänge hinzu ◦ von lokaler Festplatte ◦ aus der DA (optional) • Daten in Nachrichtenentwurf speichern
Fehlerfälle	
Schritt 5	**Entscheidungsknoten: Ende-zu-Ende Signatur erwünscht?**
Kurzbeschreibung	Auswertung, ob der Absender den Nachrichtenentwurf elektronisch signieren möchte.
ja	Schritt 6
nein	Schritt 7

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Schritt 6	**Elektronisch signieren**
Kurzbeschreibung	Der Absender signiert den Nachrichtenentwurf und/oder Anhänge des Nachrichtenentwurfs.
Akteure	Signaturanwendungskomponente (SAK)
Auslöser	Absender
Vorbedingung	
Input	Nachrichtenentwurf
Ergebnis	Signierter Nachrichtenentwurf
Nachbedingung	
Ablauf	• Übergabe der zu signierenden Informationen an eine SAK • Signieren des Nachrichtenentwurfs innerhalb der SAK • Integration der signierten Nachrichtenbestandteile und der Signatur in den Nachrichtenentwurf
Fehlerfälle	FC-01: Warnung: Versenden der Adresse unter einer Pseudonym-Adresse, Zertifikatsinformationen können weitere Informationen zur Person enthalten. FC-02: Keine SAK gefunden FC-03: Keine gültige SSEE gefunden
Schritt 7	**Entscheidungsknoten: Ende-zu-Ende-Verschlüsselung erwünscht?**
Kurzbeschreibung	Auswertung, ob der Absender den Nachrichtenentwurf Ende-zu-Ende-verschlüsseln möchte.
ja	Schritt 8
nein	Schritt 9
Schritt 8	**Nachrichtenentwurf verschlüsseln**
Kurzbeschreibung	Der Absender verschlüsselt den Nachrichtenentwurf für die Empfänger.
Akteure	Absender
Auslöser	Absender
Vorbedingung	Der Absender hat die Empfänger-Adressen angegeben und den Nachrichtenentwurf ggf. signiert. Die Zertifikate der Empfänger liegen dem Absender über das persönliche Adressbuch oder den ÖVD vor.
Input	Nachrichtenentwurf
Ergebnis	Verschlüsselter Nachrichtenentwurf
Nachbedingung	
Ablauf	• Der zu verschlüsselnde Nachrichtenentwurf inklusive der Dateianhänge wird an eine Verschlüsselungsfunktion übergeben.

	• Die Verschlüsselungsfunktion sucht die Zertifikate der Empfänger im persönlichen Adressbuch und/oder dem ÖVD. • Die Zertifikate werden hinsichtlich der Vertrauenswürdigkeit und der Gültigkeit verifiziert. • Es werden die symmetrischen Verschlüsselungsschlüssel generiert. • Der Nachrichtentext des Nachrichtenentwurfs wird mit dem Verschlüsselungsschlüssel verschlüsselt. • Der Verschlüsselungsschlüssel wird mit den öffentlichen Schlüsseln des Absenders und der Empfänger verschlüsselt. • Der symmetrische Verschlüsselungsschlüssel wird sicher gelöscht. • Die Verschlüsslungsinformationen und die verschlüsselten Nachrichtenbestandteile werden in den Nachrichtenentwurf eingebettet. • Der zu verschlüsselnde Inhalt wird verworfen. Hinweis: Die Generierung des Verschlüsselungsschlüssels und die Verschlüsselung des Nachrichtenentwurfs müssen auf dem System des Nutzers erfolgen. Der zu verschlüsselnde Nachrichtenentwurf darf nicht auf dem DMDA-Server temporär zwischengespeichert werden.
Fehlerfälle	FC-01: Kein Zertifikat gefunden FC-02: Zertifikat nicht vertrauenswürdig FC-03: Zertifikat ungültig
Schritt 9	**Nachrichtenentwurf an Postfachdienst Absender versenden**
Kurzbeschreibung	Der Nachrichtenentwurf wird vom Web- oder Nachrichten-Client des Absenders zu dessen Postfachdienst gesendet.
Akteure	Absender, Postfachdienst Absender
Auslöser	Absender
Vorbedingung	• Absender an seinem De-Mail-Konto angemeldet • Sicherer Kanal zwischen Client des Nutzers und dem Postfachdienst des Absenders aufgebaut
Input	Nachrichtenentwurf
Ergebnis	Nachrichtenentwurf ist zum Postfachdienst des Absenders abgeschickt
Nachbedingung	
Ablauf	Nachrichtenentwurf wird vom zum Postfachdienst übermittelt
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto angemeldet FC-02: Absender nicht autorisiert, Nachrichten zu verschicken (z.B. De-Mail-Konto gesperrt) FC-03: Postfachdienst hat Nachrichtenentwurf nicht vollständig angenommen

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Tabelle 5: Schritte zum Erstellen von Nachrichten

7.2 Entgegennahme von Nachrichten durch Postfachdienst des Absenders

Schritt 10	**Nachrichtenentwurf vom Absender empfangen**
Kurzbeschreibung	Der Postfachdienst des Absenders empfängt den Nachrichtenentwurf vom System des Absenders.
Akteure	Postfachdienst Absender
Auslöser	Absender
Vorbedingung	
Input	Nachrichtenentwurf
Ergebnis	Nachrichtenentwurf vom Postfachdienst angenommen
Nachbedingung	
Ablauf	• Nachrichtenentwurf wird vom Postfachdienst empfangen • Prüfen, ob Nachricht syntaktisch korrekt ist
Fehlerfälle	FC-01: Nachrichtenentwurf nicht vollständig übertragen FC-02: Nachricht enthält syntaktische Fehler
Schritt 11	**Nachrichtenentwurf im Postausgang ablegen**
Kurzbeschreibung	Der Nachrichtenentwurf wird vom Postfachdienst im Postausgang des Absender-Postfaches abgelegt.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	
Input	Nachrichtenentwurf
Ergebnis	Nachrichtenentwurf im Postausgang
Nachbedingung	
Ablauf	Nachrichtenentwurf wird im Postausgang des Absender-Postfaches abgelegt.
Fehlerfälle	FC-01: Kapazitätsgrenze des Absender-Postfaches erreicht
Schritt 12	**Prüfung Absender-Adresse**
Kurzbeschreibung	Prüfung, ob die im Nachrichtenentwurf angegebene Absender-Adresse dem De-Mail-Konto zugeordnet ist.
Akteure	Postfachdienst Absender, Account-Dienst
Auslöser	Postfachdienst Absender

Vorbedingung	
Input	Nachrichtenentwurf
Ergebnis	Ergebnis der Prüfung (ok / nicht ok)
Nachbedingung	
Ablauf	• Unter Zuhilfenahme des De-Mail-Kontos, an dem der Absender angemeldet ist, werden die dem De-Mail-Konto zugeordneten De-Mail-Adresse ermittelt. • Absender-Adresse (Nr. 6) des Nachrichtenentwurfs prüfen, ob diese dem De-Mail-Konto zugeordnet ist. • Prüfung, ob die optionale Antwort-Adresse (Nr. 10) eine De-Mail-Adresse ist.
Fehlerfälle	FC-01: Antwort-Adresse ist keine De-Mail-Adresse
Schritt 13	**Entscheidungsknoten: Prüfung OK?**
Kurzbeschreibung	Ergebnis der Prüfung, ob Absender-Adresse dem De-Mail-Konto des Absenders zugeordnet ist.
ja	Schritt 15
nein	Schritt 14
Schritt 14	**Meldung an Absender**
Kurzbeschreibung	Der Postfachdienst erzeugt eine Meldung für den Absender, dass in seinem Nachrichtenentwurf eine ihm nicht zugeordnete Absender-Adresse gefunden wurde.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	
Input	Prüfergebnis aus Schritt 12
Ergebnis	Meldung
Nachbedingung	Anhalten
Ablauf	• Meldung an den Nutzer • Nachrichtenentwurf löschen und aus Postausgang entfernen
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden.
Schritt 15	**Prüfung der Empfänger-Adressen**
Kurzbeschreibung	Prüfung des Nachrichtenentwurfs, ob die dort eingetragenen Empfänger-Adressen De-Mail-Adressen sind.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Es sind Empfänger im Nachrichtenentwurf angegeben.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Input	Nachrichtenentwurf
Ergebnis	Ergebnis der Prüfung (ok / nicht ok)
Nachbedingung	
Ablauf	Prüfen, ob jede Empfänger-Adresse eine De-Mail-Adresse ist
Fehlerfälle	
Schritt 16	**Entscheidungsknoten: Prüfung OK?**
Kurzbeschreibung	Ergebnis der Empfänger-Adressen-Prüfung auswerten
ja	Schritt 18
nein	Schritt 17
Schritt 17	**Meldung an Absender**
Kurzbeschreibung	Der Postfachdienst erzeugt eine Meldung für den Absender, dass in seinem Nachrichtenentwurf Empfänger außerhalb von De-Mail adressiert sind.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	
Input	Prüfergebnis aus Schritt 15
Ergebnis	Meldung
Nachbedingung	Anhalten
Ablauf	• Meldung an den Nutzer • Nachrichtenentwurf löschen und aus Postausgang entfernen
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden
Schritt 18	**Aktuelles Authentisierungsniveau des Absenders ermitteln**
Kurzbeschreibung	Das aktuelle Authentisierungsniveau des Absenders wird ermittelt.
Akteure	Postfachdienst Absender, Account-Dienst
Auslöser	Postfachdienst Absender
Vorbedingung	
Input	Nutzer-Kennung des De-Mail-Kontos, Nachrichtenentwurf
Ergebnis	Aktuelles Authentisierungsniveau des Absenders
Nachbedingung	
Ablauf	• De-Mail-Konto ermitteln • Anfrage an Account-Dienst, welches aktuelle Authentisierungsniveau der Absender besitzt
Fehlerfälle	
Schritt 19	**Entscheidungsknoten: Authentisierungsniveau für Versandoptionen**

	OK?
Kurzbeschreibung	Wert für Versandoption „Absenderbestätigt“ aus Metadaten des Nachrichtenentwurfs ermitteln Wert für Versandoption „Persönlich“ aus Metadaten des Nachrichtenentwurfs ermitteln Wert für Versandoption „Abholbestätigung“ aus Metadaten des Nachrichtenentwurfs ermitteln Prüfung, ob die Versandoption „Abholbestätigung“, „Absenderbestätigt“ und/oder „Persönlich“ im Nachrichtenentwurf gewählt wurde und ob in diesem Fall das Authentisierungsniveau des Absenders „hoch“ ist.
ja	Schritt 21
nein	Schritt 20
Schritt 20	**Meldung an Absender: „Versandoptionen ‚Abholbestätigung’, ‚Absenderbestätigt’ und ‚Persönlich’ erfordern min. Authentisierungsniveau ‚hoch’“**
Kurzbeschreibung	Der Postfachdienst erzeugt eine Meldung für den Absender mit der Aufforderung, sich mit Authentisierungsniveau „hoch“ am De-Mail-Konto anzumelden.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Prüfung Versandoption „Abholbestätigung“, „Absenderbestätigt“ / „Persönlich“ nicht ok
Input	Nachrichtenentwurf
Ergebnis	Meldung
Nachbedingung	Anhalten
Ablauf	• Meldung an den Nutzer • Nachrichtenentwurf löschen und aus Postausgang entfernen
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden
Schritt 21	**Prüfung der Berechtigung zur Nutzung Versandoption „Abholbestätigung“**
Kurzbeschreibung	Prüfung des Nachrichtenentwurfs, ob eine Berechtigung zur Nutzung der Versandoption Abholbestätigung für den Nutzer besteht
Akteure	Postfachdienst Absender, Account-Dienst
Auslöser	Postfachdienst Absender
Vorbedingung	Es ist die Versandoption „Abholbestätigung“ im Nachrichtenentwurf angegeben.
Input	Nachrichtenentwurf
Ergebnis	Ergebnis der Prüfung (ok / nicht ok)

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Nachbedingung	
Ablauf	Prüfen, ob die Nutzung der Versandoption „Abholbestätigung“ durch den Nutzer möglich ist (vgl. [TR DM ACM FU])
Fehlerfälle	
Schritt 22	**Entscheidungsknoten: Berechtigung zur Nutzung der Versandoption „Abholbestätigung“ OK?**
Kurzbeschreibung	Ergebnis der Berechtigung zur Nutzung der Versandoption „Abholbestätigung“ auswerten.
ja	Schritt 24
nein	Schritt 23
Schritt 23	**Meldung an Absender: „Versandoptionen ‚Abholbestätigung’ nicht gestattet**
Kurzbeschreibung	Der Postfachdienst erzeugt eine Meldung für den Absender, dass die Nutzung der Versandoption „Abholberechtigung“ aufgrund der Berechtigungen nicht möglich ist
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Berechtigung zur Nutzung der Versandoption „Abholbestätigung“ nicht OK
Input	Nachrichtenentwurf
Ergebnis	Meldung
Nachbedingung	Anhalten
Ablauf	• Meldung an den Nutzer • Nachrichtenentwurf löschen und aus Postausgang entfernen
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden
Schritt 24	**Auf Nachrichtenbegrenzung und Schadsoftware prüfen**
Kurzbeschreibung	Hat der Absender sich nur mit dem Authentisierungsniveau „normal“ am Postfachdienst angemeldet, so kann er nur eine begrenzte Anzahl von Nachrichten in einem bestimmten Zeitraum versenden (vgl. 3.1.1.1) Danach erfolgt eine Prüfung auf Schadsoftware.
Akteure	Postfachdienst Absender, Account-Dienst, Schadsoftware-Dienst
Auslöser	Postfachdienst Absender
Vorbedingung	Prüfung der Berechtigung bei Nutzung der Versandoption „Abholbestätigung“ OK
Input	Nachrichtenentwurf
Ergebnis	Ergebnis der Schadsoftware-Prüfung
Nachbedingung	

Ablauf	• Falls Authentisierungsniveau des Absenders „normal“, dann ◦ Anzahl der versendeten Nachrichten für den vergangenen Zeitraum bestimmen, ◦ Prüfen, ob noch weitere Nachrichten mit Authentisierungsniveau „normal“ verschickt werden können (vgl. Abschnitt 3.1.1.1). • Nachrichtenentwurf an Schadsoftware-Dienst übergeben (s. a. Funktion 2, Abschnitt 8).
Fehlerfälle	FC-01: Nachrichtenentwurf nicht prüfbar
Schritt 25	**Entscheidungsknoten: Prüfung OK?**
Kurzbeschreibung	Ergebnis der Schadsoftware-Prüfung auswerten
ja	Schritt 27
nein	Schritt 26
Schritt 26	**Meldung an Absender**
Kurzbeschreibung	Der Postfachdienst erzeugt eine Meldung dass • zum aktuellen Zeitpunkt keine Nachrichten mit Authentisierungsniveau „normal“ versenden darf oder • in seinem Nachrichtenentwurf Schadsoftware gefunden wurde.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Schadsoftware-Prüfung durchgeführt
Input	Ergebnis der Schadsoftware-Prüfung
Ergebnis	Meldung
Nachbedingung	Anhalten
Ablauf	• Meldung an den Nutzer • Nachrichtenentwurf löschen und aus Postausgang entfernen
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden
Schritt 27	**Metadaten setzen und Integrität sichern**
Kurzbeschreibung	Die Metadaten in dem Nachrichtenentwurf, die nicht durch den Nutzer vorgegeben werden, werden durch den Postfachdienst ausgefüllt. Anschließend wird der Hash-Wert zum Nachrichtenentwurf berechnet und in den Metadaten gespeichert.
Akteure	Postfachdienst Absender, Zeitdienst, Account-Dienst
Auslöser	Postfachdienst Absender
Vorbedingung	
Input	Nachrichtentwurf

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Ergebnis	Aktuelle Metadaten in der Nachricht gesetzt
Nachbedingung	
Ablauf	Falls Empfänger mit BCC adressiert werden, müssen in diesem Schritt a) die BCC-Empfänger-Adressen aus Element <Empfänger-Adresse(n)> (Nr. 7) und Element <Empfänger-Adressen für den Transport> (Nr. 19) entfernt werden, sowie b) für die BCC-Empfänger-Adressen jeweils eigene Nachrichten mit eigener eindeutiger Message-ID in Element <Message-ID> (Nr. 14) generiert werden (siehe nachfolgende Beschreibung). Hinweis: Dieses Vorgehen ermöglicht, dass die BCC-Empfänger für die über TO und CC adressierten Empfänger nicht erkennbar sind, und trotzdem die Hash-Werte für jeden Nachrichten-Empfänger korrekt erstellt werden. Folgende Metadaten werden vom Postfachdienst in der Nachricht gesetzt: • Zeit in Element <Versanddatum und –Zeit> (Nr. 13) der Metadaten schreiben. • Aktuelles Authentisierungsniveau in Element <Authentisierungsniveau> (Nr. 11) schreiben. • Aktuellen Authentisierungs-Mechanismus in Element <Authentisierungs-Mechanismus> (Nr. 12) schreiben. • Name des aktuellen Servers in Element <De-Mail-Server> (Nr. 15) schreiben. • Empfänger-Adressen aus dem Element <Empfänger-Adresse(n)> (Nr. 7) in das Element <Empfänger-Adressen für den Transport> (Nr. 19) schreiben. • In Element <Nachrichten-Typ> (Nr. 16) den Typ der Nachricht setzen. • Eindeutige Message-ID generieren und in Element <Message-ID> (Nr. 14) schreiben. • Hash-Wert über Metadaten Nr. 1 bis Nr. 16 und Nachrichtentext berechnen und in Element <Hash-Wert> (Nr. 17) schreiben. Hinweis: Mit dem Setzen der Metadaten innerhalb des Nachrichtenentwurfes wird aus diesem eine Nachricht.
Fehlerfälle	FC-01: Keine De-Mail-Zeit ermittelbar
Schritt 28	**Entscheidungsknoten: Nachricht signieren?**
Kurzbeschreibung	Prüfung, ob die Nachricht signiert verschickt werden soll. Dies ist der Fall, wenn • die Versandoption „absenderbestätigt“ gesetz ist oder • es sich um eine Bestätigungsnachricht handelt

ja	Schritt 29
nein	Schritt 30
Schritt 29	**Signatur durch DMDA**
Kurzbeschreibung	Der DMDA signiert den Hash-Wert (Nr. 17) in den Metadaten. der Nachricht, dass er diese Nachricht vom Absender unverändert entgegengenommen hat, dieser mit Authentisierungsniveau „hoch“ am De-Mail-Konto angemeldet war und die Versandoption „Absenderbestätigt“ gewählt hat.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Versandoption „Absenderbestätigte“ Nachricht vom Absender gewählt oder es handelt sich um eine Bestätigungsnachricht
Input	Nachricht
Ergebnis	Qualifizierte elektronische Signatur über Hash-Wert (Nr. 17) in Element <Signatur des DMDA> (Nr. 18) der Metadaten der Nachricht gespeichert.
Nachbedingung	
Ablauf	• Hash-Wert aus Metadaten (Nr. 17) der Nachricht mit einer qualifizierten elektronischen Signatur signieren. • Signatur in Feld <Signatur des DMDA> (Nr. 18) der Metadaten der Nachricht speichern.
Fehlerfälle	FC-01: Signatur konnte nicht erstellt werden.
Schritt 30	**Nachrichteninhalt verschlüsseln**
Kurzbeschreibung	Die Nachricht wird ohne Metadaten an den eigenen (sendenden) und den empfangenden DMDA verschlüsselt.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	
Input	Nachricht, Verschlüsselungsschlüssel des eigenen und des empfangenden DMDA
Ergebnis	Verschlüsselte Nachricht
Nachbedingung	
Ablauf	• Nachricht mit Verschlüsselungsschlüssel des Empfänger-DMDA und des Absender-DMDA verschlüsseln • Nicht-verschlüsselte Nachricht wird durch verschlüsselte Nachricht ersetzt • Löschen der nicht-verschlüsselten Nachricht
Fehlerfälle	FC-01: Verschlüsselung nicht durchführbar

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Schritt 31	**Nachricht an Versanddienst Absender übermitteln**
Kurzbeschreibung	Die (verschlüsselte) Nachricht wird vom Postfachdienst des Absenders zum Versanddienst des Absenders übermittelt.
Akteure	Postfachdienst Absender, Versanddienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Sicherer Kommunikationskanal zwischen Postfachdienst und Versanddienst
Input	Nachricht
Ergebnis	Nachricht zum Versanddienst gesendet
Nachbedingung	Anhalten
Ablauf	Nachricht wird vom Postfachdienst des Absenders zum Versanddienst des Absenders übermittelt.
Fehlerfälle	FC-01: Versanddienst hat Nachricht nicht vollständig angenommen.
Schritt 32	**Nachricht als gesendet kennzeichnen**
Kurzbeschreibung	Nach erfolgreicher Übermittlung der Nachricht vom Postfachdienst zum Versanddienst wird sie im Postfach des Senders als „gesendet“ gekennzeichnet.
Akteure	Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Erfolgreiche Übermittlung der Nachricht vom Postfachdienst zum Versanddienst.
Input	Nachricht
Ergebnis	Nachricht als gesendet gekennzeichnet
Nachbedingung	Anhalten
Ablauf	Nachricht als „gesendet“ kennzeichnen
Fehlerfälle	

Tabelle 6: Schritte zum Versenden von Nachrichten

7.3 Transport von Nachrichten durch Versanddienst des Absenders

Schritt 33	**Nachricht vom Postfachdienst des Absenders entgegennehmen**
Kurzbeschreibung	Nachricht wird vom Postfachdienst des Absenders entgegengenommen.
Akteure	Versanddienst Absender, Postfachdienst Absender
Auslöser	Postfachdienst Absender
Vorbedingung	Schritt 31 sicherer Kommunikationskanal zwischen Postfachdienst und Versanddienst

Input	Nachricht
Ergebnis	Nachricht vom Postfachdienst des Absenders entgegennehmen
Nachbedingung	
Ablauf	Nachricht wird entgegengenommen
Fehlerfälle	FC-01: Nachricht nicht vollständig übertragen
Schritt 34	**Prüfung, ob Versandbestätigung erstellt werden soll**
Kurzbeschreibung	Metadaten der Nachricht auswerten, ob eine Versandbestätigung angefordert wurde. Im Rahmen von automatisierten Weiterleitungen und Nachsendeaufträgen darf keine erneute Versandbestätigung erstellt werden, da eine Versandbestätigung nur vom ursprünglichen Absender angefordert werden soll.
Akteure	Versanddienst Absender
Auslöser	Versanddienst Absender
Vorbedingung	
Input	Nachricht
Ergebnis	Versandbestätigung erstellen / nicht erstellen
Nachbedingung	
Ablauf	• Wert für Versandoption „Versandbestätigung“ ermitteln • Prüfung, ob Empfänger-Adresse in den Elementen <Empfänger-Adresse(n)> (Nr.) und <Empfänger-Adressen für den Transport> (Nr.) unterschiedlich sind, • dann ist Nachricht ein Nachsendeauftrag oder Weiterleitung und es wird keine Versandbestätigung erstellt
Fehlerfall	
Schritt 35	**Entscheidungsknoten: Versandbestätigung?**
Kurzbeschreibung	Metadaten der Nachricht auswerten, ob eine Versandbestätigung angefordert wurde. Hinweis: Im Rahmen von automatisierten Weiterleitungen (siehe Schritt 68) und Nachsendeaufträgen (siehe Schritt 48) darf keine erneute Versandbestätigung erstellt werden, da eine Versandbestätigung nur vom ursprünglichen Absender angefordert werden soll.
ja	Schritt 36
nein	Schritt 38
Schritt 36	**Versandbestätigung erstellen**
Kurzbeschreibung	Vom Versanddienst des Absenders wird eine Versandbestätigung erstellt.
Akteure	Versanddienst Absender
Auslöser	Versanddienst Absender

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Vorbedingung	
Input	Nachricht
Ergebnis	Bestätigungsnachricht
Nachbedingung	
Ablauf	• Versandbestätigung erzeugen (siehe Abschnitt 5) • Bestätigungsnachricht auf Grundlage der Versandbestätigung erstellen • Es werden keine Versandoptionen gesetzt, nur falls in der ursprünglichen Nachricht die Versandoption „Persönlich“ gesetzt war, wird auch die Bestätigungsnachricht mit der Versandoption „Persönlich“ versendet. • Empfänger-Adresse ist auf die Absender-Adresse bzw. falls angegeben, auf die Antwort-Adresse, der ursprünglichen Nachricht zu setzen • Element <Nachrichten-Kennung des Absenders> (Nr. 9) von der ursprünglichen Nachricht in die Bestätigungsnachricht übernehmen. • Absender-Adresse ist auf die System-Adresse des DMDA für Versandbestätigungen zu setzen • Die Bestätigung ist mit einer qualifizierten elektronischen Signatur zu signieren
Fehlerfälle	FC-01: keine Signaturerstellung möglich
Schritt 37	**Bestätigungsnachricht an Absender versenden**
Kurzbeschreibung	Eine Bestätigungsnachricht mit der Versandbestätigung wird zum Absender versendet.
Akteure	Versanddienst Absender, Postfachdienst Absender
Auslöser	Versanddienst Absender
Vorbedingung	
Input	Versandbestätigung
Ergebnis	Bestätigungsnachricht versendet
Nachbedingung	
Ablauf	Die Bestätigungsnachricht versenden
Fehlerfälle	FC-01: Nachricht kann nicht versendet werden
Schritt 38	**Nachricht an Versanddienst Empfänger übermitteln**
Kurzbeschreibung	Die Nachricht wird, für Empfänger innerhalb von De-Mail, zum Versanddienst des Empfängers übermittelt.
Akteure	Versanddienst Absender, Versanddienst Empfänger
Auslöser	Versanddienst Absender

Vorbedingung	Sicherer Kanal zwischen Versanddiensten von Absender und Empfänger aufgebaut
Input	Transportgesicherte Nachricht
Ergebnis	Nachricht zum Versanddienst Empfänger übermittelt
Nachbedingung	Anhalten
Ablauf	• Die Adresse des Versanddienst Empfänger aus Empfänger-Adresse ermitteln • Nachricht zum Versanddienst Empfänger übermitteln
Fehlerfälle	FC-01: Nachricht vom Versanddienst Empfänger nicht vollständig angenommen

Tabelle 7: Schritte zum Transport von Nachrichten durch Versanddienst des Absenders

7.4 Transport von Nachrichten durch Versanddienst des Empfängers

Schritt 39	**Nachricht vom Versanddienst des Absenders entgegennehmen**
Kurzbeschreibung	Der Versanddienst des Empfängers nimmt die Nachricht vom Versanddienst des Absenders entgegen.
Akteure	Versanddienst Empfänger, Versanddienst Absender
Auslöser	Versanddienst Absender
Vorbedingung	Sicherer Kanal zwischen Versanddiensten des Absenders und Empfängers aufgebaut
Input	Nachricht
Ergebnis	Nachricht vom Versanddienst des Empfängers entgegengenommen
Nachbedingung	
Ablauf	• Nachricht wird entgegengenommen. • Prüfen, ob Nachricht syntaktisch korrekt ist.
Fehlerfälle	FC-01: Nachricht nicht vollständig übertragen FC-02: Nachricht enthält syntaktische Fehler
Schritt 40	**Zustellbarkeit prüfen**
Kurzbeschreibung	Der Versanddienst des Empfängers überprüft, ob die Nachricht zustellbar ist: • Der Empfänger muss existieren. • Bei Nachrichten mit gewählter Versandoption „Persönlich“: ◦ der Empfänger muss sich mit Authentisierungsniveau „hoch“ am De-Mail-Konto anmelden können. • Bei Nachrichten mit gewählter Versandoption „Abholbestätigung“:

	◦ der Empfänger muss sich mit Authentisierungsniveau „hoch“ am De-Mail-Konto anmelden können. • Das De-Mail-Konto des Empfängers darf nicht vollständig gesperrt sein.
Akteure	Versanddienst Empfänger, Account-Dienst Empfänger, Postfachdienst Empfänger
Auslöser	Versanddienst Empfänger, Account-Dienst Empfänger
Vorbedingung	
Input	Nachricht
Ergebnis	Prüfergebnis: Nachricht ist zustellbar oder nicht
Nachbedingung	
Ablauf	• Empfänger-Adresse aus Nachricht ermitteln • Anfrage beim Accountmanagement, ob Empfänger existiert ◦ Falls nein: nicht zustellbar • Anfrage beim Postfachdienst, ob Nachsendeauftrag aktiv ◦ falls nein, zusätzlich prüfen: ▪ Bei Versandoption „Persönlich“: Anfrage beim Account-Dienst, ob Empfänger „persönliche“ Nachrichten abrufen kann • Falls nein: nicht zustellbar • Anfrage beim Account-Dienst, ob das De-Mail-Konto vollständig gesperrt ist ◦ Falls ja: nicht zustellbar • Anfragen auswerten
Fehlerfälle	FC-01: Account-Dienst nicht erreichbar FC-02: Postfachdienst nicht erreichbar FC-03: Versanddienst für Empfänger-Adresse nicht zuständig (weil z.B. falscher DMDA)
Schritt 41	**Entscheidungsknoten: Zustellbarkeit OK?**
Kurzbeschreibung	Das Ergebnis der Prüfung der Zustellbarkeit wird ausgewertet. • ja: bei Ergebnis „OK“ • nein: bei Ergebnissen: „Empfänger unbekannt“, „Empfänger kann keine Nachrichten mit Versandoption ‚Persönlich’ abrufen“ oder „Empfänger-De-Mail-Konto vollständig gesperrt“
ja	Schritt 42
nein	Schritt 43

Schritt 42	**Nachricht an den Postfachdienst Empfänger übermitteln**
Kurzbeschreibung	Die Nachricht wird vom Versanddienst des Empfängers zum Postfachdienst des Empfängers übermittelt.
Akteure	Versanddienst Empfänger, Postfachdienst Empfänger
Auslöser	Versanddienst Empfänger
Vorbedingung	Sicherer Kommunikationskanal zwischen Versanddienst und Postfachdienst
Input	Nachricht
Ergebnis	Nachricht an den Postfachdienst des Empfängers übermittelt
Nachbedingung	Anhalten
Ablauf	Nachricht wird zum Postfachdienst des Empfängers übermittelt
Fehlerfälle	FC-01: Nachricht vom Postfachdienst des Empfängers nicht vollständig angenommen.
Schritt 43	**Meldungsnachricht an ursprünglichen Absender versenden**
Kurzbeschreibung	
Akteure	Versanddienst Empfänger
Auslöser	Versanddienst Empfänger
Vorbedingung	
Input	Prüfergebnis, (ursprüngliche) Nachricht
Ergebnis	Meldungsnachricht an den Absender versendet
Nachbedingung	Anhalten
Ablauf	• Absender-Adresse aus der ursprünglichen Nachricht ermitteln • Falls Absender-Adresse eine System-Adresse ist (d.h. die ursprüngliche Nachricht ist i.d.R. eine Meldungs- oder Bestätigungsnachricht), dann ◦ die ursprüngliche Nachricht löschen ◦ Anhalten • ansonsten: ◦ Meldungstext muss das Prüfergebnis und die entsprechende Empfänger-Adresse beinhalten und der Meldungstext muss ermöglichen, die ursprüngliche Nachricht zu referenzieren. ◦ Meldungsnachricht erstellen. ◦ Keine Versandoptionen werden gesetzt. ◦ Element <Nachrichten-Kennung des Absenders> (Nr. 9) von der ursprünglichen Nachricht in die Meldungsnachricht übernehmen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	◦ Prüfung, ob ein Element <Weiterleitungs-Absender> (Nr. 20) gesetzt ist. ▪ Falls ja: Empfänger-Adresse ist auf Weiterleitungs-Absender zu setzen. ▪ Falls nein: Empfänger-Adresse ist auf die Absender- bzw. falls angegeben, auf die Antwort-Adresse, der ursprünglichen Nachricht zu setzen. • Absender-Adresse ist auf die System-Adresse für Meldungsnachrichten zu setzen. • Die Meldungsnachricht wird an den Versanddienst des Absenders übermittelt • Ursprüngliche Nachricht, die nicht im Postfach des Empfängers abgelegt werden kann, löschen
Fehlerfälle	FC-01: Meldungsnachricht kann nicht versendet werden.

Tabelle 8: Schritte zum Transport von Nachrichten durch Versanddienst des Empfängers

7.5 Empfangen der Nachrichten durch Postfachdienst des Empfängers

Schritt 44	**Nachricht vom Versanddienst Empfänger entgegennehmen**
Kurzbeschreibung	Die vom Versanddienst des Empfängers übermittelte Nachricht wird vom Postfachdienst des Empfängers entgegengenommen.
Akteure	Versanddienst Empfänger, Postfachdienst Empfänger
Auslöser	Versanddienst Empfänger
Vorbedingung	Sicherer Kommunikationskanal zwischen Versanddienst und Postfachdienst des Empfängers
Input	Nachricht
Ergebnis	Nachricht vom Postfachdienst des Empfängers entgegengenommen
Nachbedingung	
Ablauf	Nachricht wird vom Postfachdienst Empfänger entgegengenommen.
Fehlerfälle	FC-01: Nachricht nicht vollständig übertragen.
Schritt 45	**Von Kopie der Nachrichten Transport-Verschlüsselung entfernen**
Kurzbeschreibung	Der Postfachdienst des Empfängers erstellt eine Kopie der empfangenen Nachricht und entfernt von dieser die Transport-Verschlüsselung.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	

Input	Nachricht
Ergebnis	Entschlüsselte Nachrichten-Kopie
Nachbedingung	Spätestens nach Beendigung / Abbruch der Schritte zum „Empfang von Nachrichten durch den Postfachdienst des Empfängers“ muss die entschlüsselte Nachrichten-Kopie gelöscht werden.
Ablauf	Kopie der verschlüsselten Nachrichten erstellen und diese entschlüsseln. Hinweis: Im weiteren Verlauf wird bis zur Ablage der Nachricht in das Postfach des Empfänger mit der entschlüsselten Kopie weitergearbeitet (sofern nicht anders angegeben).
Fehlerfälle	FC-01: Entschlüsselung konnte nicht durchgeführt werden.
Schritt 46	**Integritätssicherung prüfen**
Kurzbeschreibung	Die Integritätsicherung der Nachricht wird geprüft. Bei normalen Nachrichten handelt es sich um einen hashwert. Bei Nachrichten mit der Versandoption „Absenderbestätigt“ und Bestätigungsnachrichten handelt es sich um eine Signatur.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht, Signatur, Zertifikat (von DMDA des Absender)
Ergebnis	Prüfergebnis
Nachbedingung	
Ablauf	• Berechnung des Hash-Wertes und Vergleich mit dem in den Metadaten der Nachricht gespeicherten Hash (Metadaten Nr. 17). • Bei Signatur durch DMDA (Metadaten Nr. 17) ◦ Mathematische Prüfung der Signatur mit Signaturprüfschlüssel aus Zertifikat ◦ Prüfung der Gültigkeit des Zertifikates ◦ Prüfung Zertifikatskette ◦ Prüfung Status des Zertifikates • Aggregation der Prüfergebnisse
Fehlerfälle	FC-01: Integritätsverletzung FC-02: Zertifikat ungültig FC-03: Der Status des Zertifikates konnte nicht online geprüft werden FC-04: Keine Signatur bei einer Nachricht mit Versandoption „Absenderbestätigt“
Schritt 47	**Entscheidungsknoten: Nachsendeauftrag aktiv?**

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Kurzbeschreibung	Überprüfung, ob vom Empfänger ein Nachsendeauftrag[1] (an eine andere De-Mail-Adresse) verlangt wurde (siehe Funktion 3 in Abschnitt 8).
ja	Schritt 48
nein	Schritt 52
Schritt 48	**Nachricht als Nachsendeauftrag aufbereiten**
Kurzbeschreibung	Der Empfänger der Nachricht wird an die im Nachsendeauftrag angegebene Adresse umgeschrieben.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	Nachsendeauftrag ist aktiv
Input	Nachricht, Nachsendeauftrag
Ergebnis	Nachricht mit geänderter Empfänger-Adresse
Nachbedingung	
Ablauf	• Prüfung auf Nachrichten-Schleife (*forwarding loop*) • Empfänger-Adresse aus Nachsendeauftrag ermitteln • Empfänger-Adresse aus Nachsendeauftrag in Element <Empfänger-Adressen für den Transport> (Feld 19) schreiben.
Fehlerfälle	FC-01: Nachrichten-Schleife entdeckt
Schritt 49	**Nachrichteninhalt an neuen Empfänger verschlüsseln**
Kurzbeschreibung	Die Nachricht wird ohne Metadaten an den eigenen und den neuen empfangenden DMDA verschlüsselt (s. a. Schritt 30).
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht, Verschlüsselungsschlüssel des eigenen und des neuen empfangenden DMDA
Ergebnis	Verschlüsselte Nachricht
Nachbedingung	
Ablauf	Nachricht mit Verschlüsselungsschlüssel des eigenen DMDA und des neuen Empfänger-DMDA verschlüsseln.
Fehlerfälle	FC-01: Verschlüsselung nicht durchführbar
Schritt 50	**Nachrichten-Kopie ohne Transport-Verschlüsselung löschen**
Kurzbeschreibung	Der Postfachdienst löscht die entschlüsselte Kopie der Nachricht.

1 Von einem Nachsendeauftrag ist eine Weiterleitung (siehe Schritt 69) zu unterscheiden. Bei einem Nachsendeauftrag werden Eingangsbestätigungen erst durch den Postfachdienst ausgestellt, an den der Nachsendeauftrag gerichtet war.

Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht ohne Transport-Verschlüsselung
Ergebnis	Entschlüsselte Nachricht ist gelöscht
Nachbedingung	
Ablauf	Entschlüsselte Nachrichten löschen
Fehlerfälle	
Schritt 51	**Nachricht an neuen Empfänger versenden**
Kurzbeschreibung	Die Nachricht wird über eigenen Versanddienst zum neuen Empfänger versendet.
Akteure	Postfachdienst Empfänger, Versanddienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	Sicherer Kommunikationskanal zwischen Postfachdienst Empfänger und Versanddienst Empfänger
Input	Nachricht
Ergebnis	Nachricht an Versanddienst Empfänger versendet
Nachbedingung	• Aufgrund des Nachsendeauftrags darf der Versanddienst keine neue Versandbestätigung ausstellen. • Anhalten
Ablauf	Nachricht an den neuen Empfänger ohne weitere Änderungen in den Metadaten versenden Hinweis: Eine ggf. angeforderte Versandbestätigung des ursprünglichen Absenders wird an dieser Stelle nicht ausgestellt.
Fehlerfälle	FC-01: Versanddienst hat Nachricht nicht vollständig angenommen.
Schritt 52	**Auf Schadsoftware prüfen**
Kurzbeschreibung	Nachricht wird auf Schadsoftware geprüft.
Akteure	Postfachdienst Empfänger, Schadsoftware-Dienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht
Ergebnis	Nachricht auf Schadsoftware geprüft
Nachbedingung	
Ablauf	Wenn Nachricht nicht Ende-zu-Ende-verschlüsselt, Nachricht an Schadsoftware-Dienst übergeben (s. a. Funktion 2, Abschnitt 8)

Fehlerfälle	FC-01: Schadsoftware-Prüfung konnte nicht durchgeführt werden. FC-02: Nachricht für Empfänger verschlüsselt, nicht prüfbar.
Schritt 53	**Entscheidungsknoten: Schadsoftware-Prüfung OK?**
Kurzbeschreibung	Ergebnis der Schadsoftware-Prüfung auswerten
ja	Schritt 56
nein	Schritt 54
Schritt 54	**Meldungs-/ Bestätigungnachricht über gefundene Schadsoftware versenden**
Kurzbeschreibung	Der Postfachdienst versendet eine Meldungsnachricht über gefundene Schadsoftware an den Absender und Empfänger. Bei Nachrichten, die eine Versand- und/oder Eingangsbestätigung angefordert haben, wird anstelle der einfachen Meldungsnachricht eine Schadsoftware-Bestätigungsnachricht an den Absender und Empfänger gesendet. In der Schadsoftware-Meldungs- oder Bestätigungsnachricht wird zum Ausdruck gebracht, dass eine Kenntnisnahme aufgrund der enthaltenen Schadsoftware ggf. nicht möglich ist.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht, Ergebnis
Ergebnis	Meldung und/oder Bestätigung über gefundene Schadsoftware erstellt und versendet
Nachbedingung	
Ablauf	• Prüfung, ob Nachricht eine Versand-, Eingangs- und/oder Abholbestätigung erfordert • Falls nein: ◦ Eine Meldungsnachricht an den Absender (oder falls angegeben an dessen Antwort-Adresse) und den Empfänger der ursprünglichen Nachricht erzeugen, dass die empfangene Nachricht Schadsoftware enthält. ◦ Element <Nachrichten-Kennung des Absenders> (Nr. 9) von der ursprünglichen Nachricht in die Meldungsnachricht übernehmen ◦ Meldung versenden/darstellen • Falls ja: ◦ Schadsoftware-Bestätigung erzeugen mit dem expliziten Hinweis, dass für die betreffende Nachricht eine Versand-, Eingangs-und/oder Abholbestätigung angefordert worden ist. ◦ Schadsoftware-Bestätigung um den Hinweis ergänzen, dass aufgrund der gefundenen Schadsoftware nicht von einer

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Kenntnisnahme der Nachricht durch den Empfänger ausgegangen werden kann. ◦ Die Bestätigung ist mit einer qualifizierten elektronischen Signatur zu signieren. ◦ Bestätigungsnachricht auf Grundlage der Schadsoftware-Bestätigung erstellen ◦ Keine Versandoptionen werden gesetzt ◦ Element <Nachrichten-Kennung des Absenders> (Nr. 9) von der ursprünglichen Nachricht in die Schadsoftware-Bestätigungsnachricht übernehmen. ◦ Empfänger-Adresse ist auf den Absender der ursprünglichen Nachricht zu setzen (mit Absender- oder falls angegeben mit seiner Antwort-Adresse) ◦ In Kopie (Carbon Copy, CC) ist der Empfänger der ursprünglichen Nachricht zu setzen ◦ Absender-Adresse ist auf die System-Adresse des DMDA für Schadsoftware-Warnung zu setzen • Die Bestätigungsnachricht versenden
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden. FC-02: Signatur konnte nicht erstellt werden. FC-03: Bestätigungsnachricht konnte nicht versendet werden.
Schritt 55	**Nachricht mit Schadsoftware löschen**
Kurzbeschreibung	Der Postfachdienst löscht die Nachricht mit der gefundenen Schadsoftware.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht mit Schadsoftware
Ergebnis	Nachricht ist gelöscht
Nachbedingung	Anhalten
Ablauf	Der Postfachdienst löscht die Nachricht mit der gefundenen Schadsoftware.
Fehlerfälle	
Schritt 56	**Entscheidungsknoten: Versandoption „Persönlich“ oder Abholbestätigung?**
Kurzbeschreibung	Metadaten der Nachricht auswerten, ob die Versandoption „Persönlich“ oder „Abholbestätigung“ gewählt wurde.
ja	Schritt 57
nein	Schritt 58

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Schritt 57	**Meldung an Empfänger versenden**
Kurzbeschreibung	Der Postfachdienst des Empfängers kann eine Meldung mit der Information für den Empfänger erstellen, dass für ihn eine (andere) Nachricht mit der Versandoption „Persönlich“ oder „Abholbestätigung“ vorliegt, die zum Abruf und zum Lesen das Authentisierungsniveau „hoch“ erfordert. Die Abholbestätigung hat die höhere Priorität, wenn beide Versandoptionen gewählt wurden.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	
Ergebnis	Meldung an den Empfänger versendet
Nachbedingung	Anhalten
Ablauf	• Meldung erstellen. • Informationstext einfügen, dass eine Nachricht vorliegt und mit dem Authentisierungsniveau „hoch“ abgerufen werden muss. Bei Nachrichten, für die eine Versand- und/oder eine Eingangsbestätigung angefordert worden ist, ist explizit darauf hinzuweisen. • Die Meldung an den Empfänger versenden.
Fehlerfälle	FC-01: Meldung kann nicht versendet werden.
Schritt 58	**Entscheidungsknoten: Spezieller Nachrichten-Typ?**
Kurzbeschreibung	Feststellen, ob Nachricht ein spezieller Nachrichten-Typ (Metadaten Nr. 16) ist, um Validitätsprüfungen durchzuführen. Hinweis: Dieser Schritt, Schritt 59 und Schritt 60 sind optional und können – müssen jedoch nicht – vom DMDA angeboten werden.
ja	Schritt 59
nein	Schritt 61
Schritt 59	**Validitätsprüfung für spezielle Nachrichten-Typen durchführen**
Kurzbeschreibung	Der Postfachdienst führt für spezielle Nachrichten-Typen[2] eine Validitätsprüfung durch. Der Nachrichten-Typ ist in den Metadaten (Nr. 16) einer Nachricht definiert.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	Spezieller Nachrichten-Typ
Input	Nachricht

2 Andere De-Mail-Dienste können neue Nachrichten-Typen definieren und damit auch neue spezifische Validitätsprüfungen für diesen Schritt erfordern.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Ergebnis	Prüfprotokoll der Validitätsprüfung
Nachbedingung	
Ablauf	• Bei Bestätigungsnachrichten: ◦ Prüfung, ob Nachrichten-spezifische Absender-Adresse des DMDA für Versand-, Eingangs- und Abholbestätigung verwendet wurde. ◦ Prüfung, ob Aussteller der Bestätigung auch zum Absender der Nachricht passt. • Bei Meldungsnachrichten: ◦ Prüfung, ob Nachrichten-spezifische Absender-Adresse verwendet wurde. ◦ Prüfung, ob Aussteller der Meldung auch zum Absender der Nachricht passt.
Fehlerfälle	
Schritt 60	**Ergebnis der Prüfung als Meldung versenden**
Kurzbeschreibung	Das Ergebnis (Prüfprotokoll) der Validitätsprüfung wird als Meldung an den Empfänger versendet.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht, Prüfprotokoll der Validitätsprüfung
Ergebnis	Prüfprotokoll als Meldung an Empfänger versendet
Nachbedingung	
Ablauf	Aus dem Protokoll der Validitätsprüfung eine Meldung erzeugen.
Fehlerfälle	FC-01: Die Meldung konnte nicht versendet werden.
Schritt 61	**Nachricht signiert und nicht verschlüsselt?**
Kurzbeschreibung	Feststellen, ob die Nachricht oder Nachrichtenanhänge durch den Absender qualifiziert signiert wurden und nicht verschlüsselt sind. Hinweis:Dieser Schritt, Schritt 62 und Schritt 63 sind optional und können aber vom DMDA angeboten werden.
ja	Schritt 62
nein	Schritt 64
Schritt 62	**Signatur- und Zertifikatsprüfung für Anhänge durchführen**
Kurzbeschreibung	Der Postfachdienst führt eine Prüfung der qualifizierten Signatur(en) sowie des Zertifikates für Nachrichtenanhänge durch.
Akteure	Postfachdienst Empfänger

Auslöser	Postfachdienst Empfänger
Vorbedingung	Nachricht qualifiziert signiert und nicht verschlüsselt
Input	Nachricht
Ergebnis	Prüfprotokoll der Signatur- und Zertifikatsprüfung
Nachbedingung	
Ablauf	• Mathematische Prüfung der qualifizierten Signatur(en) mit Signaturprüfschlüssel aus Zertifikat • Prüfung der Gültigkeit des Zertifikates • Prüfung Zertifikatskette • Prüfung Status des Zertifikates • Prüfergebnisse zusammenfassen in Prüfprotokoll
Fehlerfälle	FC-01: Integritätsverletzung FC-02: Zertifikat ungültig FC-03: Der Status des Zertifikates konnte nicht online geprüft werden
Schritt 63	**Ergebnis der Prüfung als Meldung versenden**
Kurzbeschreibung	Das Ergebnis (Prüfprotokoll) der Signatur- und Zertifikatsprüfung wird als Meldung an den Empfänger versendet.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht, Prüfprotokoll
Ergebnis	Prüfprotokoll als Meldung versendet.
Nachbedingung	
Ablauf	Aus dem Protokoll der Signatur- und Zertifikatsprüfung eine Meldung erzeugen.
Fehlerfälle	FC-01: Meldung kann nicht versendet werden.
Schritt 64	**Nachricht mit Transport-Sicherung ins Postfach des Empfängers ablegen**
Kurzbeschreibung	Der Postfachdienst des Empfängers legt die empfangene Nachricht verschlüsselt ins Postfach des Empfängers ab. Hinweis: Ab diesem Schritt ist die Nachricht im Eingangsbereich des Empfängers.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	

Input	Nachricht mit Transport-Sicherung
Ergebnis	Nachricht im Postfach des Empfängers abgelegt
Nachbedingung	
Ablauf	• Nachricht mit der nicht entfernten Transport-Verschlüsselung im Postfach des Empfängers ablegen • Aufruf Funktion 11 (siehe Abschnitt 8) zur automatischen Sortierung von Nachrichten • Optional: Meldung versenden, dass eine neue Nachricht eingetroffen ist[3]
Fehlerfälle	FC-01: Nachricht kann nicht ins Postfach des Empfängers abgelegt werden
Schritt 65	**Prüfung, ob Eingangsbestätigung erstellt werden soll**
Kurzbeschreibung	Metadaten der Nachricht auswerten, ob eine Eingangsbestätigung angefordert wurde. Im Rahmen von automatisierten Weiterleitungen (siehe Schritt 68) darf keine erneute Eingangsbestätigung erstellt werden, da eine Eingangsbestätigung nur vom ursprünglichen Empfänger verschickt werden soll.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht
Ergebnis	Eingangsbestätigung erstellen / nicht erstellen
Nachbedingung	
Ablauf	• Wert für Versandoption „Eingangsbestätigung“ ermitteln • Prüfung, ob das Elemente <Weiterleitungs-Absender)> (Nr.) und gesetzt ist, dann handelt es sich um eine weitergeleitete Nachricht und es wird keine Eingangsbestätigung erstellen
Fehlerfälle	
Schritt 66	**Entscheidungsknoten: Eingangsbestätigung?**
Kurzbeschreibung	Metadaten der Nachricht auswerten, ob eine Eingangsbestätigung gewünscht wird.
Ja	Schritt 67
Nein	Schritt 69
Schritt 67	**Eingangsbestätigung erstellen**
Kurzbeschreibung	Vom Postfachdienst des Empfängers wird eine Eingangsbestätigung erstellt.
Akteure	Postfachdienst Empfänger

3 Diese Meldung kann bspw. genutzt werden, um den Nutzer auf seinen Wunsch hin über den Eingang neuer Nachrichten mittels SMS zu informieren.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht ohne Transport-Verschlüsselung
Ergebnis	Eingangsbestätigung
Nachbedingung	
Ablauf	• Berechnung des Hash-Wertes und Vergleich mit dem in den Metadaten der Nachricht gespeicherten (Metadatum Nr. 17)[4]. • Falls Vergleich der Hash-Werte OK: ◦ Eingangsbestätigung erstellen (siehe Abschnitt 5.2). ◦ Die Bestätigung ist mit einer qualifizierten elektronischen Signatur zu signieren. • Falls Vergleich der Hash-Werte nicht OK: ◦ Es ist eine Meldung an den Empfänger und Absender der Nachricht zu übermitteln. ◦ Die Meldung ist mit einer qualifizierten elektronischen Signatur zu signieren. ◦ Bestätigungsnachricht auf Grundlage der Eingangsbestätigung erstellen. • Es werden keine Versandoptionen gesetzt, nur falls in der ursprünglichen Nachricht die Versandoption „Persönlich“ gesetzt war, wird auch die Bestätigungsnachricht mit der Versandoption „Persönlich“ versendet. • Element <Nachrichten-Kennung des Absenders> (Nr. 9) von der ursprünglichen Nachricht in die Bestätigungsnachricht übernehmen. • Die Empfänger-Adresse ist auf die Absender- bzw. falls angegeben, auf die Antwort-Adresse, der ursprünglichen Nachricht zu setzen. • In Kopie (Carbon Copy, CC) ist der Empfänger der ursprünglichen Nachricht zu setzen. • Absender-Adresse ist auf die System-Adresse des DMDA für Eingangsbestätigungen zu setzen.
Fehlerfälle	FC-01: Berechneter Hash-Wert stimmt nicht mit dem in den Metadaten gespeicherten Hash-Wert überein. FC-02: Keine Signaturerstellung möglich.
Schritt 68	**Bestätigungsnachricht an Absender und Empfänger versenden**
Kurzbeschreibung	Die Bestätigungsnachricht wird an den Absender und den Empfänger der Nachricht versendet.

