



Bundesamt  
für Sicherheit in der  
Informationstechnik



# De-Mail

Sicherer elektronischer Nachrichtenverkehr –  
einfach und nachweisbar

# Inhaltsverzeichnis

---

Vorwort	3
Das BSI im Dienst der Öffentlichkeit	5
<b>1 Einleitung</b>	<b>8</b>
<b>2 Vorteile und Funktionsweise von De-Mail</b>	<b>11</b>
2.1 Weboberfläche oder E-Mail-Client	12
2.2 Registrierung und Identifizierung	12
2.3 Zwei Anmeldeverfahren	13
2.4 Postfach- und Versanddienst	14
2.5 Transportverschlüsselung	16
2.6 Ende-zu-Ende-Verschlüsselung	17
2.7 Verzeichnisdienst für De-Mail-Adressen	18
2.8 Dokumentenablage – Ihr Tresor für elektronische Dokumente	18
2.9 Sperrung Ihres De-Mail-Kontos	18
<b>3 Akkreditierung von De-Mail-Anbietern</b>	<b>21</b>
3.1 Beispiele für Anforderungen an De-Mail-Anbieter	21
3.2 De-Mail-Anbieter werden überprüft	22
3.3 Akkreditierung durch das BSI	23
<b>4 Informationsquellen und Ansprechpartner</b>	<b>25</b>
4.1 Internetseiten	25
4.2 Ihr direkter Draht zu BSI-für-Bürger	25



# Vorwort

---

De-Mail hat das Potential, die Kommunikationsprozesse von Behörden, Unternehmen und Privatpersonen nachhaltig zu beeinflussen. Damit De-Mail mit all seinen Vorzügen in Hinblick auf eine schnelle, zuverlässige, nachweisbare und vor allem auch sichere Kommunikation rasch Verbreitung finden kann, muss, neben dem Aufbau einer sicheren Basisinfrastruktur, auch das Vertrauen und die Akzeptanz innerhalb der Bevölkerung gefördert werden.



Dieses Ziel kann einerseits nur durch eine transparente Darstellung der De-Mail zu Grunde liegenden technischen Abläufe und des anspruchsvollen Akkreditierungsverfahrens geschehen, das ein potentieller De-Mail-Diensteanbieter vor Betriebsaufnahme absolvieren muss.

Andererseits müssen auch die Vorteile von De-Mail sowohl für Behörden und Unternehmen als auch für die Bürgerinnen und Bürger verständlich vermittelt und aufgezeigt werden.

Die Rolle des BSI ist in diesem Prozess präzise definiert: Auf Basis des im Mai 2011 in Kraft getretenen „Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“ (kurz: De-Mail-Gesetz) ist das BSI zuständig für die Akkreditierung der potentiellen De-Mail-Diensteanbieter. Zusätzlich war das BSI mit der Konzeption der technischen Richtlinien zu De-Mail maßgeblich an der sicherheitstechnischen Ausgestaltung von De-Mail beteiligt.

Seit Frühjahr 2012 sind die ersten De-Mail-Diensteanbieter akkreditiert und am Markt vertreten, andere stehen kurz vor der Akkreditierung und Markteinführung.

Die Basisinfrastruktur steht dem Nutzer somit zur Verfügung. De-Mail kann Einzug in die Kommunikationsprozesse von Wirtschaft, Verwaltung und Privatanwendern halten.

Dem weiteren Informationsbedarf möchten wir mit dieser Broschüre Rechnung tragen.

Ich wünsche Ihnen eine aufschlussreiche Lektüre,

A handwritten signature in black ink, reading "Michael Hange". The signature is written in a cursive, flowing style.

Michael Hange

Präsident des Bundesamtes für Sicherheit in der Informationstechnik

# Das BSI im Dienst der Öffentlichkeit

---

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.



Mit seinen derzeit rund 550 Mitarbeiterinnen und Mitarbeitern und 62 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppe sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

Diese Broschüre beschreibt De-Mail als spezielle Kommunikationslösung über das Internet und beleuchtet sowohl die technischen Hintergründe, als auch die Vorteile, die De-Mail dem Anwender bietet.

# 1 Einleitung

# 1 Einleitung

---

Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Auf der Grundlage dieses „Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“ können nun De-Mail-Dienste angeboten werden.

Mit De-Mail-Diensten wird der verbindliche und vertrauliche Versand elektronischer Dokumente und Nachrichten deutlich einfacher sein als bisher. In der Handhabung gleichen De-Mails den herkömmlichen E-Mails, verfügen jedoch über wichtige Eigenschaften, die der E-Mail fehlen:

- » Die Identitäten von Absender und Adressat können eindeutig nachgewiesen und nicht gefälscht werden.
- » Die Nachrichten werden ausschließlich über verschlüsselte Kanäle übertragen und verschlüsselt abgelegt. Sie sind für Unbefugte zu keiner Zeit zugänglich und können weder mitgelesen, noch verändert werden.

Mit De-Mail sparen Sie Zeit und Geld für den Versand oder gar die persönliche Überbringung von gedruckten Unterlagen. Sie nutzen die Schnelligkeit der E-Mail in Verbindung mit der Sicherheit eines Briefes und der Nachweisbarkeit eines Einschreibens.

Diese Vorzüge werden möglich, weil De-Mail eine gesetzliche Grundlage hat und die Anbieter von De-Mail-Diensten strenge Auflagen erfüllen müssen, um die erforderliche Akkreditierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu erhalten. Zudem müssen sie eine gültige Datenschutzprüfung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vorweisen. Auch nach der Akkreditierung müssen Anbieter von De-Mail-Diensten ihre Prozesse und Systeme regelmäßig von unabhängigen Prüfstellen kontrollieren lassen. Auf diese Weise wird sichergestellt, dass alle technischen und organisatorischen Vorgaben, u. a. zum Schutz der Daten vor dem Zugriff Unbefugter, jederzeit erfüllt werden.

Um Sie umfassend auf die neuen De-Mail-Dienste vorzubereiten, haben wir die wichtigsten Informationen für Sie hier zusammengestellt. Im Folgenden erfahren Sie mehr über

- » die Vorteile und die Funktionsweise von De-Mail,
- » die Akkreditierung von De-Mail-Dienste-Anbietern und
- » Informationsquellen sowie Ansprechstellen.

## 2 Vorteile und Funktionsweise von De-Mail

---

## 2 Vorteile und Funktionsweise von De-Mail

---

Beruflich und privat erledigen wir heute viele Aufgaben per E-Mail. Allerdings fehlen der E-Mail entscheidende Sicherheitsmerkmale:

- » In der Regel werden E-Mails unverschlüsselt versandt. Unverschlüsselte E-Mails können von Dritten auf ihrem Weg durch das Internet mitgelesen und manipuliert werden.
- » Im Internet ist es leicht, eine falsche Identität anzunehmen. Bei der Eröffnung eines E-Mail-Kontos erfolgt keine Überprüfung der persönlichen Angaben des künftigen Kontoinhabers. Deshalb können sich Absender und Empfänger einer E-Mail der Identität ihres Kommunikationspartners nie ganz sicher sein.
- » Zudem können E-Mails im Internet verloren gehen oder herausgefiltert werden. Der Absender einer E-Mail hat daher keine Gewissheit, dass seine Nachricht den gewünschten Empfänger auch wirklich erreicht hat.

Deshalb müssen wir viele Dokumente ausdrucken, kuvertieren, frankieren und zur Post bringen. Oder wir überbringen sie dem Empfänger persönlich und nehmen lange Wartezeiten in Kauf. Jedes Mal kostet uns dies Zeit und Geld.

Technologien für den verschlüsselten Versand von E-Mails gibt es zwar seit langem, doch sie konnten sich bisher in der Praxis nicht durchsetzen: Weiterhin werden 95 Prozent aller E-Mails unverschlüsselt versendet. Das mag auch daran liegen, dass die Verschlüsselung elektronischer Nachrichten in der Regel zusätzliche Installationen auf dem Rechner (Zertifikate, Kartenlesegerät usw.) und Fachwissen erfordert.

Jetzt gibt es mit De-Mail eine sehr einfache Möglichkeit, elektronische Nachrichten verschlüsselt, authentisch und nachweisbar zu versenden. Wenn Sie E-Mails versenden können, verstehen Sie auch De-Mail!

Lesen Sie im Folgenden, was De-Mail so einfach macht und wie De-Mail funktioniert.