4 Eine Prüfung des Hash-Wertes erfolgt auch bereits in Schritt 46. Das Ergebnis dieser Berechnung kann verwendet werden.

Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Eingangsbestätigung
Ergebnis	Bestätigungsnachricht versendet
Nachbedingung	
Ablauf	Die Bestätigungsnachricht versenden.
Fehlerfälle	FC-01: Nachricht kann nicht versendet werden.
Schritt 69	**Entscheidungsknoten: Weiterleitung aktiv?**
Kurzbeschreibung	Überprüfung, ob vom Empfänger eine automatische Weiterleitung[5] aktiviert wurde (siehe Funktion 8 in Abschnitt 8).
Ja	Schritt 70
Nein	Schritt 73
Schritt 70	**Nachricht zur Weiterleitung aufbereiten**
Kurzbeschreibung	Der Empfänger der Nachricht wird an die im Weiterleitungsauftrag angegebene Adresse umgeschrieben.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	Weiterleitung ist aktiv
Input	Nachricht, Weiterleitungsauftrag
Ergebnis	Nachricht mit geänderter Empfänger-Adresse
Nachbedingung	
Ablauf	• Prüfung auf Nachrichten-Schleife (forwarding loop). ◦ Wird eine Nachrichtenschleife festgestellt, wird die Nachricht nicht weitergeleitet. • Empfänger-Adresse aus Weiterleitungsauftrag in Element <Empfänger-Adressen für den Transport> (Nr. 19) schreiben. • In Element <Weiterleitungs-Absender> (Nr. 20) die aktuelle De-Mail-Adresse des Empfängers schreiben. Hinweis: Alle anderen Metadaten bleiben erhalten. Insbesondere erfolgt keine erneute Integritätssicherung.
Fehlerfälle	FC-01: Nachrichten-Schleife entdeckt.
Schritt 71	**Nachrichteninhalt an neuen Empfänger verschlüsseln**
Kurzbeschreibung	Die Nachricht wird ohne Metadaten an den neuen Empfänger-DMDA verschlüsselt (s. a. Schritt 30).

5 Weiterleitungen sind von Nachsendeaufträgen zu unterscheiden (siehe 7.5).

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht, Verschlüsselungsschlüssel des neuen Empfänger-DMDA
Ergebnis	Verschlüsselte Nachricht
Nachbedingung	
Ablauf	Nachricht mit Verschlüsselungsschlüssel des eigenen DMDA und des neuen Empfänger-DMDA verschlüsseln
Fehlerfälle	FC-01: Verschlüsselung nicht durchführbar
Schritt 72	**Nachricht an neuen Empfänger versenden**
Kurzbeschreibung	Die Nachricht wird über eigenen Versanddienst an neuen Empfänger versendet.
Akteure	Postfachdienst Empfänger, Versanddienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	Sicherer Kommunikationskanal zwischen Postfachdienst Empfänger und Versanddienst Empfänger aufgebaut
Input	Nachricht
Ergebnis	Nachricht an Versanddienst Empfänger versendet
Nachbedingung	Aufgrund der Weiterleitung darf der Versanddienst keine neue Versandbestätigung ausstellen.
Ablauf	Nachricht an den neuen Empfänger versenden.
Fehlerfälle	FC-01: Versanddienst hat Nachricht nicht vollständig angenommen.
Schritt 73	**Nachrichten-Kopie ohne Transport-Verschlüsselung löschen**
Kurzbeschreibung	Der Postfachdienst löscht die entschlüsselte Kopie der Nachricht.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht ohne Transport-Verschlüsselung
Ergebnis	Entschlüsselte Nachricht ist gelöscht
Nachbedingung	Anhalten
Ablauf	Entschlüsselte Nachrichten löschen.
Fehlerfälle	

Tabelle 9: Schritte zum Empfangen der Nachrichten

7.6 Abrufen der Nachrichten durch Empfänger

Schritt 74	**Empfänger greift auf Postfachdienst zu**
Kurzbeschreibung	Der Empfänger greift auf den Postfachdienst zu, um eingegangene Nachrichten abzurufen.
Akteure	Empfänger, Postfachdienst Empfänger
Auslöser	Empfänger
Vorbedingung	Empfänger an seinem De-Mail-Konto angemeldet Sicherer Kommunikationskanal aufgebaut
Input	
Ergebnis	Postfachdienst geöffnet
Nachbedingung	
Ablauf	- Autorisierung des Empfängers prüfen.
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto angemeldet. FC-02: Empfänger nicht autorisiert, Nachrichten abzurufen.
Schritt 75	**Aktuelles Authentisierungsniveau des Empfängers ermitteln**
Kurzbeschreibung	Das aktuelle Authentisierungsniveau des Empfängers wird ermittelt.
Akteure	Postfachdienst Empfänger, Account-Dienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nutzer-Kennung des De-Mail-Kontos
Ergebnis	Aktuelles Authentisierungsniveau
Nachbedingung	
Ablauf	De-Mail-Konto ermitteln. Anfrage an Account-Dienst, welches aktuelle Authentisierungsniveau der Empfänger besitzt.
Fehlerfälle	FC-01: Account-Dienst nicht erreichbar.
Schritt 76	**Entscheidungsknoten: Aktuelles Authentisierungsniveau „hoch“**
Kurzbeschreibung	Prüfen, ob das aktuelle Authentisierungsniveau des Empfängers „hoch“ ist.
ja	Schritt 77
nein	Schritt 79
Schritt 77	**Entscheidungsknoten: Nachrichten mit Abholbestätigung vorhanden?**
Kurzbeschreibung	Es wird geprüft, ob Nachrichten im Postfach abgelegt wurden, für die eine Abholbestätigung versendet werden muss. Bei automatisch weitergeleiteten Nachrichten wird keine (erneute)

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Abholbestätigung ausgestellt.
ja	Funktion 1 ausführen und anschließend Schritt 78
nein	Schritt 78
Schritt 78	**Alle Nachrichten zum Abruf anbieten**
Kurzbeschreibung	Alle Nachrichten werden zum Abruf angeboten.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Liste aller Nachrichten
Ergebnis	Alle vorhandenen Nachrichten aufgelistet.
Nachbedingung	Schritt 80
Ablauf	Nachrichten auflisten
Fehlerfälle	
Schritt 79	**Nur Nachrichten mit Authentisierungsniveau-Empfänger „hoch“ zum Abruf anbieten**
Kurzbeschreibung	Nur Nachrichten, die mit Authentisierungsniveau “normal“ gelesen werden dürfen, werden zum Abruf angeboten (d.h. keine Nachrichten mit der Versandoption „Persönlich“ und „Abholbestätigung“).
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Liste aller Nachrichten
Ergebnis	Alle vorhandenen Nachrichten mit Authentisierungsniveau-Empfänger < „hoch“ aufgelistet
Nachbedingung	
Ablauf	• Nur Nachrichten anzeigen, für die die Versandoption „Persönlich“ und Abholbestätigung“ nicht gewählt wurden- • Falls Nachrichten vorhanden sind, die nur mit Authentifizierungsniveau „hoch“ einsehbar sind, wird mit einer Meldung auf diese Tatsache hingewiesen.
Fehlerfälle	
Schritt 80	**Nachrichten auswählen**
Kurzbeschreibung	Der Empfänger wählt eine oder mehrere Nachrichten zum Abruf aus.
Akteure	Empfänger, Postfachdienst Empfänger
Auslöser	Empfänger

Vorbedingung	Liste von auswählbaren Nachrichten
Input	Nachrichtenliste
Ergebnis	Ausgewählte Nachrichten
Nachbedingung	
Ablauf	Empfänger wählt Nachrichten aus Nachrichtenliste aus.
Fehlerfälle	
Schritt 81	**Nachrichteninhalt entschlüsseln**
Kurzbeschreibung	Zum Abruf oder zum Lesen der Nachrichten entschlüsselt der Postfachdienst die Nachrichten (s. a. Schritt 45).
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht(en), Entschlüsselungsschlüssel
Ergebnis	Entschlüsselte Nachrichten-Kopie
Nachbedingung	
Ablauf	• Ursprünglich verschlüsselte Nachrichten verbleiben in Postfach des Empfängers. • Kopie der verschlüsselten Nachrichten erstellen und diese entschlüsseln. Hinweis: Im weiteren Verlauf wird bis zum vollständigen Abruf der Nachrichten durch den Empfänger mit den entschlüsselten Kopien weitergearbeitet (sofern nicht anders angegeben).
Fehlerfälle	FC-01: Entschlüsselung konnte nicht durchgeführt werden.
Schritt 82	**Integritätssicherung prüfen**
Kurzbeschreibung	Eine durch den Postfachdienst des Absenders angebrachte Integritätssicherung (Hash-Wert und – sofern Versandoption „Absenderbestätigt“ gewählt – die Signatur des DMDA) wird vom Postfachdienst des Empfängers geprüft.
Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht, Signatur, Zertifikat (DMDA Absender)
Ergebnis	Prüfergebnis
Nachbedingung	
Ablauf	• Berechnung des Hash-Wertes und Vergleich mit dem in den Metadaten der Nachricht gespeicherten Hash-Wertes (Metadatum

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Nr. 17). • Bei Signatur durch DMDA (Metadatum Nr. 18) ◦ Mathematische Prüfung der Signatur mit Signaturprüfschlüssel aus Zertifikat ◦ Prüfung der Gültigkeit des Zertifikates (sofern vorhanden) ◦ Prüfung Zertifikatskette (sofern vorhanden) ◦ Prüfung Status des Zertifikates (sofern vorhanden) • Aggregation der Prüfergebnisse Hinweis: Eine Prüfung der Integritätssicherung erfolgte bereits bei der Annahme der Nachricht durch den Versanddienst des Empfängers in Schritt 46. In Schritt 82 muss zumindest die Berechnung des Hash-Wertes inkl. Vergleich mit dem Wert aus den Metadaten und die mathematische Prüfung der Signatur des DMDA neu erfolgen, um zwischenzeitliche Änderungen an der Nachricht erkennen zu können.
Fehlerfälle	FC-01: Integritätsverletzung FC-02: Zertifikat ungültig FC-03: Der Status des Zertifikates konnte nicht online geprüft werden FC-04: Keine Signatur bei einer Nachricht mit Versandoption „Absenderbestätigt“
Schritt 83	**Nachricht zum Empfänger übertragen**
Kurzbeschreibung	Die Nachricht wird vom Postfachdienst des Empfängers zum Client des Empfängers übertragen.
Akteure	Empfänger, Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	Sicherer Kanal zwischen Postfachdienst Empfänger und Client
Input	• Nachricht • Parameter, ob Integritätssicherung zusammen mit der Nachricht übertragen werden soll (vgl. Funktion 14 in Abschnitt 8)
Ergebnis	Nachricht übertragen
Nachbedingung	
Ablauf	• Ermittlung, ob die Integritätssicherung zusammen mit der Nachricht übertragen werden soll. • Übertragung der Nachricht vom Postfachdienst zum Client des Empfängers.
Fehlerfälle	FC-01: Client hat Nachricht nicht entgegengenommen.
Schritt 84	**Nachrichten-Kopie ohne Transport-Verschlüsselung löschen**
Kurzbeschreibung	Der Postfachdienst löscht die entschlüsselte Kopie der Nachricht.

Akteure	Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	
Input	Nachricht ohne Transport-Verschlüsselung
Ergebnis	Entschlüsselte Nachricht ist gelöscht
Nachbedingung	Anhalten
Ablauf	Entschlüsselte Nachricht löschen.
Fehlerfälle	

Tabelle 10: Schritte zum Abrufen und Lesen der Nachrichten

7.7 Empfang und Lesen der Nachricht durch Empfänger

Schritt 85	**Nachricht vom Postfachdienst entgegennehmen**
Kurzbeschreibung	Der Client des Empfängers nimmt die Nachricht vom Postfachdienst des Empfängers entgegen.
Akteure	Empfänger, Postfachdienst Empfänger
Auslöser	Postfachdienst Empfänger
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Nachricht
Ergebnis	Nachricht vom Client des Empfängers entgegengenommen
Nachbedingung	
Ablauf	Der Client des Empfängers nimmt die Nachricht vom Postfachdienst entgegen. Prüfen, ob Nachricht syntaktisch korrekt ist.
Fehlerfälle	FC-01: Nachricht nicht vollständig übertragen. FC-02: Nachricht enthält syntaktische Fehler.
Schritt 86	**Entscheidungsknoten: Nachricht -verschlüsselt?**
Kurzbeschreibung	Feststellen, ob die Nachricht Ende-zu-Ende-verschlüsselt ist.
ja	Schritt 87
nein	Schritt 88
Schritt 87	**Nachricht entschlüsseln**
Kurzbeschreibung	Die Nachricht wird lokal beim Empfänger entschlüsselt.
Akteure	Empfänger
Auslöser	Empfänger

Vorbedingung	Nachricht ist verschlüsselt
Input	Nachricht, Entschlüsselungsschlüssel von Empfänger
Ergebnis	Entschlüsselte Nachricht
Nachbedingung	
Ablauf	• Die zu entschlüsselnde Nachricht inklusive der Anhänge wird an die Entschlüsselungsfunktion übergeben. • Die Entschlüsselungsfunktion greift auf den privaten Schlüssel des Empfängers zu. • Die Entschlüsselungsfunktion entschlüsselt mit dem privaten Schlüssel des Empfängers den symmetrischen Verschlüsselungsschlüssel der Nachricht. • Der Nachrichtentext der Nachricht inklusive der Dateianhänge wird mit dem symmetrischen Verschlüsselungschlüssel entschlüsselt. Hinweis: Die Entschlüsselung der Nachricht muss auf dem System des Nutzers erfolgen. Die entschlüsselte Nachricht darf auf dem DMDA-Server auch nicht temporär zwischengespeichert werden.
Fehlerfälle	FC-01: Nachricht konnte nicht entschlüsselt werden.
Schritt 88	**Entscheidungsknoten: Signatur prüfen?**
Kurzbeschreibung	Feststellen, ob eine Signatur vorhanden ist und der Empfänger die Signatur prüfen möchte.
ja	Schritt 89
nein	Schritt 90
Schritt 89	**Signatur- und Zertifikatsprüfung durchführen**
Kurzbeschreibung	Der Client des Empfängers führt eine Prüfung der Signatur sowie des Zertifikates durch.
Akteure	Empfänger
Auslöser	Empfänger
Vorbedingung	Nachricht signiert
Input	Nachricht
Ergebnis	Ergebnis der Prüfung
Nachbedingung	
Ablauf	• Mathematische Prüfung der Signatur mit Signaturprüfschlüssel aus Zertifikat • Prüfung der Gültigkeit des Zertifikates • Prüfung Zertifikatskette • Prüfung Status des Zertifikates • Prüfergebnisse zusammenfassen in Prüfprotokoll

– Seite 177 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Fehlerfälle	FC-01: Integritätsverletzung FC-02: Zertifikat ungültig FC-03: Der Status des Zertifikates konnte nicht online geprüft werden.
Schritt 90	**Nachricht darstellen**
Kurzbeschreibung	Die Nachricht, die Ergebnisse der Signatur- und Zertifikatsprüfung des Clients, sowie die Prüfprotokolle vom Postfachdienst werden dargestellt.
Akteure	Empfänger
Auslöser	Empfänger
Vorbedingung	
Input	Nachricht
Ergebnis	Nachricht dargestellt
Nachbedingung	Anhalten
Ablauf	Die Nachricht, die Ergebnisse der Signatur- und Zertifikatsprüfung des Clients sowie ggf. vorhandene Prüfprotokolle vom Postfachdienst darstellen.
Fehlerfälle	

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

8 Weitere Funktionen

Die in diesem Abschnitt beschriebenen Funktionen werden entweder vom System ausgeführt oder können vom Nutzer interaktiv aufgerufen werden, während dieser am De-Mail-Konto angemeldet ist. Eine Beschreibung, wie die einzelnen Funktionen dargestellt werden, findet sich in Abschnitt 10.2.

8.1 Durch das System ausgeführte Funktionen

Funktion 1	**Abholbestätigungen versenden**
Kurzbeschreibung	Für alle Nachrichten in dem Postfach, die eine Abholbestätigung erfordern und für die noch keine Abholbestätigung erstellt und versendet wurde, wird jeweils eine Abholbestätigung erstellt und versendet.
Akteure	Postfachdienst Empfänger
Auslöser	Empfänger
Vorbedingung	Anmeldung am De-Mail-Konto mit Authentisierungsniveau „hoch“. Nachrichten, die eine Abholbestätigung erfordern und für die noch keine Abholbestätigung erstellt und versendet wurde
Input	Nachrichten, die eine Abholbestätigung erfordern
Ergebnis	• Erfolgter Versand der Abholbestätigungen für Nachrichten, die mit dieser Versandoption erstellt wurden • Nachrichten wurden gekennzeichnet, dass die Abholbestätigung versendet wurde
Nachbedingung	
Ablauf	• Selektion der Nachrichten mit der Versandoption „Abholbestätigung“, mit folgenden Bedingung: ◦ noch keine Abholbestätigung erstellt und versendet ◦ keine automatisch weitergeleiteten Nachrichten sind • Bestätigungsnachrichten auf Grundlage der Abholbestätigung erstellen. • Es wird jeweils die Versandoption „Persönlich“ gesetzt. • Element <Nachrichten-Kennung des Absenders> (Nr. 9) von der ursprünglichen Nachricht in die jeweilige Bestätigungsnachricht übernehmen. • Die Empfänger-Adresse ist auf die Absender- bzw. falls angegeben, auf die Antwort-Adresse, der jeweiligen ursprünglichen Nachricht zu setzen. • In Kopie (Carbon Copy, CC) ist der Empfänger der jeweiligen ursprünglichen Nachricht zu setzen.

	• Absender-Adresse ist auf die System-Adresse des DMDA für Abholbestätigungen zu setzen. • Die Bestätigungsnachrichten versenden. • Kennzeichnung der Nachrichten, für die eine Abholbestätigung erstellt wurden
Fehlerfälle	FC-01: Nachricht kann nicht versendet werden

Tabelle 11: Durch das System ausgeführte Funktionen

8.2 Durch den Nutzer initiierte Funktionen

Funktion 2	**Schadsoftware-Dienst: Prüfung auf Schadsoftware**
Kurzbeschreibung	Es erfolgt eine Prüfung der vom Nutzer ausgewählten Nachrichten auf Schadsoftware (z.B. Viren, Würmer und Trojaner)
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Prüfprogramme mit aktuellen Prüfkonfigurationen
Input	Nachricht
Ergebnis	Warnung, wenn Inhalt Schadsoftware enthält
Nachbedingung	Auf Nachrichten mit Schadsoftware darf ein Nutzer nur nach expliziter Warnung zugreifen, dass das Öffnen der Nachricht auf eigene Gefahr erfolgt und er sich mit dem Absender in Verbindung setzen sollte.
Ablauf	• Nachrichten werden zum Schadsoftware-Scanner übergeben • Bei Erkennung von Schadsoftware werden die Nachrichten entsprechend gekennzeichnet. Auf Nachrichten mit Schadsoftware darf der Nutzer nur nach expliziter Warnung zugreifen.
Fehlerfälle	FC-01: Dateianhang unbekannt und kann nicht auf Schadsoftware geprüft werden.
Funktion 3	**Nachsendeauftrag an eine andere De-Mail-Adresse einrichten**
Kurzbeschreibung	Der Nutzer stellt einen Nachsendeauftrag an eine andere De-Mail-Adresse. Alle empfangenen Nachrichten werden während einer festgelegten Übergangszeit an diese weitergeleitet. Hinweis: Bei einem Nachsendeauftrag wird keine Kopie im Postfach des Empfängers abgelegt und eine ggf. angeforderte Eingangsbestätigung wird erst durch den Postfachdienst erzeugt, an den die Nachricht nachgesendet wird (siehe Abschnitt 3.1.3.2).
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto mit Authentisierungsniveau „hoch“,

	Antrag auf Vertragbeendigung des De-Mail-Kontos liegt vor (vgl. [TR DM ACM FU]).
Input	Nachsendeauftrag
Ergebnis	Nachsendeauftrag aktiviert
Nachbedingung	
Ablauf	• Nutzer stellt einen Nachsendeauftrag. • DMDA prüft, ob eine Vertragsbeendigung des De-Mail-Kontos beantragt wurde. • Nachsendeauftrag wird mit der Vertragsbeendigung des De-Mail-Kontos aktiviert. • Automatische Sortierung von neuen Nachrichten wird für den Posteingang (Funktion 11) deaktiviert/gelöscht. • Nach einem durch den Nutzer vorgegebenem Zeitraum wird der Nachsendeauftrag automatisch deaktiviert.
Fehlerfälle	FC-01: Keine Änderung möglich, da nicht hinreichendes Authentisierungsniveau bei der Anmeldung genutzt. FC-02: De-Mail-Konto-Vertragsbeendigung nicht beantragt FC-03: Keine gültige De-Mail-Adresse. FC-04: Zeitraum der Aktivierung nicht zulässig. FC-05: Angegebene De-Mail-Adresse für den Nachsendeauftrag entspricht der aktuellen De-Mail-Adresse
Funktion 4	**Export von Nachrichten**
Kurzbeschreibung	Der Nutzer exportiert Nachrichten aus seinem Postfach zu seinem lokalen IT-System.
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto
Input	Kennung(en) der zu exportierenden Nachricht(en)
Ergebnis	Nachricht(en) inkl. Anhänge und Metadaten; Bestätigungen; Signatur-Prüfprotokolle sind in ein für Im- und Export standardisiertes De-Mail-Format exportiert
Nachbedingung	
Ablauf	• Nachrichten werden durch entsprechende Kennungen (bspw. Message-ID) ausgewählt. • Der Nutzer wählt einen Speicherort auf seinem lokalen IT-System für die zu exportierenden Nachricht(en). • Die Nachricht(en) wird in ein für Im- und Export standardisiertes De-Mail-Format konvertiert.

	• Die Nachricht mitsamt den Metadaten und der Integritätssicherung wird zum lokalen IT-System des Nutzers übertragen und dort gespeichert.
Fehlerfälle	FC-01: Authentisierungsniveau des Anfragenden ist kleiner als das Authentisierungsniveau (Versandoption „Persönlich“) der Nachricht FC-02: Keine Nachricht ausgewählt.
Funktion 5	**Import von Nachrichten (optional)**
Kurzbeschreibung	Der Nutzer importiert Nachrichten von seinem lokalen IT-System zu seinem Postfach.
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto mit hinreichendem Authentisierungsniveau
Input	Importdatei in einem für Im- und Export standardisiertem De-Mail-Format
Ergebnis	Nachricht(en) (Nachricht(en) inkl. Anhänge und Metadaten; Bestätigungen; Signatur-Prüfprotokolle) sind im Postfach.
Nachbedingung	
Ablauf	• Importdatei wird für den Import ausgewählt. • Die Datei wird zum DMDA versandt. • Die Nachrichten werden in das Postfach abgelegt, zuvor sollte eine Schadsoftwareprüfung durchgeführt werden..
Fehlerfälle	FC-01: Keine Nachricht gefunden. FC-02: Nachricht existiert bereits im Postfach.
Funktion 6	**Zugriff auf persönliches Adressbuch**
Kurzbeschreibung	Der Nutzer greift auf sein persönliches Adressbuch zu, um Kontakte einzusehen, zu erfassen, zu ändern oder zu löschen (vgl. [TR DM IT-BInfra FU]).
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto
Input	Folgende Möglichkeiten zum Auffinden eines Kontakts existieren: • Liste der vorhandenen Kontakte • Suche über Bestandteile der Kontaktdaten Lesen der Kontaktdaten • Darstellung mit Kopier- bzw. Übernahmemöglichkeit der Kontaktdaten Editieren der Kontaktdaten

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	• Erfassung von neuen oder geänderten Daten zum Kontakt Löschung des Kontaktes • Auswahl bzw. Angabe des zu löschenden Kontaktes
Ergebnis	Kontakt angelegt, geändert, gelöscht, gelesen
Nachbedingung	
Ablauf	• Adressbuch wird geöffnet • Bei Einsicht, Löschung oder Änderung eines Kontakts: ◦ Auffinden des entsprechenden Kontakts ◦ Darstellung des Kontakts ◦ Änderung oder Löschung des Kontakts • Bei Erfassung eines neuen Kontaktes: ◦ neu anlegen ◦ manuelle Erfassung ▪ Kontaktinformationen aus Nachricht entnehmen ▪ Kontaktinformationen vom ÖVD übernehmen • Speicherung
Fehlerfälle	FC-01: Kontakt enthält keine Daten FC-02: Übernahme von Empfängeradresse und Zertifikat nicht möglich
Funktion 7	**Anfrage an ÖVD**
Kurzbeschreibung	Der Nutzer greift auf den ÖVD seines DMDAs zu
Akteure	Nutzer, ÖVD
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto
Input	Suchbegriffe (Kombination [Vorname, Name, [Ort oder Unternehmen]] oder De-Mail-Adresse)
Ergebnis	Informationen aus ÖVD (De-Mail-Adresse, Zertifikate, etc.)
Nachbedingung	
Ablauf	• ÖVD aufrufen • Suchbegriff(e) eingeben • Suchergebnisse des ÖVD auswerten • Suchergebnisse in Nachrichtenentwurf oder persönliches Adressbuch übernehmen
Fehlerfälle	FC-01: Zu wenig Merkmal zur Suche FC-02: Über 200 Treffer. Schränken Sie die Suche weiter ein.

Funktion 8	**Automatisierte Weiterleitungen von Nachrichten verwalten (Erstellen, Löschen, Ändern)**
Kurzbeschreibung	Der Nutzer verwaltet eine Weiterleitung von Nachrichten. Hierbei kann die automatisierte Weiterleitung erstellt, geändert oder auch gelöscht werden. Hinweis: Bei einer automatisierten Weiterleitung von Nachrichten wird jeweils eine Kopie der Nachricht im Postfach des Empfängers abgelegt. Eine ggf. angeforderte Eingangsbestätigung wird bei Ablage der Nachricht nur im Postfach des ursprünglichen Empfängers erzeugt (siehe Abschnitt 3.1.3.2).
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto mit Authentisierungsniveau „hoch“. Nur bei Änderung oder Löschung: Weiterleitung existiert bereits
Input	a) Bei Erstellung: Angabe einer Weiterleitungsadresse (De-Mail-Adresse) b) Bei Änderung: andere Weiterleitungsadresse (De-Mail-Adresse) c) Bei Löschung: Markierung der zu löschenden Weiterleitungsadresse
Ergebnis	a+b) Weiterleitungsfunktion definiert bzw. geändert c) Angaben zur Weiterleitungsfunktion gelöscht
Nachbedingung	Ist eine Weiterleitungsfunktion aktiviert, muss der Nutzer bei jedem Zugriff auf sein Postfach darauf hingewiesen werden
Ablauf	• Bei Erstellung und Änderung: ◦ Nutzer definiert die Weiterleitungsadresse ◦ Nutzer bestätigt die editierte Adresse • Bei Löschung: ◦ Nutzer löscht die Angaben zur Weiterleitungsfunktion ◦ Nutzer bestätigt die Löschung
Fehlerfälle	FC-01: Weiterleitungsadresse ist keine De-Mail-Adresse FC-02: Keine De-Mail-Adresse angegeben FC-03: Weiterleitungsadresse entspricht der aktuellen De-Mail-Adresse
Funktion 9	**Verwaltung von Kategorien**
Kurzbeschreibung	Der Nutzer legt beliebige eigene Kategorien in seinem Postfach an bzw. benennt diese um oder löscht diese. Eine hierarchische Anordnung der Kategorien ist optional möglich.
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto

	Bei Umbenennen oder Löschung: Vorhandensein von zu behandelnden Kategorien
Input	a) Funktion Erstellen: Kategorie-Bezeichnung b) Funktion Löschen: Kategorie-Bezeichnung c) Funktion Umbenennung: Kategorie-Bezeichnung_alt, Kategorie-Bezeichnung_neu
Ergebnis	a) Kategorie existiert b) Kategorie existiert nicht mehr c) Kategorie existiert mit neuem Namen (vorherige Zuordnungen von Nachrichten bleiben bestehen)
Nachbedingung	
Ablauf	a) Funktion Erstellen • Aufruf der Funktion zum Erstellen von Kategorien im Postfach • Angabe der Bezeichnung (ggf. inklusive der übergeordneten Kategorien) • Bestätigung und Anlegen der Kategorie b) Funktion Löschen • Aufruf der Funktion zum Löschen von Kategorien im Postfach • Angabe der Bezeichnung (ggf. inklusive der übergeordneten Kategorien) • Bestätigung und Löschen der Kategorie c) Funktion Umbenennung • Aufruf der Funktion zum Umbenennen von Kategorien im Postfach • Auswahl der umzubenennenden Kategorie • Angabe der neuen Bezeichnung • Bestätigung und Umbenennung der Kategorie
Fehlerfälle	FC-01: Kategorie kann nicht gelöscht werden, da noch Nachrichten zugeordnet sind FC-02: Kategorie-Bezeichnung schon vorhanden
Funktion 10	**Manuelle Zuordnung von Nachrichten zu Kategorien**
Kurzbeschreibung	Der Nutzer ordnet manuell Nachrichten den im Postfach angelegten Kategorien zu.
Akteure	Nutzer, Postfachdienst

Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto mit hinreichendem Authentisierungsniveau
Input	Nachrichten, Kategorien
Ergebnis	Nachrichten sind in Kategorien auffindbar
Nachbedingung	
Ablauf	• Markierung der entsprechenden Nachrichten • Aufruf der Funktion zur Zuordnung zu einer Kategorie • Wahl bzw. Anlegen der Kategorie • Bestätigung zum Verschieben (optional)
Fehlerfälle	FC-01: Keine Nachrichten zum Verschieben vorhanden/gewählt FC-02: Kategorie nicht definiert
Funktion 11	**Verwaltung von Regeln zur automatische Zuordnung von Nachrichten zu Kategorien**
Kurzbeschreibung	Der Nutzer definiert, ändert oder löscht Regeln, nach denen Nachrichten automatisch nach dem Empfang im Postfach vom Nutzer angegebenen Kategorien zugeordnet werden.
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto Bei Löschung, Änderung: Vorhandensein einer Regel
Input	a) Erstellung • Definition zur Parametrisierung eines Regelwerkes zum automatisierten Zuordnen von Nachrichten Parameter sind dabei mindestens: - Zeichenkette im Betreff der Nachricht - Absender-Adresse bzw. Domäne des Absenders - Versandoption „Absenderbestätigt“ ja/nein - Versandoption „Persönlich“ ja/nein - Versandoption „Versandbestätigung ja/nein - Versandoption „Eingangsbestätigung ja/nein - Versandoption „Abholbestätigung ja/nein - Ende-zu-Ende-Verschlüsselung ja/nein - Signatur der Nachricht ja/nein - Dateianhänge (ja/nein, Speichergröße) - Nachrichten-Typ

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	• Bezeichnung der Regel • Angabe der Abarbeitungsreihenfolge hinsichtlich bereits existierender Regeln b) Änderung • Angabe der Änderungen hinsichtlich Bezeichnung und/oder Parameter der Regel c) Löschung • Angabe der zu löschenden Regel
Ergebnis	a) Neue Regel erstellt b) Definierte Regel geändert c) Definierte Regel gelöscht
Nachbedingung	
Ablauf	a) Regel erstellen • Angabe eines Bezeichners • Angabe der Parameter • Angabe der Abarbeitungsreihenfolge • Bestätigung der Regeldefinition (Bezeichnung und Parameter) b) Regel ändern • Auswahl der Zu ändernden Regel • Angabe der zu ändernden Parameter • Bestätigung der Regeldefinition c) Regel löschen • Auswahl der zu löschenden Regel • Bestätigung zum Löschen
Fehlerfälle	FC-01: Parameter der Regel nicht nutzbar FC-02: Bezeichnung existiert bereits
Funktion 12	**Such- bzw. Filter-/Sortierfunktionen für Nachrichten**
Kurzbeschreibung	Der Nutzer sucht anhand von Suchkriterien bzw. Filterdefinitionen oder über Sortierungen nach Nachrichten in seinem Postfach Hinweis: Die Suche in Anhängen von Nachrichten ist optional.
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto mit hinreichendem Authentisierungsniveau
Input	• Filter- bzw. Sortierkriterien (Absender-/ Empfänger-Adresse,

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Subjekt, Versanddatum, Versandoption, Signatur/Verschlüsselung, Bestätigungen/Meldung) und/oder • Suchkriterien (Wort bzw. Wortgruppen in Verbindung mit einer Definition, über welche Felder/Attribute (Nachrichtentext, Dateianhänge, Metadaten-Attribute) die Suchfunktion angewandt wird Hinweis: Es werden nur Nachrichten angezeigt, für die ein ausreichendes Authentisierungsniveau vorliegt.
Ergebnis	List der gefundenen Nachrichten
Nachbedingung	
Ablauf	• Such- bzw. Filter-/Sortierkriterien angeben • Suche/Filterung bzw. Sortierung starten • Suchergebnisse darstellen
Fehlerfälle	
Funktion 13	**Löschen von Nachrichten**
Kurzbeschreibung	Der Nutzer löscht Nachrichten aus seinen Postfach-Kategorien. Dabei ist zu unterscheiden: a) Löschen durch Zuordnung zu der Kategorie „Papierkorb“ und b) Endgültiges und unwiederbringliches Löschen aus der Kategorie „Papierkorb“ Sowohl Bestätigungsnachrichten (Versand-, Eingang- und Abholbestätigungen) als auch Nachrichten, die eine Eingangs- oder Abholbestätigung verlangt haben, müssen mind. mit Authentisierungsniveau „hoch“ gelöscht werden oder älter als 90 Tage alt sein.
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto
Input	Nachricht
Ergebnis	a) Nachricht in Papierkorb-Kategorie b) Nachricht gelöscht
Nachbedingung	
Ablauf	Zu löschende Nachricht(en) auswählen a) Zuordnung der zu löschenden Nachricht zu der Kategorie Papierkorb b) endgültiges und unwiederbringliches Löschen aus dem Papierkorb nach einer Bestätigung durch den Nutzer

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Hinweis: Es können nur Nachrichten ausgewählt werden, für die ein ausreichendes Authentisierungsniveau vorliegt.
Fehlerfälle	FC-01: Nicht löschbar, da aktuelles Authentisierungsniveau niedriger ist als für ein Lesen der Nachricht benötigt wird (Versandoption „Persönlich“). FC-02: Nicht löschbar, da Nachricht mit Eingangs- bzw. Abholbestätigung nur mit Authentisierungsniveau „hoch“ gelöscht werden kann oder älter als 90 Tage sein muss. FC-03: Nicht löschbar, da Nachricht eine Bestätigungsnachricht ist und nur mit Authentisierungsniveau „hoch“ gelöscht werden kann oder älter als 90 Tage sein muss.
Funktion 14	**Konfiguration der Übermittlung der Integritätssicherung**
Kurzbeschreibung	Der Nutzer konfiguriert, bei welchen Protokollen die Integritätssicherung der Nachrichten mit auf den lokalen PC des Nutzers übertragen werden soll, da ggf. bei einigen Clients Probleme bei der Verarbeitung der Integritätssicherung auftreten können.
Akteure	Nutzer, Postfachdienst
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto
Input	• Angabe des Protokolls • Angabe ob Integritätssicherung übermittelt werden soll (Ja/Nein)
Ergebnis	Konfiguration der Übermittlung der Integritätssicherung bei ausgewählten Protokoll
Nachbedingung	
Ablauf	• Nutzer öffnet entsprechenden Dialog • Nutzer wählt Aktivierung/Deaktivierung für Protokoll • Nutzer speichert die Änderung
Fehlerfälle	

Tabelle 12: Durch den Nutzer initiierte Funktionen

9 Obligatorische und optionale Funktionalität

Die hier beschriebene Funktionalität des PVD ist obligatorisch, sofern sie in den vorherigen Abschnitten oder in der nachfolgenden Tabelle nicht explizit als optional gekennzeichnet ist.

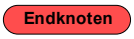
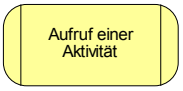
Funktionalität	Referenz	Status[6]
Erstellen und Versenden von Nachrichten	Kap. 3.1.1	+
Empfang von Nachrichten	Kap. 3.1.2	+
Prüfung auf Schadsoftware	Kap. 3.1.3.1	+
Automatisierte Weiterleitung an eine andere De-Mail-Adresse	Kap. 3.1.3.2	+
Nachsendeauftrag an eine andere De-Mail-Adresse	Kap. 3.1.3.3	+
Export von Nachrichten und -inhalten	Kap. 3.1.3.4	+
Zugriff auf persönliches Adressbuch	Kap. 3.1.3.5	+
Zugriff auf ÖVD	Kap. 3.1.3.5	+
Weiterleiten und Beantworten von Nachrichten	Kap. 3.1.3.6	+
Ablage von Nachrichten in Kategorien	Kap. 3.1.3.7	+
Suchfunktionen für Nachrichten	Kap. 3.1.3.8	+
Löschen von Nachrichten	Kap. 3.1.3.9	+
Benachrichtigung bei falscher Adressierung	Kap. 3.2.1	+
Transport von Nachrichten innerhalb von De-Mail	Kap. 3.2.2	+
Durchleitung von Ende-zu-Ende gesicherten (signierten und/oder verschlüsselten) Nachrichten	Kap. 3.2.2	+
Versandoptionen	Kap. 3.3	+

Tabelle 13: Obligatorische und optionale Funktionalität

6 „+“ Funktionalität ist obligatorisch, „–“ Funktionalität ist optional

10 Anhang

10.1 Legende zum Aktivitätsdiagramm

	Startknoten Der Startknoten ist der Startpunkt eines Prozesses. Ein Prozess darf mehrere Startknoten haben, in diesem Fall beginnen beim Start des Prozesses mehrere Abläufe. Es ist möglich, dass ein Prozess keinen Startknoten besitzt, sondern von einem Ereignis angestoßen wird.
	Endknoten Der Endknoten gibt an, dass die Ausführung des Prozesses abgeschlossen ist. Es kann in einem Prozessdiagramm mehrere Ausgänge in Form dieser Endknoten geben. Gibt es zum Zeitpunkt des Erreichens des Endknotens mehrere parallele Abläufe innerhalb des Prozesses, werden beim Erreichen eines Endknotens alle Abläufe gestoppt.
	Ablaufende Das Ablaufende terminiert einen Ablauf. Im Unterschied zum Endknoten, der einen ganzen Prozess beendet, hat das Erreichen des Ablaufendes keinen Effekt auf andere parallele Abläufe, die zu diesem Zeitpunkt innerhalb des Prozesses abgearbeitet werden. Auf diese Weise lassen sich parallele Abläufe gezielt und einzeln beenden.
	Kante Die als Pfeile dargestellten Kanten verbinden die einzelnen Komponenten des Diagramms und stellen den Kontrollfluss dar.
	Aktion Eine Aktion ist ein einzelner Schritt innerhalb eines Prozesses, der nicht mehr weiter zerlegt wird. Das bedeutet nicht unbedingt, dass die Aktion in der realen Welt nicht mehr weiter zerlegbar wäre, sondern dass die Aktion in diesem Diagramm nicht mehr weiter verfeinert wird. Die Aktion kann Ein- und Ausgabeinformationen besitzen. Der Output einer Aktion kann der Input einer Folge-Aktion sein.
	Aufruf einer Aktivität Mit diesem Symbol kann aus einer Aktivität (Prozess) heraus eine weitere Aktivität aufgerufen werden. Der Aufruf selbst ist eine Aktion, der aufgerufene Ablauf eine weitere Aktivität.
	Empfang eines Ereignisses Diese Aktion wartet auf das Eintreten eines Ereignisses. Nach dem Empfang des Ereignisses wird der im Aktivitätsdiagramm definierte, von dieser Aktion ausgehende Ablauf abgearbeitet.

	Auslösen eines Ereignisses Das Senden von Signalen bedeutet, dass ein Signal an eine empfangende Aktivität gesendet wird. Die empfangende Aktivität nimmt das Signal mit der Aktion „Ereignis empfangen“ entgegen und kann entsprechend darauf reagieren.
	Entscheidungsknoten Die Raute stellt eine Verzweigung im Kontrollfluss dar. Eine Verzweigung hat einen Eingang und zwei oder mehrere Ausgänge. Jeder Ausgang wird mit einer Bedingung versehen. Trifft eine Bedingung zu, wird am entsprechenden Ausgang weiter verfahren.
	Datenobjekt Datenobjekte gehören üblicherweise nicht zum Symbolumfang in UML-Aktivitätsdiagrammen. Sie sind hier jedoch eingeführt worden, um an entscheidender Stelle zu verdeutlichen, welche Datenobjekte, insbesondere im Fokus der Schutzbedarfsanalyse, vorliegen.

Tabelle 14: Legende zum Aktivitätsdiagramm

10.2 Legende zu Schritten und Funktionen

Schritte im Aktivitätsdiagramm bezeichnen im Kontrollfluss eingebundene, einmalig ablaufende Aktionen.