## **2.1 Weboberfläche oder E-Mail-Client**

Im einfachsten Fall verwenden Sie die Webanwendungen von De-Mail-Anbietern. Sie werden große Ähnlichkeit mit den bekannten E-Mail-Oberflächen im Internet haben. Das macht den Einstieg besonders einfach. Außerdem müssen Sie dann keine weitere Software installieren, um De-Mail nutzen zu können.

Sie können auch ein E-Mail-Programm wie Microsoft Outlook oder Mozilla Thunderbird für De-Mail nutzen, sofern Ihr De-Mail-Anbieter diese Option ermöglicht. Informationen hierzu sowie detaillierte Anleitungen erfragen Sie bitte bei Ihrem Anbieter.

Unternehmen und öffentliche Einrichtungen nutzen oft eigene E-Mail-Server und Programme für den Versand elektronischer Nachrichten. Auch sie müssen sich nicht umstellen: Ihre Systeme lassen sich über ein Gateway an den De-Mail-Dienst anschließen. Der Aufwand für die Integration des Gateways ist in der Regel gering. Die bestehenden E-Mail-Clients können anschließend wie gewohnt weiterverwendet werden.

## **2.2 Registrierung und Identifizierung**

Für die Nutzung von De-Mail benötigen Sie ein De-Mail-Konto und die dazu gehörende De-Mail-Adresse. Aus dieser Adresse muss eindeutig hervorgehen, dass es sich um eine De-Mail-Adresse handelt, z. B. `vorname.nachname@Ihr_De-Mail-Anbieter.de`.

Sie erhalten die De-Mail-Adresse, indem Sie sich bei dem De-Mail-Anbieter Ihrer Wahl (s. Ansprechstellen) für ein De-Mail-Konto registrieren. Je früher Sie sich registrieren, desto wahrscheinlicher ist es, dass Ihre Wunschadresse noch frei ist.

Nach der Registrierung erfolgt eine Überprüfung Ihrer Identität. Das ist einer der großen Vorteile von De-Mail: Niemand kann sich hinter einer falschen Identität verstecken, denn nur Nutzer mit einer überprüften Identität können De-Mails versenden und empfangen.

Die Überprüfung Ihrer Identität erfolgt durch ein vom De-Mail-Anbieter vorgegebenes Verfahren. Ein hierzu vom Anbieter Bevollmächtigter wird Ihre Identität anhand Ihres Personalausweises oder Reisepasses persönlich prüfen und bestätigen. Darüber hinaus kann Ihr De-Mail-Anbieter auch eine Identifizierung anhand der Online-Ausweisfunktion (eID-Funktion) im neuen Personalausweis (nPA) anbieten.

Sind beide Schritte, Registrierung und Identifizierung, erfolgreich abgeschlossen, wird Ihr De-Mail-Konto freigeschaltet und Sie erhalten die Zugangsdaten.

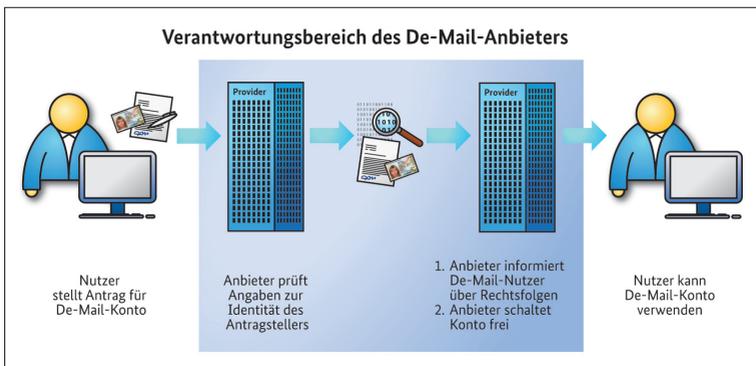


Abbildung 1: Nur Nutzer mit einer überprüften Identität können De-Mails versenden und empfangen.

### 2.3 Zwei Anmeldeverfahren

Um eine De-Mail zu versenden oder eine empfangene De-Mail zu lesen, melden Sie sich an Ihrem De-Mail-Konto an. Hier stehen Ihnen zwei Anmeldeverfahren zur Auswahl, die unterschiedlichen Sicherheitsniveaus entsprechen und verschiedene Aktionen im De-Mail-Konto ermöglichen.