In Abgrenzung zu Schritten bezeichnen Funktionen im gesamten Prozess wiederkehrende bzw. unabhängig vom Ablauf existierende Aktionen.

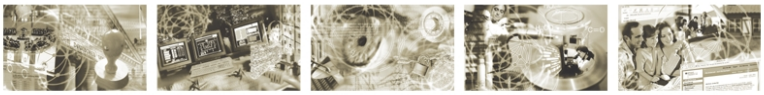
Schritte und Funktionen werden in diesem Dokument als Aktionen auf folgende Art und Weise beschrieben:

Schritt / Funktion <Nr.>	Eindeutigen Name der Aktion
Kurzbeschreibung	Innerhalb der Kurzbeschreibung erfolgt eine verbale Beschreibung der wesentlichen Funktionalität der Aktion.
Akteure	Alle Rollen bzw. Dienste, die innerhalb der Aktion in irgendeiner Weise beteiligt sind, werden aufgezählt.
Auslöser	Der Auslöser ist ein Akteur, durch den die Aktion aufgerufen bzw. initialisiert wird.
Vorbedingung	Unter Vorbedingungen werden die Bedingungen verstanden, die nicht aus einer unmittelbar vorhergehenden Aktion folgen, sondern asynchron erzielt werden müssen. Diese Aktivitäten sind nicht unbedingt in diesem Dokument beschrieben, die Ergebnisse sind jedoch als Vorbedingungen für die Ausführung der hier beschriebenen Aktion notwendig. Auf die Erfüllung dieser Vorbedingungen muss sich die nutzende Aktion verlassen können
Input	Der Auslöser muss bei Initialisierung der Aktion die entsprechenden

	Informationen an diese übergeben oder durch die Aktion abfragen lassen, so dass eine Verarbeitung der Informationen innerhalb der Aktion erfolgen kann.
Ergebnis	Nach Beendigung der Aktion muss eine bestimmte Information als Resultat erarbeitet bzw. bereitgestellt werden.
Nachbedingung	Unter Nachbedingungen werden Bedingungen verstanden, die innerhalb dieser Aktion nicht betrachtet werden und durch unmittelbar nachfolgende Aktionen aufgegriffen und dort behandelt werden müssen.
Ablauf	Für die innerhalb der Aktion definierte Logik wird ein konkreter Ablauf beschrieben. Die definierte Abfolge muss innerhalb der Aktion durchgeführt und abgeschlossen werden.
Fehlerfälle	Als Fehlerfall wird ein Ergebnis einer Funktion bezeichnet, der innerhalb der Funktionsspezifikation liegt, aber vom erwarteten Ergebnis abweicht, jedoch nicht zu einem unkontrollierten Abbruch führt. Die konkrete Behandlung eines Fehlerfalls ist implementationsabhängig. Je nach Fall können unterschiedliche Lösungsstrategien verwendet werden, bspw. kann eine Aktion zu einem späteren Zeitpunkt wiederholt oder die Aktion abgebrochen werden. Bei Abbruch einer Aktion ist der Nutzer mindestens darüber zu informieren und alle bis zu diesem Schritt generierten temporären Daten müssen gelöscht werden. In den Beschreibungen der Fehlerfälle der Aktionen werden nur mögliche Fehler beschrieben, die innerhalb der Funktionsspezifikation liegen.

Tabelle 15: Legende zu Schritten und Funktionen

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Postfach- und Versanddienst IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 3.3
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die IT-Sicherheitsanforderungen, die über die generellen Anforderungen aus dem Modul [TR DM Si M] hinausgehen und speziell für den PVD anzuwenden sind, und ist Bestandteil von [TR DM PVD M].

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die angenommene Netzinfrastruktur eines typischen De-Mail-Dienstes.

Bei der Erstellung des realen IT-Sicherheitskonzepts sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der bereits in [TR DM Si ÜK] skizziert ist.

3 Bedrohungen

Es werden in diesem Abschnitt nur die Bedrohungen für den PVD betrachtet, die sich zusätzlich zu den Bedrohungen aus [TR DM Si ÜK] durch die Funktionalität des PVD ergeben.

3.1 Bedrohung durch Schadsoftware

Über elektronische Nachrichten kann Schadsoftware verbreitet werden. Dies kann beim Empfänger erhebliche Schäden, beispielsweise durch den Verlust von Daten oder durch die Kompromittierung von Daten, verursachen. Die Gefahr droht dem Rechnersystem des Nutzers.

3.2 Abstreiten der Kommunikation

Ein Nutzer kann die Kommunikation mit einem anderen Nutzer abstreiten. Er kann behaupten, dass er eine Nachricht nicht erhalten hat.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

4 Sicherheitsziele

Im Folgenden werden weitergehende Sicherheitsziele des PVD beschrieben, die über die in [TR DM Si ÜK] Aufgeführten gelten.

4.1 Schutz des Nutzers vor Schadsoftware

Der Nutzer muss durch geeignete Maßnahmen vor Schäden durch Schadsoftware geschützt werden.

4.2 Vertrauliche Speicherung und Verarbeitung der Nachrichten

Es ist durch geeignete Maßnahmen sicherzustellen, dass die Möglichkeit der Einsichtnahme des Nachrichteninhalts durch Unbefugte (u.a. auch Innentäter) verhindert wird.

4.3 Nachvollziehbarkeit der Kommunikation

Der Versand und die Zustellung einer Nachricht müssen für den Absender nachvollziehbar sein, so dass dieser seine gesamte De-Mail-Kommunikation auch gegenüber Dritten nachweisen kann (vgl. [TR DM PVD FU]).

5 Anforderungen

5.1 Prüfung auf Schadsoftware

Durch geeignete Maßnahmen ist sicherzustellen, dass Nachrichtenentwürfe, die vom Absender dem Postfach- und Versanddienst übergeben werden, unmittelbar nach Übermittlung auf Schadsoftware geprüft werden.

5.2 Kryptokonzept

5.2.1 Integritätssicherung

Alle Nachrichten werden gegen unbefugte Veränderungen insoweit geschützt, als dass unbefugte Veränderungen zuverlässig erkannt werden können (vgl. [TR DM PVD FU]).

5.2.2 Prüfung der Integrität

Der PVD des Empfängers prüft bei Abruf der Nachrichten durch den Empfänger die Integrität der Nachrichten. Ist das Prüfergebnis negativ, so ist mit vorab festgelegten Maßnahmen darauf zu reagieren.

5.2.3 Verschlüsselung von Nachrichten

Nachrichten werden durch den PVD des Absenders unmittelbar nach Anbringen der Transportsicherung verschlüsselt gespeichert und übertragen. Die Metadaten werden dabei nicht verschlüsselt.

Die Verschlüsselung der Daten hat unmittelbar nach Eingang auf den Systemen des DMDA zu erfolgen.

Die Gültigkeit der öffentlichen Schlüssel muss regelmäßig geprüft werden.

5.2.4 Entschlüsselung von Nachrichten

Die Entschlüsselung darf ausschließlich zur Prüfung auf Schadsoftware und zur Auslieferung an den Nutzer zu durchgeführt werden. Dieser Vorgang erfolgt automatisiert.

5.2.5 Datenspeicherung

Die Speicherung der Daten beim DMDA muss verschlüsselt erfolgen.

Es gelten folgende Regelungen für die Daten:

- langfristige Speicherung (z.B. Nachrichten im Postfach)
  - Die Daten müssen einzeln oder gesammelt verschlüsselt und vor unberechtigtem Zugriff gespeichert werden
- kurzfristige Speicherung (z.B. in Warteschlange bei Virenscanner)
  - Das Dateisystem, auf dem die Daten abgelegt werden, muss verschlüsselt sein.

5.3 Erstellung von Bestätigungen

Der DMDA erstellt sowohl Versand-, Eingangs- und Abholbestätigungen.

5.4 Prüfen und Setzen von Metadaten

Der DMDA prüft die korrekte Verwendung von Metadaten, setzt weitere Metadaten und ersetzt nicht-korrekte Metadaten vor der Erstellung von Nachrichten.

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:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2.2 Bestätigungen und Bestätigungsnachrichten

Bestätigungsnachrichten sind Nachrichten, die vom PVD generiert werden, um gewisse Ereignisse über versendete Nachrichten, wie bspw. deren Versand oder Eingang beim Empfänger zu bestätigen. Bestätigungsnachrichten enthalten die eigentliche Bestätigung des DMDA im Nachrichten-Body.

Die Bestätigung muss mindestens folgende Informationen, die von der referenzierten Nachricht stammen, enthalten:

Nr.	*Bezeichnung*	*Wert*	*Bemerkung*
1	Betreff	[Bestätigungsart]: Betreff aus der ursprünglichen Nachricht	Text, der die Art der Bestätigung widerspiegelt und für den Nutzer eine einfache Verknüpfung zur ursprünglichen Nachricht über deren Betreff ermöglichen soll.
2	Bestätigungstext	Text	Weitergehende Erläuterungen zur Bestätigung.
3	Metadaten	Metadaten der ursprünglichen Nachricht, über die der Hash-Wert berechnet wird	Die Metadaten ermöglichen eine Verknüpfung dieser Bestätigungsnachricht mit der ursprünglichen versendeten Nachricht.
4	Hash-Wert	Message-Digest	Hash-Wert der ursprünglichen Nachricht
5	Zeit	Datum und Uhrzeit	Zeitpunkt (sekundengenau) des Versandes (bei Versandbestätigung) bzw. des Eingangs der Nachricht (bei Eingangsbestätigung) bzw. ersten Anmeldung nach der Ablage der Nachricht durch den Nutzer (Abholbestätigung)
6	Aussteller	Kennung des DMDA	Eindeutiger Name des ausstellenden DMDA

Tabelle 1: Inhalt einer Bestätigung

Die Bestätigung muss durch den austellenden DMDA elektronisch qualifiziert signiert werden.

Das Feld Nachrichten-Typ in den Metadaten muss auf den Wert „Bestätigungsnachricht“ gesetzt werden. Der Betreff der Bestätigungsnachricht muss die Art der Bestätigung verknüpft mit dem Betreff der ursprünglichen Nachricht enthalten.

Der Absender einer Bestätigungsnachricht muss jeweils der DMDA von einer System-Adresse (vgl. [TR DM ACM FU]) sein.

2.3 Meldungen und Meldungsnachrichten

Meldungen sind Information des DMDA an den Nutzer, um ihn über bestimmte Ereignisse zu informieren. Meldungen können in Abhängigkeit der Benutzerschnittstelle, die der Nutzer zur Interaktion mit dem PVD verwendet, unterschiedlich dargestellt und bekannt gemacht werden. Bei einem Webbrowser können Meldungen bspw. als Text in eine Webseite eingebettet werden. Alternativ können sie auch als Nachricht über den PVD an den Nutzer verschickt werden.

Meldungen müssen mindestens folgende Informationen beinhalten:

Nr.	*Bezeichnung*	*Wert*	*Bemerkung*
1	Betreff	Text	Text, der die Art der Meldung widerspiegelt und den Bezug zum auslösenden Ereignis ermöglicht
2	Meldungstext	Text	Weitergehende Erläuterungen
3	Zeit	Datum und Uhrzeit	Sekundengenauer Zeitpunkt der Erstellung der Meldung
4	Aussteller	Kennung des DMDA	Eindeutiger Name des ausstellenden DMDA

Tabelle 2: Inhalt einer Meldung

Werden Meldungen in Form von Nachrichten verschickt, so werden diese Nachrichten Meldungsnachrichten genannt.

Das Feld Nachrichten-Typ in den Metadaten einer Meldungsnachricht muss auf den Wert „Meldungsnachricht“ gesetzt werden. Der Betreff der Nachricht muss gleich dem Betreff der Meldung sein. Der Absender einer solchen Nachricht muss jeweils der DMDA von einer System-Adresse (vgl. [TR DM ACM FU]) sein. Für den lokalen Teil der Absender-Adresse muss die Bezeichnung „PVD-Meldung“ bei Meldungsnachrichten verwendet werden.

Wenn in diesem Modul von einer „Meldungsnachricht“ gesprochen wird, ist die Meldung in Form einer Meldungsnachricht zu verschicken. Ist hingegen nur von „Meldung“ die Rede, so kann diese in Abhängigkeit der Benutzerschnittstelle auch anders verschickt und dargestellt 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.

Bei der Verarbeitung der X-Header muss die Groß-/ Kleinschreibung der Namen ignoriert werden. Der X-Header-Name sollten 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
2	Eingangsbestätigung	X-de-mail-confirmation-of-receipt	XX				wie original Bestätigung wird nicht beim Eingang einer Weiterleitung, sondern nur beim

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

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Nr.	*Bezeichnung*	*Header-Name*	*Nachrichtentypen*				
			N	*B*	*M*	*I*	*W/F*
							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-recipients	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	Message-ID	X-de-mail-message-id	XX	XX	XX	XX	wie original
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

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Nr.	*Bezeichnung*	*Header-Name*	*Nachrichtentypen*				
			N	*B*	*M*	*I*	*W/F*
19	Empfänger-Adressen für den Transport	X-de-mail-actual-recipients	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

Tabelle 3: 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 4: 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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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

Tabelle 5: 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 6: 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 7: 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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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

Tabelle 8: 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 9: 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-recipients = [FWS] „to“ / „cc“ / „bcc“ [FWS] “=“ [FWS] address-list[5] [FWS] [“;” X-de-mail-chosen-recipients]

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

Tabelle 10: Felddefinition des Feld X-de-mail-chosen-recipient

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.

4 ABNF-Notation gemäß RFC 2234

5 Mehrfachbelegung mit „;“ getrennten De-Mail-Adresse

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

3.1.9 X-de-mail-auth-level

Dieses Feld bezeichnet das Authentisierungsniveaus, 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 11: 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 12: 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 13: 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 reciept	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 14: Wertdefinitionen des Feld X-de-mail-message-type

Feldname	Feldwertsyntax	mögliche Werte
X-de-mail-message-type	RFC 2822 unstructured	gemäß Tabelle 13, Spalte “Typ”

Tabelle 15: 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 4781] enthalten sein.

Nachrichten mit der Versandoption „Absenderbestätigt“ müssen gemäß [RFC 4871] 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 ein von der Bundesnetzagentur als für die Erstellung qualifizierter Signaturen geeigneter Algorithmus verwendet werden.

Die Erstellung und Prüfung des Hashwerts und der Signatur sind in Abschnitt 3.1.19 ausführlich beschrieben.

Feldname	Feldwertsyntax	mögliche Werte
x-de-mail-integrity	RFC 2822 unstructured	gemäß RFC 4871

Tabelle 16: 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 X509 als BASE64-Text eingetragen werden.

Feldname	Feldwertsyntax	mögliche Werte
X-de-mail-signature-certificate	RFC 2822 „unstructured“	Base64 kodiertes X509-Zertifikat

Tabelle 17: 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-recipients entsprechen.

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

Tabelle 18: Felddefinition des Feld X-de-mail-actual-recipient

3.1.16 X-de-mail-version

Dieses Feld muss mit der aktuellen Version der Spezifikationen gefüllt werden. Es dient dazu, bei einer späteren Weiterentwicklung der Spezifikationen erkennen zu können, nach welchen Spezifikationen die Nachricht erstellt wurde.

Feldname	Feldwertsyntax	mögliche Werte
X-de-mail-version	RFC 2822 „unstructured“	1.0

Tabelle 19: 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.

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

Tabelle 20: Felddefinition des Feld X-de-mail-private-id

3.1.18 X-de-mail-message-id

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

Das Feld MessageID aus [RFC 2822] kann mit dem gleichen Wert gefüllt werden.

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

Tabelle 21: Felddefinition des Feld X-de-mail-message-id

3.1.19 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: sha256/rsa
  - für Nachrichten, die gehasht werden: sha256[6]
- 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 4781]. Wenn die Nachricht nicht signiert wird, enthält der Parameter den Hashwert (vgl. header-hash in [RFC 4781]), der in die Signaturberechnung gemäß [RFC 4781] 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
- 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 4871] beschrieben, mit den zuvor erwähnten Parametern erfolgen.

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

Die Prüfungen der DKIM-Signatur weicht von [RFC 4871] 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 4871] 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“).

3.1.20 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 (RFC2045-2049) sein. Besondere strukturelle Anforderungen bestehen für:

- Bestätigungsnachrichten (siehe Abschnitt 2.2 und 3.5)
- Meldungsnachrichten (siehe Abschnitt 2.3 und 3.5)
- Ident-Bestätigungsnachrichten (vgl. [TR DM ID IO])

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

3.4.1 Präsentation und Signatur besonderer Nachrichtentypen

Für die folgenden Nachrichtentypen gelten besondere Vorschriften zum Nachrichtenbody:

- Bestätigungsnachrichten (siehe Abschnitt 2.2 und 3.5)
- Meldungsnachrichten (siehe Abschnitt 2.3 und 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 3.1.19 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

Eine Bestätigungsnachricht muss die folgenden Elemente beinhalten:

Elementname	Datentyp	Länge	Bedeutung
Subject	xs:string	unbegrenzt	Gemäß [TR DM PVD FU] ist der Betreff aus dem Text „Bestätigungsnachricht:“ sowie dem 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

Elementname	Datentyp	Länge	Bedeutung
			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 22: Elemente der Bestätigungsnachricht

Die Metadaten der ursprünglichen Nachricht werden in Metadata wiederholt. Dieses Element enthält die Elemente des Typs „Metadate“, der die Metadaten-Headerzeilen der Originalnachricht wie folgt wiedergibt:

Elementname	Datentyp	Länge	Bedeutung
Name	xs:string	unbegrenzt	X-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 23: Metadaten der Bestätigungsnachricht

Der Betreff der Nachricht muss für Versandbestätigungen wie folgt lauten:

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

Der Betreff der Nachricht muss für Eingangsbestätigungen wie folgt lauten:

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

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

```
*Abholbestätigung* [Betreff der 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

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

- Hashwert der versendeten Nachricht

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

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]
Prüfsummer:     [Prüfsumme]


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]
Prüfsummer:     [Prüfsumme]
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
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.

3.5.2 Meldungsnachrichten

Meldungsnachrichten werden in bestimmten vordefinierten Fällen vom PVD versendet. Sie haben informatorischen Charakter.

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 24: Elemente der Meldungsnachricht

3.5.3 XML-Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:de-mail="de-mail"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  targetNamespace="de-mail"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">
  <xs:include schemaLocation=""></xs:include>
  <xs:import
    namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/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="13">
              <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" />
        <xs:element name="Signature" type="ds:SignatureType" />
      </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 einen 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.

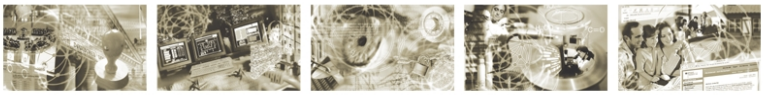
Beim Import der Nachricht ist die `From` Zeile nicht auf inhaltliche Übereinstimmung mit dem Nachrichten-Header zu prüfen, deshalb sind die enthaltenen Daten beim Export beliebig zu belegen, sie müssen nur der Spezifikation entsprechen. Beim Import werden alle in dieser Datei enthaltenen Nachrichten 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.

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

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Identitätsbestätigungsdienst Modul
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 4
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beschreibt die Struktur des Identitätsbestätigungsdienst. Das Modul ist Bestandteil der [TR DM].

Mit Hilfe des ID von De-Mail kann der Inhaber eines De-Mail-Kontos, die zuverlässig erhobenen Identitätsdaten verwenden, um gegenüber anderen De-Mail-Nutzern Angaben zu seiner Identität sicher und datenschutzkonform nachzuweisen. Der Dienst kann in den Fällen eingesetzt werden, wenn in Geschäftsabläufen üblicherweise die Vorlage eines Identitätsdokumentes zur Identifizierung der handelnden Person notwendig ist.

2 Dokumentenübersicht

2.1 Funktionale Anforderungen

Die funktionalen Anforderungen an den ID werden in [TR DM ID FU] beschrieben, sowie die besonderen nicht-funktionalen Anforderungen.

2.2 Interoperabilität

Die Datenstrukturen zur Gewährleistung der Interoperabilität des ID in [TR DM ID IO] beschrieben.

2.3 IT-Sicherheit

Die spezifischen Anforderungen an die Sicherheit des ID werden in [TR DM ID Si] beschrieben.

2.4 Funktionsprüfung

Die Spezifikation der Prüffälle für die Funktionsprüfung erfolgt in [TR DM ID FU-PS].

2.5 Interoperabilitätsprüfung

Die Spezifikation der Prüffälle für die Interoperabilitätsprüfung erfolgt in [TR DM ID IO-PS].

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Identitätsbestätigungsdienst Funktionalitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 4.1
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Abbildungsverzeichnis

Tabellenverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die funktionalen Spezifikationen des Identitätsbestätigungsdienstes und ist Bestandteil von [TR DM ID M].

In diesem Modul werden die zwingenden Anforderungen an den ID von De-Mail technikneutral beschrieben, sofern dieser angeboten wird. Eine Spezifikation von Protokollen und zugehörigen Parametern erfolgt nur dort, wo dies aus funktionaler Sicht explizit erforderlich ist.

2 Gesamtüberblick

Der ID ermöglicht es allen Nutzern von De-Mail-Konten und insbesondere SPn (SP), wie bspw. einem Web-Shop oder Auktionsportal, zuverlässig die Identitätsdaten eines De-Mail-Nutzers zu erhalten. Der ID übermittelt die im De-Mail-Konto des Nutzers hinterlegten und vom Nutzer explizit für diese Zwecke freigegebenen Identitätsattribute. Der Zeitpunkt der Verifikation wird immer zusammen mit den Identitätsdaten übertragen, so dass der Empfänger entscheiden kann, ob die Aktualität der Daten für seinen Geschäftsvorfall ausreichend ist.

Folgende Rollen sind beim ID involviert:

- Ein Nuzer von De-Mail ist eine bei einem DMDA registrierte natürliche Person oder Institution. Wenn er seinen DMDA beauftragt, seine Identitätsdaten über den ID einem SP zu übermitteln, wird er auch als Ident-Auftraggeber bezeichnet.
- Ein SP ist i. d. R. ein Anbieter von Produkten oder Dienstleistungen im Internet. Er ist selbst als De-Mail-Nutzer bei einem DMDA registriert. Im Zusammenhang mit dem ID treten SP in erster Linie als diejenigen auf, die den ID zur Feststellung der Identität eines anderen De-Mail-Nutzers verwenden. Neben den SP können aber auch andere natürliche Personen oder Institutionen Empfänger der Identitätsdaten sein.

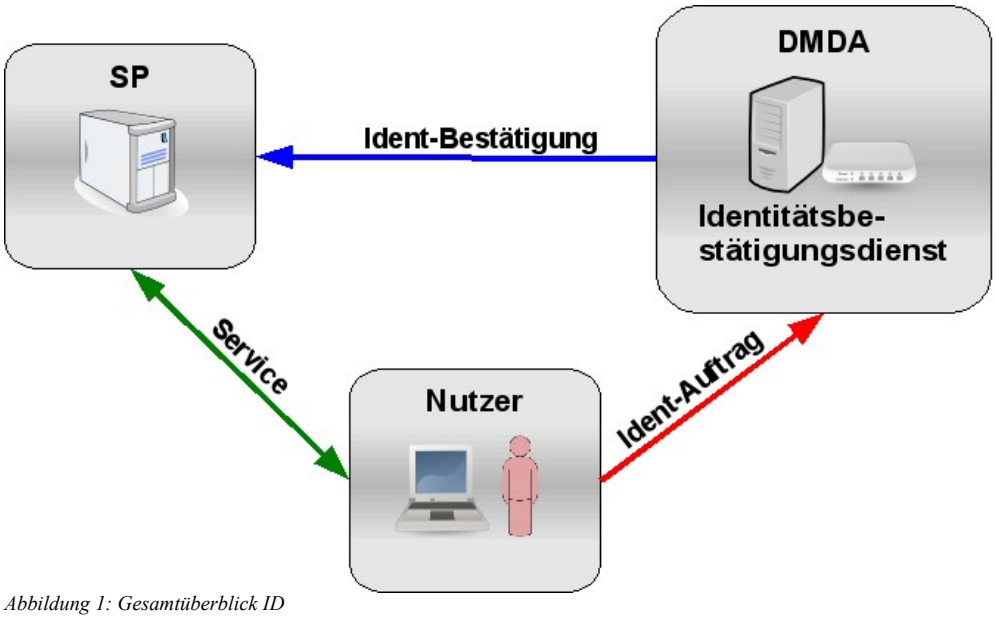


Abbildung 1: Gesamtüberblick ID

Im Folgenden wird die Anwendung des ID kurz beschrieben:

Ein Nutzer will einen Dienst eines SP (linker, dunkelgrüner Pfeil in Abbildung 1) nutzen. Der SP benötigt zur Erbringung des Dienstes zuverlässige Informationen über den Nutzer, wie bspw. Name, Vorname, Adresse oder Alter. Sofern der SP eine Identifizierung des Nutzers via De-Mail akzeptiert, teilt der SP dem Nutzer mit, welche Identitätsinformationen er vom Nutzer benötigt und an welche De-Mail-Adresse diese Informationen gesendet werden sollen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Der Nutzer meldet sich an seinem De-Mail-Konto zwingend mit Authentisierungsniveau „hoch“ an und veranlasst einen Ident-Auftrag (rechter, roter Pfeil in Abbildung 1), mit dem er auswählt, welche Identitätsinformationen an den SP gesendet werden sollen.

Der DMDA des Nutzers erstellt im Rahmen des Ident-Auftrags eine sogenannte Ident-Bestätigung (vgl. Abschnitt 3.3), die anschließend in einer Nachricht (Ident-Bestätigungsnachricht) über den PVD von De-Mail (siehe [TR DM PVD FU]) zum SP übermittelt wird (oberer, blauer Pfeil in Abbildung 1). Der SP prüft die erhaltene Ident-Bestätigung.

Eine detaillierte Beschreibung des Ablaufs erfolgt in Abschnitt 4.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

3 Funktionale Anforderungen und Datenstrukturen

Die Definition und Beschreibung der relevanten Datenstrukturen erfolgen [TR DM ID IO].

3.1 Ident-Karten

Bei De-Mail existiert eine Mindestanzahl an Ident-Karten, die einheitlich von allen DMDA umgesetzt werden müssen. Ident-Karten können Identitäts- oder Adresskarten sein. Jede Ident-Karte enthält unterschiedliche Identitätsattribute. Zu jedem Identitätsattribut muss das dazugehörige Meta-Attribut Datum und Uhrzeit der letzten Verifikation (vgl. [TR DM ACM FU]) angegeben werden.

Im Folgenden werden die Ident-Karten definiert, die mindestens vom DMDA umgesetzt werden müssen. Der DMDA kann weitere definieren und anbieten.

3.1.1 De-Mail-Adresskarte

Die De-Mail-Adresskarte enthält nur die vom Nutzer verwendete De-Mail-Adresse und kann eingesetzt werden, um die De-Mail-Adresse gegenüber einem SP als valide zu bestätigen. Diese De-Mail-Adresse ist identisch zu der Adresse, die der Ident-Bestätigung durch den ID hinzugefügt wird (vgl. Abschnitt 3.3). Als De-Mail-Adresse kann hierbei auch eine Pseudonym-Adresse angegeben werden.

3.1.2 Identitätskarte einer natürlichen Person

Die Identitätskarte beinhaltet alle Attribute, die zur vollständigen Beschreibung der Identität einer natürlichen Person erforderlich sind:

- Name,
- Vorname,
- Straße,
- Hausnummer,
- Ort,
- Staat,
- Geburtsdatum,
- Geburtsort.

3.1.3 Adresskarte einer natürlichen Person

Die Adresskarte beinhaltet alle Attribute, die zur vollständigen Beschreibung der Adresse einer natürlichen Person erforderlich sind:

- Name,
- Vorname,

– Seite 240 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

- Straße,
- Hausnummer,
- Ort,
- Staat.

3.1.4 Alters-Karte einer natürlichen Person

Die Alters-Karte existiert in folgenden drei Ausprägungen:

- Genaue Altersangabe in Jahren (z. B. 43 Jahre),
- Alterskategorie 16 Jahre oder älter,
- Alterskategorie 18 Jahre oder älter.

Die Alterskategorie-Karten dürfen dem Nutzer im Rahmen der Ident-Auftragserstellung nur dann zur Auswahl angeboten werden, wenn das aktuelle Alter des Nutzers tatsächlich innerhalb des jeweiligen Kategorieintervalles liegt.

Nicht bei allen natürlichen Personen ist das Geburtsdatum vollständig bekannt. Für die spezielle Funktion Alters-Karte muss in diesen Fällen das gemäß der bekannten Teildaten späteste mögliche Datum als Vergleichsdatum abgebildet werden (z. B. falls vom Geburtsdatum nur das Jahr bekannt ist der 31.12. des Jahres). So wird sichergestellt, dass auch im Falle unvollständiger Geburtsdaten eine Altersberechnung so erfolgt, dass das jüngste Alter berechnet wird.

3.1.5 Adresskarte einer Institution

Die Adresskarte einer Institution beinhaltet alle Attribute, die zur vollständigen Beschreibung dieser erforderlich sind:

- Name der Institution,
- Straße,
- Hausnummer,
- Ort,
- Staat.

3.2 Ident-Auftrag

Um einen Ident-Auftrag zu erteilen, ist zwingend eine Authentisierung mit Authentisierungsniveau „hoch“erforderlich.

Für einen Ident-Auftrag ist zum einen die De-Mail-Adresse des Empfängers notwendig, an die die Ident-Bestätigung geschickt werden soll, und zum anderen die Ident-Karte, die die Identitätsattribute spezifiziert, die in der Ident-Bestätigung ausgewiesen werden sollen.

Hat der Nutzer für Identitätsattribute, die von der ausgewählten Ident-Karte referenziert werden, verschiedene Angaben im De-Mail-Konto hinterlegt, so muss er bei der Erstellung des Ident-

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Auftrages auswählen können, welche konkreten Daten in der Ident-Bestätigung ausgewiesen werden sollen.

Weiterhin ist die De-Mail-Adresse des Ident-Auftraggebers erforderlich, die in der Ident-Bestätigung hinterlegt wird. Anstelle der primären De-Mail-Adresse, die seinen Namen im Klartext enthält (siehe [TR DM ACM FU]), kann dies auch eine Pseudonym-De-Mail-Adresse sein. In diesem Fall kann keine Ident-Karte ausgewählt werden, die einen Namen, einen Teil oder die vollständige postalische Adresse des Ident-Auftraggebers als Attribut enthält.

Der Ident-Auftraggeber muss die Möglichkeit haben, die Inhalte der zu erstellenden Ident-Bestätigung zu überprüfen, bevor er den Ident-Auftrag bestätigt.

3.3 Ident-Bestätigung

Unmittelbar nach Erhalt eines Ident-Auftrages erstellt der DMDA für die gewünschte De-Mail-Adresse eine Ident-Bestätigung. Dazu werden vom DMDA die auf der Ident-Karte vorgegebenen Attribute mit den konkreten Identitätsdaten des Ident-Auftraggebers ausgefüllt, um Metadaten ergänzt und anschließend mit einer qualifizierten elektronischen Signatur signiert.

Die Ident-Bestätigung wird vom DMDA signiert, um einerseits die Korrektheit aller Daten zu bestätigen, und um andererseits zu versichern, dass der Nutzer mit Authentisierungsniveau „hoch“ an seinem De-Mail-Konto angemeldet war, als er den Ident-Auftrag gestellt hat.

Die Ident-Bestätigung enthält neben dem Meta-Attribut „Verifikationszeitpunkt der Identitätsdaten“ für jedes Identitätsattribut (vgl. [TR DM ACM FU]) folgende Metadaten:

- die spezifische System-Adresse für den ID mit der Bezeichnung Ident-Bestaetigung@<DMDA> (vgl. [TR DM ACM FU]) des ausstellenden DMDA,
- die vom Ident-Auftraggeber verwendete De-Mail-Adresse,
- die De-Mail-Adresse des Empfängers, für den die Bestätigung ausgestellt wird,
- den Ausstellungszeitpunkt der Ident-Bestätigung.

3.4 Ident-Bestätigungsnachricht

Die Ident-Bestätigungsnachricht ist eine Nachricht, die der DMDA ausschließlich aufgrund eines Ident-Auftrages an den angegebenen Empfänger über den PVD sendet.

Absender der Ident-Bestätigungsnachricht ist jeweils der ID seiner System-Adresse. Empfänger der Nachricht ist der SP, der über seine De-Mail-Adresse adressiert wird. Der Ident-Auftraggeber wird in Kopie gesetzt, damit er nachvollziehen kann, an wen er welche Ident-Bestätigungen hat versenden lassen. Der Betreff der Nachricht ist auf „Ident-Bestätigung“ zu setzen. Um die Nachricht auch automatisiert als Ident-Bestätigungsnachricht erkennen zu können, wird in den Metadaten der Nachricht das Feld „Nachrichten-Typ“ auf den Wert „Ident-Bestätigungsnachricht“ gesetzt. Die Nachricht wird weiterhin mit der Versandoption „Persönlich“ versendet (vgl. [TR DM PVD FU]), um sicherzustellen, dass keine unautorisierten Personen die Identitätsattribute einsehen können.

Die vom DMDA des Nutzers erstellte und signierte Ident-Bestätigung wird also als Anhang der Nachricht über den PVD an die De-Mail-Adresse des SPs und in Kopie an den Ident-Auftraggeber zugestellt. Anhand der speziellen Absender-Adresse, die eine System-Adresse ist, kann der SP bzw.

der Empfänger erkennen, ob die Nachricht tatsächlich im Rahmen eines Ident-Auftrages durch den DMDA erstellt wurde.

Ident-Bestätigungsnachrichten müssen einen Hinweis zur Verwendung und Interpretation der Anhänge in Textform enthalten. Des Weiteren müssen diese Hinweise die wesentlichen Informationen aus der signierten Bestätigung referenzieren, wie z. B. die De-Mail-Adresse des Ident-Auftraggebers oder des SPs.

3.5 Meldungen

Meldungen sind Informationen des ID an den Nutzer und können in Abhängigkeit der Benutzerschnittstelle, die der Nutzer verwendet, unterschiedlich dargestellt und bekannt gemacht werden. Bspw. können sie in einem Webbrowser dargestellt oder auch als Meldungsnachricht (siehe [TR DM PVD FU]) übermittelt werden. Es muss sichergestellt werden, dass der Nutzer Meldungen über die von ihm verwendete Benutzerschnittstelle unmittelbar zur Kenntnis nehmen kann.

3.6 System-Adressen

In der nachfolgenden Tabelle werden die System-Adressen (siehe [TR DM ACM FU]) aufgelistet, die innerhalb des ID verwendet werden.

Verwendungszweck	***De-Mail-Adresse***
Ident-Bestätigungen	Ident-Bestaetigung@<DMDA>
Meldungen	Ident-Meldung@<DMDA>

Tabelle 1: Liste der im ID verwendeten System-Adressen

4 Ablauf des Verfahrens

In der nachfolgenden Abbildung 2 ist der funktionale und zeitliche Ablauf für die Erstellung und den Versand einer Ident-Bestätigung zwischen Nutzer, d. h. dem Ident-Auftraggeber, dem SP und dem DMDA des Nutzers, dargestellt. Die eigentliche Funktionalität des ID ist dabei mit einem Rahmen gekennzeichnet und wird in den nachfolgenden Abschnitten näher spezifiziert.

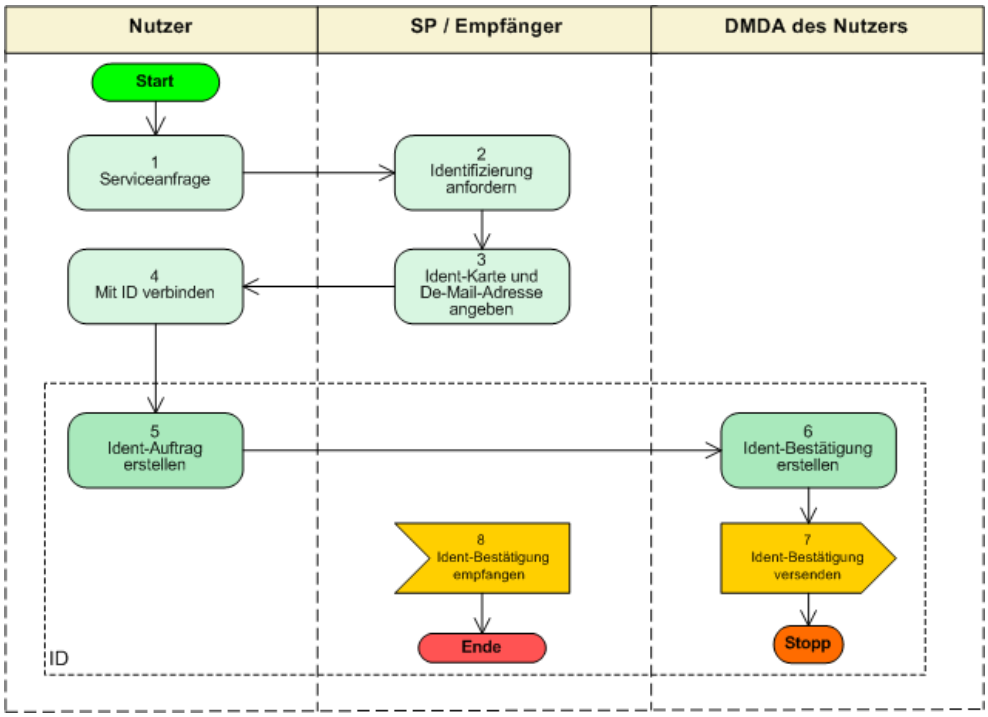


Abbildung 2: Funktionaler Ablauf des ID

Schritt	*Bezeichnung*	*Übermittlung*	*Beschreibung*
1	Serviceanfrage	Web	Der Nutzer möchte bspw. einen Warenkorb füllen und bestellen oder einen Konto beim SP einrichten.
2	Identifizierung anfordern	Web	Die dazu notwendige Identifizierung soll via ID eines DMDA geschehen.
3	Ident-Karte und De-Mail-Adresse angeben	Web	Der SP nennt dem Nutzer eine De-Mail-Adresse, an die der DMDA die Ident-Bestätigung sendet. Ferner teilt der SP dem Nutzer mit, welche Ident-Karte er benötigt.
4	Mit Ident-Dienst verbinden	Web	Der Benutzer verbindet sich mit dem Authentisierungsniveau „hoch“ mit dem ID

Schritt	*Bezeichnung*	*Übermittlung*	*Beschreibung*
			seines DMDA.
5	Ident-Auftrag erstellen	Web	Der Nutzer veranlasst die Erstellung einer Ident-Nachricht. Dabei teilt der Nutzer dem DMDA die De-Mail-Adresse des SP, die zu verwendende Ident-Karte und seine eigene De-Mail-Adresse mit, die für die Kommunikation mit dem SP verwendet wird.
6	Ident-Bestätigung erstellen		Der ID erstellt eine Ident-Bestätigung.
7	Ident-Bestätigung versenden	Nachricht	Der ID versendet die Ident-Bestätigung mittels einer Nachricht über den PVD zum SP. Eine Kopie der Nachricht erhält der Nutzer.
8	Ident-Bestätigung empfangen	Nachricht	Der SP empfängt die Ident-Bestätigung vom ID mittels des PVD.

Tabelle 2: Ablaufbeschreibung ID

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

5 Aktivitätsdiagramm

In Abbildung 3 wird der funktionale Ablauf des ID von der Erstellung eines Ident-Auftrages durch einen Nutzer bis zum Versenden einer Ident-Bestätigung an einen SP über den PVD (siehe [TR DM PVD FU]) in einem Aktivitätsdiagramm[1] dargestellt. Eine detaillierte technisch-funktionale Beschreibung der einzelnen Aktionen und Schritte des Aktivitätsdiagramms erfolgt in Abschnitt 6.

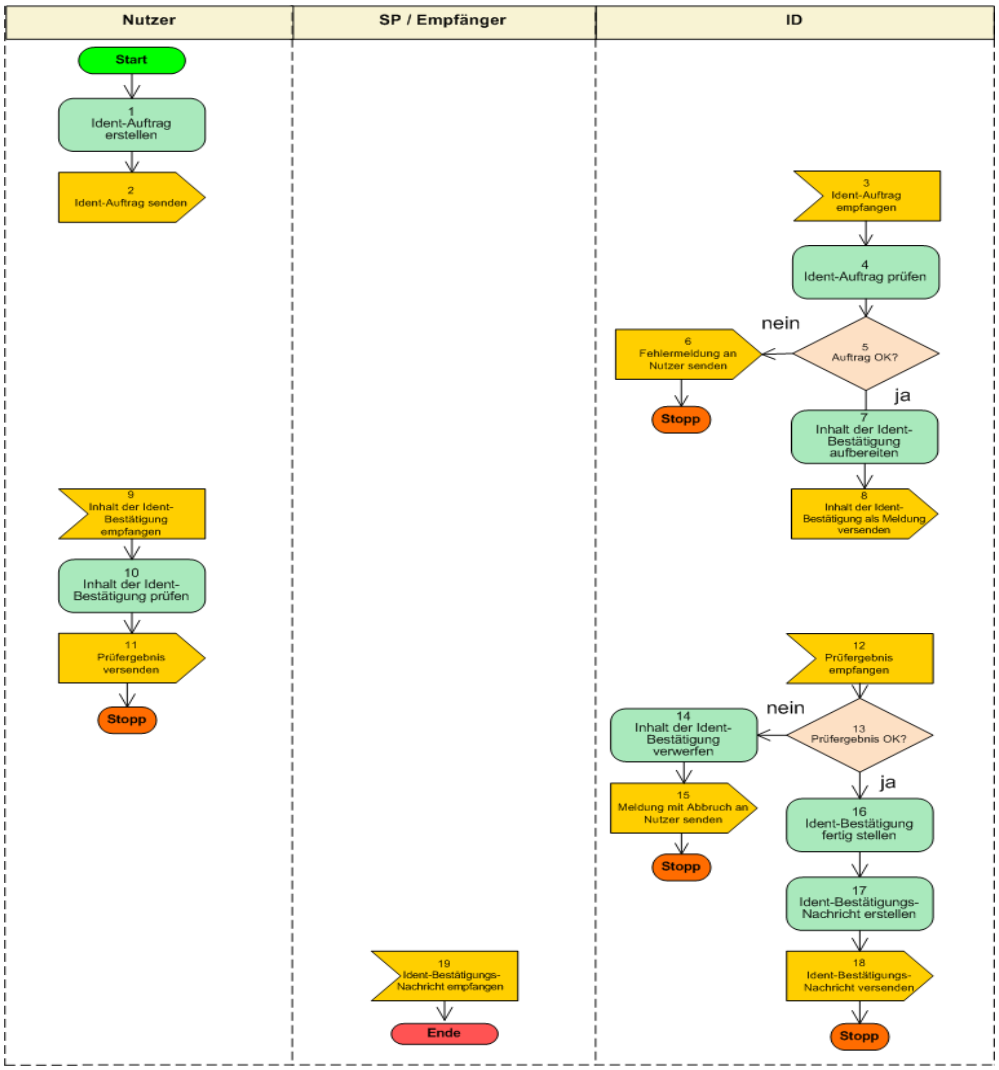


Abbildung 3: Aktivitätsdiagramm des ID

1 Eine Legende zu den Symbolen des Aktivitätsdiagramms findet sich in Abschnitt 7.1.

6 Funktionale Beschreibung

Im Folgenden werden die einzelnen Schritte des Aktivitätsdiagramms aus Abschnitt 4 von der Erstellung eines Ident-Auftrages durch einen Nutzer bis zum Versenden einer Ident-Bestätigung an einen SP über den PVD von De-Mail beschrieben. Die referenzierten Funktionen des Account- und Zeitdienstes werden in [TR DM ACM FU] und in [TR DM IT-BInfra] erläutert. Eine Beschreibung, wie die einzelnen Schritte strukturiert sind, findet sich in Abschnitt 8.2.

6.1 Einbindung des ID beim SP

Der SP muss dem Nutzer im Vorfeld in geeigneter Form (z. B. auf seiner Website) eine De-Mail-Adresse und die geforderte Ident-Karte angeben, damit der Nutzer den Ident-Auftrag stellen kann, auf dessen Grundlage die Ident-Bestätigung vom DMDA erstellt wird.

6.2 Identitätsbestätigung erstellen

6.2.1 Ident-Auftrag erstellen

Schritt 1	**Ident-Auftrag erstellen**
Kurzbeschreibung	Der Nutzer erstellt einen Ident-Auftrag.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	• De-Mail-Adresse vom SP erhalten • SP hat Ident-Karte mit benötigten Attributen mitgeteilt • Anmeldung am De-Mail-Konto mit Authentisierungsniveau „hoch“
Input	De-Mail-Adresse des SP Typ der benötigten Ident-Karte
Ergebnis	Ident-Auftrag ist erstellt
Nachbedingung	
Ablauf	• Ident-Auftrag-Maske aufrufen • De-Mail-Adresse des SP eingeben • Ident-Karte auswählen ◦ ggf. Spezifikation, welche im De-Mail-Konto hinterlegten Daten in der Ident-Bestätigung verwendet werden müssen (vgl. Abschnitt 3.2) • Auftrag ausführen
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto mit Authentisierungsniveau „hoch“

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	angemeldet
Schritt 2	**Ident-Auftrag senden**
Kurzbeschreibung	Der Nutzer sendet den Ident-Auftrag zum ID.
Akteure	Nutzer, ID
Auslöser	Nutzer
Vorbedingung	
Input	Ident-Auftrag
Ergebnis	Ident-Auftrag zum ID versendet
Nachbedingung	
Ablauf	Ident-Auftrag zum ID senden
Fehlerfälle	FC-01: Ident-Auftrag wird nicht angenommen

Tabelle 3: Schritte zum Erstellen eines Ident-Auftrages

6.2.2 Ident-Auftrag durch DMDA prüfen

Schritt 3	**Ident-Auftrag empfangen**
Kurzbeschreibung	Der ID empfängt den Ident-Auftrag.
Akteure	Nutzer, ID
Auslöser	Nutzer
Vorbedingung	• Sicheren Kanal zwischen den Kommunikationspartnern aufgebaut • Authentisierungsniveau des Nutzers „hoch“
Input	Ident-Auftrag
Ergebnis	Ident-Auftrag vom ID empfangen
Nachbedingung	
Ablauf	Ident-Auftrag empfangen
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto mit Authentisierungsniveau „hoch“ angemeldet
Schritt 4	**Ident-Auftrag prüfen**
Kurzbeschreibung	Der ID prüft den Ident-Auftrag.
Akteure	ID, Account-Dienst
Auslöser	ID
Vorbedingung	
Input	Ident-Auftrag Aktuelles Authentisierungsniveau des Nutzers

– Seite 248 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Ergebnis	Ident-Auftrag geprüft
Nachbedingung	
Ablauf	• De-Mail-Adresse des SP syntaktisch prüfen • Ident-Karte prüfen, ob der Nutzer sie auswählen darf (z.B. bei Alterskategorie-Karte) • Prüfen, ob explizit referenzierte Identitätsdaten für Ident-Karte genutzt werden dürfen (vgl. Abschnitt 3.2)
Fehlerfälle	FC-01: De-Mail-Adresse des SP ist syntaktisch fehlerhaft FC-02: Ident-Karte (für Nutzer) nicht vorhanden FC-03: Referenzierte Identitätsdaten nicht erlaubt/nicht gültig
Schritt 5	**Entscheidungsknoten: Auftrag OK?**
Kurzbeschreibung	Auswertung durch ID, ob der Ident-Auftrag korrekt gestellt wurde.
ja	Schritt 7
nein	Schritt 6
Schritt 6	**Fehlermeldung an Nutzer senden**
Kurzbeschreibung	Der ID sendet eine Fehlermeldung an den Nutzer (vgl. Abschnitt 3.4).
Akteure	ID
Auslöser	ID
Vorbedingung	
Input	Fehlerfälle aus Schritt 4
Ergebnis	Meldung an Nutzer gesendet
Nachbedingung	Stopp
Ablauf	• Fehlerfälle aus Schritt 4 zu einer Meldung verarbeiten • Meldung an Nutzer senden
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden
Schritt 7	**Inhalt der Ident-Bestätigung aufbereiten**
Kurzbeschreibung	Der ID erstellt die Inhalte der späteren Ident-Bestätigung
Akteure	ID, Account-Dienst, Zeitdienst
Auslöser	ID
Vorbedingung	
Input	• Ident-Karte • Nutzerkennung des Ident-Auftraggebers (De-Mail-Adresse des Nutzers) • Nutzerkennung des Empfängers (De-Mail-Adresse des SP)

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	• Nutzerkennung des Ausstellers (De-Mail-Adresse des DMDA) • Authentisierungsniveau und –Methode des Nutzers • Ausstellungszeitpunkt (gesetzliche Zeit)
Ergebnis	Inhalte der Ident-Bestätigung erstellt
Nachbedingung	
Ablauf	• Anfrage an Account-Dienst (Attribute von Ident-Karte). • Identitätsdaten und deren Metadaten in die Ident-Bestätigung einfügen • Nutzerkennung des Ident-Auftraggebers (De-Mail-Adresse des Nutzers) in die Ident-Bestätigung einfügen • Nutzerkennung des Empfängers (De-Mail-Adresse des SP) in die Ident-Bestätigung einfügen • Nutzerkennung des Ausstellers (De-Mail-Adresse des DMDA) in die Ident-Bestätigung einfügen • Authentisierungsniveau des Nutzers in die Ident-Bestätigung einfügen • Ausstellungszeitpunkt in die Ident-Bestätigung einfügen
Fehlerfälle	FC-01: Identitätsattribut für Nutzer nicht vorhanden
Schritt 8	**Inhalt der Ident-Bestätigung als Meldung versenden**
Kurzbeschreibung	Der ID erstellt eine Meldung an den Nutzer, der den Ident-Auftrag erstellt hat. Die Meldung beinhaltet die Inhalte der späteren Ident-Bestätigung.
Akteure	ID, Nutzer
Auslöser	ID
Vorbedingung	
Input	Inhalte der Ident-Bestätigung
Ergebnis	Inhalt der Ident-Bestätigung zum Nutzer versendet
Nachbedingung	
Ablauf	• Meldung mit Informationen aus Schritt 7 erstellen • Meldung zum Nutzer senden
Fehlerfälle	FC-01: Meldung wird nicht angenommen

Tabelle 4: Schritte zum Prüfen eines Ident-Auftrages durch DMDA

6.2.3 Inhalte der Ident-Bestätigung durch Nutzer prüfen

Schritt 9	**Inhalt der Ident-Bestätigung empfangen**
Kurzbeschreibung	Der Nutzer empfängt den Inhalt der (späteren) Ident-Bestätigung.

Akteure	ID, Nutzer
Auslöser	ID
Vorbedingung	
Input	Ident-Auftrag
Ergebnis	Inhalt der Ident-Bestätigung vom ID empfangen
Nachbedingung	
Ablauf	Inhalt der Ident-Bestätigung empfangen
Fehlerfälle	
Schritt 10	**Inhalt der Ident-Bestätigung prüfen**
Kurzbeschreibung	Der Nutzer prüft die Richtigkeit der Inhalte der späteren Ident-Bestätigung. Im Anschluss an die Prüfung kann er den Ident-Auftrag bestätigen oder abbrechen.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Inhalt der Ident-Bestätigung
Ergebnis	Ident-Auftrag geprüft
Nachbedingung	
Ablauf	• Darstellung des Inhalts • Bestätigung oder Abbrechen des initiierten Ident-Auftrages
Fehlerfälle	
Schritt 11	**Prüfergebnis senden**
Kurzbeschreibung	Das Prüfergebnis des Nutzers wird zum ID gesendet.
Akteure	Nutzer, ID
Auslöser	Nutzer
Vorbedingung	
Input	Prüfergebnis (Bestätigung oder Abbrechen)
Ergebnis	Prüfergebnis zum ID versendet
Nachbedingung	
Ablauf	Prüfergebnis zum ID senden
Fehlerfälle	FC-01: Prüfergebnis wird nicht angenommen

Tabelle 5: Schritte zur Prüfung der Ident-Bestätigung durch den Nutzer

6.2.4 Ident-Bestätigung erstellen und versenden

Schritt 12	**Prüfergebnis empfangen**
Kurzbeschreibung	Der ID empfängt das Prüfergebnis für den Ident-Auftrag.
Akteure	Nutzer, ID
Auslöser	Nutzer
Vorbedingung	
Input	Prüfergebnis
Ergebnis	Prüfergebnis vom ID empfangen
Nachbedingung	Wenn kein Prüfergebnis empfangen wurde: Schritt 14.
Ablauf	Prüfergebnis empfangen
Fehlerfälle	
Schritt 13	**Entscheidungsknoten: Prüfergebnis OK?**
Kurzbeschreibung	Auswertung, ob der Nutzer den Ident-Auftrag bestätigt (ja) oder abgebrochen (nein) hat.
ja	Schritt 16
nein	Schritt 14
Schritt 14	**Inhalt der Ident-Bestätigung verwerfen**
Kurzbeschreibung	Der Inhalt der Ident-Bestätigung wird vom ID verworfen.
Akteure	ID
Auslöser	ID
Vorbedingung	
Input	Inhalt der Ident-Bestätigung
Ergebnis	Inhalt der Ident-Bestätigung gelöscht
Nachbedingung	
Ablauf	Löschen der Inhalte der Ident-Bestätigung
Fehlerfälle	
Schritt 15	**Meldung mit Abbruch an Nutzer senden**
Kurzbeschreibung	Der ID sendet eine Meldung an den Nutzer, dass der Ident-Auftrag abgebrochen wurde.
Akteure	ID
Auslöser	ID
Vorbedingung	
Input	

Ergebnis	Meldung an Nutzer gesendet
Nachbedingung	Stopp
Ablauf	Meldung mit Abbruch an Nutzer senden
Fehlerfälle	FC-01: Meldung konnte nicht abgesendet/dargestellt werden
Schritt 16	**Ident-Bestätigung fertig stellen**
Kurzbeschreibung	Die in Schritt 7 erstellen Inhalte werden zur Ident-Bestätigung zusammengestellt und vom ID mit einer qualifizierten elektronischen Signatur signiert.
Akteure	ID
Auslöser	ID
Vorbedingung	
Input	Inhalte der Ident-Bestätigung aus Schritt 7
Ergebnis	Ident-Bestätigung fertig erstellt
Nachbedingung	
Ablauf	- Inhalte der Ident-Bestätigung aus Schritt 7 in das Format für eine Ident-Bestätigung strukturieren. - Die Ident-Bestätigung mit einer qualifizierten elektronischen Signatur versehen
Fehlerfälle	
Schritt 17	**Ident-Bestätigungsnachricht erstellen**
Kurzbeschreibung	Der ID erstellt eine Ident-Bestätigungsnachricht.
Akteure	ID
Auslöser	ID
Vorbedingung	
Input	• Ident-Bestätigung • Nutzerkennung des Absenders (De-Mail-Adresse des DMDA) • Nutzerkennung des Empfängers SP (De-Mail-Adresse des SP) • Nutzerkennung des Empfängers Nutzer (De-Mail-Adresse des Nutzers)
Ergebnis	Ident-Bestätigungsnachricht erstellt
Nachbedingung	
Ablauf	• Ident-Bestätigung in Ident-Bestätigungsnachricht einfügen • Nutzerkennung des Ausstellers als Absender-Adresse der Ident-Bestätigungsnachricht einfügen • Nutzerkennung des SP als Empfänger-Adresse der Ident-Bestätigungsnachricht einfügen

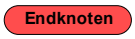
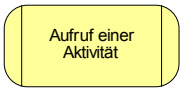
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	• Nutzerkennung des Ident-Auftraggebers in Kopie (Carbon Copy, CC) als Empfänger-Adresse der Ident-Bestätigungsnachricht einfügen • Versandoption „Persönlich“ wählen
Fehlerfälle	
Schritt 18	**Ident-Bestätigungsnachricht versenden**
Kurzbeschreibung	Der ID sendet die Ident-Bestätigungsnachricht über den PVD an den SP und Nutzer.
Akteure	ID, Postfachdienst des Ausstellers
Auslöser	ID
Vorbedingung	Sicheren Kanal mit PVD aufgebaut
Input	Ident-Bestätigungsnachricht
Ergebnis	Ident-Bestätigungsnachricht an SP und Nutzer gesendet
Nachbedingung	
Ablauf	Ident-Bestätigungsnachricht über den PVD versenden
Fehlerfälle	FC-01: Ident-Bestätigungsnachricht wurde nicht angenommen

Tabelle 6: Schritte zum Erstellen und Versenden der Ident-Bestätigung

7 Anhang

7.1 Legende zum Aktivitätsdiagramm

	Startknoten Der Startknoten ist der Startpunkt eines Prozesses. Ein Prozess darf mehrere Startknoten haben, in diesem Fall beginnen beim Start des Prozesses mehrere Abläufe. Es ist möglich, dass ein Prozess keinen Startknoten besitzt, sondern von einem Ereignis angestoßen wird.
	Endknoten Der Endknoten gibt an, dass die Ausführung des Prozesses abgeschlossen ist. Es kann in einem Prozessdiagramm mehrere Ausgänge in Form dieser Endknoten geben. Gibt es zum Zeitpunkt des Erreichens des Endknotens mehrere parallele Abläufe innerhalb des Prozesses, werden beim Erreichen eines Endknotens alle Abläufe gestoppt.
	Ablaufende Das Ablaufende terminiert einen Ablauf. Im Unterschied zum Endknoten, der einen ganzen Prozess beendet, hat das Erreichen des Ablaufendes keinen Effekt auf andere parallele Abläufe, die zu diesem Zeitpunkt innerhalb des Prozesses abgearbeitet werden. Auf diese Weise lassen sich parallele Abläufe gezielt und einzeln beenden.
	Kante Die als Pfeile dargestellten Kanten verbinden die einzelnen Komponenten des Diagramms und stellen den Kontrollfluss dar.
	Aktion Eine Aktion ist ein einzelner Schritt innerhalb eines Prozesses, der nicht mehr weiter zerlegt wird. Das bedeutet nicht unbedingt, dass die Aktion in der realen Welt nicht mehr weiter zerlegbar wäre, sondern dass die Aktion in diesem Diagramm nicht mehr weiter verfeinert wird. Die Aktion kann Ein- und Ausgabeinformationen besitzen. Der Output einer Aktion kann der Input einer Folge-Aktion sein.
	Aufruf einer Aktivität Mit diesem Symbol kann aus einer Aktivität (Prozess) heraus eine weitere Aktivität aufgerufen werden. Der Aufruf selbst ist eine Aktion, der aufgerufene Ablauf eine weitere Aktivität.

	Empfang eines Ereignisses Diese Aktion wartet auf das Eintreten eines Ereignisses. Nach dem Empfang des Ereignisses wird der im Aktivitätsdiagramm definierte, von dieser Aktion ausgehende Ablauf abgearbeitet.
	Senden von Signalen Das Senden von Signalen bedeutet, dass ein Signal an eine empfangende Aktivität gesendet wird. Die empfangende Aktivität nimmt das Signal mit der Aktion „Ereignis empfangen“ entgegen und kann entsprechend darauf reagieren.
	Entscheidungsknoten Die Raute stellt eine Verzweigung im Kontrollfluss dar. Eine Verzweigung hat einen Eingang und zwei oder mehrere Ausgänge. Jeder Ausgang wird mit einer Bedingung versehen. Trifft eine Bedingung zu, wird am entsprechenden Ausgang weiterverfahren.
	Datenobjekt Datenobjekte gehören üblicherweise nicht zum Symbolumfang in UML-Aktivitätsdiagrammen. Sie sind hier jedoch eingeführt worden, um an entscheidender Stelle zu verdeutlichen, welche Datenobjekte, insbesondere im Fokus der Schutzbedarfsanalyse, vorliegen.

Tabelle 7: Legende zum Aktivitätsdiagramm

7.2 Legende zu Schritten der Ablaufbeschreibung

Schritte im Aktivitätsdiagramm bezeichnen im Kontrollfluss eingebundene einmalig ablaufende Aktionen, wie z. B. einen vom Nutzer erstellten Ident-Auftrag zu prüfen (Schritt 4 in Abschnitt 4).

Schritte werden in diesem Modul als Aktionen auf folgende Art und Weise beschrieben:

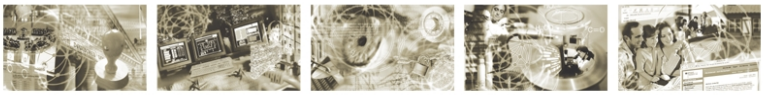
Schritt <Nr.>	Eindeutigen Name der Aktion
Kurzbeschreibung	Innerhalb der Kurzbeschreibung erfolgt eine verbale Beschreibung der wesentlichen Funktionalität der Aktion.
Akteure	Alle Rollen bzw. Dienste, die innerhalb der Aktion in irgendeiner Weise beteiligt sind, werden aufgezählt.
Auslöser	Der Auslöser ist ein Akteur, durch den die Aktion aufgerufen bzw. initialisiert wird.
Vorbedingung	Unter Vorbedingungen werden die Bedingungen verstanden, die nicht aus einer unmittelbar vorhergehenden Aktion folgen, sondern asynchron erzielt werden müssen. Diese Aktivitäten sind nicht unbedingt in diesem Dokument beschrieben, die Ergebnisse sind jedoch als Vorbedingungen für die Ausführung der hier beschriebenen Aktion notwendig. Auf die Erfüllung dieser Vorbedingungen muss sich die nutzende Aktion verlassen können.

Input	Der Auslöser muss bei Initialisierung der Aktion die entsprechenden Informationen an diese übergeben oder durch die Aktion abfragen lassen, so dass eine Verarbeitung der Informationen innerhalb der Aktion erfolgen kann.
Ergebnis	Nach Beendigung der Aktion muss eine bestimmte Information als Resultat erarbeitet bzw. bereitgestellt werden.
Nachbedingung	Unter Nachbedingungen werden Bedingungen verstanden, die innerhalb dieser Aktion nicht betrachtet werden und durch unmittelbar nachfolgende Aktionen aufgegriffen und dort behandelt werden müssen.
Ablauf	Für die innerhalb der Aktion definierte Logik wird ein konkreter Ablauf beschrieben. Die definierte Abfolge muss innerhalb der Aktion durchgeführt und abgeschlossen werden.
Fehlerfälle	Als Fehlerfall wird ein Ergebnis einer Funktion bezeichnet, der innerhalb der Funktionsspezifikation liegt, aber kein Standard-Ergebnis darstellt. Die konkrete Behandlung eines Fehlerfalls ist implementierungsabhängig. Je nach Fall können unterschiedliche Lösungsstrategien verwendet werden, bspw. kann eine Aktion zu einem späteren Zeitpunkt wiederholt oder die Aktion abgebrochen werden. Bei Abbruch einer Aktion ist der Nutzer mindestens darüber zu informieren und alle bis zu diesem Schritt generierten temporären Daten müssen gelöscht werden. In den Beschreibungen der Fehlerfälle der Aktionen werden nur mögliche Fehler beschrieben, die innerhalb der Funktionsspezifikation liegen.

Tabelle 8: Legende zu Schritten

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Identitätsbestätigungsdienst IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 4.3
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
+49 (0)228 99 9582-0
E-Mail: de-mail@bsi.bund.de
Internet: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die IT-Sicherheitsanforderungen, die über die generellen Anforderungen aus dem Modul [TR DM Si M] hinausgehen und speziell für den ID anzuwenden sind, und ist Bestandteil von [TR DM ID M]. Dies gilt, sofern der ID angeboten wird.

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die in [TR DM Si ÜK] angenommene Netzinfrastruktur eines typischen De-Mail-Dienstes.

Bei der Erstellung des realen IT-Sicherheitskonzepts sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der bereits in der [TR DM Si ÜK] skizziert ist.

– Seite 262 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

3 Bedrohungen

Es gelten die in [TR DM Si ÜK] formulierten Bedrohungen, sowie weitere speziell für den ID geltenden Aspekte.

3.1 Falsche Versendung von Ident-Nachweisen

Durch technisches Versagen oder bewusste Manipulation (beispielsweise von Innentätern) können Ident-Nachweise mit falschem Inhalt unter der spezifischen Adresse versendet werden.

3.2 Manipulierte Inhalte der Ident-Nachweise

Durch technisches Versagen oder bewusste Manipulation (beispielsweise von Innentätern) können Ident-Nachweise manipuliert und versendet werden oder der Inhalt der Ident-Nachweise kann bei der Übertragung unbefugt verändert werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

4 Sicherheitsziele

Es gelten die Sicherheitsziele, die in [TR DM Si ÜK] formuliert wurden.

4.1 Schutz der Systemadresse

Es müssen geeignete Maßnahmen getroffen werden, um ein unberechtigtes Versenden unter der spezifischen Adresse zu verhindern. Damit soll unterbunden werden, dass Ident-Nachrichten mit manipulierten Inhalten ausgestellt und versendet werden.

4.2 Schutz vor Manipulation der Daten

Die Identnachweise müssen vor unbefugter Änderung geschützt werden.

5 Anforderungen

5.1 Verwendung der Systemadressen nur durch den DMDA

Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass die Systemadressen nicht missbräuchlich verwendet werden können.

5.2 Signatur der Ident-Nachweise

Die Ident-Nachweise müssen durch den DMDA qualifiziert signiert (vgl [TR DM ID FU]) werden.

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Identitätsbestätigungsdienst Interoperabilitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 4.4
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul ist Bestandteil von [TR DM ID M]. Hier werden Datenstrukturen und Datenformate des Identitätsbestätigungsdienstes spezifiziert.

2 Datenstrukturen

In diesem Abschnitt werden die im ID verwendeten Datenstrukturen beschrieben.

2.1 Datenformate

Gemäß [TR DM ID FU] muss eine Ident-Bestätigung eine von mehreren möglichen Ident-Karten gemäß [TR DM ID FU] sowie zusätzliche Metadaten beinhalten. In die Metadaten der Ident-Bestätigungsnachricht müssen diese Metadaten übernommen werden und darüber hinaus weitere Metadaten auf bestimmte Werte gesetzt werden. Nachfolgend werden die Metadaten der Ident-Bestätigungsnachricht spezifiziert. Die Spezifikation der Metadaten der Ident-Bestätigung erfolgt im Rahmen der Beschreibung der XML-Struktur in Abschnitt 2.6.

2.1.1 Metadaten einer Ident-Bestätigungsnachricht

Eine Ident-Bestätigungsnachricht muss die folgenden Metadaten gemäß [TR DM PVD FU] beinhalten:

Metadatum-Nummer	Bezeichnung	Inhalt
5	Versandoption:	Persönlich="yes"
	Empfänger	Service Provider der Ident-Bestätigung erhalten soll
6	Absender:	Ident-Bestaetigung@<DMDA>
7,19	CC:	Auftraggeber der Ident-Bestätigung
8	Betreff:	„Ident-Bestätigung"
16	Nachrichten-Typ:	Ident-Bestätigung (X-De-Mail-Message-Type: identification)

Tabelle 1: Metadaten einer Ident-Bestätigung

Der Inhalt der Nachricht muss folgenden Text enthalten:

```
Hiermit werden die folgende Identitätsdaten zur angegebenen De-Mail-
Adresse bestätigt:

<Es werden alle Attribute aufgeführt, die auch in der XML-Datei enthalten
sind. Dazu SOLLTE die Bedeutung der Felder und der Werte des Feldes
dargestellt werden.>
```

2.2 Ident-Karten

Identitätsinformationen werden in verschiedenen Ident-Karten (siehe [TR DM ID FU]) übermittelt. Eine Ident-Bestätigungsnachricht muss eine dieser Karten enthalten. Als Darstellungsformat werden

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

im Folgenden für jeden Kartentyp XML-Datenstrukturen in Form einer XML Schema Definition (XSD) definiert. Aus Gründen der Übersichtlichkeit fehlen in den folgenden Darstellungen an jedem XML-Element einer Karte ein weiteres XML-Attribut (Validierungszeitpunkt), das immer vorhanden sein muss. Das Element `ValidationTime` enthält den Zeitpunkt, zu dem die Ausprägung des Attributes überprüft wurde.

2.2.1 Identitätskarte einer natürlichen Person

Für die Identitätskarte einer natürliche Person können folgende Attribute verwendet werden.

Die einzelnen Datenelemente sind:

Name	Datentyp	Maximale Länge	Bedeutung
personalTitle	xs:string	40	Titel (akademischer Grad)
pseudonym	xs:string	60	Künstler- oder Ordensname (optional)
surname	xs:string	120	Nachname
givenname	xs:string	80	Vorname(n)
street	xs:string	100	Straße und Hausnummer
locality	xs:string	100	Wohnort
country	xs:string	2	Staat (nach DIN EN ISO 3166 ALPHA-2)
dateOfBirth	xs:string	10	Geburtsdatum
locationOfBirth	xs:string	100	Geburtsort
age	xs:int		Alter als Zahl
de-mail-address	xs:string	255	De-Mail-Adresse

Tabelle 2: Identitätskarte einer natürlichen Person

Die Felder „pseudonym“ und die Kombination der Felder „personalTitle“, „surname“ und „givenname“ können wahlweise zum Einsatz kommen. Es muss nur jeweils eines dieser Felder vorhanden sein. Bei Nutzung einer Pseudonym-Adresse als De-Mail-Adresse muss „pseudonym“ verwendet werden.

Wenn für einen Nutzer kein vollständiges Geburtsdatum erfasst werde konnte, werden die nicht erfassten Teile mit dem Zeichen < im Feld „dateOfBirth“ aufgefüllt. Das Datum muss die Form dd.mm.yyyy (z.B. 01.01.2000) haben.

2.2.2 Identitätskarte einer Institution

Die Identitätskarte einer Institution kann folgende Felder enthalten:

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Name	Datentyp	Maximale Länge	Bedeutung
commonName	xs:string	60	Name der Institution
street	xs:string	100	Straße und Hausnummer
locality	xs:string	100	Ort
postOfficeBox	xs:string	10	Postfach
country	xs:string	2	Staat
legalForm	xs:string	60	Rechtsform
authorisedRepresentative	xs:string	255	Namen der Mitglieder des Vertretungsorgans oder der gesetzliche Vertreter
commercialRegisterType	xs:string	255	Art des Registereintrag
commercialRegisterEntry	xs:string	255	Registereintrag
commercialRegisterLocality	xs:string	255	Ort des Register
de-mail-address	xs:string	255	De-Mail-Adresse

Tabelle 3: Identitätskarte einer Institution

2.3 Altersnachweise

Die Identitätskarte für einen Altersnachweis muss folgende Felder enthalten:

Name	Datentyp	Maximale Länge	Bedeutung
age	xs:int		Alter des Nutzers
de-mail-address	xs:string	255	De-Mail-Adresse

Tabelle 4: Allgemeiner Altersnachweis

Name	Datentyp	Maximale Länge	Bedeutung
over16	xs:boolean		Wahr, wenn der Nutzer älter als 16 Jahre ist, ansonsten unwahr
de-mail-address	xs:string	255	De-Mail-Adresse

Tabelle 5: Alternachweis für Nutzer über 16 Jahre

– Seite 272 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Name	Datentyp	Maximale Länge	Bedeutung
over18	xs:boolean		Wahr, wenn der Nutzer älter als 18 Jahre ist, ansonsten unwahr
de-mail-address	xs:string	255	De-Mail-Adresse

Tabelle 6: Alternachweis für Nutzer über 18 Jahre

2.4 Adresskarte

Die Identitätskarte für einen Adressnachweis muss folgende Felder enthalten:

Name	Datentyp	Maximale Länge	Bedeutung
personalTitle	xs:string	40	Titel (akademischer Grad)
pseudonym	xs:string	60	Künstler- oder Ordensname
surname	xs:string	120	Nachname
givenname	xs:string	80	Vorname(n)
street	xs:string	100	Straße
locality	xs:string	100	Wohnort
country	xs:string	2	Staat (nach DIN EN ISO 3166 ALPHA-2)
de-mail-address	xs:string	255	De-Mail-Adresse

2.5 De-Mail-Adress-Karte

Die Identitätskarte für eine De-Mail-Adress-Karte muss folgende Felder enthalten:

Name	Datentyp	Maximale Länge	Bedeutung
de-mail-address	xs:string	255	De-Mail-Adresse

2.6 XML-Format einer Ident-Bestätigung

Eine Ident-Bestätigung muss als SAML-Assertion [SAML-CORE20] dargestellt werden.

Das Attribut „Version“ muss auf den Wert „2.0“ fixiert sein.

Das Attribut „ID“ muss zufällig und eineindeutig pro DMDA für jede neue Ident-Bestätigung

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

erzeugt werden.

Das Attribut „IssueInstant“ muss den Ausstellungszeitpunkt der Nachricht enthalten.

Das Element „Issuer“ muss die De-Mail-Adresse des ausstellenden DMDA enthalten. Das Attribut „Format“ des Elements „Issuer“ muss „urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress” lauten.

Es muss ein Element „signature“ vorhanden sein. Das Element „signature“ muss eine qualifizierte elektronische Signatur über die XML-Struktur „Ident-Message“ enthalten. Es muss gemäß Abschnitt 5.4 in [SAML-CORE20] erstellt werden. Als Transformationen für die Erzeugung der Signatur müssen `Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"` und `Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"` verwendet werden.

Es muss ein Element „subject“ vorhanden sein. Das Element „subject“ muss den Auftraggeber der Ident-Bestätigungsnachricht angeben, dem die in der Assertion enthaltene Ident-Karte zugeordnet ist. Das Element „subject“ enthält nur das Element „NameID“, dessen Attribut „Format“ „urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress” lauten muss. Hier muss die De-Mail-Adresse (Primäre oder Pseudonym-De-Mail-Adresse) des Auftraggebers angegeben werden.

Es muss ein Element „conditions“ vorhanden sein. Das Element „conditions“ enthält genau ein Element „audienceRestriction“. Das Element „audience“ enthält die De-Mail-Adresse des Empfängers der Karte.

Eine Ident-Bestätigung gemäß dieser Spezfikation enthält genau ein „AuthnStatement“ und genau ein „AttributeStatement“.

Das Element „AuthnStatement“ muss im Attribut „AuthInstant“ den Zeitpunkt enthalten, zu dem sich der Auftraggeber das letzte Mal gegenüber dem die Ident-Bestätigung ausstellenden De-Mail-Portal authentifiziert hat. Das Authentisierungsverfahren muss im Element „AuthnContext“ angegeben werden. Dies muss genau ein „AuthnContextClassRef“-Element enthalten, dessen Wert gemäß Abschnitt 3.4 [SAML-CORE20] das verwendete Verfahren bezeichnet. Da die Nutzung des ID nur mit Authentisierungsniveau „hoch“ möglich ist, kann unabhängig von dem angegebenen Verfahren von mindestens hohem Authentisierungsniveau ausgegangen werden.

Ein Beispiel:

```
<saml:AuthnStatement AuthnInstant="2001-12-17T09:30:47.0Z"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     <saml:AuthnContext>
          <saml:AuthnContextClassRef>
          urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
          </saml:AuthnContextClassRef>
     </saml:AuthnContext>
</saml:AuthnStatement>
```

Das Element „AttributeStatement“ muss die übermittelte Identitätskarte enthalten. Diese muss als „Ident-Card“-Struktur im „AttributeValue“-Element des „Attribute“-Elements dieses Statements abgelegt werden. Ein Beispiel:

```
<saml:AttributeStatement
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     <saml:Attribute Name="Card">
          <saml:AttributeValue xsi:type=”de-mail:Identcard”>
               <Identcard><NaturalPerson>…</NaturalPerson>
               </Identcard>
           </saml:AttributeValue>
     </saml:Attribute>
</saml:AttributeStatement>
```

Die „Ident-Card“-Struktur beinhaltet ein Element des Type NaturalPerson oder LegalPerson.

Weitere mögliche Elemente einer SAML-Assertion werden nicht benutzt.

2.7 XSD der Ident-Bestätigung

Alle vom DMDA erstellten Ident-Bestätigungen müssen den Definitionen in der XSD entsprechen:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.de-mail.de/xml/2010/01/ident"
    elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:de-mail="http://www.de-mail.de/xml/2010/01/ident"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <xs:simpleType name="Char2SimpleType">
        <xs:restriction base="xs:string">
            <xs:maxLength value="2"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Char10SimpleType">
        <xs:restriction base="xs:string">
            <xs:maxLength value="10"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Char40SimpleType">
        <xs:restriction base="xs:string">
            <xs:maxLength value="40"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Char60SimpleType">
```

```
        <xs:restriction base="xs:string">
            <xs:maxLength value="60"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Char80SimpleType">
        <xs:restriction base="xs:string">
            <xs:maxLength value="80"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Char100SimpleType">
        <xs:restriction base="xs:string">
            <xs:maxLength value="100"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Char120SimpleType">
        <xs:restriction base="xs:string">
            <xs:maxLength value="120"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Char255SimpleType">
        <xs:restriction base="xs:string">
            <xs:maxLength value="255"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="BooleanSimpleType">
        <xs:restriction base="xs:boolean">
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="Char2Type">
        <xs:simpleContent>
            <xs:extension base="de-mail:Char2SimpleType">
                <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
                </xs:attribute>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
    <xs:complexType name="Char10Type">
        <xs:simpleContent>
            <xs:extension base="de-mail:Char10SimpleType">
                <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
                </xs:attribute>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="Char40Type">
        <xs:simpleContent>
            <xs:extension base="de-mail:Char40SimpleType">
                <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
                </xs:attribute>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="Char60Type">
        <xs:simpleContent>
            <xs:extension base="de-mail:Char60SimpleType">
                <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
                </xs:attribute>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="Char80Type">
        <xs:simpleContent>
            <xs:extension base="de-mail:Char80SimpleType">
                <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
                </xs:attribute>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="Char100Type">
        <xs:simpleContent>
            <xs:extension base="de-mail:Char100SimpleType">
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
            <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
            </xs:attribute>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="Char120Type">
    <xs:simpleContent>
        <xs:extension base="de-mail:Char120SimpleType">
            <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
            </xs:attribute>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="Char255Type">
    <xs:simpleContent>
        <xs:extension base="de-mail:Char255SimpleType">
            <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
            </xs:attribute>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="BooleanType">
    <xs:simpleContent>
        <xs:extension base="de-mail:BooleanSimpleType">
            <xs:attribute name="validationTime" type="xs:dateTime"
use="required">
            </xs:attribute>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="Identcard">
    <xs:choice>
        <xs:element name="LegalPerson" maxOccurs="1" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Identitaetskarte einer Institution
                </xs:documentation>
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="commonName" type="de-mail:Char60Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="street" type="de-mail:Char100Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="postOfficeBox" type="de-mail:Char10Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="locality" type="de-mail:Char100Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="country" type="de-mail:Char2Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="legalForm" type="de-mail:Char60Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="authorisedRepresentative" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="unbounded">
                    </xs:element>
                    <xs:element name="commercialRegisterType" type="de-
mail:Char255Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="commercialRegisterEntry" type="de-
mail:Char255Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="commercialRegisterLocality" type="de-
mail:Char255Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="de-mail-address" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="1">
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="NaturalPerson" maxOccurs="1" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Identitaetskarte einer natuerlichen
Person</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="personalTitle" type="de-mail:Char40Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="surname" type="de-mail:Char120Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="givenname" type="de-mail:Char80Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="religiousnameOrPseudonym" type="de-
mail:Char60Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="street" type="de-mail:Char100Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="locationOfBirth" type="de-
mail:Char100Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="dateOfBirth" type="de-mail:Char10Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="locality" type="de-mail:Char100Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="country" type="de-mail:Char2Type"
                        minOccurs="1" maxOccurs="1">
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
                    </xs:element>
                    <xs:element name="age" type="de-mail:Char10Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="de-mail-address" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="Address" maxOccurs="1" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Adresskarte einer natuerlichen
Person</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="personalTitle" type="de-mail:Char40Type"
                        minOccurs="0" maxOccurs="1">
                    </xs:element>
                    <xs:element name="surname" type="de-mail:Char120Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="givenname" type="de-mail:Char80Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="street" type="de-mail:Char100Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="locality" type="de-mail:Char100Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="country" type="de-mail:Char2Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="de-mail-address" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="1">
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="Age" maxOccurs="1" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Alterskarte</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="age" type="de-mail:Char10Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                    <xs:element name="de-mail-address" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="AgeOver16" maxOccurs="1" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Alterskarte</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="over16" type="de-mail:BooleanType"
minOccurs="1"
                        maxOccurs="1">
                    </xs:element>
                    <xs:element name="de-mail-address" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="AgeOver18" maxOccurs="1" minOccurs="0">
            <xs:annotation>
```


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

```
                <xs:documentation>Alterskarte</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="over18" type="de-mail:BooleanType"
minOccurs="1"
                        maxOccurs="1">
                    </xs:element>
                    <xs:element name="de-mail-address" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="DeMailAddress" maxOccurs="1" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Adresskarte</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="de-mail-address" type="de-
mail:Char255Type"
                        minOccurs="1" maxOccurs="1">
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
    </xs:choice>
  </xs:complexType>
</xs:schema>
```

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Dokumentenablage Modul
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 5
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

1 Einleitung

Dieses Modul beschreibt die Dokumentstruktur der Module der Dokumentenablage. Das Modul ist Bestandteil der [TR DM].

Die Dokumentenablage (DA) bietet dem Nutzer eine Möglichkeit zur sicheren Ablage von elektronischen Dokumenten unter Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit der ablegten Dokumente.

2 Dokumentenübersicht

2.1 Funktionale Anforderungen

Die funktionalen Anforderungen an die DA werden in [TR DM DA FU] beschrieben, sowie die besonderen nicht-funktionalen Anforderungen.

2.2 IT-Sicherheit

Die spezifischen Anforderungen an die Sicherheit die DA werden in [TR DM DA Si] beschrieben.

2.3 Funktionsprüfung

Die Spezifikation der Prüffälle für die Funktionsprüfung erfolgt in [TR DM DA FU-PS].

Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Dokumentenablage Funktionalitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 5.1
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die funktionalen Spezifikationen der Dokumentenablage und ist Bestandteil von [TR DM DA M].

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2 Funktionale Anforderungen

Nachfolgend werden die funktionalen Anforderungen beschrieben, die erfüllt werden müssen, damit ein Dienst zur Ablage und Verwaltung von elektronischen Dokumenten und anderen Dateien als De-Mail-Dienst anerkannt werden kann.

Über den De-Mail-Versanddienst empfangene Dokumente kann der Nutzer von seinem De-Mail-Postfach in seine DA kopieren. Weiterhin kann der Nutzer Dokumente aus seiner DA über den PVD an Dritte verschicken (vgl. [TR DM PVD FU]).

Alle Aktionen sind in geeigneter Weise zu protokollieren.

2.1 Zugriff auf Dokumente in der DA

Ein Nutzer darf auf Dokumente in seiner DA nur Zugriff erhalten, wenn er sich vorher erfolgreich an seinem De-Mail-Konto angemeldet hat.

2.1.1 Authentisierung und Autorisierung

Nach erfolgreicher Anmeldung am De-Mail-Konto hat der Nutzer Zugriff auf alle Dokumente und Kategorien in der seinem Konto zugeordneten DA (vgl. Abschnitt 2.2.1).

Um auf den Inhalt und die Metadaten eines Dokumentes oder einer Kategorie zugreifen zu können, muss der Nutzer beim Einstellen festlegen können, für welche Zugriffsoperationen welches Authentisierungsniveau notwendig sein soll. Legt der Nutzer die Berechtigungen nicht fest, so wird automatisch das Authentisierungsniveau verwendet, mit dem der Nutzer zu diesem Zeitpunkt angemeldet ist. Ein Zugriff auf das Dokument erfordert sodann eine Anmeldung des Nutzers mit mindestens diesem Authentisierungsniveau.

Das Authentisierungsniveau für einen Zugriff auf ein Dokument kann durch den Nutzer herabgestuft werden, wenn sein aktuelles Authentisierungsniveau einen Zugriff auf das Dokument erlaubt. Das minimale Authentisierungsniveau eines Dokuments kann durch den Nutzer bis auf das Niveau erhöht werden, das seinem aktuellen Authentisierungsniveau entspricht.

2.1.2 Zugriffsoperationen

Folgende Zugriffsoperationen auf Dokumente müssen in Abhängigkeit von den jeweiligen Authentisierungsniveaus von der DA unterstützt werden:

- Lesen
- Schreiben (und Löschen)
  Unter „Schreiben“ fallen das Einstellen von neuen Dokumenten und das Ändern von vorhandenen Dokumenten.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2.2 Ablage von Dokumenten

2.2.1 Kategorien

Um das spätere Suchen und Auffinden von Dokumenten zu erleichtern, muss es in der DA möglich sein, Dokumente bestimmten Kategorien zuzuordnen, die bspw. als Ordner in einer Hierarchie abgebildet werden können. Es müssen mindestens zwei vordefinierte Kategorien existieren. Eine Standardkategorie, der Dokumente zugeordnet werden, z.B. wenn vom Nutzer noch keine Kategorie erstellt wurde, sowie die Kategorie „Papierkorb“, der Dokumente zugeordnet werden, die gelöscht werden sollen.

Kategorien können hierarchisch in mehreren Ebenen gestaffelt werden.

2.2.2 Erstellung neuer Kategorien

Bei der Erstellung einer neuen Kategorie muss geprüft werden, ob bereits eine Kategorie mit dem selben Namen existiert und ob für den Nutzer in der übergeordneten Kategorie Schreibrechte bestehen.

Das Authentisierungsniveau für die neue Kategorie muss mindestens dem der übergeordneten Kategorie entsprechen. In Unterkategorien kann das geforderte Authentisierungsniveau nur erhöht werden.

2.2.3 Einstellen neuer Dokumente

Der Nutzer kann neue Dokumente

- von seinem Rechnersystem in die DA hochladen,
- eine Nachricht aus seinem Postfach in die DA speichern oder,
- einen Anhang einer Nachricht aus dem Postfach in der DA ablegen.

Die Dokumente können einer oder mehreren Kategorien zugeordnet werden. Wird für ein Dokument keine Kategorie ausgewählt, so wird es der Standardkategorie zugeordnet. Der Nutzer muss die notwendige Zugriffsberechtigung für die Kategorie(n) besitzen.

Das Dokument wird durch den DMDA einer Prüfung auf Schadsoftware unterzogen. Bei einer positiven Prüfung wird das Dokument nicht gespeichert, der Nutzer erhält eine entsprechende Meldung.

Wenn nicht genügend freier Speicherplatz verfügbar ist, muss der Nutzer per Meldung informiert werden.

Für das Dokument wird standardmäßig folgende Berechtigung gesetzt:

- Lesen: Dies ist gestattet für den angemeldeten Nutzer mit dem aktuellen Authentisierungsniveau,

- Schreiben: Dies ist gestattet für den angemeldeten Nutzer mit dem aktuellen Authentisierungsniveau. Die Berechtigung des Dokuments muss mindestens dem geforderten Authentisierungsniveau der Kategorie entsprechen, der das Dokument zugeordnet wird.

Es wird für jede eingestellte Datei ein Hashwert berechnet und gespeichert.

2.2.4 Herunterladen von Dokumenten

Der Nutzer darf nur Dokumente herunterladen können, für die er die Zugriffsberechtigung zum Lesen besitzt.

Vor dem Herunterladen muss der DMDA das Dokument auf Schadsoftware prüfen. Bei einer positiven Prüfung ist der Nutzer per Meldung zu informieren.

Der DMDA muss den Hashwert des Dokumentes prüfen. Stimmt der neu berechnete Hashwert nicht mit dem ursprünglichen Wert überein, so ist der Nutzer per Meldung zu informieren.

Danach ist das Herunterladen des Dokuments möglich.

2.2.5 Umbenennen von Dokumenten und Kategorien

Dokumente und Kategorien müssen umbenannt werden können.

Die Umbenennung findet statt, wenn der Nutzer schreibend auf das Dokument oder die Kategorie zugriffsberechtigt ist und der neue Name in der übergeordneten Kategorie noch nicht vorhanden ist.

Der Nutzer kann Dokumente und Kategorien nur umbenennen, wenn er die notwendige Berechtigung besitzt.

2.2.6 Löschen von Dokumenten

Der Nutzer kann Dokumente nur löschen, wenn er die notwendige Berechtigung besitzt.

Für die Löschung von Dokumenten ist ein zweistufiges Verfahren vorzusehen. Im ersten Schritt werden die Dokumente in die Kategorie „Papierkorb“ verschoben. Alle Zuordnungen zu anderen Kategorien werden entfernt. Im zweiten Schritt können die Dokumente aus der Kategorie „Papierkorb“ endgültig gelöscht werden.

Bei der endgültigen Löschung müssen die Dokumente sicher gelöscht werden. Alle Informationen zu den Dokumenten sind vollständig zu entfernen. Dies betrifft auch die Metadaten der Dokumente.

Der Nutzer muss ein oder mehrere Dokumente löschen können.

2.2.7 Löschen von Kategorien

Zur Löschung einer Kategorie muss der Nutzer die notwendige Berechtigung haben.

Die zu löschende Kategorie darf keine untergeordneten Kategorien oder zugeordnete Dateien enthalten.

Die vordefinierten Kategorien (Standardkategorie und„Papierkorb“) können nicht gelöscht werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2.2.8 Änderung der Berechtigungen für Dokumente und Kategorien

Bei der Änderung einer Berechtigung muss geprüft werden, ob

- das Authentisierungsniveau des Nutzers ausreichend ist, um die Dokumente oder Kategorie zu ändern.
- das aktuelle Authentisierungsniveau des Nutzers mindestens dem Authentisierungsniveau entspricht, das gesetzt werden soll.

Wenn die Bedingungen erfüllt sind, werden die Berechtigungen innerhalb der Metadaten entsprechend geändert.

Bei der rekursiven Änderung von Berechtigungen (wenn eine Kategorie geändert wird, die weitere Kategorien oder Dateien enthält) gelten folgende Regeln:

- Wird das Authentisierungsniveau einer Kategorie erhöht, so werden die Berechtigungen aller darin enthaltenen Dokumenten und Kategorien erhöht, für die das Authentisierungsniveau „normal“ benötigt wird. Die Berechtigungen aller anderen Dokumenten und Kategorien bleiben bestehen.
- Wenn das Authentisierungsniveau herabgesetzt wird, können die Berechtigungen aller enthaltenen Dokumente und Kategorien bestehen bleiben oder auf Wunsch ebenfalls herabgesetzt werden.

2.3 Suchen und Finden

Die Suchfunktion muss sowohl die Suche nach Kriterien wie Dateinamen und Kategorien als auch nach Dokumentinhalten von Standard-Dateiformaten in nicht durch den Nutzer zusätzlich verschlüsselten Dokumenten ermöglichen.

Suchkriterien können sein:

- Teile des Namens oder vollständiger Name der Datei, einschließlich Datei-Endung
- Teile des Namens oder vollständiger Name der Kategorie
- Datei-MIME-Typ (Format)
- Inhalt der Datei (Text)
- Einschränkungen hinsichtlich der Kategorien
- Datum und Zeit der letzten Änderung in der DA

Der Suchindex muss verschlüsselt gespeichert werden.

Die Ergebnisliste muss beinhalten:

- bei Kategorien:
  - Kategorie-Pfad inkl. aller Kategoriebezeichnungen
  - URL
- bei Dokumenten
  - Kategorie-Pfad inkl. aller Kategoriebezeichnungen
  - Dateiname
  - Datum der letzten Änderung in der DA
  - URL

Bei der Suche wird beachtet, dass ausschließlich die Dokumente oder Kategorien berücksichtigt werden, die für den Nutzer und seinem derzeitigen Authentisierungsniveau lesbar sind.

Die Ergebnisliste muss nach Abschluss der Suche durch den DMDA sicher gelöscht werden.

2.4 Protokollierung der Aktivitäten

Um Anwendungsfehler oder Missbrauch feststellen zu können, müssen alle Aktionen protokolliert werden, die Dokumente und Kategorien betreffen.

Bei der Protokollierung der Aktionen ist sicher festzuhalten:

- Nutzerkennung
- Authentisierungsniveau des Nutzers
- Neue Metadaten
- Datum und Uhrzeit.

Der Nutzer kann auf Wunsch ein Protokoll über die Aktivitäten in der DA anfordern, das mit einer qualifizierten Signatur des DMDA versehen ist. Das Protokoll kann dem Nutzer mittels Anhang einer De-Mail oder als Download zur Verfügung gestellt werden.

Das Protokoll muss beinhalten:

- eine Liste der eingestellten Dokumente mit dem jeweiligen Hashwert und dem Namen des Hashalgorithmus,
- das aktuelle Authentisierungsniveau,
- eine Änderungshistorie der Dokumente.

Das Protokoll kann anhand folgender Merkmale eingeschränkt werden:

- Kategorie,
- Dateinamen,
- Zeitraum.

2.5 Verschlüsselung

Alle in der DA von De-Mail abgelegten Dokumente müssen durch den DMDA verschlüsselt abgelegt werden. Der DMDA hat zudem Sorge dafür zu tragen, dass vom Nutzer aus der DA angeforderten Dokumente entschlüsselt werden.

Darüber hinaus muss der Nutzer bei Bedarf auch seinerseits zusätzlich verschlüsselte Dokumente ablegen können. Der DMDA sollte hierzu geeignete Software empfehlen oder kann diese selbst zur Verfügung stellen.