Für das „normale“ Sicherheitsniveau reicht die Anmeldung mit Benutzername und Passwort. Man spricht in diesem Fall von Authentifizierung durch Wissen.

Für das „hohe“ Sicherheitsniveau setzen Sie zusätzlich zu Benutzername und Passwort einen „Token“ ein, d. h. einen Gegenstand.

Dann spricht man von einer Zwei-Faktor-Authentifizierung durch Wissen und Besitz. Es gibt unterschiedliche Token von verschiedenen Herstellern:

- » Chipkarte mit eID-Funktion, z. B. der neue Personalausweis oder eine Signaturkarte,
- » USB-Gerät in der Größe eines Speicher-Sticks, das eine mit PIN oder Passwort geschützte Authentisierungsfunktion enthält,
- » One-Time-Password-Generator (OTP, Einmalpasswortverfahren), mit dem Sie bei Bedarf ein Passwort anfordern, das Sie nur für eine Anmeldung nutzen können.

Welche Art von Token Sie für die Authentifizierung nutzen können, hängt von Ihrem De-Mail-Anbieter und Ihren persönlichen Vorlieben ab.

## **2.4 Postfach- und Versanddienst**

Im De-Mail-Verbund können Sie Ihre Nachrichten ausschließlich an Personen und Unternehmen schicken, die ebenfalls eine De-Mail-Adresse haben. Sie kommunizieren also stets mit einem eindeutig identifizierbaren Partner. Dabei spielt es keine Rolle, bei welchem Anbieter der Adressat Ihrer De-Mail registriert ist. Adressaten ohne De-Mail-Konto können Sie über De-Mail grundsätzlich nicht erreichen.

Beim Versand einer De-Mail stehen Ihnen verschiedene Optionen zur Auswahl.

Mit dem Standard-Versand ist die De-Mail gegen den Verlust der Vertraulichkeit, gegen Änderungen des Nachrichteninhaltes und der so genannten Metadaten (z. B. Absenderadresse, Versandzeit, Versandart) geschützt.

Zusätzlich können Sie zwischen mehreren Versandarten wählen, die Sie kombinieren können:

- » **Versandbestätigung:** Ihr Versanddienst bestätigt Ihnen den Versand der De-Mail.
- » **Eingangsbestätigung:** Der Postfachdienst des Empfängers bestätigt Ihnen und dem Empfänger den Eingang der De-Mail Nachricht.

Dazu sendet der De-Mail-Anbieter Ihnen eine qualifiziert elektronisch signierte Bestätigung darüber, wann und an wen Sie die De-Mail verschickt haben, bzw. wann die Nachricht im Postfach des Empfängers einging. Damit haben Sie jederzeit einen belastbaren Nachweis für Ihre elektronisch übermittelte Nachricht.

Darüber hinaus stehen Ihnen weitere Versandarten zur Verfügung, wenn Sie sich mit hohem Sicherheitsniveau (Besitz und Wissen) an Ihrem De-Mail-Konto angemeldet haben:

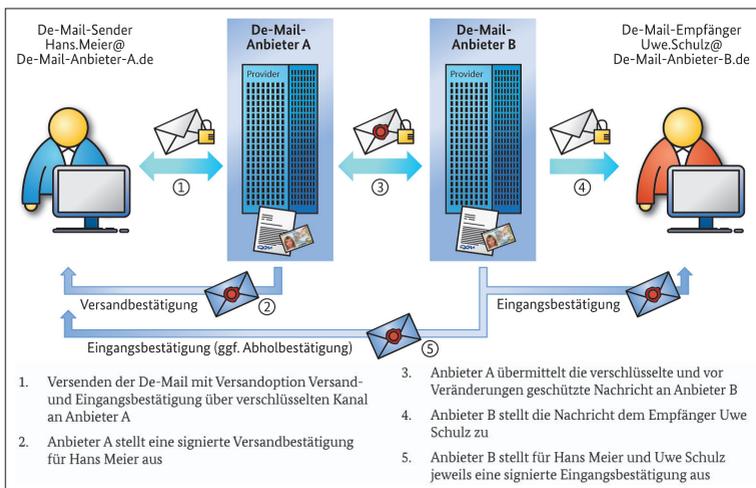


Abbildung 2: Versand und Empfang erfolgen nur innerhalb des De-Mail-Verbundes aller De-Mail-Provider.

- » **Persönlich:** Der Empfänger kann Ihre Nachricht nur lesen, wenn er sich ebenfalls mit dem hohen Anmeldeniveau eingeloggt hat.
- » **Absender-bestätigt:** Sie bestätigen mit dieser Option, dass Sie sich vor dem Versand mit hohem Niveau angemeldet haben.

## 2.5 Transportverschlüsselung

Jede De-Mail ist bei der Übermittlung zwischen dem Absender und seinem De-Mail-Anbieter sowie zwischen zwei De-Mail-Anbietern untereinander und zwischen De-Mail-Anbieter und Empfänger verschlüsselt. Diese so genannte Transportverschlüsselung schützt die De-Mail vor unberechtigtem Zugriff.

Erreicht die De-Mail den De-Mail-Anbieter, wird die Nachricht entschlüsselt. Die Daten liegen dann für einen sehr kurzen Moment unverschlüsselt vor. In dieser Zeitspanne wird die De-Mail auf Schadsoftware (wie z. B. Vi-

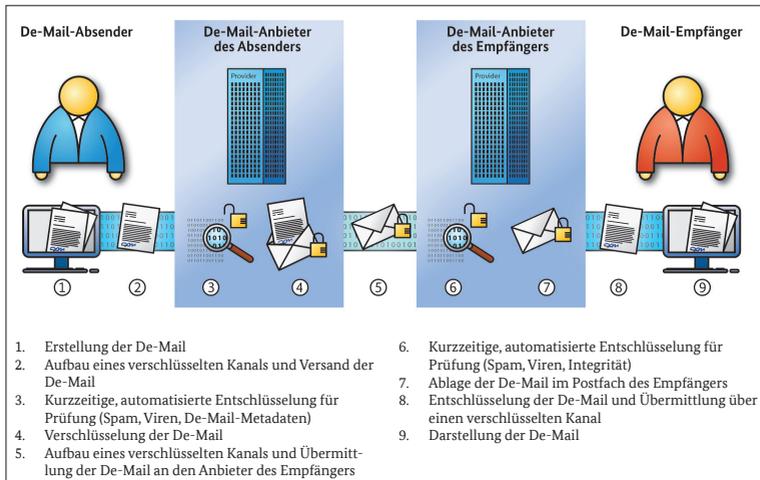


Abbildung 3: De-Mails sind auf ihrem Weg durch das Internet geschützt.

ren und Trojaner) geprüft. Erkennt das System ein Schadprogramm, warnt es den Empfänger durch Kennzeichnung der Nachricht.

Dieser Prüfprozess erfolgt automatisiert auf Servern in Rechenzentren des Anbieters, die den strengen Vorgaben des BSI entsprechen. In keinem Fall erhalten Beschäftigte der De-Mail-Anbieter Einsicht in die entschlüsselte Nachricht.

## **2.6 Ende-zu-Ende-Verschlüsselung**

Für besonders sensible Nachrichten können zusätzlich zu dem Transportkanal auch die Inhalte der De-Mail verschlüsselt werden. Um diese so genannte Ende-zu-Ende-Verschlüsselung verwenden zu können, benötigen Sie ebenso wie der Empfänger Ihrer Nachricht entsprechende Verschlüsselungssoftware, die auf den eigenen Rechnern installiert sein muss.

Mit dieser Software verschlüsseln Sie Ihre De-Mail persönlich vor dem Versand. Entschlüsselt wird sie erst durch den Empfänger auf dessen Rechner. Eine automatische Prüfung auf Schadprogramme erfolgt nicht, da der De-Mail-Anbieter keinen Zugriff auf die Nachrichteninhalte hat.

Die Nutzung der Ende-zu-Ende-Verschlüsselung wird durch einen Verzeichnisdienst erleichtert, den alle De-Mail-Anbieter zur Verfügung stellen müssen. Der Empfänger Ihrer De-Mail kann hier seinen öffentlichen Schlüssel hinterlegen, den Sie verwenden, um Ihre De-Mail zu verschlüsseln. Zur Entschlüsselung Ihrer De-Mail nutzt der Empfänger anschließend seinen privaten, nur ihm bekannten Schlüssel.