2.6 Konfiguration

Die Konfiguration der DA sollte der Nutzer über eine Web-Oberfläche durchführen können.

Folgende Merkmale müssen je Dokument bzw. je Kategorie konfigurierbar sein:

- Erlaubte Zugriffsoperationen (vgl. Abschnitt 2.1.2)
- Minimales Authentisierungsniveau für die jeweilige Zugriffsoperation (vgl. Abschnitt 2.1.1)

3 Nicht-funktionale Anforderungen

Die in der DA eingestellten Dokumente müssen dem Nutzer vollständig und unverändert zur Verfügung gestellt werden, bis der Nutzer die betreffenden Dokumente selbst löscht oder das zugehörige De-Mail-Konto aufgelöst worden ist.

Jeder Nutzer eines De-Mail-Kontos hat einen minimalen Speicherplatz pro Konto zur Verfügung. Ist dieser Speicher noch nicht durch Daten des Nutzers belegt, muss ein Dokument in der DA abgelegt werden können. Der Nutzer muss gewarnt werden, falls seine DA nur noch über 10% freien Speicher verfügt, gemessen am maximal vorgesehenen Speicherplatz des De-Mail-Kontos.

4 Datenstrukturen

In diesem Abschnitt werden die in der DA verwendeten Datenstrukturen beschrieben. Es werden die Elemente der Datenstrukturen bestimmt und abstrakt definiert.

Die formale Definition der Datenstrukturen darf jeder DMDA selbst vornehmen.

4.1 Datei

In der DA eines Nutzers können beliebige Dateien gespeichert werden.

Zu jeder Datei werden die nachfolgend definierten Metadaten in der DA des Nutzers abgelegt.

Nr	*Bezeichnung*	*Werte*	*Bemerkung*
1	Nutzerkennung	Kennung und zugehörige De-Mail-Adresse	Kennzeichnung des Besitzers der Datei
2	Verweis auf Datei	Dateiname	Dateiname ist in der zugehörigen Kategorie eindeutig
3	Authentisierungs-Niveau	Normal/Hoch	Authentisierungsniveau des Nutzers bei der letzten Änderung
4	Datum und Zeit der letzten Änderung in der DA	Datum & Zeit	sekundengenau
5	Kategorie-Zuordnung	Numerische Schlüsselwerte (siehe 4.2)	Optional, Mehrfachbelegung
6	Hashwert der Datei	Message-Digest	
7	Größe der Datei	Numerischer Wert	
8	Autorisierter Nutzer	Kennung oder zugehörige De-Mail-Adresse	
9	Mindest-Auth.-Niveau - Lesen	Normal/Hoch	
10	Mindest-Auth.-Niveau – Schreiben/Löschen	Normal/Hoch	

Tabelle 1: Metadaten einer Datei

Der autorisierte Nutzer ist immer identisch mit der Nutzerkennung aus Tabelle 1. Die Metadaten werden von der DA des Nutzers erzeugt. Für jede einzelne Datei werden neue Metadaten definiert. Bei Änderungen oder Löschung der Datei oder der zugehörigen Zugriffsrechte werden die Metadaten ebenfalls geändert bzw. gelöscht.

4.2 Kategorien

Kategorien sind eigene Objekte, die hierarchisch angeordnet werden können. Sie können beispielsweise als Ordner oder Verzeichnisse abgebildet werden.

Jede Kategorie wird mindestens durch folgende Daten beschrieben:

Nr	*Bezeichnung*	*Wert*	*Bemerkung*
1	Schlüsselwert	Numerisch	Eindeutiger Wert in der DA des Nutzers (für die Zuordnung zur Datei)
2	Bezeichnung	Text	
3	Übergeordnete Kategorie-Ebene	Numerisch	Optional: Referenz zu Nr.1

Tabelle 2: Daten der Kategorie (Teil 1)

Zusätzlich muss zu jedem Kategorie-Objekt folgende Ausprägung von Metadaten existieren:

Nr	*Bezeichnung*	*Wert*	*Bemerkung*
1	Nutzerkennung	Kennung und zugehörige De-Mail-Adresse	Kennzeichnung des Besitzers der Kategorie
2	Authentisierungs-Niveau	Normal/Hoch	Authentisierungsniveau des Nutzers bei der letzten Änderung
3	Datum und Zeit der letzten Änderung	Datum & Zeit	Sekundengenau für jede Kategorie (unabhängig von Dateizuordnungen)
4	Autorisierter Nutzer	Kennung oder zugehörige De-Mail-Adresse	
5	Mindest-Auth.-Niveau - Lesen	Normal/Hoch	
6	Mindest-Auth.-Niveau – Ändern/Löschen	Normal/Hoch	

Tabelle 3: Metadaten der Kategorie (Teil 2)

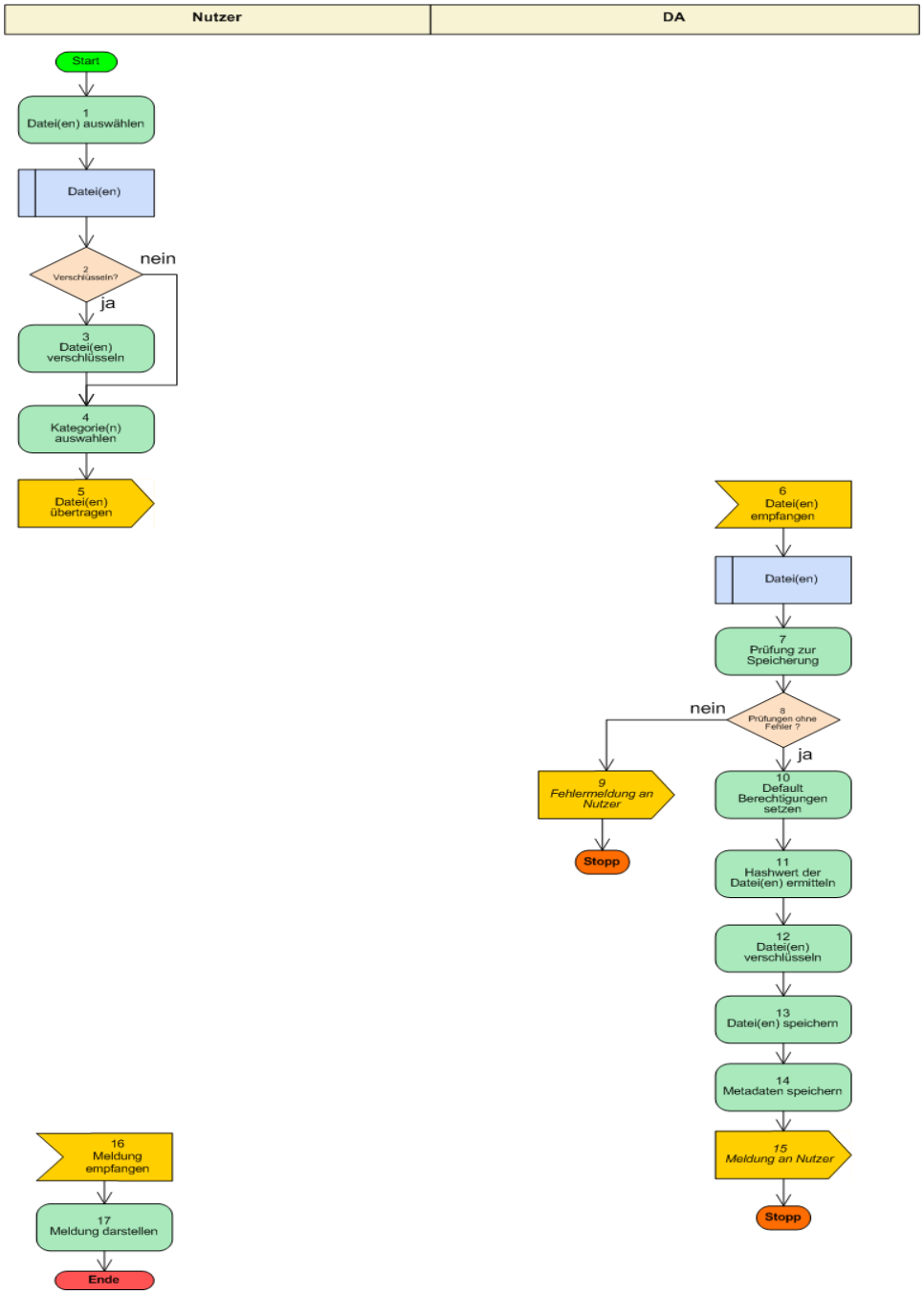
Der autorisierte Nutzer ist immer identisch mit der Nutzerkennung aus Tabelle 3.

4.3 Meldungen

Meldungen sind Informationen der DA an den Nutzer und können in Abhängigkeit der Benutzerschnittstelle, die der Nutzer verwendet, unterschiedlich dargestellt und bekannt gemacht werden. Bspw. können sie im Webbrowser dargestellt oder auch als Meldungs-Nachricht (siehe [TR DM FU PVD]) in das Postfach des Nutzers übermittelt werden.

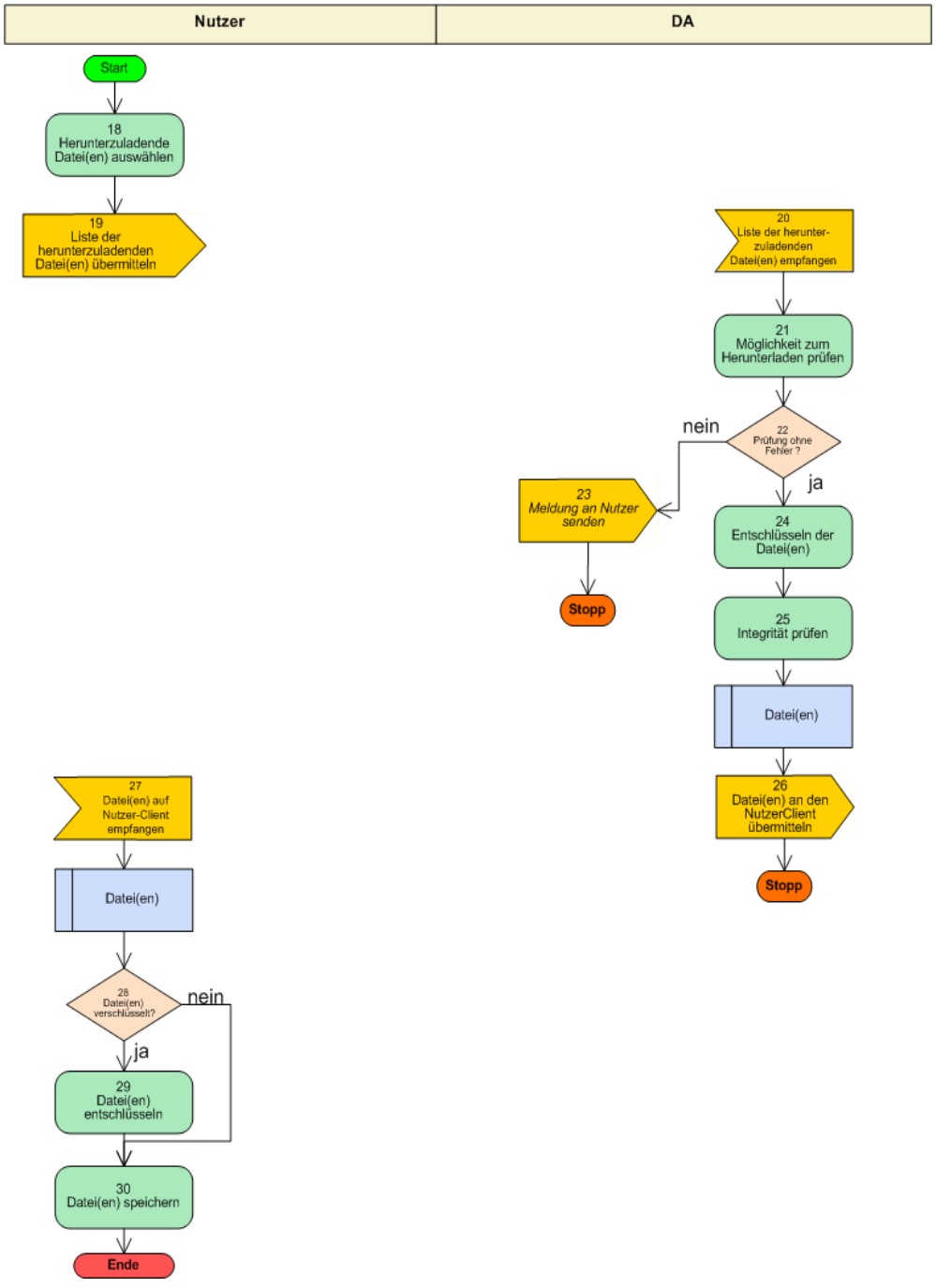
5 Aktivitätsdiagramm

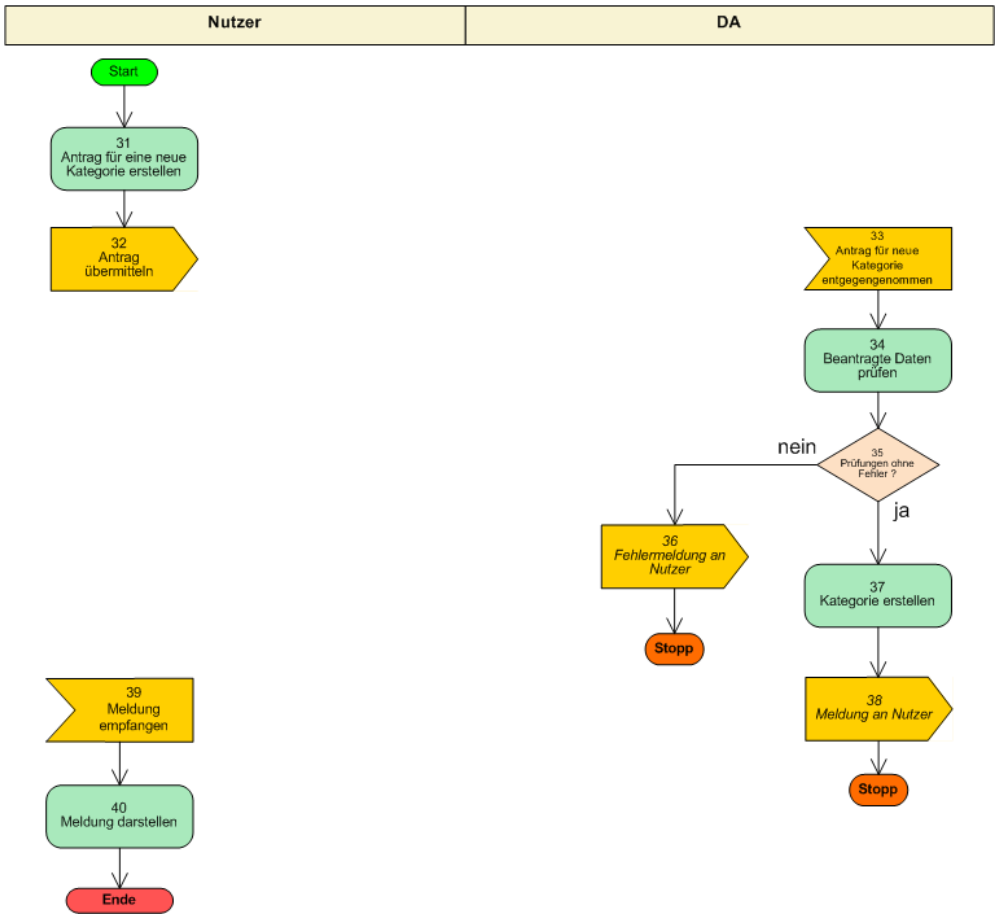
In diesem Abschnitt wird der funktionale Ablauf der DA für Upload, Download sowie zur Verwaltung und Suche von Dateien (in diesem Zusammenhang die Dokumente) in einem Aktivitätsdiagramm dargestellt. Eine Legende zu den Symbolen des Aktivitätsdiagramms findet sich in Abschnitt 8. Eine detaillierte technisch-funktionale Beschreibung der einzelnen Aktionen bzw. Schritte des Aktivitätsdiagramms erfolgt im Abschnitt 6.



Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

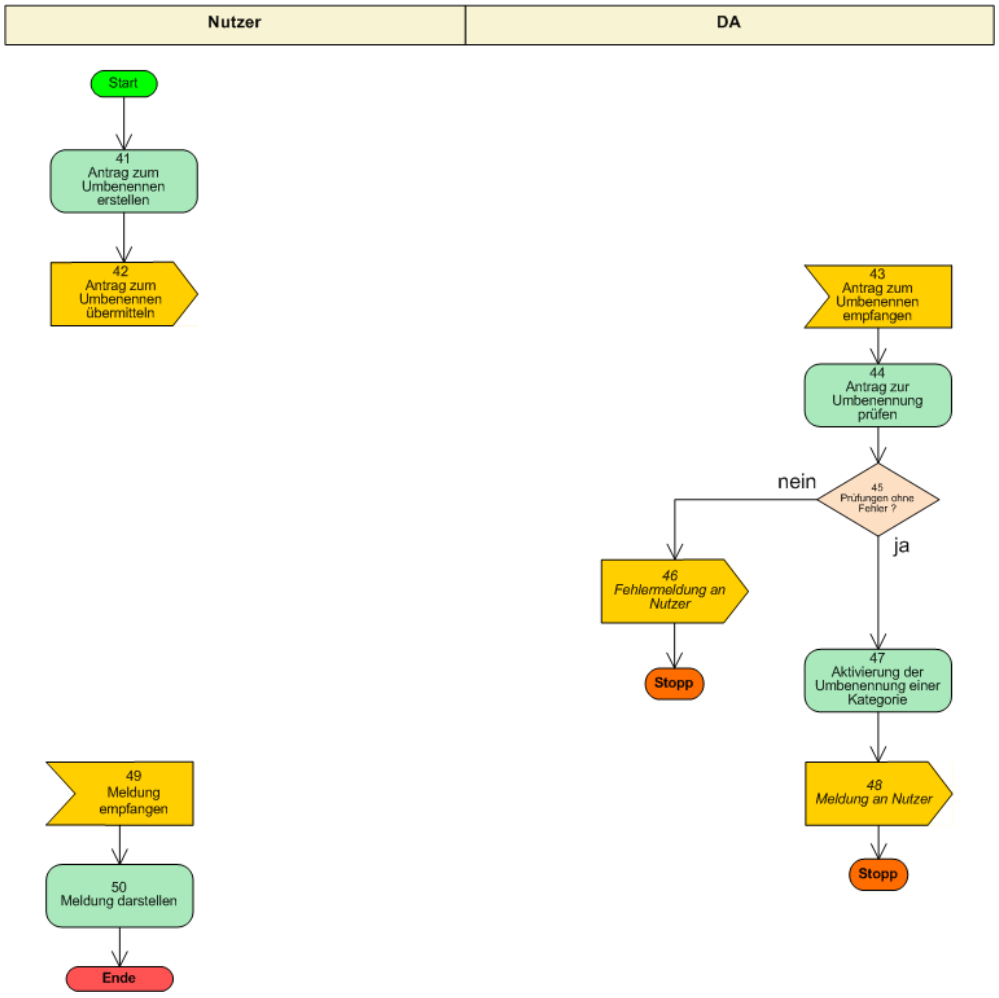
5 Aktivitätsdiagramm

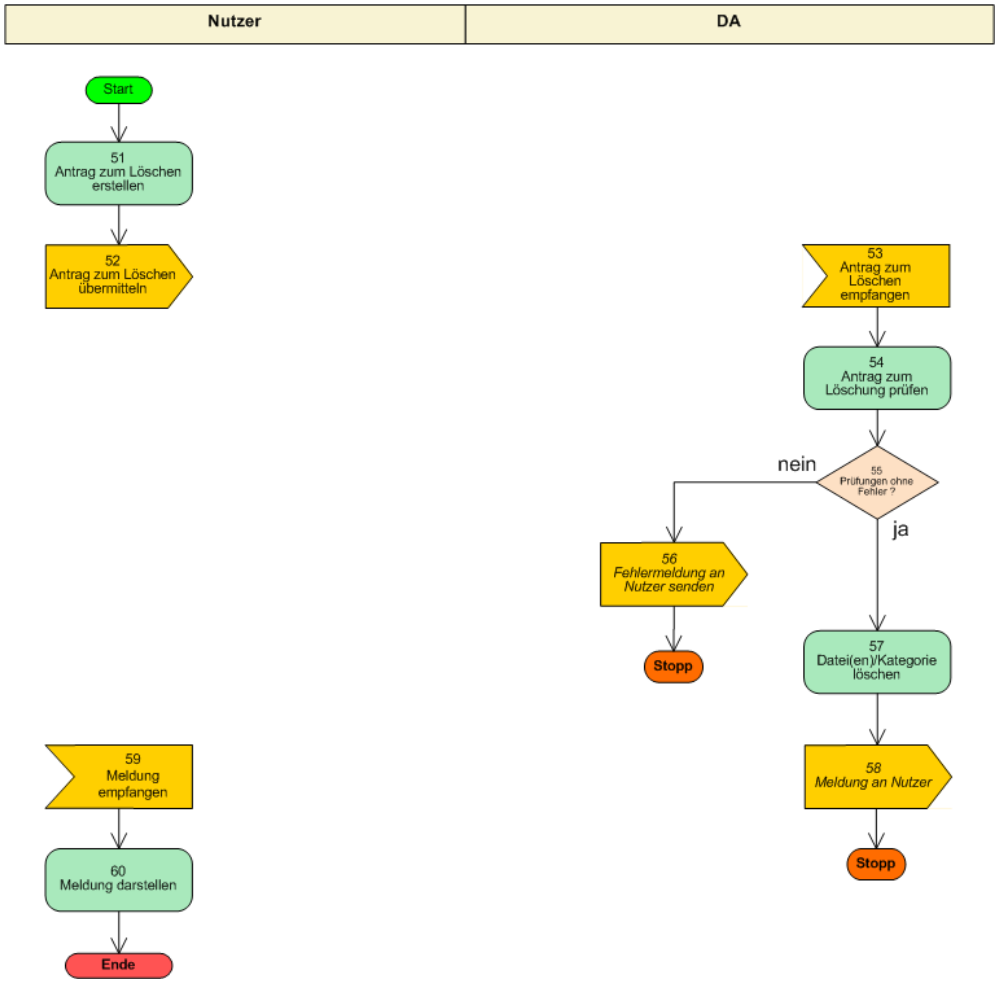




Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

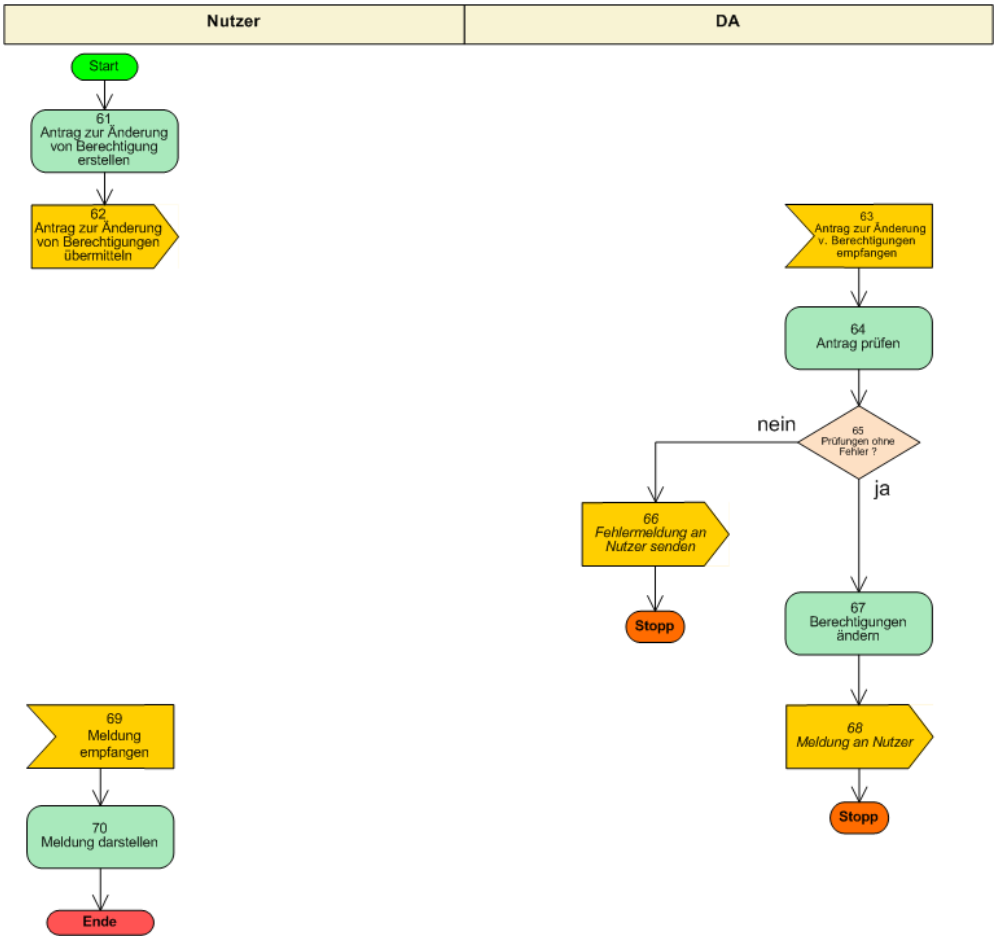
5 Aktivitätsdiagramm



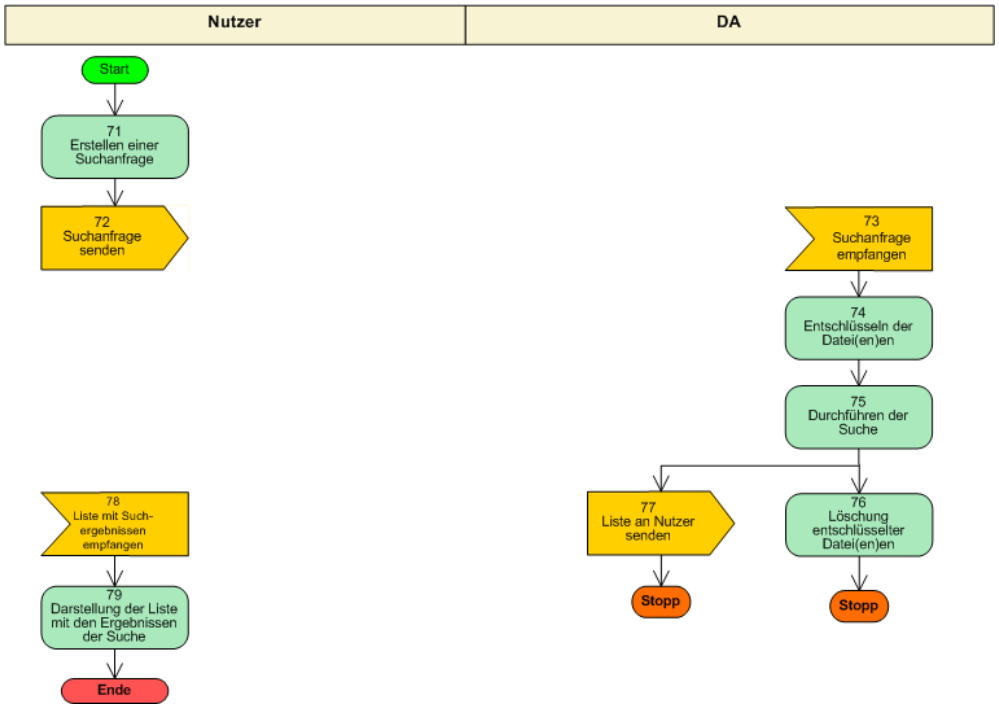


Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

5 Aktivitätsdiagramm



5 Aktivitätsdiagramm



Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

6 Funktionale Beschreibung

Im Folgenden werden die einzelnen Schritte des Aktivitätsdiagramms aus Abschnitt 5 für Upload, Download sowie zur Verwaltung und Suche von Dokumenten und Dateien beschrieben. Eine Beschreibung, wie die einzelnen Schritte strukturiert sind, findet sich in Abschnitt 9. Alternativ zu der unten dargestellten Schrittfolge kann eine Anmeldung auch vor Schritt 1 erfolgen, z.B. bei Web-basierten Anwendungen. Funktionen, die vom System wiederholt ausgeführt werden oder vom Nutzer interaktiv aufgerufen werden können, wenn er an seiner DA angemeldet ist, werden in Abschnitt 7 dargestellt. Die referenzierten Funktionen des Account-, Schadsoftware- und Zeitdienstes werden in [TR DM ACM FU] und [TR DM IT-BInfra FU] erläutert.

6.1 Upload und Download von Dateien

6.1.1 Upload einer Datei in die DA

Schritt 1	**Datei(en) auswählen**
Kurzbeschreibung	Der Nutzer wählt die Datei(en) im lokalen System, die er in der DA speichern möchte.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Datei(en) (Die ausgewählten Dateien können bereits durch den Nutzer verschlüsselt worden sein)
Ergebnis	Datei(en) ausgewählt
Nachbedingung	
Ablauf	Auswahl der Datei(en) in einem lokal verfügbaren Speicherbereich
Fehlerfälle	FC-01: Keine Auswahl getroffen
Schritt 2	**Entscheidungsknoten: Soll die Datei(en) verschlüsselt werden, bevor sie auf dem Server gespeichert wird**
Kurzbeschreibung	Durch den Nutzer wird entschieden, ob die Datei(en) verschlüsselt werden soll.
ja	Schritt 3
nein	Schritt 4
Schritt 3	**Datei(en) auf Nutzer-Seite verschlüsseln**
Kurzbeschreibung	Die Datei(en) werden auf Seite des Nutzers verschlüsselt.
Akteure	Nutzer

Auslöser	Nutzer
Vorbedingung	
Input	Verschlüsselungsmethode Verschlüsselungsschlüssel des Nutzers Datei(en)
Ergebnis	Verschlüsselte Datei(en)
Nachbedingung	
Ablauf	Es wird mit einem auf dem Nutzer-System verfügbaren Verschlüsselungstool eine Verschlüsselung der Datei vorgenommen.
Fehlerfälle	FC-01: kein geeigneter Verschlüsselungsschlüssel vorhanden FC-02: Verschlüsselungsmethode wird nicht unterstützt
Schritt 4	**Kategorie(n) auswählen**
Kurzbeschreibung	Es wird definiert, zu welchen Kategorie(n) und welcher Kategorie-Ebene die Datei(en) zugeordnet werden sollen. Hinweis: Welche Kategorien existieren, kann über die Suche-Funktion in Abschnitt 6.3 erfahren werden.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Kategorie-Ebene Kategorie(n)
Ergebnis	Zuordnung der Kategorie(n) bzw. der Kategorie-Ebene(n) getroffen.
Nachbedingung	
Ablauf	Der Nutzer wählt die Kategorie(n) aus, die der heraufzuladenden Datei(en) zugeordnet werden sollen.
Fehlerfälle	FC-01: Keine Kategorie(n) ausgewählt. FC-02: Kategorie vom Typ Papierkorb kann nicht gewählt werden.
Schritt 5	**Datei(en) auf den De-Mail-Server übertragen**
Kurzbeschreibung	Die Datei(en) werden an den DA-Dienst übertragen, der diese entgegennimmt.
Akteure	Nutzer, DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut Kategorie(n) und Datei(en) ausgewählt.
Input	Kategorie(n) und jeweilige Kategorie-Ebenen

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Datei(en)
Ergebnis	Datei(en) auf Seite des Nutzers versendet.
Nachbedingung	
Ablauf	Der Nutzer initiiert den Upload der Datei(en). Der DA-Dienst nimmt die Daten entgegen.
Fehlerfälle	FC-01: DA hat die Datei(en) nicht angenommen.
Schritt 6	**Datei(en) auf dem De-Mail-Server empfangen**
Kurzbeschreibung	Die Datei(en) werden durch den DA-Dienst empfangen.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut.
Input	Kategorie(n) und jeweilige Kategorie-Ebene Datei(en)
Ergebnis	Datei(en) sind auf Seiten des DA-Dienstes entgegengenommen worden.
Nachbedingung	
Ablauf	Der DA-Dienst nimmt die Daten entgegen.
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto angemeldet.
Schritt 7	**Prüfung zur Speicherung**
Kurzbeschreibung	Der Upload wird hinsichtlich der Berechtigungen geprüft.
Akteure	DA-Dienst, Account-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Kategorie(n) und zugehörige Kategorie-Ebenen Datei(en) Authentisierungsniveau des Nutzers
Ergebnis	Prüfungen sind abgeschlossen
Nachbedingung	
Ablauf	• Prüfung, ob die Kategorien in der jeweiligen Kategorie-Ebenen existieren, • Prüfung, ob die Berechtigungen zum Schreiben gegeben sind, • Prüfung, ob die Datei(en) nicht bereits mit dem gleichen Dateinamen in den Kategorien existieren, • Prüfung, ob ausreichend Speicher in der DA verfügbar ist, • Aufruf der Funktion 2.

Fehlerfälle	FC-01: Kategorien nicht existent FC-02: Berechtigungen reichen nicht aus FC-03: Dateiname ist bereits in einer der angegebenen Kategorien existent FC-04: Zu wenig Speicherplatz FC-05: Datei(en) enthalten Malware
Schritt 8	**Entscheidungsknoten: positiv abgeschlossene Prüfung**
Kurzbeschreibung	Existieren aus Schritt 7 keine Fehler, gilt die Prüfung als positiv abgeschlossen.
ja	Schritt 10
nein	Schritt 9
Schritt 9	**Fehlermeldung erstellen**
Kurzbeschreibung	Es wird eine Fehlermeldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Fehlercode
Ergebnis	Fehlermeldung ist erstellt und an den Nutzer gesandt.
Nachbedingung	Stopp
Ablauf	• Der Fehlermeldung wird aus dem Fehlercode abgeleitet. • Die Fehlermeldung wird an den Nutzer gesandt.
Fehlerfälle	
Schritt 10	**Default-Berechtigungen setzen**
Kurzbeschreibung	Für die Datei(en) werden die Default-Berechtigungen gesetzt.
Akteure	DA-Dienst, Account-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Datei(en) Authentisierungsniveau
Ergebnis	Default-Berechtigungen sind gesetzt.
Nachbedingung	
Ablauf	Durch das System werden die Standard-Werte für die Berechtigungen gesetzt: • Lesen – gestattet für angemeldeten Nutzer mit aktuellen Authentisierungsniveau,

	• Schreiben – gestattet für angemeldeten Nutzer mit aktuellen Authentisierungsniveau • Die Berechtigung des Dokuments muss mindestens dem geforderten Authentisierungniveau der Kategorie entsprechen, in die das Dokument eingefügt wird.
Fehlerfälle	
Schritt 11	**Hashwerte der Datei ermitteln**
Kurzbeschreibung	Es werden die Hashwerte der Datei(en) ermittelt.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Datei(en)
Ergebnis	Ein Hashwert für die Metadaten wurde pro Datei ermittelt.
Nachbedingung	
Ablauf	Es werden Hashwerte der Datei(en) ermittelt, der in den Metadaten der jeweiligen Datei gespeichert wird.
Fehlerfälle	
Schritt 12	**Datei(en) durch den DMDA verschlüsseln**
Kurzbeschreibung	Die Datei(en) werden mittels einem DMDA-Schlüssel verschlüsselt
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Unverschlüsselte Datei(en), Verschlüsselungsschlüssel (DMDA)
Ergebnis	Die Datei(en) liegen nur noch als verschlüsselte Datei auf Seite des DMDA vor.
Nachbedingung	
Ablauf	• Verschlüsselung der Datei(en) • Unverschlüsselte Datei(en) im Speicher löschen
Fehlerfälle	FC-01: kein DMDA-bezogenere Verschlüsselungsschlüssel vorhanden
Schritt 13	**Datei(en) speichern**
Kurzbeschreibung	Die verschlüsselten Datei(en) werden in der DA gespeichert.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Kategorie-Ebene, Kategorie(n)

	Verschlüsselte Datei(en)
Ergebnis	Verschlüsselte Datei(en) im DA des Nutzers gespeichert.
Nachbedingung	
Ablauf	• Die Datei(en) werden im DA gespeichert. • Ist nur noch <10 % des Speicherplatzes innerhalb der DA frei, ist eine Meldung an den Nutzer zu senden (Funktion 3).
Fehlerfälle	
Schritt 14	**Meta-Daten speichern**
Kurzbeschreibung	Die Metadaten zu den Datei(en) werden gespeichert.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Dateizuordnung Authentisierungsniveau Berechtigungen Datum und Zeit zum Zeitpunkt der Speicherung im De-Safe Hashwerte der Datei(en)
Ergebnis	Die Metadaten wurden in der DA des Nutzers gespeichert und der jeweiligen Datei(en) zugeordnet.
Nachbedingung	Funktion 1
Ablauf	• Die einzelnen Attribute der Metadaten werden genommen und als Metadatensatz gespeichert. • Es erfolgt eine Meldung an den Nutzer.
Fehlerfälle	
Schritt 15	**Meldung an den Nutzer**
Kurzbeschreibung	Es wird eine Erfolgsmeldung an den Nutzer geschickt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Erfolgsmeldung
Ergebnis	Eine Erfolgsmeldung wurde erstellt und an den Nutzer übermittelt.
Nachbedingung	
Ablauf	• Es wird eine Meldung erstellt. • Diese Meldung wird an den Nutzer übermittelt.

Fehlerfälle	
Schritt 16	**Meldung empfangen**
Kurzbeschreibung	Eine Meldung wird auf Nutzerseite empfangen.
Akteure	Nutzer
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Meldung
Ergebnis	Die Meldung wurde auf Nutzerseite empfangen.
Nachbedingung	
Ablauf	Die Meldung wird vom Nutzer entgegengenommen.
Fehlerfälle	
Schritt 17	**Meldung darstellen**
Kurzbeschreibung	Die Meldung wird auf Seite des Nutzers dargestellt.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Meldung
Ergebnis	Die Darstellung der Meldung erfolgte.
Nachbedingung	
Ablauf	• Die Meldungsinformationen werden durch die Client-Komponente interpretiert. • Die Darstellung erfolgt entsprechend den Inhalten der Meldung (Fehler, Erfolg).
Fehlerfälle	

Tabelle 4: Schritte zum Upload von Dateien

6.1.2 Download von Dateien

Schritt 18	**Herunterzuladende Datei(en) auswählen**
Kurzbeschreibung	Der Nutzer wählt die Dateien, die aus seiner DA auf den Speicher des Nutzersystems als Kopie heruntergeladen werden sollen.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Zusammenstellung der Liste, ggf. über die Suche-Funktion (siehe 6.3)

Input	Datei(en) und die zugehörigen Kategorie-Ebenen und Kategorien
Ergebnis	Liste der herunterzuladenden Dateien
Nachbedingung	
Ablauf	Erstellung der Liste der herunterzuladenden Dateien mit Adressierung (Kategorie)
Fehlerfälle	FC-01: Liste ist leer
Schritt 19	**Liste der herunterzuladenden Dateien übermitteln**
Kurzbeschreibung	Die Liste wird durch den Nutzer an den DA-Dienst übergeben.
Akteure	Nutzer, DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Liste der herunterzuladenden Dateien mit Adressierung (Kategorie)
Ergebnis	Die Liste der herunterzuladenden Dateien wurde an den DA-Dienst übergeben.
Nachbedingung	
Ablauf	Der Nutzer übergibt die Liste an den DA-Dienst.
Fehlerfälle	FC-01: keine Liste übermittelt FC-02: Liste ist leer
Schritt 20	**Liste der herunterzuladenden Dateien empfangen**
Kurzbeschreibung	Die Liste wird durch den DA-Dienst empfangen.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Liste der herunterzuladenden Dateien mit Adressierung (Kategorie)
Ergebnis	Die Liste der herunterzuladenden Dateien wurde vom DA-Dienst empfangen.
Nachbedingung	
Ablauf	Die Liste wird durch den DA-Dienst zur weiteren Verarbeitung empfangen.
Fehlerfälle	FC-01: keine Liste übermittelt FC-02: Liste ist leer FC-03: Nutzer am De-Mail-Konto nicht angemeldet
Schritt 21	**Möglichkeit zum Herunterladen prüfen**

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Kurzbeschreibung	Die Liste zum Herunterladen von Dateien wird hinsichtlich der Berechtigungen geprüft.
Akteure	DA-Dienst, Account-Dienst
Auslöser	Nutzer
Vorbedingung	Liste der herunterzuladenden Dateien wurde an den DA-Dienst übertragen.
Input	Liste der herunterzuladenden Dateien Authentisierungsniveau
Ergebnis	Prüfungen sind abgeschlossen.
Nachbedingung	
Ablauf	• Prüfung, ob die Dateien in den jeweiligen angegebenen Kategorie-Ebene existieren • Prüfung, ob die Berechtigung zum Lesen mit dem Authentisierungsniveau des angemeldeten Nutzers gegeben ist • Aufruf von Funktion 2
Fehlerfälle	FC-01: Datei nicht existent FC-02: Berechtigungen reichen nicht aus FC-03: Datei enthält Malware
Schritt 22	**Entscheidungsknoten: positiv abgeschlossene Prüfung**
Kurzbeschreibung	Existieren aus Schritt 21 keine Fehler, gilt die Prüfung als positiv abgeschlossen.
ja	Schritt 24
nein	Schritt 23
Schritt 23	**Fehler- bzw. Warnmeldung an den Nutzer**
Kurzbeschreibung	Im Fall von FC-01 und FC-02 wird eine Fehlermeldung erstellt und an den Nutzer übermittelt. Im Fall von FC-03 Warnmeldung mit Auswahl für den Nutzer, ob die Malware-infizierte Datei trotz der Gefahren heruntergeladen werden soll.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Fehlercode
Ergebnis	Eine Meldung mit der Fehlerbeschreibung wurde erstellt.
Nachbedingung	Bei FC-01, FC-02 und bei Nutzer-bestätigten Abbruch bei FC-03: Stopp

	Bei Nutzer-bestätigten Fortführung des Downloads: Schritt 24
Ablauf	• Bei FC01-, FC-02: ◦ Das System erstellt eine Fehlermeldung. ◦ Das System übermittelt diese Fehlermeldung an den Nutzer. • Bei FC-03: ◦ Das System erstellt eine Warnmeldung mit der Wahl zur Fortführung des Downloads oder Abbruch des Downloads durch den Nutzer ◦ Das System übermittelt diese Warnmeldung an den Nutzer. ◦ Das System wertet die Entscheidung des Nutzers aus. ◦ Das System führt die entsprechende Nachbedingung aus.
Fehlerfälle	FC-01: Fehlermeldung wird vom Nutzer-System nicht angenommen.
Schritt 24	**Entschlüsseln der Datei durch den DMDA**
Kurzbeschreibung	Die durch den DMDA verschlüsselte Datei wird durch den DMDA entschlüsselt.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Positiv abgeschlossene Prüfung in Schritt 22
Input	Verschlüsselte Datei, Entschlüsselungsschlüssel des DMDA
Ergebnis	Entschlüsselte Datei für die Übermittlung an den Nutzer, die in der DA gespeicherte Datei bleibt verschlüsselt
Nachbedingung	
Ablauf	Entschlüsselung der Datei
Fehlerfälle	FC-01: Kein DMDA-bezogener Entschlüsselungsschlüssel vorhanden
Schritt 25	**Integrität prüfen**
Kurzbeschreibung	Es wird geprüft, ob die Dateien dem Zustand entsprechen, in dem sie bei der Speicherung durch den Nutzer übergeben wurden.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Herunterzuladende Dateien und zugehörige Metadaten
Ergebnis	Abgeschlossene Verifikation hinsichtlich der Integrität der Dateien
Nachbedingung	
Ablauf	Das System erstellt den Hashwert der herunterzuladenden Datei und vergleicht diesen mit dem Hashwert, der bei der Speicherung der Datei in den Metadaten erfasst wurde.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Fehlerfälle	FC-01: Integrität nicht gegeben, Datei oder Metadaten-Eintrag wurde geändert
Schritt 26	**Dateien an den Nutzer-Client übermitteln**
Kurzbeschreibung	Die Dateien, die zum Herunterladen angefragt sind, werden an den Nutzer-Client übertragen.
Akteure	DA-Dienst, Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Dateien und zugehörige Kategorie
Ergebnis	Dateien wurden an das Client-System transferiert.
Nachbedingung	
Ablauf	Es werden die Dateien inkl. der Kategorien an das Client-System transferiert.
Fehlerfälle	FC-01: Daten werden vom Client nicht angenommen
Schritt 27	**Dateien auf dem Nutzer-Client empfangen**
Kurzbeschreibung	Die Dateien, die zum Herunterladen angefragt sind, werden auf Seite des Nutzer-Client empfangen.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Dateien und zugehörige Kategorie
Ergebnis	Dateien wurden auf dem Client-System gespeichert
Nachbedingung	
Ablauf	Das Client-System übernimmt die Daten oder Meldungen in den Speicher.
Fehlerfälle	
Schritt 28	**Entscheidungsknoten: Ist die Datei auf dem Nutzer-Client verschlüsselt worden**
Kurzbeschreibung	Prüfung, ob die Datei durch den Nutzer vor der Übermittlung an den DA-Dienst verschlüsselt wurde.
ja	Schritt 29
nein	Schritt 30
Schritt 29	**Dateien auf dem Nutzer-Client entschlüsseln**
Kurzbeschreibung	Die Dateien, die durch den Nutzer verschlüsselt an den DA-Dienst übertragen worden sind, werden auf dem Client wieder entschlüsselt.
Akteure	Nutzer

Auslöser	Nutzer
Vorbedingung	Die Daten waren vor der Speicherung in der DA verschlüsselt.
Input	Zu entschlüsselnde Datei Entschlüsselungsmethode Entschlüsselungsschlüssel des Nutzers
Ergebnis	Dateien wurden wieder entschlüsselt und liegen unverschlüsselt vor
Nachbedingung	
Ablauf	• Entschlüsselung der verschlüsselten Datei • Löschen der verschlüsselten Datei
Fehlerfälle	FC-01: Ungültiger Nutzer-bezogener Entschlüsselungsschlüssel FC-02: Nicht unterstützte Entschlüsselungsmethode
Schritt 30	**Dateien auf dem Datenträger des Nutzers speichern**
Kurzbeschreibung	Die heruntergeladenen und unverschlüsselten Dateien werden auf dem Datenträger des Nutzers gespeichert.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Schritt 29 (bei verschlüsselten Dateien) oder Schritt 28 (bei unverschlüsselten Dateien)
Input	Heruntergeladene Dateien und zugehörige Kategorien Datenträger des Nutzers und Download-Verzeichnisses
Ergebnis	Dateien sind auf dem Datenträger innerhalb des Download-Verzeichnisses des Nutzers gespeichert. (Wenn die Datei durch den Nutzer vor dem Hochladen bereits verschlüsselt wurde, muss der Nutzer die Datei noch entschlüsseln)
Nachbedingung	
Ablauf	• Der Nutzer gibt den Datenträger und das Download-Verzeichnis an. • Das Client-System speichert die Dateien im Download-Verzeichnis ab.
Fehlerfälle	FC-01: Datenträger existiert nicht FC-02: Download-Verzeichnis existiert nicht FC-03: Datei existiert bereits im entsprechenden Datenträger-Verzeichnis

Tabelle 5: Schritte zum Download von Dateien

6.2 Verwaltung von Dateien/Kategorien

6.2.1 Erstellen einer Kategorie

Schritt 31	**Antrag für eine neue Kategorie erstellen**
Kurzbeschreibung	Der Nutzer beantragt eine beliebige neue Kategorie in seiner DA.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Kategorie-Bezeichnung Kategorie-Ebene (Default: Wurzel im DA des Nutzers)
Ergebnis	Antrag für eine neue Kategorie wurde erstellt
Nachbedingung	
Ablauf	• Aufruf der Funktion zum Erstellen von Kategorien im DA • Angabe der Bezeichnung und weiterer Daten zur Kategorie
Fehlerfälle	FC-01: Keine Bezeichnung angegeben FC-02: Ungültige Bezeichnung
Schritt 32	**Antrag für neue Kategorie übermitteln**
Kurzbeschreibung	Der Antrag für neue Kategorie wurde übermittelt.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Antrag (Kategorie-Bezeichnung, Kategorie-Ebene)
Ergebnis	Antrag wurde an den DA-Dienst übergeben
Nachbedingung	
Ablauf	Antrag wurde an den DA-Dienst übermittelt
Fehlerfälle	FC-01: Antrag wird vom DA-Dienst nicht angenommen
Schritt 33	**Antrag für neue Kategorie entgegengenommen**
Kurzbeschreibung	Der DA-Dienst nimmt den Antrag für eine neue Kategorie entgegen.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Antrag (Kategorie-Bezeichnung, Kategorie-Ebene)

Ergebnis	Antrag wurde durch den DA-Dienst entgegengenommen.
Nachbedingung	
Ablauf	Antrag wird durch den DA-Dienst entgegengenommen.
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto angemeldet
Schritt 34	**Beantragte Daten prüfen**
Kurzbeschreibung	Der DA-Dienst prüft den Antrag.
Akteure	DA-Dienst, Account-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Kategorie-Bezeichnung Kategorie-Ebene Authentisierungsniveau des Nutzers Weitere Metadaten zur eigenen Berechtigung
Ergebnis	Kategorie verifiziert
Nachbedingung	
Ablauf	• Entgegennahme der Antragsdaten • Prüfung, ob die Kategorie-Ebene existiert • Prüfung, ob die Schreibrechte innerhalb der Kategorie-Ebene bei genutztem Authentisierungsniveau ausreichen • Prüfung, ob bereits die gleiche Kategorie-Bezeichnung in der Kategorie-Ebene existiert
Fehlerfälle	FC-01: Kategorie-Bezeichnung in der Kategorie-Ebene schon vorhanden FC-02: angegebene Kategorie-Ebene existiert nicht FC-03: Keine Schreibberechtigung bei genutztem Authentisierungsniveau
Schritt 35	**Entscheidungsknoten: positiv abgeschlossene Prüfung**
Kurzbeschreibung	Existieren aus Schritt 34 keine Fehler, gilt die Prüfung als positiv abgeschlossen.
ja	Schritt 37
nein	Schritt 36
Schritt 36	**Fehlermeldung an den Nutzer senden**
Kurzbeschreibung	Es wird eine Fehlermeldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Fehlercode
Ergebnis	Eine Meldung mit der Fehlerbeschreibung wurde erstellt.
Nachbedingung	Stopp
Ablauf	• Das System erstellt eine Fehlermeldung. • Das System übermittelt diese Fehlermeldung an den Nutzer.
Fehlerfälle	
Schritt 37	**Kategorie erstellen**
Kurzbeschreibung	Im DA wird eine neue Kategorie erstellt.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Schritt 34 ohne Fehlermeldung
Input	Kategorie-Bezeichnung Kategorie-Ebene Authentisierungsniveau Weitere Metadaten zur eigenen Berechtigung
Ergebnis	Kategorie existiert
Nachbedingung	Funktion 1
Ablauf	• Erstellung der Meta-Daten • Anlegen der Kategorie • Das Authentisierungsniveau muss mindestens dem der übergeordneten Kategorie entsprechen. In Unterkategorien kann das geforderte Authentisierungsniveau nur erhöht werden. • Meldung an den Nutzer
Fehlerfälle	
Schritt 38	**Meldung an den Nutzer**
Kurzbeschreibung	Es wird eine Meldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Erfolgsmeldung
Ergebnis	Eine Meldung wurde erstellt.
Nachbedingung	
Ablauf	• Das System erstellt eine Meldung.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	• Das System übermittelt diese Meldung an den Nutzer.
Fehlerfälle	
Schritt 39	**Meldung empfangen**
Kurzbeschreibung	Es wird eine Meldung durch den Nutzer empfangen.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	
Ergebnis	Meldung wurde auf Seite des Nutzers empfangen.
Nachbedingung	
Ablauf	Empfang der Meldung des DA-Dienstes durch den Nutzer
Fehlerfälle	
Schritt 40	**Meldung darstellen**
Kurzbeschreibung	Die Inhalte der Meldung
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Meldungsinhalte
Ergebnis	Die Meldung wurde dem Nutzer dargestellt.
Nachbedingung	
Ablauf	Die vom DA-Dienst empfangene Nachricht wird dem Benutzer nach Aufarbeitung dargestellt.
Fehlerfälle	

Tabelle 6: Schritte zum Erstellen einer Kategorie

6.2.2 Umbenennen von Dateien/Kategorien

Schritt 41	**Antrag zum Umbenennen einer Datei/Kategorie erstellen**
Kurzbeschreibung	Der Nutzer beantragt eine Umbenennung einer in seiner DA existierenden Datei/Kategorie
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Kenntnis der umzubenennenden Datei/Kategorie und der Kategorie-Ebene, ggf. über die Suche-Funktion (siehe 6.3)
Input	Datei/Kategorie-Bezeichnung_alt

	Kategorie-Ebene Datei/Kategorie-Bezeichnung_neu
Ergebnis	Antrag für die Umbenennung einer Datei/Kategorie wurde erstellt
Nachbedingung	
Ablauf	• Angabe der umzubenennenden Datei/Kategorie und der Kategorie-Ebene • Angabe der neuen Bezeichnung
Fehlerfälle	FC-01: Fehlende neue Bezeichnung FC-02: Fehlende Bezeichnung der umzubenennenden Datei/Kategorie
Schritt 42	**Antrag zum Umbenennen einer Datei/Kategorie übermitteln**
Kurzbeschreibung	Antrag zum Umbenennen einer Datei/Kategorie an den DA-Dienst übermitteln
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Antrag
Ergebnis	Antrag wurde an den DA-Dienst übergeben.
Nachbedingung	
Ablauf	Antrag wurde an den DA-Dienst übermittelt.
Fehlerfälle	
Schritt 43	**Antrag zum Umbenennen einer Datei/Kategorie empfangen**
Kurzbeschreibung	Der Antrag zum Umbenennen einer Datei/Kategorie wird vom DA-Dienst empfangen.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Antrag
Ergebnis	Antrag ist entgegengenommen.
Nachbedingung	
Ablauf	Der Antrag wird vom DA-Dienst entgegengenommen.
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto angemeldet
Schritt 44	**Antrag zur Umbenennung einer Datei/Kategorie prüfen**
Kurzbeschreibung	Es wird geprüft, ob der Antrag zur Umbenennung der Datei/Kategorie angenommen werden kann.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Akteure	DA-Dienst, Account-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Datei/Kategorie-Bezeichnung_alt Kategorie-Ebene Datei/Kategorie-Bezeichnung_neu Authentisierungsniveau
Ergebnis	Antrag wurde geprüft
Nachbedingung	
Ablauf	• Prüfung der Berechtigung zur Umbenennung • Prüfung, ob die umzubenennende Datei/Kategorie existiert • Prüfung, ob die neue Datei/Kategorie bereits existiert • Prüfung, ob die umzubenennende Kategorie vom Typ Papierkorb ist
Fehlerfälle	FC-01: die umzubenennende Datei/Kategorie existiert nicht FC-02: der gewünschte Datei-/Kategoriename existiert bereits in der Kategorieebene FC-03: Funktion ist bei dem genutzten Authentisierungsniveau nicht gestattet FC-04: Kategorie vom Typ Papierkorb kann nicht umbenannt werden
Schritt 45	**Entscheidungsknoten: positiv abgeschlossene Prüfung**
Kurzbeschreibung	Existieren aus Schritt 44 keine Fehler, gilt die Prüfung als positiv abgeschlossen.
ja	Schritt 47
nein	Schritt 46
Schritt 46	**Fehlermeldung an den Nutzer**
Kurzbeschreibung	Es wird eine Fehlermeldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Fehlercode
Ergebnis	Eine Meldung mit der Fehlerbeschreibung wurde erstellt.
Nachbedingung	Stopp
Ablauf	• Das System erstellt eine Fehlermeldung. • Das System übermittelt diese Fehlermeldung an den Nutzer.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Fehlerfälle	
Schritt 47	**Aktivierung der Umbenennung einer Datei/Kategorie**
Kurzbeschreibung	Die Datei / Kategorie wird umbenannt.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Positiv abgeschlossenen Prüfung in Schritt 45
Input	Datei/Kategorie-Bezeichnung_alt Kategorie-Ebene Datei/Kategorie-Bezeichnung_neu Authentisierungsniveau
Ergebnis	Datei/Kategorie existiert mit neuem Namen
Nachbedingung	Funktion 1
Ablauf	Die Metadaten zur Datei/Kategorie werden geändert. Es erfolgt eine Meldung an den Nutzer. Hinweis: Sollte der Dateiname der gespeicherten Datei nicht über Meta-Daten, sondern direkt an der gespeicherten Datei geändert werden, ist vor der Umbenennung eine DMDA-bezogenen Entschlüsselung der Datei und nach der Umbenennung eine DMDA-bezogene Verschlüsselung der Datei mit anschließender Löschung der entschlüsselten Datei zu realisieren.
Fehlerfälle	
Schritt 48	**Meldung an den Nutzer**
Kurzbeschreibung	Es wird eine Meldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Erfolgsmeldung
Ergebnis	Eine Meldung wurde erstellt.
Nachbedingung	
Ablauf	• Das System erstellt eine Meldung. • Das System übermittelt diese Meldung an den Nutzer.
Fehlerfälle	
Schritt 49	**Meldung empfangen**
Kurzbeschreibung	Es wird eine Meldung durch den Nutzer empfangen.
Akteure	Nutzer

Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	
Ergebnis	Meldung wurde auf Seite des Nutzers empfangen.
Nachbedingung	
Ablauf	Empfang der Meldung des DA-Dienstes durch den Nutzer
Fehlerfälle	
Schritt 50	**Meldung darstellen**
Kurzbeschreibung	Die Inhalte der Meldung werden dem Nutzer dargestellt.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Meldungsinhalte
Ergebnis	Die Meldung wurde dem Nutzer dargestellt.
Nachbedingung	
Ablauf	Die vom DA-Dienst empfangene Nachricht wird dem Benutzer nach Aufarbeitung dargestellt.
Fehlerfälle	

Tabelle 7: Schritte zum Umbenennen

6.2.3 Löschen von Dateien/Kategorien

Schritt 51	**Antrag auf Löschung einer Datei/Kategorie erstellen**
Kurzbeschreibung	Der Nutzer wählt die Dateien/Kategorien, die in seiner DA gelöscht werden sollen.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Zusammenstellung der Liste, ggf. über die Suche-Funktion (siehe 6.3)
Input	Bei Dateien: Datei(en) und die zugehörigen Kategorie-Ebenen und Bei Kategorien: Kategorie-Bezeichnung und Kategorie-Ebene
Ergebnis	Liste der zu löschenden Dateien/Kategorien
Nachbedingung	
Ablauf	Erstellung der Liste der zu löschenden Dateien bzw. Kategorien
Fehlerfälle	FC-01: Liste ist leer FC-02: Keine Bezeichnung angegeben

	FC-03: Ungültige Bezeichnung
Schritt 52	**Liste der zu löschenden Dateien/Kategorien übermitteln**
Kurzbeschreibung	Antrag zum Löschen einer Kategorie an den DA-Dienst übermitteln
Akteure	Nutzer, DA-Dienst
Auslöser	Nutzer
Vorbedingung	Gegenseitig authentisierter und verschlüsselter Kommunikationskanal aufgebaut
Input	Liste der zu löschenden Dateien/Kategorien
Ergebnis	Die Liste der zu löschenden Dateien/Kategorien wurde an den DA-Dienst übergeben
Nachbedingung	
Ablauf	Liste wurde an den DA-Dienst übermittelt.
Fehlerfälle	
Schritt 53	**Liste der zu löschenden Dateien/Kategorien empfangen**
Kurzbeschreibung	Die Liste wird vom DA-Dienst empfangen.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Liste der zu löschenden Dateien/Kategorien
Ergebnis	Die Liste der zu löschenden Dateien/Kategorien wurde von dem DA-Dienst empfangen.
Nachbedingung	
Ablauf	Die Liste wird vom DA-Dienst entgegengenommen.
Fehlerfälle	FC-01: Nutzer nicht am De-Mail-Konto angemeldet FC-02: Liste ist leer
Schritt 54	**Antrag zum Löschen prüfen**
Kurzbeschreibung	Die in der Liste angegebenen Dateien/Kategorien werden hinsichtlich der Berechtigungen zum Löschen geprüft.
Akteure	DA-Dienst, Account-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Liste der zu löschenden Dateien/Kategorien Authentisierungsniveau des Nutzers
Ergebnis	Prüfungen sind abgeschlossen.

Nachbedingung	
Ablauf	Für Dateien • Prüfung, ob die Datei(en) in der jeweiligen angegebenen Kategorie-Ebene existiert. • Prüfung, ob die Berechtigung zum Löschen mit dem Authentisierungsniveau des Nutzers gegeben ist. Für Kategorien • Prüfung, ob die zu löschende Kategorie existiert. • Prüfung, ob die Löschung bei dem Authentisierungsniveau gestattet ist. • Prüfung, ob keine weiteren Kategorien in der Kategorie existieren. • Prüfung, ob der Kategorie keine Dateien zugeordnet sind. • Prüfung, ob die zu löschende Kategorie vom Typ Papierkorb ist.
Fehlerfälle	FC-01: Berechtigungen reichen nicht aus FC-02: Kategorie/Datei existiert nicht FC-03: Dateien sind der Kategorie zugeordnet FC-04: Es gibt Kategorien in dieser Kategorie FC-05: Kategorie vom Typ Papierkorb kann nicht gelöscht werden
Schritt 55	**Entscheidungsknoten: positiv abgeschlossene Prüfung**
Kurzbeschreibung	Existieren aus Schritt 54 keine Fehler, gilt die Prüfung als positiv abgeschlossen.
ja	Schritt 57
nein	Schritt 56
Schritt 56	**Fehlermeldung an den Nutzer**
Kurzbeschreibung	Es wird eine Fehlermeldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Fehlercode
Ergebnis	Eine Meldung mit der Fehlerbeschreibung wurde erstellt.
Nachbedingung	Stopp
Ablauf	• Das System erstellt eine Fehlermeldung. • Das System übermittelt diese Fehlermeldung an den Nutzer.
Fehlerfälle	

Schritt 57	**Dateien/Kategorien löschen**
Kurzbeschreibung	Die Dateien, die in der Liste der zu löschenden Dateien enthalten sind, und die zugehörigen Metadaten werden in die Kategorie Papierkorb verschoben. Dateien der Kategorie Papierkorb werden unwiederbringlich gelöscht. Zu löschende Kategorien werden entfernt.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Liste zu löschender Dateien/Kategorien
Ergebnis	Für Dateien: Dateien sind der Kategorie Papierkorb zugeordnet, oder gelöscht und lassen sich nicht wiederherstellen. Für Kategorien: Kategorie existiert nicht mehr.
Nachbedingung	Funktion 1
Ablauf	Für Dateien: • Das System löscht die in der Liste angegebenen Dateien innerhalb des DA des angemeldeten Benutzers, wenn diese der Kategorie Papierkorb zugeordnet waren. Die zugehörigen Metadaten der Dateien werden ebenfalls gelöscht. oder • Das System setzt für die zu löschenden Dateien, die bisher nicht der Kategorie Papierkorb zugeordnet waren, die Kategorie Papierkorb und entfernt Zuordnungen zu anderen Kategorien. Für Kategorien: • Die Kategorie wird mit den zugehörigen Metadaten gelöscht.
Fehlerfälle	
Schritt 58	**Meldung an den Nutzer**
Kurzbeschreibung	Es wird eine Meldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Erfolgsmeldung
Ergebnis	Eine Meldung wurde erstellt.
Nachbedingung	
Ablauf	• Das System erstellt eine Meldung. • Das System übermittelt diese Meldung an den Nutzer.
Fehlerfälle	FC-01: Meldung wird vom Nutzer-System nicht angenommen.

– Seite 334 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Schritt 59	**Meldung empfangen**
Kurzbeschreibung	Es wird eine Meldung durch den Nutzer empfangen.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	
Ergebnis	Meldung wurde auf Seite des Nutzers empfangen.
Nachbedingung	
Ablauf	Empfang der Meldung des DA-Dienstes durch den Nutzer.
Fehlerfälle	
Schritt 60	**Meldung darstellen**
Kurzbeschreibung	Die Inhalte der Meldung werden dem Nutzer dargestellt.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Meldungsinhalte
Ergebnis	Die Meldung wurde dem Nutzer dargestellt.
Nachbedingung	
Ablauf	Die vom DA-Dienst empfangene Nachricht wird dem Benutzer nach Aufarbeitung dargestellt.
Fehlerfälle	

Tabelle 8: Schritte zum Löschen

6.2.4 Ändern der Berechtigungen für Dokumente und Kategorien

Schritt 61	**Antrag auf Änderung der Berechtigung erstellen**
Kurzbeschreibung	Der Nutzer beantragt eine Änderung einer Berechtigung von Dateien/ Kategorien in seiner DA.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Kenntnis der Dateien/Kategorien, für die die Änderung durchgeführt werden soll, ggf. über die Suche-Funktion (siehe 6.3)
Input	Kategorie-Ebene Kategorie-Bezeichnung Unterkategorien rekursiv ändern Datei (optional)

	Neue Berechtigungsdaten
Ergebnis	Antrag auf Änderung der Berechtigung wurde erstellt
Nachbedingung	
Ablauf	Angabe der Änderungen
Fehlerfälle	FC-01: Keine Änderung angegeben
Schritt 62	**Antrag zur Änderung von Berechtigungen übermitteln**
Kurzbeschreibung	Antrag zur Änderung von Berechtigungen an den DA-Dienst übermitteln
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Antrag
Ergebnis	Antrag wurde an den DA-Dienst übergeben.
Nachbedingung	
Ablauf	Antrag wurde an den DA-Dienst übermittelt.
Fehlerfälle	
Schritt 63	**Antrag zur Änderung von Berechtigungen empfangen**
Kurzbeschreibung	Antrag zur Änderung von Berechtigungen durch den DA-Dienst empfangen
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Antrag
Ergebnis	Antrag wurde durch den DA-Dienst empfangen.
Nachbedingung	
Ablauf	Empfang des Antrages
Fehlerfälle	FC-01: Nutzer am De-Mail-Konto nicht angemeldet
Schritt 64	**Antrag prüfen**
Kurzbeschreibung	Der DA-Dienst prüft den Antrag zur Änderung der Berechtigungen.
Akteure	DA-Dienst, Account-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Kategorie-Ebene Kategorie-Bezeichnung

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Unterkategorien rekursiv ändern Datei (optional) Neue Berechtigungsdaten Für die Anmeldung genutztes Authentisierungsniveau
Ergebnis	Der Antrag wurde geprüft.
Nachbedingung	
Ablauf	• Prüfung, ob die Kategorie bzw. die Datei innerhalb der Kategorie existiert. • Prüfung, ob das genutzte Authentisierungsniveau ausreicht. • Prüfung, ob das Authentisierungsniveau der Anmeldung gleich oder höher dem zu setzenden Authentisierungsniveau in den Berechtigungsdaten ist. • Prüfung, ob die Berechtigung zum Ändern der Kategorie oder Datei vorhanden ist. • Prüfung, ob die Berechtigung in sich stimmig ist. Das Authentisierungsniveau für die Datei/Kategorie muss mindestens der übergeordneten Kategorie entsprechen.
Fehlerfälle	FC-01: Datei existiert nicht FC-02: Kategorie existiert nicht FC-03: Keine Berechtigungen zur Änderung FC-04: Authentisierungsniveau zu niedrig FC-05: Berechtigungen in sich nicht stimmig FC-06: Authentisierungsniveau kann nicht zugeordnet werden
Schritt 65	**Entscheidungsknoten: positiv abgeschlossene Prüfung**
Kurzbeschreibung	Existieren aus Schritt 64 keine Fehler, gilt die Prüfung als positiv abgeschlossen.
ja	Schritt 67
nein	Schritt 66
Schritt 66	**Fehlermeldung an den Nutzer**
Kurzbeschreibung	Es wird eine Fehlermeldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Fehlercode
Ergebnis	Eine Meldung mit der Fehlerbeschreibung wurde erstellt.
Nachbedingung	Stopp

Ablauf	• Das System erstellt eine Fehlermeldung • Das System übermittelt diese Fehlermeldung an den Nutzer
Fehlerfälle	
Schritt 67	**Berechtigungen ändern**
Kurzbeschreibung	Die beantragten Berechtigungen werden in der DA geändert.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Kategorie-Ebene Kategorie-Bezeichnung Unterkategorien rekursiv ändern Datei (optional) Neue Berechtigungsdaten Für die Anmeldung genutztes Authentisierungsniveau
Ergebnis	Die Berechtigungen sind neu gesetzt.
Nachbedingung	Funktion 1
Ablauf	• Die Berechtigungen werden innerhalb der Metadaten neu erfasst. • Bei der rekursiven Änderung gelten folgende Regeln: ◦ Wenn das Authentisierungsniveau erhöht wird, bleiben höhere Anforderungen bestehen ◦ Wenn das Authentisierungsniveau erniedrigt wird, werden die Rechte komplett überschrieben. ◦ Die Datei/Kategorie hat das Mindest-Auth.-Niveau gleich oder höher als seine Kategorie in der sie sich befindet.
Fehlerfälle	
Schritt 68	**Meldung an den Nutzer**
Kurzbeschreibung	Es wird eine Meldung erstellt und an den Nutzer übermittelt.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Erfolgsmeldung
Ergebnis	Eine Meldung wurde erstellt.
Nachbedingung	
Ablauf	• Das System erstellt eine Meldung.

	• Das System übermittelt diese Meldung an den Nutzer.
Fehlerfälle	
Schritt 69	**Meldung empfangen**
Kurzbeschreibung	Es wird eine Meldung durch den Nutzer empfangen.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	
Ergebnis	Meldung wurde auf Seite des Nutzers empfangen.
Nachbedingung	
Ablauf	Empfang der Meldung des DA-Dienstes durch den Nutzer
Fehlerfälle	
Schritt 70	**Meldung darstellen**
Kurzbeschreibung	Die Inhalte der Meldung werden dem Nutzer dargestellt.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	Meldungsinhalte
Ergebnis	Die Meldung wurde dem Nutzer dargestellt.
Nachbedingung	
Ablauf	Die vom DA-Dienst empfangene Nachricht wird dem Benutzer nach Aufarbeitung dargestellt.
Fehlerfälle	

Tabelle 9: Schritte zur Änderung von Berechtigungen

6.3 Suche und Anzeige von Dokumenten und Kategorien

Schritt 71	**Erstellen einer Suchanfrage**
Kurzbeschreibung	Der Nutzer erstellt eine Suchanfrage, in der die Suchkriterien enthalten sind.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	

Input	Suchkriterien können sein: • Teile des Namens oder vollständiger Name der Datei, einschließlich Datei-Endung • Teile des Namens oder vollständige Bezeichnung der Kategorie • Datei-MIME-Typ (Format) • Inhalt der Datei (Text) • Einschränkungen hinsichtlich der Kategorien • Letztes Änderungsddatum der Datei •
Ergebnis	Anfrage erstellt
Nachbedingung	
Ablauf	Angabe der Suchkriterien
Fehlerfälle	FC-01: Keine Suchkriterien erfasst
Schritt 72	**Suchanfrage übermitteln**
Kurzbeschreibung	Suchanfrage an den DA-Dienst übermitteln
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Suchanfrage
Ergebnis	Suchanfrage wurde an den DA-Dienst übergeben.
Nachbedingung	
Ablauf	Suchanfrage wird an den DA-Dienst übermittelt.
Fehlerfälle	FC-01: Suchanfrage wurde vom DA-Dienst nicht angenommen.
Schritt 73	**Suchanfrage empfangen**
Kurzbeschreibung	Suchanfrage wird vom DA-Dienst empfangen.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Suchanfrage
Ergebnis	Suchanfrage ist entgegengenommen
Nachbedingung	
Ablauf	Suchanfrage wird vom DA-Dienst entgegengenommen.
Fehlerfälle	FC-01: Nutzer am De-Mail-Konto nicht angemeldet

Schritt 74	**Entschlüsseln der Dateien**
Kurzbeschreibung	Die durch den DMDA verschlüsselten Dateien bzw. die nutzerbezogenen Suchindex-Dateien werden durch den DMDA entschlüsselt.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Verschlüsselte Dateien / Suchindex-Dateien, Entschlüsselungsschlüssel des DMDA
Ergebnis	Entschlüsselte Dateien / Suchindex-Dateien für die Durchführung der Suche, die im DA gespeicherte Dateien/Suchindex-Dateien bleibt verschlüsselt.
Nachbedingung	
Ablauf	Entschlüsselung der Dateien / Suchindex-Dateien
Fehlerfälle	FC-01: Kein DMDA-bezogener Entschlüsselungsschlüssel vorhanden
Schritt 75	**Suche durchführen**
Kurzbeschreibung	Die Suche wird innerhalb der DA des angemeldeten Nutzers ausgeführt. Eine Ergebnisliste wird erstellt.
Akteure	DA-Dienst
Auslöser	Nutzer
Vorbedingung	
Input	Suchkriterien Authentisierungsniveau
Ergebnis	Es wurde eine Liste mit den Ergebnissen der Suche erstellt und dem Nutzer übermittelt. Liste beinhaltet • bei Kategorie: ◦ Kategorie-Pfad inkl. aller Kategoriebezeichnungen ◦ URL • bei Dateien ◦ Kategorie-Pfad inkl. aller Kategoriebezeichnungen ◦ Dateiname ◦ Datum der letzten Änderung in der DA ◦ URL
Nachbedingung	
Ablauf	Die auf der Basis der Suchkriterien definierte Suche wird ausgeführt.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

	Dabei wird beachtet, dass die Suche ausschließlich die Kategorien bzw. Dateien berücksichtigt, die für den Nutzer und seinem derzeitigen Authentisierungsniveau lesbar sind.
Fehlerfälle	
Schritt 76	**Löschung entschlüsselter Dateien**
Kurzbeschreibung	Die für die Suchanfrage entschlüsselten Dateien /Suchindex-Dateien werden sicher gelöscht.
Akteure	DA-Dienst
Auslöser	DA-Dienst
Vorbedingung	
Input	Entschlüsselte Dateien / Suchindex-Dateien
Ergebnis	Entschlüsselte Dateien / Suchindex-Dateien sind gelöscht
Nachbedingung	
Ablauf	Der DA-Dienst löscht die durch den DMDA entschlüsselten Dateien / Suchindex-Dateien unwiederbringlich.
Fehlerfälle	
Schritt 77	**Liste an den Nutzer senden**
Kurzbeschreibung	Es wird die Liste mit den Suchergebnissen an den Nutzer übermittelt.
Akteure	DA-Dienst, Nutzer
Auslöser	DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Liste mit Suchergebnissen
Ergebnis	Eine Liste wurde an den Nutzer gesandt.
Nachbedingung	Die Ergebnisliste wird durch den DMDA sicher gelöscht.
Ablauf	Das System übermittelt die Liste an den Nutzer.
Fehlerfälle	FC-01: Suchergebnisse werden vom Nutzer-System nicht angenommen
Schritt 78	**Liste mit Suchergebnissen empfangen**
Kurzbeschreibung	Es wird eine Liste durch den Nutzer empfangen.
Akteure	Nutzer
Auslöser	Nutzer, DA-Dienst
Vorbedingung	Sicherer Kanal zwischen Kommunikationspartnern aufgebaut
Input	Liste
Ergebnis	Liste wurde auf Seite des Nutzers empfangen.
Nachbedingung	

Ablauf	Empfang der Liste des DA-Dienstes durch den Nutzer
Fehlerfälle	
Schritt 79	**Darstellung der Liste mit den Ergebnissen der Suche**
Kurzbeschreibung	Der Nutzer sieht die List der Suchergebnisse ein.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	
Input	
Ergebnis	Es wurde eine Liste mit den Ergebnissen der Suche dargestellt.
Nachbedingung	
Ablauf	Die Ergebnisliste wird für den Nutzer dargestellt.
Fehlerfälle	

Tabelle 10: Schritte zur Suche und Anzeige von Kategorien/ Dateien

7 Weitere Funktionen

Die in diesem Abschnitt beschriebenen Funktionen werden entweder vom System ausgeführt oder können vom Nutzer interaktiv aufgerufen werden, während er an seiner DA angemeldet ist. Eine Beschreibung, wie die einzelnen Funktionen dargestellt werden, findet sich in Abschnitt 9.

7.1 Durch das System ausgeführte Funktionen

Funktion 1	**Protokollierung von Änderung**
Kurzbeschreibung	Aktionen, die zur Änderung der Metadaten führen, werden protokolliert.
Akteure	DA-Dienst
Auslöser	jede Änderung der Metadaten zu einer Kategorie bzw. einer Datei
Vorbedingung	Änderung eines Meta-Datums
Input	• Nutzerkennung • Authentisierungsniveau • neue Metadaten • Datum und Zeit
Ergebnis	Revisionssichere Speicherung der Änderung von Metadaten
Nachbedingung	Auswertbarkeit der Protokolldaten muss zu jeder Zeit gegeben sein.
Ablauf	• Erstellung des Logs • Revisionssichere Speicherung und Archivierung
Fehlerfälle	
Funktion 2	**Prüfung Schadsoftware**
Kurzbeschreibung	Es wird eine Prüfung von zu speichernden Dateien hinsichtlich Schadsoftware: • Viren, • Trojanern, • Würmer vorgenommen.
Akteure	DA-Dienst, Schadsoftware-Dienst
Auslöser	Upload und Download von Dateien (siehe Abschnitt 6.1)
Vorbedingung	Prüfprogramme mit aktuellen Prüfkonfigurationen
Input	Datei
Ergebnis	Information, falls in der Datei Schadsoftware gefunden wird

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Nachbedingung	
Ablauf	• Datei wird zum Schadsoftware-Scanner übergeben. • Datei wird vom Schadsoftware-Scanner entgegengenommen. • Datei wird an die Schadsoftware-Prüfung übergeben.
Fehlerfälle	FC-01: Dateiformat unbekannt und kann nicht auf Schadsoftware geprüft werden.
Funktion 3	**Benachrichtigung bei hohem verbrauchten Speicher**
Kurzbeschreibung	Wenn der Nutzer nur noch 10 % seines Speichers in seinem DA frei hat, meldet das System bei Übergang dieser Grenze diesen Zustand.
Akteure	DA-Dienst
Auslöser	Speicherung von Dateien (siehe Abschnitt 6.1.1)
Vorbedingung	10 % des zugeordnetes Speichers frei
Input	
Ergebnis	Meldung erfolgte an den Nutzer.
Nachbedingung	
Ablauf	• DA-Dienst misst freien Speicher. • Bei Unterschreiten der Grenze von 11 nach 10 % des noch verfügbaren freien Speicherplatzes wird eine Meldung erstellt. • Die Meldung wird an den Nutzer übermittelt.
Fehlerfälle	

Tabelle 11: Durch das System ausgeführte Funktionen

7.2 Durch den Nutzer initiierte Funktionen

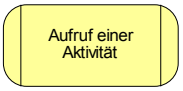
Funktion 4	**Einsicht in das Protokoll**
Kurzbeschreibung	Einsicht in das Protokoll der DA Hinweis: Es werden nur Kategorien bzw. Dateien berücksichtigt, die mit dem aktuellen Authentisierungsniveau des Nutzers lesbar sind.
Akteure	Nutzer
Auslöser	Nutzer
Vorbedingung	Anmeldung am De-Mail-Konto
Input	Kategorie-Ebene Kategoriebezeichnung Optional: [Dateiname] oder [Liste über alle in der Kategorie vorhanden Dateien]

	Zeitraum Einschluss aller Sub-Kategorien Bei der Anmeldung genutztes Authentisierungsniveau
Ergebnis	Logging-Protokoll
Nachbedingung	
Ablauf	• Der Nutzer stellt eine Anfrage für die Einsicht in das Protokoll. • In der Anfrage gibt er an: Kategorie-Ebene, Kategoriebezeichnung, optional ein Dateiname, einen Zeitraum. • Der Antrag wird vom DA-Dienst entgegengenommen. • Der DA-Dienst erstellt über den Filter der im Antrag angegebenen Daten und dem angemeldeten Nutzer inkl. dessen genutztes Authentisierungsniveau ein Protokoll. • Der DA-Dienst signiert dieses Protokoll mit einer dauerhaft überprüfbaren qualifizierten Signatur und stellt dem Nutzer das Protokoll zur Verfügung (Download oder per Meldungsnachricht)sendet dieses über den Versanddienst an das Postfach des Nutzers. Hinweis: Es werden nur Kategorien bzw. Dateien berücksichtigt, die mit dem Authentisierungsniveau bei der Anmeldung lesbar sind.
Fehlerfälle	FC-01: Kein Protokoll für die Datei / Kategorie gefunden FC-02: angegebene Kategorie nicht gefunden FC-03: angegebene Datei nicht gefunden

Tabelle 12: Durch den Nutzer initiierte Funktionen

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

8 Legende zum Aktivitätsdiagramm

	Startknoten Der Startknoten ist der Startpunkt eines Prozesses. Ein Prozess darf mehrere Startknoten haben, in diesem Fall beginnen beim Start des Prozesses mehrere Abläufe. Es ist möglich, dass ein Prozess keinen Startknoten besitzt, sondern von einem Ereignis angestoßen wird.
	Endknoten Der Endknoten gibt an, dass die Ausführung des Prozesses abgeschlossen ist. Es kann in einem Prozessdiagramm mehrere Ausgänge in Form dieser Endknoten geben. Gibt es zum Zeitpunkt des Erreichens des Endknoten mehrere parallele Abläufe innerhalb des Prozesses, werden beim Erreichen eines Endknoten alle Abläufe gestoppt.
	Ablaufende Das Ablaufende terminiert einen Ablauf. Im Unterschied zum Endknoten, der einen ganzen Prozess beendet, hat das Erreichen des Ablaufenden keinen Effekt auf andere parallele Abläufe, die zu diesem Zeitpunkt innerhalb des Prozesses abgearbeitet werden. Auf diese Weise lassen sich parallele Abläufe gezielt und einzeln beenden.
	Kante Die als Pfeile dargestellten Kanten verbinden die einzelnen Komponenten des Diagramms und stellen den Kontrollfluss dar.
	Aktion Eine Aktion ist ein einzelner Schritt innerhalb eines Prozesses, der nicht mehr weiter zerlegt wird. Das bedeutet nicht unbedingt, dass die Aktion in der realen Welt nicht mehr weiter zerlegbar wäre, sondern dass die Aktion in diesem Diagramm nicht mehr weiter verfeinert wird. Die Aktion kann Ein- und Ausgabeinformationen besitzen. Der Output einer Aktion kann der Input einer Folge-Aktion sein.
	Aufruf einer Aktivität Mit diesem Symbol kann aus einer Aktivität (Prozess) heraus eine weitere Aktivität aufgerufen werden. Der Aufruf selbst ist eine Aktion, der aufgerufene Ablauf eine weitere Aktivität.
	Empfang eines Ereignisses Diese Aktion wartet auf das Eintreten eines Ereignisses. Nach dem Empfang des Ereignisses wird der im Aktivitätsdiagramm definierte, von dieser Aktion ausgehende Ablauf abgearbeitet.
	Senden von Signalen Das Senden von Signalen bedeutet, dass ein Signal an eine empfangende Aktivität gesendet wird. Die empfangende Aktivität

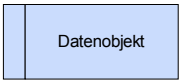
	nimmt das Signal mit der Aktion „Ereignis empfangen“ entgegen und kann entsprechend darauf reagieren.
	Entscheidungsknoten Die Raute stellt eine Verzweigung im Kontrollfluss dar. Eine Verzweigung hat einen Eingang und zwei oder mehrere Ausgänge. Jeder Ausgang wird mit einer Bedingung versehen. Trifft eine Bedingung zu, wird am entsprechenden Ausgang weiter verfahren.
	Datenobjekt Datenobjekte gehören üblicherweise nicht zum Symbolumfang in UML-Aktivitätsdiagrammen. Sie sind hier jedoch eingeführt worden, um an entscheidender Stelle zu verdeutlichen, welche Datenobjekte, insbesondere im Fokus der Schutzbedarfsanalyse, vorliegen.

Tabelle 13: Legende zum Aktivitätsdiagramm

9 Legende zu Schritten der Ablaufbeschreibung

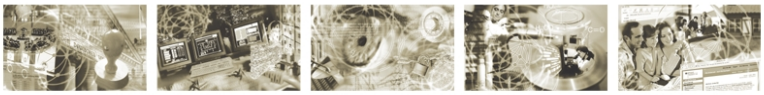
Schritte im Aktivitätsdiagramm bezeichnen im Kontrollfluss eingebundene einmalig ablaufende Aktionen.

Schritte werden in diesem Modul als Aktionen auf folgende Art und Weise beschrieben:

Schritt <Nr.>	Eindeutigen Name der Aktion
Kurzbeschreibung	Innerhalb der Kurzbeschreibung erfolgt eine verbale Beschreibung der wesentlichen Funktionalität der Aktion.
Akteure	Alle Rollen bzw. Dienste, die innerhalb der Aktion in irgendeiner Weise beteiligt sind, werden aufgezählt.
Auslöser	Der Auslöser ist ein Akteur, durch den die Aktion aufgerufen bzw. initialisiert wird.
Vorbedingung	Unter Vorbedingungen werden die Bedingungen verstanden, die nicht aus einer unmittelbar vorhergehenden Aktion folgen, sondern asynchron erzielt werden müssen. Diese Aktivitäten sind nicht unbedingt in diesem Dokument beschrieben, die Ergebnisse sind jedoch als Vorbedingungen für die Ausführung der hier beschriebenen Aktion notwendig. Auf die Erfüllung dieser Vorbedingungen muss sich die nutzende Aktion verlassen können.
Input	Der Auslöser muss bei Initialisierung der Aktion die entsprechenden Informationen an diese übergeben oder durch die Aktion abfragen lassen, so dass eine Verarbeitung der Informationen innerhalb der Aktion erfolgen kann.
Ergebnis	Nach Beendigung der Aktion muss eine bestimmte Information als Resultat erarbeitet bzw. bereitgestellt werden.
Nachbedingung	Unter Nachbedingungen werden Bedingungen verstanden, die innerhalb dieser Aktion nicht betrachtet werden und durch unmittelbar nachfolgende Aktionen aufgegriffen und dort behandelt werden müssen.
Ablauf	Für die innerhalb der Aktion definierte Logik wird ein konkreter Ablauf beschrieben. Die definierte Abfolge muss innerhalb der Aktion durchgeführt und abgeschlossen werden.
Fehlerfälle	Als Fehlerfall wird ein Ergebnis einer Funktion bezeichnet, der innerhalb der Funktionsspezifikation liegt, aber kein Standard-Ergebnis darstellt. Die konkrete Behandlung eines Fehlerfalls ist implementierungsabhängig. Je nach Fall können unterschiedliche Lösungsstrategien verwendet werden, bspw. kann eine Aktion zu einem späteren Zeitpunkt wiederholt oder die Aktion abgebrochen werden. Bei Abbruch einer Aktion ist der Nutzer mindestens darüber zu informieren und alle bis zu diesem Schritt generierten temporären Daten müssen gelöscht werden. In den Beschreibungen der Fehlerfälle der Aktionen werden nur mögliche Fehler beschrieben, die innerhalb der Funktionsspezifikation liegen.

Tabelle 14: Legende zu Schritten

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Dokumentenablage IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 5.3
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul beinhaltet die IT-Sicherheitsanforderungen, die über die generellen Anforderungen aus dem Modul [TR DM Si M] hinausgehen und speziell für die DA anzuwenden sind, und ist Bestandteil von [TR DM DA M]. Dies gilt sofern die DA angeboten wird.

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die angenommene Netzinfrastruktur eines typischen De-Mail-Dienst.

Bei der Erstellung des realen IT-Sicherheitskonzeptes sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt das Modul [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der bereits in der [TR DM Si ÜK] skizziert ist.

3 Bedrohungen

Es gelten die in [TR DM Si ÜK] formulierten Bedrohungen, sowie weitere speziell für die DA geltenden Aspekte.

3.1 Verlust der Vertraulichkeit

Der Verlust der Vertraulichkeit wird bereits in [TR DM Si ÜK] berücksichtigt. Die Gefahr des Verlustes der Vertraulichkeit besteht im Fall der Dokumentenablage auf unterschiedlichen Ebenen:

- durch den Zugriff von Administratoren, auf die Daten oder auf die Suchindizes, die eine Suche in den Daten ermöglichen,
- durch den Diebstahl von Speichermedien.

3.2 Verlust der Integrität

Der Verlust der Integrität betrifft in diesem Zusammenhang zum einen die Manipulation von Daten durch Unbefugte und zum anderen die Veränderung der Daten durch technisches Versagen.

3.3 Verlust der Verfügbarkeit

Der Verlust der Verfügbarkeit betrifft in diesem Zusammenhang zum einen die Nicht-Erreichbarkeit des Dienstes insgesamt sowie die Verfügbarkeit der in der Dokumentenablage abgelegten Daten. Eine unberechtigte Löschung der Daten kann z. B. dazu führen, dass der Nutzer nicht mehr auf seine Daten zugreifen kann.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

4 Sicherheitsziele

Es gelten die Sicherheitsziele, die in [TR DM Si ÜK] formuliert wurden.

5 Anforderungen

5.1 Kryptokonzept

Da die Speicherung personenbezogener Daten durch den Nutzer ein wesentlicher Zweck der Dokumentenablage ist, sind besondere Maßnahmen bei der Speicherung zu ergreifen. Es sind daher neben den Anforderungen aus [TR DM Si ÜK] zum Kryptokonzept, die nachfolgenden Anforderungen an die Dokumentenablage umzusetzen.

5.1.1 Vertrauliche Speicherung der Daten

Die Speicherung sämtlicher vom Nutzer eingestellter Daten auf den Systemen des DMDA hat verschlüsselt zu erfolgen.

Die Verschlüsselung der Daten hat so früh wie möglich nach Eingang auf den Systemen des DMDA zu erfolgen.

Danach darf eine Entschlüsselung der Daten nur automatisiert erfolgen und ausschließlich

- zur Prüfung auf Viren oder Schadsoftware und
- zur Auslieferung an den Nutzer.

Die Verschlüsselung kann mit einem Schlüssel für alle Nutzer erfolgen.

Es gelten folgende Regelungen für die Daten hinsichtlich

- langfristiger Speicherung (z.B. Daten in der DA):
  - Die Daten müssen einzeln oder in einem Container verschlüsselt gespeichert werden.
- kurzfristiger Speicherung (z.B. in Warteschlange bei Virenscanner):
  - Das Dateisystem, auf dem die Daten abgelegt werden, muss verschlüsselt sein.

Bei der Erstellung von Suchindizes, für die Suche innerhalb der in der DA abgelegten Daten sind diese ebenfalls verschlüsselt abzulegen.

5.1.2 Integere Speicherung der Daten

Die Speicherung der Daten auf den Systemen des DMDA hat unverfälscht zu erfolgen.

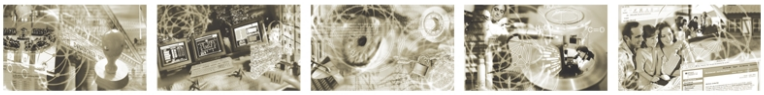
Dazu muss die Integritätssicherung der Daten so früh wie möglich nach Eingang auf den Systemen des DMDA erfolgen.

Die Integritätsprüfung erfolgt bei der Speicherung sowie beim Abruf der Daten.

5.2 Backup-Konzept

Maßnahmen zur Sicherung der Daten sind in zu berücksichtigen (vgl. [TR DM Si ÜK]).

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Sicherheit Modulübergreifend
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 – Teil 6
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Abbildungsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

Dieses Modul spezifiziert die Anforderungen und den Ablauf der Testierung entsprechend ISO 27001 auf der Basis von IT-Grundschutz. Es wird ein Überblick gegeben über die notwendigen Schritte zur Erstellung des konkreten IT-Sicherheitskonzepts des IT-Verbunds (Untersuchungsgegenstand).

Dieses Modul beschreibt den Nachweis über die Erbringung der Anforderungen an eine sichere De-Mail-Infrastruktur. Es richtet sich einerseits an den DMDA, indem es aufzeigt, welche Anforderungen an ihn aus der Anforderung an ein Informationssicherheitsmanagementsystem (ISMS) auf der Basis von IT-Grundschutz resultieren.

Andererseits ist auch der zertifizierte De-Mail Auditor adressiert, der die Umsetzung der Anforderungen prüfen und bestätigen muss. Für diesen werden in diesem Modul zusätzliche – über das Prüfschema für ISO 27001-Audits [Zert ISO 27001] hinausgehende – Prüfanforderungen definiert.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2 Aufbau des Moduls IT-Sicherheit

Konzeptionelle Vorgaben für die Erstellung eines Sicherheitskonzeptes sind in folgenden Dokumenten enthalten. Die Dokumente enthalten die IT-Sicherheitsziele sowie daraus abgeleitet Maßnahmen, die zwingend umgesetzt werden müssen (Vorgaben) und solche, die durch alternative Maßnahmen ersetzt werden können (empfohlene Maßnahmen).

a) Technische Richtlinie De-Mail Sicherheit Übergeordnete Komponenten [TR DM Si ÜK]
Dieses Modul enthält eine beispielhafte, technische Abbildung einer De-Mail-Infrastruktur. Der in diesem Dokument skizzierte Ansatz kann dem DMDA als Beispiel für sein Sicherheitskonzept dienen. Die Anforderungen sind analog den Anforderungen für eine ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz keinesfalls vollständig und müssen an die jeweiligen individuellen Gegebenheiten angepasst werden.