Wenn Sie sich eingehender mit dem Thema Ende-zu-Ende-Verschlüsselung beschäftigen möchten, finden Sie auf der Internetseite [www.bsi-fuerbuerger.de](http://www.bsi-fuerbuerger.de) die entsprechenden Informationen.

## 2.7 Verzeichnisdienst für De-Mail-Adressen

Der Verzeichnisdienst für De-Mail-Adressen funktioniert wie eine Art Telefonbuch und wird von den De-Mail-Anbietern für die Kunden gepflegt. Jeder Nutzer kann dort freiwillig seine De-Mail-Adresse und weitere Kontaktdaten veröffentlichen. Hier wird auch der öffentliche Schlüssel für die Ende-zu-Ende-Verschlüsselung abgelegt. Ohne Ihr Einverständnis darf der Anbieter Ihre Daten nicht in das Verzeichnis aufnehmen.

Wenn Sie die De-Mail-Adresse des Empfängers Ihrer Nachricht nicht kennen, stellen Sie eine Suchanfrage an den Verzeichnisdienst Ihres Anbieters. Dieser sucht dann in allen Verzeichnisdiensten des De-Mail-Verbundes nach der gewünschten Adresse.

## 2.8 Dokumentenablage – Ihr Tresor für elektronische Dokumente

Mit De-Mail können Sie wichtige Dokumente elektronisch versenden. Damit Sie diese und andere Dokumente elektronisch und zugleich gut geschützt aufbewahren können, können die De-Mail-Anbieter eine Dokumentenablage bereitstellen, die Ihnen eine langfristige Speicherung und einen sicheren Schutz vor Verlust und Manipulation ermöglicht. Alle hier abgelegten Dokumente werden unmittelbar nach der Entgegennahme durch den De-Mail-Anbieter verschlüsselt. Die Entschlüsselung eines Dokumentes durch den De-Mail-Anbieter erfolgt immer erst in dem Moment, in dem Sie auf dieses Dokument zugreifen.

Die Dokumentenablage ist somit Ihr persönlicher Online-Tresor für besonders wichtige Dokumente wie beispielsweise Vertragsunterlagen, Kontoauszüge oder Urkunden.

## 2.9 Sperrung Ihres De-Mail-Kontos

Sollten Ihre Zugangsdaten für die Anmeldung an Ihrem De-Mail-Konto in falsche Hände geraten sein, können Sie das Konto jederzeit über die Hot-

line Ihres De-Mail-Anbieters sperren lassen. Die entsprechende Telefonnummer finden Sie in der Regel auf der Webseite des Anbieters.

Wenn mehrfach falsche Authentifizierungsdaten verwendet werden, wird das betreffende De-Mail-Konto automatisch gesperrt. Auf diese Weise wird Ihr Konto vor dem Zugriff Unbefugter geschützt.

### **De-Mail auf einen Blick**

- » Verbindliches und vertrauliches Versenden von Nachrichten und Dokumenten über das Internet
- » Einfache Bedienung:
  - Versand von Nachrichten mit normalem Sicherheitsbedarf ohne Installation von zusätzlichen Programmen oder Geräten auf Standard-Computern
  - Versand von Nachrichten mit besonders hohem Sicherheitsbedarf mit eigenen Verschlüsselungslösungen
- » Eindeutig identifizierbare Sender und Empfänger
- » Schutz vor Manipulation der Nachrichten
- » Keine unerwünschten Werbe-Mails (kein „Spam“)
- » Automatische Erkennung von Schadprogrammen (Viren, Trojaner) und Warnung des Empfängers
- » Dokumentenablage als persönlicher Tresor für Ihre Dokumente im Internet

## 3 Akkreditierung von De-Mail-Anbietern

---

# 3 Akkreditierung von De-Mail-Anbietern

---

Ihre Nachrichten sollen mit hoher Sicherheit übertragen werden. Darum müssen sich alle De-Mail-Anbieter vor ihrer Zulassung intensiv testen und durchleuchten lassen.