Spezifische Sicherheitsaspekte einzelner De-Mail-Dienste werden in den nachfolgend benannten Modulen betrachtet:

b) Technische Richtlinie De-Mail Sicherheit Accountmanagement [TR DM ACM Si]
Es ist Bestandteil des Moduls Accountmanagement.

c) Technische Richtlinie De-Mail Sicherheit IT-Basisinfrastruktur [TR DM IT-BInfra Si]
Es ist Bestandteil des Moduls IT-Basisinfrastruktur.

d) Technische Richtlinie De-Mail Sicherheit – Postfach- und Versanddienst [TR DM PVD Si]
Es ist Bestandteil des Moduls Postfach- und Versanddienst.

e) Technische Richtlinie De-Mail Sicherheit – Dokumentenablage [TR DM DA Si]
Es ist Bestandteil des Moduls Dokumentenablage.

f) Technische Richtlinie De-Mail Sicherheit – Identitätsbestätigungsdienst [TR DM ID Si]
Es ist Bestandteil des Moduls Identitätsbestätigungsdienst.

Der Inhalt von a) bis d) ist in jedem Fall anzuwenden; hingegen ist eine Anwendung von e) bis f) nur notwendig, wenn der DMDA auch den jeweiligen Dienst tatsächlich anbietet.

3 Ablauf des Verfahrens

Im Folgenden wird der Ablauf des Testierungsverfahrens auf der Basis von IT-Grundschutz unter besonderer Berücksichtigung der Anforderungen von De-Mail beschrieben.

3.1 Fokus

Grundlage für das durch den DMDA zu erstellende IT-Sicherheitskonzept sind folgende Standards: [BSI 100-1], [BSI 100-2] und [BSI 100-3] sowie [IT-GS Katalog]. Die darin enthaltenen Standard-Sicherheitsmaßnahmen decken bei vollständiger Umsetzung den normalen Schutzbedarf ab und stellen eine Basis für die adäquate Absicherung von höherem Schutzbedarf dar.

Gegenstand dieses Abschnitts ist es, die wesentlichen Schritte aufzuzeigen, die für die Erstellung eines IT-Sicherheitskonzeptes erforderlich sind. Voraussetzung für ein Testat über die IT-Sicherheit ist die erfolgreiche Etablierung eines Informationssicherheitsmanagementsystems (ISMS) und die Umsetzung aller für den betroffenen De-Mail-Dienst erforderlichen Maßnahmen.

3.2 Etablierung eines ISMS

Die Schaffung, Aufrechterhaltung und stetige Verbesserung von Informationssicherheit ist ein kontinuierlicher Prozess. Um die notwendigen Rahmenbedingungen zu schaffen, sieht der Standard [BSI 100-1] die Einsetzung eines Informationssicherheitsmanagements als Grundlage für ein Testat zwingend vor. Dies bezieht sich verpflichtend auf den betrachteten Informationsverbund, dessen Grundlage der jeweilige De-Mail-Dienst darstellt.

Als Informationssicherheitsmanagement im Sinne dieses Standards wird dabei die Planungs- und Lenkungsaufgabe bezeichnet, die zum sinnvollen Aufbau, zur praktischen Umsetzbarkeit und zur Sicherstellung der Effektivität eines durchdachten und planmäßigen Informationssicherheits-prozesses sowie aller dafür erforderlichen Informationssicherheitsmaßnahmen notwendig ist.

Ziel des Sicherheitsmanagements ist es, das angestrebte Sicherheitsniveau zu erreichen und dieses auch dauerhaft aufrechtzuerhalten sowie zu verbessern. Daher müssen der Sicherheitsprozess und die Organisationsstrukturen für Informationssicherheit regelmäßig daraufhin überprüft werden, ob sie angemessen, wirksam und effizient sind. Ebenso ist zu überprüfen, ob die Maßnahmen des Sicherheitskonzeptes praxisnah sind und ob sie korrekt umgesetzt wurden.

3.3 Erstellung des IT-Sicherheitskonzeptes

Im Folgenden werden die einzelnen Schritte beschrieben, die notwendig sind, um ein individuelles IT-Sicherheitskonzept zur erstellen. Detaillierte Handlungsanweisungen zu diesen Schritten sind in [BSI 100-2] enthalten:

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

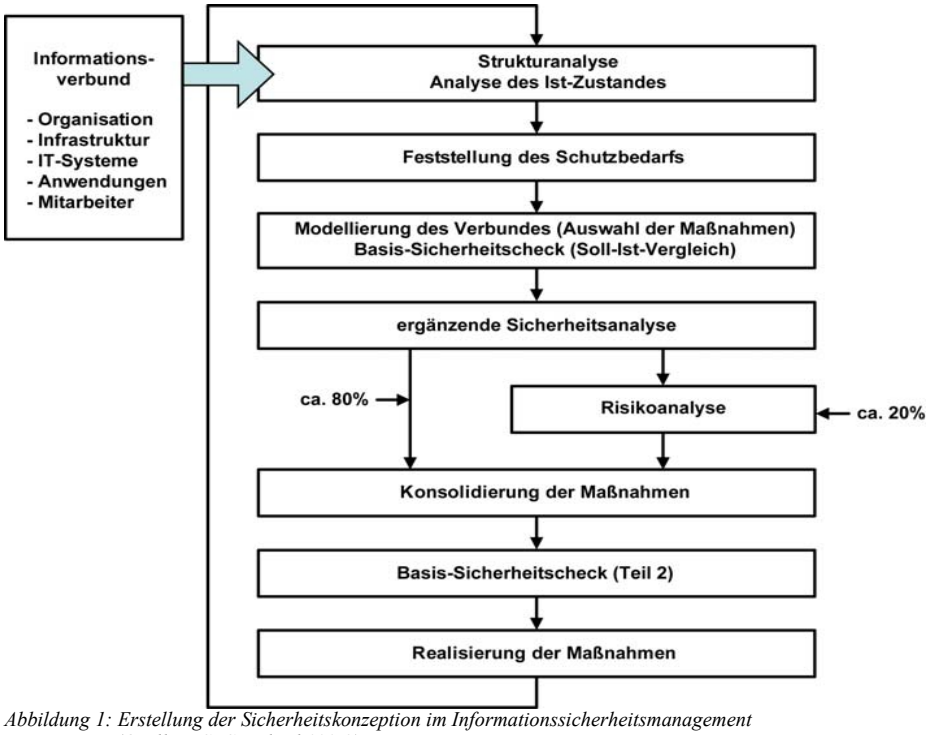


Abbildung 1: Erstellung der Sicherheitskonzeption im Informationssicherheitsmanagement (Quelle: BSI-Standard 100-2)

3.3.1 Definition des Informationsverbundes

In den Geltungsbereich fallen alle Dienste, die der DMDA im Rahmen dieses Projektes anbietet. Dazu ist durch den DMDA innerhalb des Sicherheitskonzepts der Untersuchungsgegenstand darstellen und ggf. zu anderen von ihm angebotenen Diensten abzugrenzen.

3.3.2 IT-Strukturanalyse

Im Rahmen der IT-Strukturanalyse erfolgt eine Aufnahme und Abgrenzung des zu betrachtenden IT-Verbundes. Die Analyse bezieht die vorhandene Infrastruktur, die organisatorischen und personellen Rahmenbedingungen, die eingesetzten IT-Systeme, die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen sowie die im IT-Verbund betriebenen Anwendungen ein.

3.3.3 Schutzbedarfsfeststellung

Mit der Schutzbedarfsfeststellung stellt der DMDA den Schutzbedarf für die zu schützenden Objekte (IT-Anwendungen, Kommunikationsverbindungen, IT-Systeme und Infrastruktur) fest.

Angesichts der regelmäßig bei den De-Mail-Diensten verwendeten Daten ist grundsätzlich von einem hohen Schutzbedarf für die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit auszugehen.

Der Schutzbedarf der zu schützenden Objekte ergibt sich unmittelbar aus dem Schutzbedarf, der durch die Anwendungen oder IT-Systeme transportierten, verarbeiteten und gespeicherten zu schützenden Informationen.

In der Schutzbedarfsfeststellung wird also ermittelt, welcher Schutzbedarf für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Dabei werden mögliche Schäden und Folgeschäden bei einer Beeinträchtigung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität betrachtet. Zunächst müssen Schutzbedarfskategorien definiert werden. Danach wird der Schutzbedarf der IT-Anwendungen, der IT-Systeme, der Kommunikationsverbindungen und der betroffenen IT-Räume ermittelt.

Sofern im Rahmen der notwendigen Schutzbedarfsfeststellung für einzelne Grundwerte ein sehr hoher Schutzbedarf ermittelt wird, ist insbesondere zu prüfen, welche Dienste aufgrund der konkreten Verfahrensgestaltung beim De-Mail-Diensteanbieter betroffen sind. Dies ist entsprechend im Rahmen der Sicherheits- und Risikoanalyse zu berücksichtigen. Abhängig vom Ergebnis der Sicherheits- und Risikoanalyse sind dann ggf. zusätzliche Schutzmaßnahmen bei dem jeweils betroffenen Dienst umzusetzen. Wenn Auswirkungen auf weitere Dienste im Informationsverbund nicht auszuschließen sind, ist auch für diese die Notwendigkeit der Anpassung der Maßnahmen zu prüfen.

3.3.4 Modellierung

Bei der Modellierung wird festgelegt, welche Bausteine der IT-Grundschutzkataloge auf welche Zielobjekte im betrachteten IT-Verbund angewandt werden.

Im Rahmen der Modellierung eines Informationsverbunds „De-Mail“ sind nachfolgende Bausteine zwingend umzusetzen:

- B 1.0 IT-Sicherheitsmanagement
- B 1.3 Notfallvorsorgemanagement
- B 1.7 Kryptokonzept
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.12 Archivierung

Sofern wesentliche Bereiche des IT-Verbunds (Infrastruktur, Personal) ausgelagert werden, muss der De-Mail-Diensteanbieter folgenden IT-Grundschutzbaustein umsetzen:

- B 1.11 Outsourcing

3.3.5 Basis-Sicherheitscheck

Der Basis-Sicherheitscheck stellt die Aufnahme des tatsächlichen zum jeweiligen Prüfzeitpunkt festgestellten Sicherheitszustands dar. Dabei wird für jede Maßnahme, die in den für die Modellierung herangezogenen Bausteinen enthalten ist, der Umsetzungsstatus vermerkt: "entbehrlich", "ja", "teilweise" oder "nein". Sofern eine Maßnahme als "entbehrlich" angesehen wird, muss dies gesondert begründet werden.

3.3.6 Ergänzende Sicherheitsanalyse

Es wurde festgelegt, dass der Schutzbedarf für die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität insgesamt hoch ist. Für alle Zielobjekte ist darüber hinaus eine ergänzende Sicherheitsanalyse zu erstellen. In dieser ist festzulegen, für welche Zielobjekte eine ergänzende Risikoanalyse durchgeführt werden muss. Dabei sind die Entscheidungen nachvollziehbar zu begründen. Zusätzlich sind in diesen Betrachtungen Zielobjekte einzubeziehen, die entweder mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können, oder die in Einsatzszenarien betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Für alle noch nicht durch Grundschutz abgedeckten Zielobjekte ist eine Risikoanalyse durchzuführen.

3.3.7 Risikoanalyse

Die Risikoanalyse hat die Aufgabe, relevante Gefährdungen zu identifizieren und vorhandene Risiken für die Zielobjekte abzuschätzen. Durch die geeignete Auswahl von Gegenmaßnahmen soll das Risiko auf ein vertretbares Maß gesenkt werden. Die Entscheidung, welche Bereiche in der Risikoanalyse betrachtet werden, wird durch die Leitungsebene auf Basis der ergänzenden Sicherheitsanalyse getroffen.

Für die Durchführung der Risikoanalyse kann die Vorgehensweise aus [BSI 100-3] gewählt werden. Die Risikoanalyse gliedert sich dabei in die folgenden Schritte auf:

- Erstellung der Gefährdungsübersicht,
- Ermittlung zusätzlicher Gefährdungen,
- Bewertung der ermittelten Gefährdungen,
- Behandlung der Risiken,
- Konsolidierung des Sicherheitskonzeptes und
- Rückführung in den Sicherheitsprozess.

Die Abdeckung des hohen Schutzbedarfs ist explizit zu begründen. Auch in diesem Schritt sind die durch die Technische Richtlinie De-Mail IT-Sicherheit festgelegten Bedrohungen, Sicherheitsziele und Anforderungen zwingend zu berücksichtigen. Die in der Technischen Richtlinie De-Mail IT-Sicherheit enthaltenen Empfehlungen sind dabei zu würdigen. Abweichungen sind gesondert, im IT-Sicherheitskonzept zu begründen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Wichtig:

Im Rahmen der Modellierung sind über die Maßnahmen der jeweilig zu betrachtenden Bausteine hinaus die Anforderungen aus den jeweiligen Modulen der Technische Richtlinie De-Mail [TR DM] zu berücksichtigen.

3.3.8 Konsolidierung

Es ist davon auszugehen, dass im Rahmen der ergänzenden Sicherheitsanalyse bzw. der Risikoanalyse bezogen auf die Grundschutzkataloge zusätzliche IT-Sicherheitsmaßnahmen als notwendig erkannt werden. Daher muss eine Konsolidierung des IT-Sicherheitskonzeptes erfolgen. Das Verfahren ist in [BSI 100-3], Kapitel 7 beschrieben.

3.3.9 Ergänzender Basis-Sicherheitscheck

Als nächster Schritt wird für den IT-Verbund ein zweiter Basis-Sicherheitscheck des De-Mail-Diensteanbieters durchgeführt, um den Umsetzungsgrad der zusätzlichen bzw. geänderten Maßnahmen zu überprüfen.

3.3.10 Realisierung

Zum Ende der vorab durchgeführten Prüfungsschritte müssen die erkannten Defizite abgestellt worden sein, sodass der tatsächliche Zustand der Sicherheit der geforderten Sicherheit entspricht.

3.3.11 Penetrationstests und IS-Kurz-Revision

Das Prüfteam besteht aus vom BSI zertifizierten IS-Revisoren und Penetrationstestern oder aus Mitarbeitern des BSI.

Für den erfolgreichen Abschluss der in diesem Modul beschriebenen Testierung ist für jeden betroffenen De-Mail-Dienst ein IT-Penetrationstest sowie eine IS-Kurzrevision durchzuführen und zu dokumentieren. Dies dient der Vorabkontrolle der wesentlichen Sicherheitsmerkmale und der Feststellung grober Sicherheitsmängel. Dem DMDA soll damit die möglichst reibungslose Auditierung nach ISO 27001 auf Basis von IT-Grundschutz für De-Mail-Dienste erleichtert werden. Das diesbezügliche Vorgehen wird nachfolgend beschrieben.

Das IT-Penetrations-Testverfahren für De-Mail-Provider wird mehrstufig durchgeführt. Nach einem Web-Sicherheitsscheck ermittelt das Prüfteam auf Grundlage einer Dokumentenprüfung und einer Vor-Ort-Prüfung den Sicherheitsstatus des Providers. Betrachtet werden Prüfthemen, die eine wesentliche Grundlage für die Informationssicherheit bilden [PenTest].

Im ersten Schritt wird über das Internet die Webanwendung mittels verschiedener Tools auf Schwachstellen untersucht. Bei diesem Test geht es ausdrücklich um die Überprüfung der Sicherheitseigenschaften der Webanwendung und nicht um die Eigenschaften zusätzlich eingesetzter Sicherheitsgateways. Da Firewall-Regeln oft dynamisch im Betrieb verändert werden und alle Komponenten von Sicherheitsgateways ebenso, wie andere Systeme bei Schwachstellen ausgehebelt werden können, legt die Prüfung großen Wert darauf, dass bekannte Schwachstellen

wie beispielsweise Cross-Site-Scripting oder Cross Site Request Forgery schon bei den Webanwendungen vermieden werden.

Um diese Tests durchführen zu können, ohne die Sicherheitsgateways abzuschalten, muss für das Prüfteam ein direkter Zugang zur Anwendung bestehen, der unmittelbar nach den Tests wieder entfernt werden kann. Wichtig ist, dass ein kompetenter Ansprechpartner des Providers vor Ort die Tests betreut und sie beobachtet.

Wenn der erste Web-Sicherheitscheck abgeschlossen ist, werden bei einem Vor-Ort Termin weitere Sicherheitseigenschaften getestet. Im Vorfeld der Vor-Ort-Prüfung wird die Dokumentation des Providers gesichtet, um eine Teststrategie zu entwickeln. Dazu erhält das Prüfteam Einsicht in die Dokumentation des Providers (z.B. Netzpläne, Liste der kritischen Geschäftsprozesse, IT-Sicherheitskonzept, Dokumentation der Anlage usw.). Zu Beginn der Vor-Ort-Prüfung findet ein Eröffnungsgespräch statt, in dem kurz die Vorgehensweise und die Zielrichtung der Prüfung und Tests erläutert werden. Bei der Vor-Ort-Prüfung werden Interviews geführt, die Liegenschaft begangen und die Systeme in Augenschein genommen. Das Prüfteam benötigt Shell-Zugänge zu den zu testenden Systemen, um die Konfigurationen zu überprüfen. Zur Analyse des Netzwerkverhaltens braucht das Prüfteam einen Mirror-Port an den zu testenden Stellen im Netzwerk oder die Möglichkeit, Taps anzuschließen, die bei Bedarf auch durch das Prüfteam gestellt werden können. Für Fragen zu den einzelnen Themen müssen kompetente Ansprechpartner verfügbar sein. Insbesondere sollte der IT-Sicherheitsbeauftragte das Prüfteam begleiten. Zusätzlich ist wichtig, dass ein Administrator des Providers die Tests direkt vor Ort betreut, damit Fragen geklärt werden können.

Zum Abschluss der Prüfungen und Tests wird eine Abschlussbesprechung durchgeführt. Hierbei werden die gefundenen Schwächen und Mängel präsentiert. Die Ergebnisse werden in einem Abschlussbericht zusammengefasst. Der De-Mail Provider muss bis zum Audit alle wesentlichen Mängel beseitigen und die Art und Weise der Beseitigung nachvollziehbar dokumentieren. Dieses Dokument ist dann dem zertifizierten De-Mail-Auditor zur Verfügung zu stellen.

3.4 Testat für den De-Mail IT-Verbund

Nach der Umsetzung des IT-Sicherheitskonzeptes kann ein Testat auf Basis von IT-Grundschutz bei einem zertifizierten IT-Sicherheitsdienstleister beantragt werden, der das Testat ausstellt.

Für die Durchführung von Audits eines DMDA muss ein vom BSI zertifizierter De-Mail-Auditor gewählt werden.

Im Rahmen der Auditierung müssen dem zertifizierten De-Mail-Auditor und der Testatstelle dann folgende Referenzdokumente vom Antragsteller zur Verfügung gestellt werden:

- IT-Sicherheitsrichtlinien (A.0),
- IT-Strukturanalyse (A.1),
- Schutzbedarfsfeststellung (A.2),
- Modellierung des IT-Verbundes (A.3),
- Ergebnisse des Basis-Sicherheitschecks (A.4) (optionale Vorlage bei der Testatstelle; verpflichtende Vorlage beim zertifizierten De-Mail-Auditor),
- Ergänzende Sicherheitsanalyse (A.5),
- Risikoanalyse (A.6),

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

- Ergebnisse der IT-Penetrationstests,
- Ergebnisse der IS-Revision.

Einzelheiten zum Verfahren sind analog zur Zertifizierung in dem Dokument [Zert ISO 27001] festgelegt und anzuwenden.

– Seite 369 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

4 Ergänzende Anforderungen an den zertifizierten De-Mail-Auditor

Die für eine Auditierung von De-Mail-Diensten zu erfüllenden Voraussetzungen durch den zertifizierten De-Mail-Auditor ergeben sich aus der Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen [VB_Personen] sowie dem Programm zur Kompetenzfeststellung und Zertifizierung von Personen [Program_Personen].

Hinsichtlich der Durchführung des Audits gelten grundsätzlich die Vorgaben von [Zert ISO 27001]. Der zertifizierte De-Mail-Auditor hat darüber hinaus insbesondere auch zu prüfen, ob die Festlegungen der Schutzbedarfsfeststellung in Übereinstimmung mit diesem Modul und [TR DM Si ÜK] erfolgt sind. Das Ergebnis dieser Prüfung ist gesondert darzustellen.

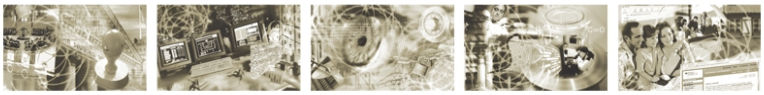
Zudem hat der zertifizierte De-Mail-Auditor zu überprüfen, ob bei der Durchführung der ergänzenden Sicherheitsanalyse und der Risikoanalyse die in den relevanten Teilen der Technischen Richtlinie De-Mail IT-Sicherheit festgelegten Sicherheitsziele und zwingenden Vorgaben beachtet und umgesetzt wurden. Das Ergebnis dieser Prüfungen ist explizit darzustellen.

In einigen der zwingenden Anforderungen ist daneben festgelegt, dass für die eingesetzten Produkte eine hinreichende Güte durch eine entsprechende Sicherheitszertifizierung nachgewiesen werden muss. Durch den zertifizierten De-Mail-Auditor ist daher zu prüfen, ob für die eingesetzten Produkte entsprechende Sicherheitszertifikate vorliegen und ob die Anforderungen an die Einsatzumgebung, die der Produktzertifizierung zugrunde liegen, eingehalten werden. Das Ergebnis dieser Prüfung ist darzustellen.

Für die Dokumentation der beschriebenen Zusatzprüfung ist wird dem zertifizierten De-Mail-Auditor ein Musterauditreport zur Verfügung gestellt, den der zertifizierte De-Mail-Auditor beim BSI anfordern kann.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt
für Sicherheit in der
Informationstechnik



BSI – Technische Richtlinie

Bezeichnung:	Sicherheit Übergeordnete Komponenten
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 6.1
Version:	1.00

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

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: http://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Abbildungsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Tabellenverzeichnis

1 Aufbau dieses Dokumentes

Dieses Modul ist Teil der [TR DM] und enthält eine generische IT-Strukturanalyse mit einem generischen Netzplan für einen De-Mail-Dienst.

Kapitel 3 enthält eine Schutzbedarfsfeststellung für IT-Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume. Kapitel 4 beschreibt die Bedrohungen, die der Ableitung von Sicherheitszielen zugrunde gelegt werden.

Die Sicherheitsziele sind in Kapitel 5 dargelegt, während Kapitel 6 die bei der Erstellung eines konkreten IT-Sicherheitskonzepts zu berücksichtigenden Anforderungen enthält. In Kapitel 7 werden schließlich Empfehlungen ausgesprochen, die bei der Erstellung eines Sicherheitskonzeptes Berücksichtigung finden sollten, von denen aber auch abgewichen werden kann. Kapitel 8 enthält eine Gegenüberstellung der Bedrohungen zu den IT-Sicherheitszielen, in Kapitel 9 werden diese den Anforderungen gegenübergestellt.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

2 IT-Strukturanalyse

Für die Erstellung des Moduls IT-Sicherheit [TR DM Si M] wurde eine generische IT-Strukturanalyse durchgeführt. Sie dient dem Zweck, Sicherheitsziele, Anforderungen und Empfehlungen zu formulieren, die eine Basis für die Erstellung des jeweils konkreten IT-Sicherheitskonzepts für den jeweiligen De-Mail-Dienst darstellen. In der Praxis kann die konkrete Ausgestaltung der eingesetzten Informationstechnik von den hier gemachten generischen Annahmen abweichen. Bei der Erstellung des konkreten IT-Sicherheitskonzepts sind dann die entsprechenden Anforderungen auf die eingesetzte Infrastruktur abzubilden.

2.1 Erfassung des IT-Verbundes

Die durch De-Mail-Dienste transportierten, verarbeiteten und gespeicherten Daten der potentiellen Benutzer werden zur Ermittlung des Schutzbedarfs herangezogen.

Hinsichtlich der Netzarchitektur, der IT-Systeme und der IT-Räume werden entsprechend der Vorgehensweise im IT-Grundschutz Annahmen für einen typischen De-Mail-Dienst getroffen.

Im Fall der Erstellung eines konkreten IT-Sicherheitskonzepts muss der DMDA:

- die Netzplanerhebung,
- die Erhebung der IT-Systeme und
- die Erfassung der IT-Räume

selbst erstellen.

2.2 Analyse der Geschäftsprozesse

Die hier dargestellten Geschäftsprozesse sind die De-Mail-Prozesse und -funktionen innerhalb eines De-Mail-Dienstes.

Die Abbildung 1: Komponenten eines De-Mail-Dienstes gibt einen Überblick über die Komponenten, beteiligten Rollen und funktionellen Kommunikationsverbindungen eines De-Mail-Dienstes.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

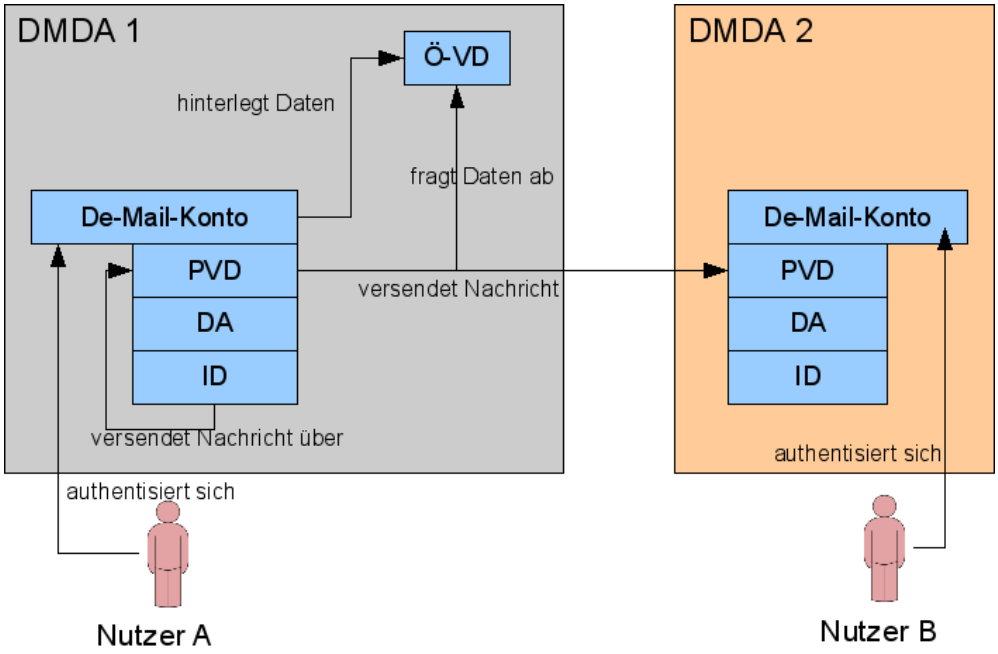


Abbildung 1: Komponenten eines De-Mail-Dienstes

2.3 Generische Netzarchitektur

Die nachfolgende Abbildung zeigt den generischen Netzplan eines typischen De-Mail-Dienstes aufgrund von hier getroffenen Annahmen. Eine Beschreibung der Komponenten erfolgt im Rahmen der Erhebung der generischen IT-Systeme. Es handelt sich bei dem generischen Netzplan um eine beispielhafte Architektur. Anhand dieser wird die allgemeine Vorgehensweise im IT-Grundschutz skizziert und die generischen Sicherheitsanforderungen abgeleitet. Die konkrete technische Umsetzung bei einem DMDA darf von der hier Dargestellten abweichen, muss aber die wesentlichen Aspekte abdecken.

Die dargestellte Netzarchitektur ist exemplarisch und kann so umgesetzt werden.

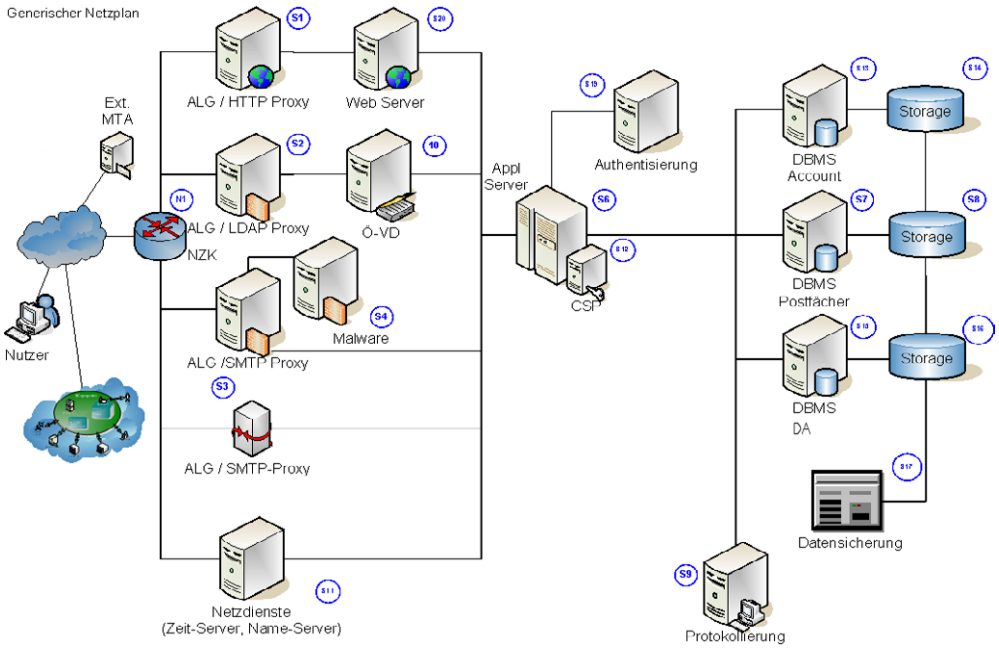


Abbildung 2: Generischer Netzplan

2.4 Generische IT-Systeme

In diesem Abschnitt werden alle typischen IT-Systeme für einen generischen De-Mail-Dienst erhoben. Die Erhebung beruht auf dem generischen Netzplan.

Nr.	*Beschreibung*	*Aufstellungs-ort*	*Verwendungszweck*	*Anwender/Admin.*
S1	ALG / HTTP Proxy	SR-DMDA	Schnittstelle zum Nutzer für den Zugriff auf Webserver	Nutzer/Admin
S2	ALG / LDAP Proxy	SR-DMDA	Schnittstelle zum Nutzer für den Zugriff auf den LDAP-Server	Nutzer/Admin
S3	ALG / Mail Proxy (Anwender)	SR-DMDA	Schnittstelle zum Nutzer für den Zugriff auf einen Mailserver	Nutzer/Admin
S4	ALG / SMTP Proxy (InterDM Gateway)	SR-DMDA	Schnittstelle zu anderen DMDA für den Nachrichtenaustausch	Nutzer/Admin
S5	Web-Server	SR-DMDA	Server zum Ausliefern der Webseiten	Admin
S6	ÖVD	SR-DMDA	Speicherung der öffentlich zugänglichen Verzeichnisdienst-Informationen	Admin
S7	Netzdienste	SR-DMDA	Allgemeine Dienste wie z.B. DNS, Zeitserver	Admin
S8	Malware-Scanner	SR-DMDA	Überprüfung des Datenflusses nach schadhaften Inhalten wie z.B. Viren, Trojaner, Würmer und andere Schadsoftware	Admin
S9	Applicationserver	SR-DMDA	Aufnahme der Anwendungs- und/oder Geschäftslogik und Vermittlung zu den Backend-Systemen z.B. DBMS	Admin
S10	Crypto Service Provider	SR-DMDA	Bereitstellung von kryptographischen Funktionen zum verschlüsseln und signieren von Transaktionen	Admin
S11	Authentisierung	SR-DMDA	Server zur Authentisierung der Nutzer	Admin
S12	DBMS ACM	SR-DMDA	Datenbank zur Speicherung der Konten	Admin
S13	DBMS PVD	SR-DMDA	Datenbank zur Speicherung des PVD	Admin
S14	DBMS DA	SR-DMDA	Datenbank zur Speicherung der	Admin

Nr.	*Beschreibung*	*Aufstellungs-ort*	*Verwendungszweck*	*Anwender/Admin.*
			DA	
S15	Datensicherung	Backup-DMDA	System zur Verwaltung und Ablage der Datensicherungen	Admin
S16	Administration / Protokollierung	BR-DMDA	Clients zum Administration und Protokollierung	Admin
S17	AMC	extern	Externer Client für die Identifizierung	DMDA-Mitarbeiter
NZK	Netzzugangsknoten			Nutzer/Admin

Tabelle 1: Erhebung der IT-Systeme

2.5 IT-Anwendungen

Es werden hier alle Anwendungen zusammengefasst, die zur Administration benötigt werden. Bei der konkreten Ausgestaltung sind die jeweiligen Anwendungen aufzuführen.

Erhebung der IT-Anwendungen																			
Beschreibung der IT-Anwendungen		***IT-Systeme***																	
Anw.-Nr.	IT-Anwendung/ Informationen	Pers.-bez. Daten	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17
A1	Webserver	X					X												
A2	ÖVD	X						X											
A3	Mailserver	X			X	X													
A4	DNS								X										
A5	Zeitserver								X										
A6	Malware-Scanner									X									
A7	Spam-Filter				X	X													
A8	Application-Container	X									X	X	X						
A9	Datenbankserver	X												X	X	X			
A10	Administrations-anwendungen	X																X	
A11	Web-Browser[1]	X																	X

Tabelle 2: Erhebung der IT-Anwendungen

1 Dies gilt für den Fall, dass die Kontoverwaltung über eine Weboberfläche durchgeführt wird. Ansonsten handelt es sich um eine andere Client-Anwendung.

2.6 Generische Räume

Hier sind die typischen IT-Räume für einen generischen De-Mail-Dienst dargestellt:

Erhebung der Räume		
Raum		*IT / Informationen*
Bezeichnung	*Art*	*IT-Systeme /Datenträger*
RZ-DMDA	Rechenzentrum	Diese Zuordnung kann nur bei der Betrachtung eines konkreten DMDA erfolgen.
SR-DMDA	Serverraum	
BR-Admin	Büroraum	
Backup-DMDA	Datenarchiv für Nutzerdaten	
Archiv-DMDA	Archiv für die langfristige Aufbewahrung	

Tabelle 3: Erhebung der Räume

2.7 Kommunikationsverbindungen

Diese Tabelle zeigt die typischen Kommunikationsverbindungen für einen generischen De-Mail-Dienst. Die Auflistung der Kommunikationsverbindungen erfolgt anhand des generischen Netzplans und stellt alle Verbindungen zwischen den beschriebenen Systemen dar.

Kommunikations verbindung	*Dienste*	*Art*	*IT-Systeme*
V1	PVD, DA, ID	extern	Nutzer - S1
V2	B-Infra	extern	Nutzer - S2
V3	PVD	extern	Nutzer - S3
V4	PVD	extern	ExtMTA - S3
V5	PVD	extern	DMDA - S4
V6	B-Infra	extern	Nutzer, DMDA - S7
V7	PVD, DA, ID	intern	S1 - S5
V8	PVD	intern	S2 - S6
V9	PVD	intern	S3 - S8
V10	PVD	intern	S4 - S8
V11	PVD, DA, ID	intern	S5 - S9
V12	PVD	intern	S6 - S9
V13	PVD	intern	S3 - S9
V14	PVD	intern	S4 - S9
V15	PVD, DA, ID	intern	S9 - S10

– Seite 383 von 412 –
Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Kommunikations verbindung	*Dienste*	*Art*	*IT-Systeme*
V16	PVD, DA, ID	intern	S9 - S11
V17	PVD, DA, ID	intern	S9 - S12
V18	PVD	intern	S9 - S13
V19	DA	intern	S9 - S14
V20	PVD, DA, ID	intern	S12 - S15
V21	PVD	intern	S13 - S15
V22	DA	intern	S14 - S15
V23	PVD, DA, ID	intern	S16 - S9

Tabelle 4: Kommunikationsverbindungen

3 Schutzbedarfsfeststellung

Mit der Schutzbedarfsfeststellung stellt der DMDA den Schutzbedarf für die zu schützende Objekte fest. Die Schutzbedarfsfeststellung beruht auf einer Analyse der Schutzbedürftigkeit der zu übermittelnden Informationen.

Der Schutzbedarf der IT-Anwendungen ergibt sich aus der Schutzbedürftigkeit der übertragenen und gespeicherten Daten. Die IT-Systeme „erben“ den Schutzbedarf von den darauf installierten IT-Anwendungen. Der Schutzbedarf der Räume ergibt sich aus dem Schutzbedarf der darin betriebenen IT-Systeme. Die Kritikalität der Verbindungen ergibt sich aus dem Schutzbedarf der übertragenen Daten. Bei den Festlegungen der Schutzbedürftigkeit findet das Maximumprinzip Anwendung. Es wird jeweils der höchste Schutzbedarf im jeweiligen als Grundlage gewählt.

Angesichts der regelmäßig bei den De-Mail-Diensten verwendeten Daten ist grundsätzlich von einem hohen Schutzbedarf für die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit auszugehen.

4 Bedrohungen

Nachfolgend werden die angenommenen generischen Bedrohungen für De-Mail-Dienste dargestellt:

4.1 Verlust der Vertraulichkeit

Verlust der Vertraulichkeit bedeutet, dass Unbefugte Kenntnis von schützenswerten Informationen erlangen. Gründe dafür können sein:

- Unbefugter Zutritt zu den Betriebsräumen
- Unbefugter Zugang zu den Systemen
- Unbefugter Zugriff auf Daten
- Einsatz unsicherer kryptografischer Funktionen und Verfahren
- Nicht bestimmungsgemäßer Einsatz kryptografischer Komponenten
- Abhören der Kommunikation inner- oder außerhalb des DMDA

Bei mangelnder Vertraulichkeit können vertrauliche Daten unbefugt von Dritten eingesehen werden.

4.2 Verlust der Integrität

Verlust der Integrität bedeutet, dass Daten unbefugt verändert werden. Gründe dafür können sein:

- Technisches Versagen
- Unbefugter Zugriff auf Daten

Integrität im Sinne des IT-Grundschutzes umfasst auch die Authentizität einer Nachricht, da in einer Gesamtbetrachtung auch Metadaten, wie z. B. die Information, wer eine Nachricht verfasst hat, zur Nachricht selbst gehören. Ein Verlust der Integrität ist auch dadurch möglich, dass die Urheberschaft nicht mehr sicher festgestellt werden kann.

Die Sicherstellung der Integrität der Nachrichten bezieht sich dabei nicht nur auf die beim DMDA gespeicherten Daten, sondern auch auf die zwischen den DMDA übertragenen Daten, sowie auf die Bestätigungen und Nachweise, die durch den DMDA ausgestellt werden.

4.3 Verlust der Verfügbarkeit

Geht die Verfügbarkeit der Systeme verloren, ist der bestimmungsgemäße Betrieb und der damit verbundenen Dienst nicht mehr möglich. Gründe dafür können sein:

- Technisches Versagen
- Bewusste Manipulation (z.B. Veränderung oder Löschung)
- Unbefugte Eingriffe (z.B. Viren oder unbefugter Zugriff)

- Katastrophale Ereignisse
- Terroristische Angriffe

Bei Verfügbarkeitsverlust sind die Nutzer während eines Ausfalls nicht mehr in der Lage, die De-Mail-Dienste bestimmungsgerecht zu nutzen.

4.4 Unberechtigte Nutzung der Dienste

Durch eine unzureichende oder fehlerhafte Authentisierung kann es möglich sein, dass Dienste durch nicht dazu berechtigte Personen genutzt werden.

5 Sicherheitsziele

5.1 Vorbemerkungen

Der Leitgedanke der De-Mail-Konzeption ist die Bereitstellung eines sicheren Kommunikationsraumes. Ein De-Mail-Dienst muss eine sichere Anmeldung, Nutzung eines PVD für sichere elektronische Post sowie die Nutzung eines ÖVD ermöglichen.

Innerhalb des Kommunikationsraumes sind insbesondere folgende Grundwerte zu gewährleisten:

- Verfügbarkeit,
  - von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern jederzeit stets wie gewünscht (mit Ausnahme zumutbarer Ausfallzeiten) zur Verfügung stehen.
- Vertraulichkeit und
  - ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich gemacht werden.
- Integrität
  - im engeren Sinne bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Informationen" wird dabei für Daten verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Bei De-Mail ist eine nutzerorientierte Datenhaltung zu realisieren. Eine strikte Trennung der Nutzer ist erforderlich, um zu verhindern, dass diese gegenseitigen Einblick in ihre Daten erhalten können.

Den Sicherheitsanker in De-Mail bildet das De-Mail-Konto. Ein De-Mail-Konto ist ein Bereich in einem De-mail-Dienst, der einem Nutzer so zugeordnet ist, dass er nur von ihm genutzt werden kann. Der DMDA hat durch technische Mittel sicherzustellen, dass nur der diesem De-Mail-Konto zugeordnete Nutzer Zugang zu dem ihm zugeordneten De-Mail-Konto erlangen kann. Das De-Mail-Konto verwaltet die Zugangsberechtigung zum De-Mail-Dienst und damit die Berechtigung, die weiteren De-Mail-Dienste zu nutzen und auf Nutzerdaten zugreifen zu können. Sämtliches Handeln eines Nutzers ist unmittelbar mit dem De-Mail-Konto verbunden und lässt sich immer darauf zurückführen.

Um im De-Mail-Verbund handeln zu können, muss ein Nutzer sich am De-Mail-Dienst anmelden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

5.2 Übergreifende Aspekte

Daraus ergeben sich die im folgenden beschriebenen übergreifenden Sicherheitsziele. Diese Ziele gelten für De-Mail mit allen Diensten, die darin betrieben werden. Ergänzend sind die zu den einzelnen Diensten spezifisch definierten Anforderungen zu berücksichtigen.

5.2.1 Wahrung der Vertraulichkeit

Die Wahrung der Vertraulichkeit der gespeicherten und zu übertragenden Daten ist durch geeignete organisatorische und technische Maßnahmen sicherzustellen.

Dies beinhaltet insbesondere:

- Vermeidung unbefugten Zutritts,
- Verhinderung des unbefugten Zugangs,
- Verhinderung des unbefugten Zugriffs auf sensible Daten und
- verschlüsselte Speicherung und Transport der Daten.

5.2.2 Sicherstellung der Integrität

Durch geeignete Maßnahmen ist sicherzustellen, dass Daten nicht unbemerkt verändert werden können. Dies betrifft die Daten, die beim DMDA gespeichert sind und die Daten, die zwischen zwei DMDA übertragen werden. Sofern unbefugte Veränderungen erfolgen, müssen diese feststellbar sein. Die Konfiguration von Diensten und Systemen darf ebenfalls nicht unbefugt verändert werden.

5.2.3 Sicherstellung der Verfügbarkeit

Durch geeignete Maßnahmen ist sicherzustellen, dass eine Verfügbarkeit von 99,5 % pro Jahr gewährleistet wird. Ein Ausfall bis zu 24 Stunden, im Falle eines katastrophalen Ereignisses bis zu 72 Stunden ist hinnehmbar.

Bei längerfristigen geplanten Ausfallzeiten von mehr als drei Stunden sind die Nutzer rechtzeitig im voraus zu informieren.

5.2.4 Aufrechterhaltung des IT-Sicherheitsniveaus

Die Aufrechterhaltung des notwendigen IT-Sicherheitsniveaus ist durch den DMDA geeignet sicherzustellen. Zu diesem Zweck ist die Einhaltung und Fortschreibung des IT-Sicherheitskonzepts sicherzustellen.

5.2.5 Korrekte Authentisierung

Der DMDA muss sicherstellen, dass die Authentisierung der Nutzer gemäß den Anforderungen aus [TR DM ACM FU] zuverlässig und mit dem jeweils vorgegebenen Authentisierungsniveau erfolgt.

6 Anforderungen

Die nachfolgend formulierten Anforderungen resultieren aus den ermittelten Bedrohungen sowie dem angenommenen hohen Schutzbedarf der durch De-Mail-Dienste verarbeiteten, transportierten und gespeicherten Nutzerdaten.

Die den Anforderungen zugrunde liegende Sicherheitsarchitektur basiert dabei insbesondere auf den folgenden Eckpunkten:

- Zugriffsschutz der Nutzerdaten durch eine verschlüsselte Speicherung,
- Zugriffsschutz der Nutzerdaten durch Transportverschlüsselung,
- Zugriffsschutz der Nutzerdaten auf IT-Systemen mit Klartext-Verarbeitung durch Zutrittsschutz,
- Zugriffsschutz der Nutzerdaten durch Rollen- und Funktionstrennung,
- Integritätssicherung der Nutzerdaten durch elektronische Signaturen,
- Verfügbarkeit der De-Mail-Dienste durch Datensicherungs-, Verfügbarkeits-, und Notfallkonzept,
- Einsatz sicherer Authentisierungsmechanismen.

Sofern bereits etablierte Sicherheitsprozesse bei dem DMDA vorliegen, können diese Anforderungen auch entsprechend referenziert werden.

6.1 Übergreifende Aspekte

6.1.1 Archivierungskonzept

Der DMDA hat ein Archivierungskonzept zu erstellen, in dem insbesondere die dauerhafte Archivierung von Protokollen und anderen Betriebsdaten, die durch einen De-Mail-Dienst entstehen, berücksichtigt werden muss.

6.1.2 Rollenkonzept

Es muss ein Rollenkonzept entwickelt und dokumentiert werden, das den Grundsätzen der Funktionstrennung und nur den berechtigten Personen den Zugriff erlaubt genügt.

Es sind dabei folgende Anforderungen zu erfüllen:

6.1.2.1 Zutrittskonzept

Der DMDA muss ein Zutrittskonzept erstellen. Die Anzahl der Zutrittsberechtigten muss dabei auf das notwendige Minimum beschränkt werden. Es ist sicherzustellen, dass sich in Räumen, in denen IT-Systeme mit vertraulichen Daten betrieben werden, niemals nur ein Mitarbeiter des DMDA allein aufhält (strikte Einhaltung des Vier-Augen-Prinzips).

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

6.1.2.2 Zugangskonzept

Zugang meint hier den Aufbau einer Verbindung zwischen einem IT-System und einem Nutzer, der ihm die Benutzung von Funktionen des IT-Systems ermöglicht.