In dieser Prüfungsphase müssen die künftigen De-Mail-Anbieter nachweisen, dass sie die im De-Mail-Gesetz geforderten hohen Auflagen an die organisatorische und technische Sicherheit der angebotenen De-Mail-Dienste erfüllen. Die Details der Auflagen sind in den Technischen Richtlinien des BSI festgeschrieben. Anbieter, die nachweisen können, dass sie die Auflagen bzw. die Technischen Richtlinien erfüllen, können sich durch das BSI akkreditieren lassen.

Nachfolgend finden Sie drei Beispiele für die Anforderungen sowie eine Erläuterung des Prüfungsprozesses durch unabhängige Prüfstellen und der Akkreditierung durch das BSI.

## 3.1 Beispiele für Anforderungen an De-Mail-Anbieter

- » Die IT-Systeme müssen in Sicherheitsrechenzentren mit Infrastrukturmaßnahmen (z. B. gegen unbefugten Zutritt und gegen Feuer-, Hitze- und Wasserschäden) untergebracht sein, die auch bei Stromausfall weiterlaufen.
- » Das Personal, das die De-Mail-Systeme technisch betreut, muss anhand polizeilicher Führungszeugnisse auf Vertrauenswürdigkeit überprüft worden sein.
- » Es muss ein Sicherheitsmanagement nach ISO 27001 auf Basis von IT-Grundschutz erstellt werden, welches neben IT-spezifischen Sicherheitsmaßnahmen (z. B. Netzsicherheit und Schutz der IT-Systeme) auch organisatorische Maßnahmen berücksichtigt (z. B. Trennung von Verantwortung bei sicherheitskritischen Aufgaben, um einen Zugriff auf die Nachrichten zu verhindern).

Die Beispiele veranschaulichen, wie die Vertraulichkeit Ihrer Daten gewahrt wird.

### 3.2 De-Mail-Anbieter werden überprüft

In der Prüfungsphase muss der potenzielle Anbieter von De-Mail-Diensten nachweisen, dass er die hohen Anforderungen insbesondere an die IT-Sicherheit, an die Interoperabilität und an die Funktionalität seines Systems erfüllt.

Bei der Prüfung handelt es sich um einen zweistufigen Prozess. Die eigentlichen Prüfungen werden durch unabhängige Prüfstellen und Auditoren durchgeführt, die vom BSI für De-Mail anerkannt bzw. zertifiziert wurden. Die Prüfberichte werden danach von unabhängigen IT-Sicherheitsdienstleistern validiert, die ebenfalls vom BSI zugelassen sein müssen. Bei erfolgreicher Prüfung stellen diese so genannte Testate aus, die den Anbietern von De-Mail-Diensten die Erfüllung der Anforderungen bescheinigen.

Eine weitere sachverständige Stelle prüft, ob die Auflagen für den Datenschutz eingehalten werden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) stellt bei erfolgreicher Prüfung den entsprechenden Nachweis aus.

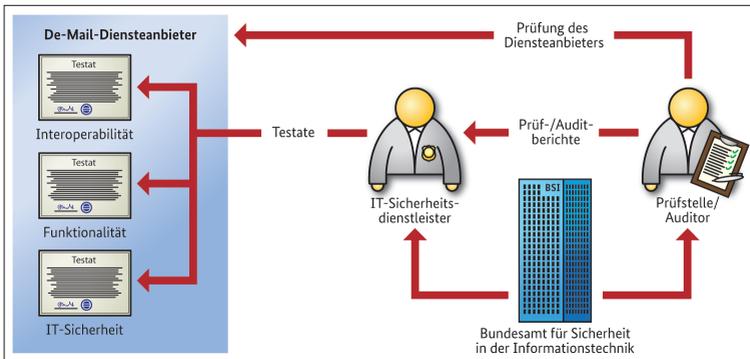


Abbildung 4: Teil des Prüfprozesses, den ein potenzieller De-Mail-Diensteanbieter durchlaufen muss.

Der Nachweis für das Testat im Bereich Sicherheit orientiert sich an der Vorgehensweise der Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz. Zusätzlich werden De-Mail-spezifische Anforderungen abgeprüft.

### 3.3 Akkreditierung durch das BSI

Die Testate und der Datenschutznachweis werden beim BSI eingereicht, das als einzige Behörde in Deutschland die Akkreditierung des De-Mail-Anbieters vornehmen darf. Erst wenn die Akkreditierung durch das BSI erfolgt ist, darf der Anbieter seine De-Mail-Dienste betreiben. Anschließend wird regelmäßig überprüft, ob der De-Mail-Anbieter auch weiterhin die technisch-organisatorischen Anforderungen erfüllt.

Die Liste der zugelassenen Anbieter wird auf der Internetseite des BSI veröffentlicht.

Sollte Ihr Anbieter seine Zulassung verlieren oder den Betrieb einstellen, sind Ihr Konto und Ihre Dokumentenablage durch gesetzliche Regelungen für den Anbieterwechsel geschützt. Gleiches gilt selbstverständlich, wenn Sie aus eigenen Gründen Ihren Anbieter wechseln möchten.

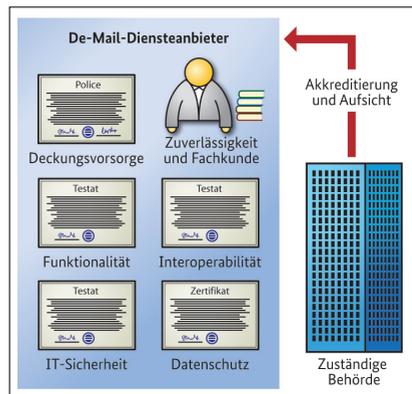


Abbildung 5: Das BSI ist zuständig für die Akkreditierung der Anbieter von De-Mail-Diensten

## 4 Informationsquellen und Ansprechstellen

---

## 4 Informationsquellen und Ansprechstellen

---

Nachfolgend haben wir die wichtigsten Informationsquellen zum Thema De-Mail für Sie zusammengestellt.

### 4.1 Internetseiten

Privatpersonen, Unternehmen und öffentliche Einrichtungen, die De-Mail-Dienste nutzen wollen, finden Informationen sowie weiterführende Hinweise u.a. zum Schutz von IT-Systemen und Daten auf der Internetseite [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de).

Unternehmen und öffentliche Einrichtungen, die De-Mail-Dienste anbieten wollen, finden Fachinformationen wie die Technischen Richtlinien und die Listen der zertifizierten De-Mail-Prüfstellen und Auditoren auf der Internetseite [www.bsi.bund.de](http://www.bsi.bund.de).

Privatpersonen, Unternehmen und öffentliche Einrichtungen finden an dieser Stelle ebenfalls eine Liste der akkreditierten De-Mail-Diensteanbieter.

Allgemeine Informationen sowie über 70 Antworten auf „Häufig gestellte Fragen“ veröffentlicht das Bundesministerium des Innern auf der Internetseite [www.de-mail.de](http://www.de-mail.de).

### 4.2 Ihr direkter Draht zu BSI-für-Bürger

Bei Verständnisfragen nicht nur zu De-Mail hilft Ihnen BSI-für-Bürger telefonisch und per E-Mail gern weiter:

E-Mail: [mail@bsi-fuer-buerger.de](mailto:mail@bsi-fuer-buerger.de)

Telefon: 01805 – 274100 (0,14 EUR inkl. Ust. pro Minute aus dem deutschen Festnetz; Mobilfunkhöchstpreis: 0,42 EUR inkl. Ust. pro Minute)

# Impressum

## **Herausgeber**

Bundesamt für Sicherheit in der Informationstechnik – BSI

Godesberger Allee 185-189

53175 Bonn

E-Mail: [bsi@bsi.bund.de](mailto:bsi@bsi.bund.de)

Internet: [www.bsi.bund.de](http://www.bsi.bund.de)

[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de) · [www.facebook.com/bsi.fuer.buerger](https://www.facebook.com/bsi.fuer.buerger)

## **Bezugsquelle**

Bundesamt für Sicherheit in der Informationstechnik – BSI

Godesberger Allee 185-189

53175 Bonn

E-Mail: [de-mail@bsi.bund.de](mailto:de-mail@bsi.bund.de)

Internet: [www.bsi.bund.de](http://www.bsi.bund.de)

Telefon: +49 (0) 22899 9582 - 0

Telefax: +49 (0) 22899 9582 - 5400

## **Stand**

Februar 2014

## **Druck**

WM Druck + Verlag

53359 Rheinbach

## **Texte und Redaktion**

Bundesamt für Sicherheit in der Informationstechnik – BSI

## **Artikelnummer**

BSI-Bro14/511

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