Das Zugangskonzept muss festlegen, dass jedes IT-System des DMDA durch Mechanismen der Zugangskontrolle vor unberechtigtem Zugang geschützt sein muss. Es sind geeignete Mechanismen zur Authentisierung einzusetzen.

Der Zugang zu Systemen, auf denen unverschlüsselte Daten der Nutzer verarbeitet werden, muss strikt beschränkt und kontrolliert werden. Es sind Mechanismen vorzusehen, die das unbefugte Ausleiten von Daten unterbinden.

6.1.2.3 Zugriffskonzept

Zugriff ist der Vorgang, der einem Nutzer eines IT-Systems Informationen zugänglich macht, die als Daten in einem IT-System gespeichert sind. Dieser Vorgang kann beispielsweise über den Namen einer Datei lesend, schreibend oder ausführend erfolgen.

Das Zugriffskonzept muss die Realisierung des Zugriffschutzes auf schützenswerte Daten darlegen.

Das Zugriffskonzept ist so zu gestalten, dass Schlüsselinhaber keinen Zugriff auf IT-Systeme bekommen, auf denen die verschlüsselten Daten gespeichert werden.

Das Zugriffskonzept muss Mechanismen beschreiben, die sicherstellen, dass nur der berechtigte Benutzer Zugriff auf die für ihn gespeicherten Daten (z.B. De-Mails) erhält.

Des Weiteren müssen innerhalb des Zugriffskonzepts die Zugriffsberechtigungen auf den einzelnen Systemen im Sinne des Rollenkonzepts festgelegt werden, d. h. der System-Administrator darf über volle Zugriffsrechte auf das entsprechende System verfügen. Für alle Anwendungen auf den IT-Systemen werden durch den System-Administrator separate Verzeichnisse angelegt und entsprechend des Rollenkonzepts die Zugriffsrechte für die weiteren Administratoren festgelegt.

6.1.2.4 Rollenausschlüsse

Rollenausschlüsse ergeben sich dabei aus den folgenden grundsätzlichen Einschränkungen:

1. Keine Leitungsfunktion darf operative oder administrative Aufgaben übernehmen.
2. Keine Kontrollfunktion darf operative oder administrative Aufgaben übernehmen (Überwachung des Logging / Monitoring).
3. Die vollen Administrationsrechte müssen auf wenige Personen reduziert werden.
4. Rollen mit Zugriff auf gespeicherte Daten oder Daten, die übertragen werden, dürfen keinen Zugriff auf die verwendeten Schlüssel haben.
5. Der Zugang zu Hardware und Netzwerkinfrastruktur darf in einer Rolle abgebildet werden. Der direkte Zugriff auf die Hardware muss im 4-Augen-Prinzip erfolgen. Aktivitäten sind mittels Logging zu protokollieren.
6. Die Aktivitäten an zur Identitätsverwaltung bzw. -erfassung müssen von der Kontoverwaltung getrennt sein.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Die Kontrollfunktion bezieht sich auf die Auswertung von kumulierten Sicherheitslogs. Logging und Monitoringinformationen, die zum Betrieb und Wartung notwendig sind, sind hiervon nicht betroffen.

6.1.3 Fachkunde und Zuverlässigkeit des Personals

Der DMDA muss die für den Betrieb von De-Mail-Diensten erforderliche Zuverlässigkeit und Fachkunde besitzen. In diesem Zusammenhang ist von besonderer Bedeutung, dass die Mitarbeiter des DMDA vor Aufnahme der Tätigkeit ausreichend geschult werden. Die Schulung beinhaltet u. a. eine Einarbeitung/Einweisung in die auszuübende Tätigkeit und eine Sensibilisierung der Mitarbeiter hinsichtlich der Sicherheitsrelevanz ihrer Arbeit sowie der datenschutzrechtlichen Rahmenbedingungen. Die Mitarbeiter müssen vom für De-Mail verantwortlichen Vorgesetzten (beispielsweise Leiter des Bereichs De-Mail) im laufenden Betrieb auf ihre Fachkunde hin beurteilt werden. Ggf. müssen durch den Vorgesetzten Nachschulungen veranlasst werden.

6.1.4 Changemanagement

Es ist ein Changemanagement zu etablieren. Insbesondere müssen Regelungen für den Lebenszyklus der eingesetzten Hard- und Software erstellt und umgesetzt werden. Dieses muss ebenso ein Freigabeverfahren für neue Hard- und Software enthalten, wie Regelungen zum Umgang mit Updates. Außerdem müssen Regelungen etabliert werden, die die Aussonderung von Hard- und Software betreffen. Hierbei ist ein besonderes Augenmerk auf den Umgang mit Datenträgern (insbesondere auch Festplatten) zu legen.

6.1.5 Verfügbarkeitskonzept

Gemäß [TR DM Si ÜK] sind die Architektur und die De-Mail-Infrastruktur so auszulegen, dass die Vorgaben an die Verfügbarkeit erfüllt werden. Dazu muss der DMDA ein entsprechendes Verfügbarkeitskonzept erstellen. Das Verfügbarkeitskonzept muss Fehlerintoleranz und Fehlertoleranz berücksichtigen. Der DMDA muss darstellen, wie er durch geeignete Maßnahmen diese Anforderungen erfüllt.

6.1.6 Notfallkonzept

Es muss ein Notfallkonzept erstellt werden. Als Notfälle werden alle Ereignisse betrachtet, die die Verfügbarkeit der bestehenden materiellen und technischen Infrastruktur derart bedrohen, dass besondere Maßnahmen zur Sicherung oder Wiederaufnahme des Betriebs notwendig sind. Das Notfallkonzept führt die Maßnahmen auf, die bei bestimmten Notsituationen durchzuführen sind, nennt weiterhin die entsprechenden Verantwortlichen und definiert die einzuleitenden Schritte nach dem Notfall zur Wiedererlangung des Wirkbetriebs. Die „max. tolerierbare Ausfallzeit“ darf 24 Stunden, bei katastrophalen Ereignissen 72 Stunden nicht überschreiten.

6.1.7 Datensicherungskonzept

Der DMDA hat zur Sicherung von Informationen ein Datensicherungskonzept zu erarbeiten, das die Sicherung von in den Speichersystemen befindlichen Daten festlegt. Die Wiederherstellung von Daten, die durch den berechtigten Nutzer gelöscht wurden, ist nicht verpflichtend.

Die Datensicherung muss folgende Anforderungen erfüllen:

- Es darf nicht zu Datenverlust von Nutzerdaten kommen.
- Soweit die Daten im Speicher verschlüsselt vorliegen, sind diese auch verschlüsselt in die Datensicherung zu übernehmen.

6.1.8 Kryptokonzept

Der DMDA muss ein Kryptokonzept unter Festlegung der folgenden Anforderungen erstellen.

6.1.8.1 Allgemeines

Das Kryptokonzept muss die aktuell geltenden Standards hinsichtlich der verwendeten Techniken, Algorithmen und Schlüssellängen berücksichtigen. In [TR 02102] sind die zurzeit geltenden Standards aufgeführt. Es ist regelmäßig zu prüfen, ob die Sicherheitseigenschaften der verwendeten Verfahren weiterhin gegeben sind. Dazu kann auf den Algorithmenkatalog für qualifizierte elektronische Signaturen zurückgegriffen werden, sowie [TR 02102].

Im Kryptokonzept ist weiter darzulegen, auf welche Weise bei Wechsel der Schlüssel die vorhandenen Datenbestände mit den neuen Schlüsseln verschlüsselt werden.

6.1.8.2 Transportverschlüsselung Nutzer - De-Mail-Dienst

Bei der Kommunikation zwischen den Nutzern und dem De-Mail-Dienst können vertrauliche Daten ausgetauscht werden. Diese Daten müssen einerseits vor dem Einblick Dritter geschützt sein, andererseits muss die Authentizität und Integrität dieser Daten gesichert sein.

Die Kommunikationsverbindungen zwischen Nutzer und De-Mail-Dienst müssen verschlüsselt erfolgen.

Die Systeme des DMDA müssen sich gegenüber dem Nutzer authentisieren. Der DMDA muss dem Nutzer den/die Fingerprints des/der verwendeten Zertifikats/Zertifikate in geeigneter Weise zur Kenntnis bringen.

6.1.8.3 Transportverschlüsselung DMDA-DMDA

Die Kommunikation von einem DMDA zu einem anderen muss über einen verschlüsselten gegenseitig authentisierten Kanal erfolgen (TLS-Verbindung siehe [TR DM IT-BInfra IO]). Bei dem Kanalaufbau hat eine gegenseitige Authentisierung stattzufinden. Die verwendeten Zertifikate sind in einer Access Control List (ACL) zu hinterlegen.

Die Sperrlisten sind regelmäßig zu prüfen. Im Falle einer Revozierung eines SSL-Zertifikates muss dieses unverzüglich aus den ACLs entfernt werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

Der DMDA hat Regelungen zur Kontrolle der kryptografischen Schlüssel für die gesicherte Verbindung im IT-Sicherheitskonzept zu treffen.

6.1.8.4 Transportverschlüsselung DMDA-intern

Die Kommunikation zwischen den Systemen des DMDA sollte verschlüsselt erfolgen. Es ist dabei nach Möglichkeit eine gegenseitige Authentisierung vorzusehen.

6.1.8.5 Schlüsselwechsel

Die verwendeten asymmetrischen Schlüssel für gespeicherte Inhalte und für die Transportverschlüsselung zwischen den DMDA sind nach zwei Jahren auszutauschen.

6.1.8.6 Schlüsselaufbewahrung

Bei der Schlüsselaufbewahrung muss gewährleistet werden, dass kein unbefugter Zugriff auf die Schlüssel erfolgen kann.

Bei der Verwendung von Softwareschlüsseln (Soft-PSE) z.B. für die TLS-Verbindung ist mit geeigneten Mitteln sicherzustellen, dass keine unberechtigten Kopien der Schlüssel erstellt werden können.

6.1.9 Dokumentation der Administrationsprozesse

Die Prozesse im Umgang mit den IT-Systemen des DMDA (Installation, Konfiguration, Administration) sind zu dokumentieren und nachzuweisen. Entsprechend der Dokumentation hat die sichere Installation, Konfiguration und Administration der eingesetzten IT-Systeme zu erfolgen. Die für die Mitarbeiter verfügbaren Dokumente zur Durchführung von Prozessen, Checklisten und Verfahrensanweisungen, sowie Handbücher sind in Zusammenarbeit mit den Mitarbeitern und insbes. des IT-Sicherheitsbeauftragten zu erstellen. Die Dokumentation muss möglichst einfach nachzuvollziehen zu sein.

6.1.10 Anforderungen an einzusetzende Hard- und Software

Der eingesetzte Authentisierungsserver muss im Hinblick auf die korrekte Implementierung der Authentisierungsverfahren und der Kryptoalgorithmen dem Stand von Wissenschaft und Technik entsprechen.

Der DMDA muss sich in geeigneter Weise von der Korrektheit der Implementierung der o.g. Verfahren und Algorithmen überzeugen.

Die eingesetzte Firewall-Technik muss im Hinblick auf den Aspekt Informationsflusskontrolle und korrekte Umsetzung eines Regelwerks zur Informationsflusskontrolle möglichst mindestens nach CC EAL 3 evaluiert und zertifiziert sein.

Der CSP des DMDA muss im Hinblick auf die korrekte Implementierung der verwendeten Kryptoalgorithmen und den Zugriffsschutz auf geheime Schlüssel dem Stand von Wissenschaft und Technik entsprechen.

6.2 Infrastruktur

Um eine Infrastruktur mit einer hohen Sicherheit zu realisieren, muss der DMDA mindestens die nachfolgend aufgeführten Anforderungen umsetzen:

6.2.1 Gebäude

Die zum Betrieb von De-Mail erforderlichen technischen Einrichtungen müssen in einem Rechenzentrum untergebracht sein (RZ-DMDA).

Die bauliche Anordnung und die Bausubstanz müssen den gängigen Richtlinien und Anordnung wie z. B: DIN, ISO, VDE, VDMA und Richtlinien des VdS entsprechen.

6.2.2 De-Mail-spezifische Sicherheitsbereiche im Rechenzentrum

Alle IT-Systeme, auf denen Klartextverarbeitung stattfinden, müssen in einem separaten Sicherheitsbereich (SR-DMDA) im Rechenzentrum (RZ-DMDA) aufgestellt und betrieben werden. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Alle weiteren IT-Systeme müssen im Raum SR-RZ aufgestellt und betrieben werden. Der Raum SR-RZ muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Für die Administration der IT-Systeme und Anwendungen muss ein separate Sicherheitsbereich (BR-Admin) im Rechenzentrum (RZ-DMDA) eingerichtet werden. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Das Datensicherungsarchiv (Backup-DMDA) muss im Rechenzentrum in einem weiteren Brandabschnitt untergebracht sein. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

6.2.3 Zutrittsschutz

IT- und Infrastrukturräume sind gegen unberechtigten Zutritt zu schützen. Dabei ist durch geeignete bauliche Maßnahmen oder auch die Verwendung anderer materieller Sicherungstechnik sicherzustellen, dass ein Zutritt Unbefugter hinreichend sicher ausgeschlossen werden kann.

Im Bezug auf externe Täter bedeutet dies, dass die eingesetzte Infrastruktur einen so hohen Widerstandswert haben muss, dass der Versuch des unbefugten Zutritts mindestens so lange abgewehrt wird, wie es dauert, bis alarmierte Einsatzkräfte eintreffen.

Es ist mindestens eine Gefahrenmeldeanlage zu betreiben ist, die dem Stand von Wissenschaft und Technik entspricht. Auf Alarmmeldungen muss unverzüglich und angemessen reagiert werden können.

Es müssen hinreichende Zutrittskontrolltechniken zum Einsatz kommen.

Der Zutritt zu und der Aufenthalt in IT- und Infrastrukturräumen muss kontrolliert, überwacht und dokumentiert werden.

Es muss eine Zutrittskontrollanlage nach den Anforderungen von [BSI 7550] installiert werden. [BSI 7551] ist dabei zu berücksichtigen.

6.3 IT-Systeme

6.3.1 Einsatz eines Management-Netzes

Die sicherheitskritischen IT-Systeme (vgl. Tabelle 1: Erhebung der IT-Systeme) dürfen nur über ein separates Management-Netz administriert werden.

6.3.2 Anforderungen an die Remote-Administration der IT-Systeme

Die Remote-Administration der IT-Systeme in den verschiedenen Sicherheitszonen und des Firewall-Systems selbst dürfen nur über einen gesicherten Weg erfolgen. Der Kanal, durch den die Administration der IT-Systeme und Applikationen erfolgt, muss durch starke Verschlüsselung und starke Authentisierung geschützt werden.

Sofern die Remote-Administration aus Räumen erfolgt, die zu der gleichen Liegenschaft wie das Rechenzentrum des jeweiligen De-Mail-Dienstes gehören, muss der administrative Remote-Zugriff auf die IT-Systeme mindestens durch ein sicheres Passwort geschützt sein.

Sofern die Remote-Administration aus einem – in Bezug auf das Rechenzentrum – externen Gebäude erfolgt, hat eine Zwei-Faktor-Authentisierung zu erfolgen. Für die Administration der Benutzerdaten von Remote besteht ein „hoher“ Schutzbedarf. Bei der Absicherung dieses Zugangs hat der DMDA diesem Rechnung zu tragen.

6.3.3 Aktualität der Software

Es ist sicherzustellen, dass alle relevanten Sicherheitspatches installiert werden. Vor der Installation sind die im Rahmen des Changemanagements entwickelten Regeln zu beachten.

Sofern sicherheitszertifizierte IT-Systeme zum Einsatz kommen gilt folgendes:

- Sofern ein relevanter Patch bereits Gegenstand einer Re-Evaluierung war, so hat auch hier nach erfolgtem Freigabeverfahren die unverzügliche Installation zu erfolgen.
- Sofern ein Sicherheitspatch noch nicht Gegenstand der Re-Evaluierung war, ist durch das IT-Management zu entscheiden, wie zu verfahren ist. Dabei sind die möglichen Risiken gegeneinander abzuwägen. Das Ergebnis dieser Abwägung ist zu dokumentieren und umzusetzen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

6.3.4 Sichere Installation und sicherer Betrieb der eingesetzten IT-Systeme

Neben den allgemeinen Anforderungen analog der IT-Grundschutzkataloge sind die folgenden Anforderungen für alle sicherheitskritischen IT-Systeme (s. Tabelle 1: Erhebung der IT-Systeme), die im Bereich von De-Mail eingesetzt werden, mit geeigneten Maßnahmen umzusetzen:

Die eingesetzten IT-Systeme sind sicher zu installieren und zu betreiben. Dabei sind insbesondere die Hinweise des jeweiligen Herstellers zu berücksichtigen.

Soweit zertifizierte IT-Systeme zum Einsatz kommen, sind die Auflagen hinsichtlich der Anforderungen an die Einsatzumgebung einzuhalten.

Alle IT-Systeme sind auf der Grundlage gehärteter Betriebssysteme zu installieren und zu betreiben. Hinsichtlich der verwendeten Betriebssysteme bedeutet dies, dass diese minimal zu installieren sind. Insbesondere sind alle nicht benötigten Dienste zu deaktivieren. Sie sind zudem zu deinstallieren, sofern dies das jeweilige Betriebssystem zulässt. Alle nicht benötigte Software darf nicht installiert werden bzw. ist zuverlässig zu deinstallieren.

Vor Inbetriebnahme sind die Systeme ausgiebig auf Funktionalität zu testen. Ein besonderer Fokus muss dabei auf den Sicherheitsfunktionen liegen. Hierzu ist ein gesondertes Testkonzept zu erstellen. Die Ergebnisse der Tests sind nachvollziehbar zu dokumentieren. Dies gilt entsprechend nach der Installation von Patches und Updates.

Es gilt der Grundsatz der minimalen Rechtevergabe für Benutzer; d. h. es dürfen nur die für die Aufgabenerfüllung absolut notwendigen Rechte vergeben werden. Die Rechtevergabe ist zu dokumentieren und zu begründen.

Durch geeignete Maßnahmen (beispielsweise Einstellung im BIOS) ist zu erzwingen, dass ein Systemstart nur vom Standard-Laufwerk aus erfolgt.

Das Betriebssystem oder die jeweilige Applikation müssen so konfiguriert werden, dass die im Rahmen des IT-Sicherheitskonzepts festgelegten Authentisierungsmechanismen genutzt werden müssen.

Durch geeignete technische Maßnahmen ist sicherzustellen, dass die Anmeldung eines Berechtigten an einem für De-Mail betriebenen IT-Systems nicht durch einen Unbefugten missbraucht werden kann. Daher ist sicherzustellen, dass, sofern der angemeldete Berechtigte seinen Arbeitsplatz auch nur kurzfristig verlässt, das betroffene IT-System für weitere Zugriffe gesperrt wird. Die Sperre darf nur aufgehoben werden, wenn eine erneute Authentisierung gegenüber dem IT-System erfolgt.

6.3.5 Schadsoftwareschutz

Alle IT-Systeme sind mit geeigneten Mitteln gegen Angriffe mit Schadsoftware zu schützen. Es ist sicherzustellen, dass Infektionen mit Schadprogrammen zuverlässig erkannt und die Schadsoftware unverzüglich beseitigt wird.

6.3.6 Integritätsschutz für IT-Systeme

Alle für De-Mail betriebenen sicherheitskritischen IT-Systeme (s. Tabelle 1: Erhebung der IT-Systeme) sind regelmäßig, mindestens einmal wöchentlich, mit geeigneten technischen Maßnahmen auf Integrität zu prüfen. Die Prüfung und das Ergebnis sind zuverlässig zu dokumentieren.

Sofern bei einer solchen Prüfung festgestellt wird, dass die Integrität des Systems verletzt wurde, sind unverzüglich geeignete Gegenmaßnahmen zu ergreifen. Hierzu ist präventiv ein entsprechender Ablaufplan, beispielsweise in Form einer Checkliste, zu erstellen.

6.3.7 Betriebshandbücher

Für jedes sicherheitskritische IT-System für De-Mail (s. Tabelle 1: Erhebung der IT-Systeme) ist ein Betriebshandbuch zu führen. Dieses muss die aktuelle Konfiguration und Parametrisierung des Betriebssystems, der Dienste und der darauf installierten Applikationen enthalten. Änderungen an der Konfiguration sind zu vermerken und zu begründen.

6.3.8 Protokollierung

Alle sicherheitskritischen IT-Systeme (s. Tabelle 1: Erhebung der IT-Systeme) müssen für den administrativen Zugriff und für Änderungen an der Konfiguration eine Protokollierungskomponente enthalten, die in der Lage ist, jedes der folgenden Ereignisse revisionsfähig zu protokollieren:

- Anmeldevorgänge am System (erfolgreiche und nicht erfolgreiche),
- versuchter Zugriff auf eine der Rechteverwaltung unterliegende Komponente,
- alle Administrations-Verbindungsversuche.

Bei nicht erlaubten Verbindungsversuchen muss eine fest definierte Alarmmeldung ausgegeben werden.

Um unbefugtes teilweises oder komplettes Löschen von Daten zu verhindern und um entsprechende Nachweise zu führen, ist sicherzustellen, dass entsprechende Zugriffe durch das mit der Administration betraute Personal zuverlässig protokolliert werden.

6.3.9 Regelmäßige Penetrationstests

Die IT-Systeme eines jeden De-Mail-Dienstes sind regelmäßigen, anlassbezogenen, mindestens aber jährlichen, Penetrationstests zu unterziehen. Sie sind nach folgendem Schema aufzubauen:

- Recherche nach Informationen über das Zielsystem,
- Scan der Zielsysteme auf angebotene Dienste,
- System- und Anwendungserkennung,
- Recherche nach Schwachstellen,
- Ausnutzen der Schwachstellen.

6.4 Netze

6.4.1 Sicherheitszonen

Das DMDA-Netzwerk muss in Sicherheitszonen eingeteilt werden. Das externe Netz ist vom internen Netz zu trennen und in bedarfsorientierte Netzbereichen aufzuteilen:

- Daten-Netz
- Internes Netz
- Externes Netz

Für das Management der sicherheitskritischen Komponenten ist ein separates Management-Netz einzurichten. Das Management-Netz muss vor Zugriffen aus anderen Netzen geschützt sein. Aufgrund dieser Anforderung ergibt sich die folgende grundlegende Netzarchitektur. Diese baut auf dem generischen Netzplan aus 2.3 auf und stellt eine beispielhafte Architektur dar:

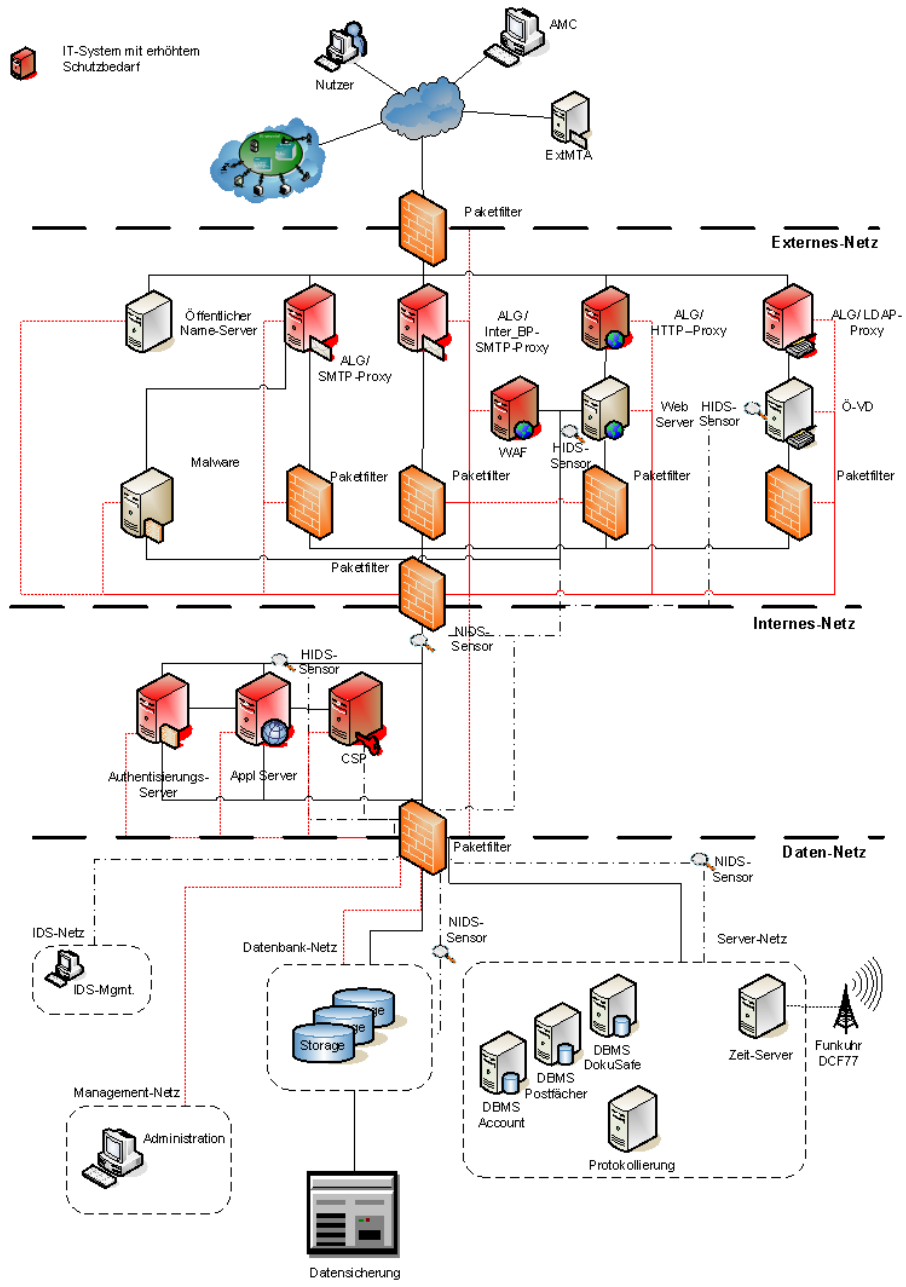


Abbildung 3: Sicherheitsnetzarchitektur

6.4.2 Firewall-System (Sicherheitsgateway)

Die Trennung der Sicherheitszonen muss durch ein Firewall-System erfolgen. Das Firewall-System muss dem Stand von Wissenschaft und Technik entsprechen. Es muss aus einer Kombination von Paktetfiltern und Applikation-Level-Gateway bestehen.

Das Firewallsystem ist so sicher zu betreiben, dass unbefugte Zugriffe auf die dahinter liegenden IT-Systeme von außerhalb wirksam unterbunden werden.

Für das System ist ein Betriebshandbuch zu führen. Die Konfiguration sowie das Patchlevel sind zu dokumentieren. Änderungen an der Hard- und Software dürfen erst in Betrieb genommen werden, wenn zuvor die Funktionalität entsprechend getestet wurde.

Die anfallenden Protokolle sind regelmäßig, mindestens aber einmal täglich, zu überprüfen. Auf erkannte Angriffsversuche ist angemessen zu reagieren.

Die Wirksamkeit des Firewall-Systems ist regelmäßig durch Pentetrationstests zu überprüfen.

Empfohlene Einzelanforderungen sind in [WebAppsec] zu finden.

6.4.3 Kommunikationsverbindungen

Nicht authentifizierte sowie direkte Verbindungsversuche auf interne Systeme sind zu blockieren.

6.4.4 Intrusion Detection System

Der DMDA hat durch den Betrieb eines Intrusion Detection Systems (IDS), das dem Stand von Wissenschaft und Technik entspricht, sicherzustellen, dass Angriffe auf das De-Mail-Portal zuverlässig entdeckt werden. Es ist zudem durch geeignete organisatorische und technische Maßnahmen sicherzustellen, dass bei sicherheitskritischen Angriffen eine zuverlässige unverzügliche Alarmierung erfolgt und unverzüglich angemessen auf einen solchen Angriff reagiert wird.

6.5 Web-Applikationen

6.5.1 Schutz der Web-Applikation

Die Web-Applikation ist durch geeignete Maßnahmen gegen unbefugte Zugriffe aus dem Internet und dem Intranet zu schützen. Zudem ist den aktuell bekannten Angriffen auf Web-Applikationen (z. B. SQL-Injection, Shell-Injection, Cross-Site-Scripting) durch geeignete Maßnahmen zu begegnen.

Es müssen alle Ein- und Ausgaben durch die Web-Applikation validiert werden. So muss vermieden werden, dass Metazeichen zu den Subsystemen weitergeleitet werden.

Zudem dürfen von der Web-Applikation keine detaillierten, systemspezifischen Fehlermeldungen an den Nutzer-Client weitergegeben werden. Interne Zustandsinformationen sollen ebenfalls an den Nutzer nicht übermittelt werden.

Zudem ist durch geeignete Maßnahmen sicherzustellen, dass durch Nutzer nur auf die öffentlichen Verzeichnisse des Webservers zugegriffen werden kann.

Ein Angreifer soll zudem keine Informationen über den verwendeten Webserver bekommen. Daher ist die Webserver-Identifizierung abzuschalten.

Die vom BSI herausgegebenen Best Practices [WebAppSec] sind zu berücksichtigen.

6.5.2 Web-Applikations-Firewall

Die Web-Applikation selbst ist durch eine hoch stabile Sicherheitskomponente für die Web-Applikationssicherheit, die in den gesamten Datenverkehr zwischen den Nutzern und der Web-Applikation eingefügt wird, zu schützen. Dabei wird der gesamte Datenverkehr überwacht. Die Web-Applikations-Firewall gewährleistet einen zusätzlichen Schutz auf Web-Applikationsebene. Damit entsteht hinter der Firewall ein zusätzlicher Sicherheitsbereich. Sämtliche Datenverbindungen in Richtung Portal- oder Web-Applikation werden in dieser Sicherheitsschleuse unterbrochen. Zugelassene Verbindungen werden permanent auf spezifische Datenstrukturen hin untersucht. Werden Angriffe erkannt, so erfolgt eine unmittelbare Unterbrechung der bestehenden Verbindung. Dies ist zu protokollieren.

6.6 Datenbanken

6.6.1 Anforderungen an die Datenbank

Für den Datenbankserver gelten neben den allgemeinen Anforderungen aus Abschnitt 6.1 folgende Mindestanforderungen:

- Der Datenbank-Server muss im Datenbank-Netz des DMDA installiert werden.
- Die Kommunikationsverbindungen zum Datenbank-Server müssen durch die Firewall, insbesondere durch ein Application-Level-Gateway entsprechend abgesichert werden.
- Die Administration des Datenbankrechners, des Datenbanksystems und die Pflege der Daten in der Datenbank dürfen nur über das Management-Netz erfolgen.
- Auf der Ebene der Datenbank sind nur die unabdingbar notwendigen Berechtigungen einzurichten.
- Zugriffe aus anderen Datenbanken auf die betrachtete Datenbank sind wirksam zu unterbinden.
- Die Datenbankanwendung muss über geeignete Mechanismen eine sichere Identifikation und Authentisierung der Benutzer ermöglichen.
- Der unbefugte Zugriff auf vertrauliche Daten ist wirksam zu unterbinden.

- Die Datenbank-Anwendung muss eine Rollentrennung zwischen Administrator und Revisor unterstützen. Der Revisor darf als Einziger über die Berechtigung verfügen, die Protokolldateien auszuwerten und zu löschen.
- Zum Schutz der Datenbankintegrität muss die Datenbank-Software über ein vollständiges Transaktionssystem verfügen, welches dem ACID-Prinzip genügt.
- Die Datenbank ist in das Datensicherungskonzept mit einzubeziehen.
- Die Regelungen für die Überwachungs- und Kontrollmechanismen sind explizit im IT-Sicherheitskonzept festzulegen.

7 Empfohlene Maßnahmen

7.1 Empfehlungen Übergreifende Komponenten

7.1.1 Rollenkonzept

Für die Umsetzung des Rollenkonzepts und der in 6.1.2 formulierten Rollenausschlüsse bietet sich die folgende Aufteilung der Rollen und Abbildung der Aufgaben an:

- Leiter DMDA
  - ist der Gesamtverantwortliche für den Betrieb.
- IT-Sicherheitbeauftragter (IT-SiBe)
  - übernimmt die Aufgaben des IT-SiBe nach ISO 27001 auf Basis von IT-Grundschutz
- Datenschutzbeauftragter (DSB)
  - übernimmt die Aufgabe des Datenschutzbeauftragten für den Bereich De-Mail und damit insbesondere für die Erfüllung der Anforderungen aus dem [DSKritKat]
- Rechenzentrumsadministrator (RZ-Admin)
  - hat Zugang zum Rechenzentrum und Zugriff auf die Hardwarekomponenten
  - ist zuständig für alle Hardwareaufgaben
  - begleitet andere Administratoren bei der Arbeit an Hardwarekomponenten
  - hat Zugriff auf die zum Betrieb und Wartung notwendigen Logdaten
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zugriff auf Schlüsselmaterial
- Log-Administrator
  - hat alleinigen Zugriff auf die Sicherheitslogging.
  - überwacht die System und Aktivitäten anhand des Logging und Monitoring
  - ist alleinig dem Leiter der Organisation unterstellt
  - hat keinen Zugang zum Rechenzentrum
  - hat keinen Zugriff auf Schlüsselmaterial
- Systemadministrator (Sys-Admin)
  - leistet halbautomatische Arbeiten zur Applikationssteuerung
  - hat keinen Zugriff auf das Logging
  - hat keinen Zugang zum Rechenzentrum
  - hat keinen Zugriff auf Schlüsselmaterial
- Anwendungsadministrator (Appl-Admin)

- betreut die Anwendungen (z.B. Webserver, E-Mailserver, usw.) und das Betriebssystem
- führt Softwareupdates, Patches, Konfigurationsänderungen durch
- hat keinen Zugriff auf das Sicherheitslogging
- hat keinen Zugang zum Rechenzentrum
- hat keinen Zugriff auf Schlüsselmaterial

- Schlüsseladministrator (Key-Admin)
  - ist zuständig für die Verwaltung von allen Schlüsseln und Zertifikaten
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zugang zum Rechenzentrum
  - hat keinen Zugriff auf verschlüsselte Daten
- Netzwerkadministrator (Net-Admin)
  - hat Zugriff auf Netzwerk- und Firewallsysteme
  - konfiguriert Firewall, Netzwerkdienst (z.B. DNS, usw.) und ähnliches
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zugriff auf Schlüsselmaterial
- Storageadministrator (Storage-Admin)
  - zuständig für den Betrieb der Datenbanken bzw. anderer Speichersysteme
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zugang zum Rechenzentrum
  - hat keinen Zugriff auf Schlüsselmaterial

Die wesentlichen Aktivitäten der Administratoren werden zuverlässig im Sicherheitslogging erfasst.

Die Rollen schließen einander aus. Das bedeutet, dass eine Person nicht gleichzeitig zwei Rollen einnehmen darf.

Die Rollen des Leiter DMDA, der Datenschutzbeauftragte und des IT-Sibe sind organisatorische Rollen, die keine operative Tätigkeit ausüben.

Die anderen Rollen sind für den Betrieb der Technik zuständig. Es ist hier abhängig vom DMDA, welche Personen für einen korrekten Betrieb anwesend sein müssen, um einen korrekten und den Sicherheitsbestimmungen entsprechenden Betrieb zu gewährleisten. Damit ist gemeint, welche Personen z.B. 24/7 verfügbar sein oder nur Rufbereitschaft gewährleisten müssen.

7.1.1.1 Empfohlene Einzelregelungen für ein Zutrittskonzept

Es wird empfohlen, folgende beispielhafte Anforderungen im Rahmen der Erstellung des Zutrittskonzepts umzusetzen; Anpassungen können, sofern aufgrund der lokalen Verhältnisse erforderlich, vorgenommen werden:

- Das Zutrittskonzept soll die Zutrittsregelungen wie folgt definieren:
  - Zutritt zum Serverraum SR-DMDA nur für den SysAdmin des DMDA.

- Zutritt für alle DMDA-Rollen zum Serverraum SR-DMDA nur gemeinsam mit SysAdmin.
- Der KeyAdmin darf keinen Zutritt zum Serverraum SR-RZ und zum Backup-DMDA haben.
- Zutritt von Besuchern im RZ-DMDA nur in Begleitung von zutrittsberechtigten DMDA-MA.
- Zutritt von Wartungspersonal zum Serverraum SR-DMDA nur in Begleitung des SysAdmin des DMDA.
- Zutritt von Reinigungspersonal zum Serverraum SR-DMDA nur in Begleitung des SysAdmin des DMDA.
- Es muss eine Zutrittskontrolltechnik verwendet werden, die durch einen ZKA-Admin administriert wird.
- Außer in Notfällen ist es verboten, die Türen mit dem Schlüssel zu öffnen. Dazu ist ein Schlüsselkonzept zu erstellen, insbesondere für den Serverraum SR-DMDA, so dass unkontrollierter Zutritt einzelner Personen unterbunden wird.

7.1.1.2 Empfohlene Einzelregelungen für ein Zugangskonzept

Der Zugang zum System darf nur im 4-Augen-Prinzip mit dem SysAdmin erfolgen

Im Zugangskonzept muss eine Passwortrichtlinie erstellt werden (vgl. [IT-GS-Katalog]).

7.1.2 Empfehlungen zum Changemanagement

Es wird empfohlen, folgende Regelungen im Rahmen des Changemanagements umzusetzen:

Auf allen Systemen des DMDA darf nur freigegebene Software installiert werden. Gleiches gilt für die einzusetzende Hardware. Die Freigabe erfolgt durch den IT-Sicherheitsbeauftragten nach definierten Kriterien und nach erfolgreicher Durchführung von Tests, soweit diese erforderlich sind. Das Changemanagement unterliegt dem IT-Sicherheitsbeauftragten. Der IT-Sicherheitsbeauftragte lagert zugriffsgeschützt die Original-Datenträger der eingesetzten Software. Hardware, die vor dem Einsatz beim DMDA bereits genutzt wurde, muss vor dem Einsatz von beeinflussenden Restdaten befreit werden.

7.1.3 Empfehlungen zum Kryptokonzept

7.1.3.1 Einsatz der qualifizierten elektronischen Signatur

Es wird empfohlen, in die Zertifikate, die zur qualifizierten elektronischen Signatur eingesetzt werden, eine Einschränkung hinsichtlich ihres Verwendungszwecks zu integrieren. Eine mögliche Einschränkung kann z.B. lauten: „Nur zur Erfüllung von DMDA-Diensten“. Damit soll klargestellt werden, dass sich der DMDA den Inhalt der Nachricht nicht zueigen macht, sondern lediglich den Transport der Nachricht bestätigt.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

7.1.3.2 Verwendung von Krypto-Hardware

Es wird empfohlen Krypto-Hardware (HSM) einzusetzen. Diese bietet den Vorteil, dass kein Zugriff auf den privaten Schlüssel erfolgen kann und somit ggf. der organisatorische Aufwand für die Verwaltung/Administration reduziert werden kann. Es sind jedoch Maßnahmen zu treffen, die die Verfügbarkeit der Dienste bei einem defekt der Hardware sicherstellen. Dies ist im Sicherheitskonzept zu berücksichtigen.

7.2 Empfehlungen Infrastruktur

7.2.1 Zutrittsschutz

Für die Infrastruktur der Räume, in denen die Systeme für De-Mail betrieben werden, wird empfohlen, die nachfolgenden Mindestanforderungen umzusetzen. Dort, wo dies aufgrund baulicher Gegebenheiten nicht möglich erscheint, sollte untersucht werden, ob ggf. der Einsatz entsprechender Schutzschränke in Betracht kommt.

- RZ-DMDA
  - Außenhaut mindestens Widerstandsklasse WK 5 (DIN V ENV 1627 bis 1630).
  - Türen und Fenster analog zur Außenhaut.
- SR-DMDA
  - Wände mindestens Widerstandsklasse WK 3 (DIN V ENV 1627 bis 1630).
  - Türen analog zu Wänden.
- SR-DMDA, BR-Admin
  - Wände mindestens Widerstandsklasse WK 1 (DIN V ENV 1627 bis 1630).
  - Türen analog zu Wänden.
- Backup-DMDA
  - Wände mindestens Widerstandsklasse WK 1 (DIN V ENV 1627 bis 1630).
  - Türen analog zu Wänden.

8 Gegenüberstellung Bedrohungen/Sicherheitsziele

Sicherheitsziele / Bedrohungen	***4.1***	***4.2***	***4.3***	***4.4***
5.2.1	X			
5.2.2		X		
5.2.3			X	
5.2.4	X			
5.2.5				X

Tabelle 5: Gegenüberstellung von Bedrohungen und Sicherheitszielen

9 Gegenüberstellung Sicherheitsziele/Anforderungen

Sicherheitsziel / Anforderungen	*5.2.1*	*5.2.2*	*5.2.3*	*5.2.4*	*5.2.5*
6.1.1		X	X		
6.1.2	X	X			
6.1.3			X	X	
6.1.4			X	X	
6.1.5			X		
6.1.6			X		
6.1.7	X	X	X		
6.1.8	X	X			X
6.1.9	X		X		
6.1.10	X				
6.2.1			X		
6.2.2			X		
6.2.3	X				
6.3.1				X	
6.3.2				X	
6.3.3				X	
6.3.4	X				
6.3.6		X			
6.3.7			X		
6.3.8				X	
6.3.9	X			X	
6.4.1			X		
6.4.2			X		
6.4.3	X			X	
6.4.4				X	
6.5.1				X	
6.5.2				X	
6.6.1				X	

Tabelle 6: Gegenüberstellung von Sicherheitszielen und Anforderungen

10 Anbindung des Postfach- und Versanddienstes über ein Gateway

Die Anbindung von Unternehmen oder Institutionen an De-Mail ist auch über ein Gateway möglich (in diesem Zusammenhang „Mandanten“). Dabei übernimmt das Gateway die Authentisierung gegenüber dem DMDA für das Authentisierungsniveau „hoch“.

Die Authentisierung des Gateways für das Authentisierungsniveau „hoch“ muss mit nicht kopierbarem Besitz und Wissen in Form eines Tokens erfolgen. Einem Token können mehrere De-Mail-Konten zugeordnet werden.

Es werden für diese Konstellation nun die Bedrohungen und Anforderungen beschrieben.

10.1. Bedrohungen

Im Folgenden werden die potentiellen Bedrohungen für die Sicherheit des De-Mail-Verbundes bei Anbindung von Nutzern über ein Gateway dargestellt.

10.1.1. Unberechtigte Nutzung der De-Mail-Dienste

Erlangt eine unberechtigte Person Zugriff auf die hinter dem Gateway liegende Infrastruktur, so kann diese über das Gateway die De-Mail-Dienste der angeschlossenen Konten nutzen und die Identität eines Kommunikationspartners im De-Mail-Verbund vortäuschen. Dies gilt es unbedingt zu vermeiden..

Folgende Möglichkeiten des Zugriffs auf Daten sind hierbei denkbar:

- Das Gateway bietet die Möglichkeit, dass von allen an der dahinter liegenden Infrastruktur angeschlossenen Nutzern, Nachrichten versendet werden können, die per De-Mail zugestellt werden.
- Das Gateway bietet die Möglichkeit, eingehende De-Mails einschließlich Versand-, Abhol- und Eingangs-Bestätigungen sowie Ident-Bestätigungsnachrichten vom Postfach abzurufen bzw. zu empfangen.
- Das Gateway bietet die Möglichkeit, Ident-Nachrichten zu versenden.
- Das Gateway bietet die Möglichkeit, den ÖVD der DMDA abzufragen.
- Das Gateway bietet die Möglichkeit, auf Inhalte der DA zu zugreifen bzw. zu ändern oder auch löschen zu können.

10.1.2. Versand unter falschem Konto

Bei der Vereinigung von mehreren Konten auf einem Gateway besteht die Gefahr, dass bei dem DMDA keine eindeutige Zuordnung der Nachrichten zu einem De-Mail-Konto mehr möglich ist. Es ist möglich, dass über ein De-Mail-Konto im Namen einer anderen Identität Nachrichten versendet werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 23. März 2011
Fundstelle: eBAnz AT40 2011 B1
– veröffentlicht am 5. April 2011 –
Quelle: elektronischer Bundesanzeiger

10.1.3. Versand von einer für einen De-Mail-Empfänger bestimmten Nachricht in das Internet

Nachrichten, die als De-Mail versandt werden sollen, könnten über das Internet versendet und dadurch im Internet mitlesbar werden bzw. könnten nicht dem adressierten Empfänger zugestellt werden. Grund dafür kann sein, dass einfache E-Mails, die als De-Mail versendet werden sollen ggf. keinem Konto zugeordnet werden können und fälschlicherweise als E-Mail eingestuft werden.

10.2 Anforderungen für Gegenmaßnahmen

Im Folgenden wird dargestellt, welche Gegenmaßnahmen zum Schutz der soeben dargestellten Bedrohungen ergriffen werden müssen.

10.2.1. Autorisierung zur Nutzung der Gatway-Dienste

Im Gateway muss eine Prüfung des Nutzers auf eine Berechtigung zur Nutzung der De-Mail-Dienste in Verbindung mit dem Zugriff über das Gateway stattfinden. Dies kann auf unterschiedliche Art und Weise erfolgen.

Beispiele hierfür sind:

- Durchgängige sichere Identifizierung des Nutzers von der Anwendung bis zum Gateway u.a. durch Prüfung der Absender-Adresse bei ausgehenden Nachrichten,
- Autorisierung des Gateway-nutzenden Systems (z.B. Fachanwendung),
- Autorisierung des Nutzers auf Basis eines im Gateway etablierten Identitäts- und Access Management-Systems.

10.2.2. Korrekte Zuordnung eines Mandanten zu seinem De-Mail-Konto

Durch den DMDA muss sichergestellt werden, dass bei mehreren Mandanten, die gemeinsam ein Gateway nutzen, eine korrekte Zuordnung der einzelnen Nutzer zu dem jeweiligen De-Mail-Konto erfolgt.

10.2.2.1. Sperrung des Tokens bei Missbrauch

Wenn ein Missbrauch des De-Mail-Kontos durch den DMDA festgestellt oder durch einen Kontoinhaber oder einen Gatewaybetreiber gemeldet wird, muss das Authentisierungstoken unverzüglich gesperrt werden.

10.2.2.2. Verpflichtung des Mandanten zur sicheren Anbindung an das Gateway

Der Mandant muss über die möglichen Gefahren, die bei der Anbindung über ein Gateway entstehen können, durch den DMDA hingewiesen werden. Der Gateway-Betreiber muss durch den DMDA zu einem sicheren Betrieb der Infrastruktur und Anbindung der Mandanten und Nutzer

verpflichtet werden. Als Nachweis dafür kann u.a. ein Sicherheitskonzept zum Betrieb des Gateways und der Infrastruktur dienen.