



Funktionen und technische Details von De-Mail

1. Hintergrund

Das Internet hat erheblich an Bedeutung gewonnen. Damit sind E-Mails zum Massenkommunikationsmittel geworden. Die vermeintlich einfache und grenzenlose Kommunikation per E-Mail bringt jedoch auch Herausforderungen mit sich. E-Mails können mit wenig Aufwand auf dem Weg abgefangen und in ihrem Inhalt verändert werden. Absender und Empfänger können sich nie sicher sein, mit wem sie gerade tatsächlich kommunizieren

Bisherige Lösungen für eine authentische, integere und vertrauliche elektronische Kommunikation setzen vielfach auf eine Ende-zu-Ende-Sicherheit. Basis dieser Lösungen sind Signaturtechnologien – der Absender signiert und/oder verschlüsselt seine Nachricht, der Empfänger entschlüsselt diese und prüft die Signatur des Absenders. Dafür sind aber passende Soft- und Hardware-Komponenten, Verwaltung zugehöriger Zertifikate, korrekte Interpretation der Prüfergebnisse etc. erforderlich. Aufgrund des hohen Komplexitätsgrades haben sich solche Lösungen bisher kaum durchgesetzt.

Um eine flächendeckende und sichere Onlinekommunikation zu ermöglichen, sollen bei De-Mail die wesentlichen Sicherungsmechanismen von vertrauenswürdigen Providern, die auf Basis eines staatlich definierten Akkreditierungsverfahrens geprüft wurden, übernommen werden. Vor Aufnahme ihrer Tätigkeit als De-Mail-Provider müssen diese Provider die Erfüllung der geforderten Funktionalität und IT-Sicherheit sowie die Einhaltung des Datenschutzes nachweisen.

Wesentliche Zielsetzung neben der integren und vertraulichen Nachrichtenübermittlung ist die Nachvollziehbarkeit der elektronischen Kommunikation und die Authentizität der Nachrichten auf Basis bekannter und verständlicher Technik. Eine grundlegende Anforderung an De-Mail ist deshalb auch die Benutzerfreundlichkeit und einfache Bedienbarkeit. Die Dienste kommen der herkömmlichen E-Mail-Kommunikation daher möglichst nahe und sollen intuitiv nutzbar sein.

2. De-Mail-Dienste

Der De-Mail Postfach- und Versanddienst ist der zentrale Dienst für die zuverlässige und vertrauliche Kommunikation. De-Mail wird ergänzt durch eine vertrauenswürdige Dokumentenablage (De-Safe) und einen zuverlässigen Identitätsnachweis (De-Ident).

2.1. De-Mail Postfach- und Versanddienst

Über den zentralen Dienst „De-Mail“ sollen Bürgerinnen und Bürger, Wirtschaft und Verwaltung zuverlässig und vertraulich elektronisch kommunizieren können. Die sichere Kommunikation basiert im Wesentlichen auf gegenseitig authentisierten und verschlüsselten Kommunikationskanälen. Alle Daten, die der Nutzer zur Übertragung oder Speicherung an einen De-Mail-Dienst übergibt, werden unmittelbar verschlüsselt und integritätsgeschützt.

Mit De-Mail sind verschiedene Versandarten möglich, die auch unabhängig voneinander genutzt werden können.

- *De-Mail*: Der Versand ist gegen den Verlust der Vertraulichkeit und gegen Änderungen am Nachrichteninhalt und den Metadaten geschützt.
- *De-Mail-Einschreiben*: Der Absender erhält zusätzlich eine qualifiziert signierte Bestätigung, wann er die Nachricht verschickt hat und wann sie in das Postfach des Empfängers eingestellt wurde.



Weiterhin kann ein Absender auch folgende Optionen vor dem Versand einer De-Mail wählen:

- *Persönlich:* Das erforderliche Authentisierungsniveau des Empfängers (z. B. wegen der besonderen Vertraulichkeit der Nachricht) muss mindestens „Hoch“ sein, um die Nachricht lesen zu können (siehe Abschnitt 3 zu den unterschiedlichen Authentisierungsniveaus).
- *Absender-bestätigt:* Der De-Mail-Provider des Absenders bestätigt nach Entgegennahme der Nachricht mittels qualifizierter Signatur, dass er den angegebenen Nachrichteninhalt von dem Absender entgegengenommen hat, der sich mindestens mit „hoch“ authentisiert hat. Der Empfänger erhält so durch die Bestätigungsnachrichten eine höhere Beweiskraft zum Nachweis der Authentizität des Absenders und Integrität der Nachricht.

Darüber hinaus kann der Absender seine Nachrichten zusätzlich mit seinen eigenen vorhandenen Komponenten (qualifiziert) signieren und/oder Ende-zu-Ende verschlüsseln. De-Mail-Provider sind verpflichtet, einen Verzeichnisdienst anzubieten, in dem Nutzer unter anderen auch Verschlüsselungs-Zertifikate zu ihren De-Mail-Adressen hinterlegen können.

De-Mail-Nutzerkonten und Adressen

De-Mail-Konten können sowohl von natürlichen als auch von juristischen Personen eröffnet werden. Für die Eröffnung müssen sich die Nutzer einmalig zuverlässig identifizieren lassen. Für natürliche Personen werden bei dieser Erstregistrierung verschiedene Pflichtdaten wie beispielsweise Vor- und Nachname, Meldeadresse und Geburtsdatum aufgenommen. Bei juristischen Personen, also z. B. Firmen, Organisationen oder öffentliche Stellen, werden neben Angaben zu der juristischen Person selbst auch die Daten ihrer vertretungsberechtigten natürlichen Personen erfasst.

Da die zuverlässige Erstregistrierung Grundlage der erforderlichen Identifizierbarkeit der Kommunikationspartner ist, werden nur Verfahren akzeptiert, die hohen Sicherheitsanforderungen genügen, beispielsweise über den künftigen elektronischen Personalausweis oder per Post-Ident-Verfahren. Diese Sicherheitsanforderungen können mit denen zur Beantragung einer qualifizierten Signaturkarte oder zur Eröffnung eines Bankkontos verglichen werden.

Jedem De-Mail-Konto sind eine oder mehrere De-Mail-Adressen in Form von E-Mail-Adressen mit der speziellen Endung „.de-mail.de“ zugeordnet. Die Adresse einer natürlichen Person setzt sich somit zusammen aus: <Vorname>.<Nachname>@<De-Mail-Provider>.de-mail.de. Kommt ein Name beim gleichen De-Mail-Provider mehrfach vor, wird die Adresse um eine Zahl ergänzt. Eine De-Mail-Adresse könnte also folgendermaßen aussehen: erika.mustermann@provider-XYZ.de-mail.de.

Neben dieser Adresse kann ein Nutzer auch weitere, frei wählbare pseudonyme De-Mail-Adressen im Rahmen seines Kontos anlegen. Diesen wird zur Kennzeichnung als Pseudonym das Präfix pn_ vorangestellt, so dass eine solche Adresse bspw. pn_mickeymouse@provider-XYZ.de-mail.de lauten könnte.

Juristische Personen erhalten als Namensraum für ihre De-Mail-Adressen eine eigene Domain der Form <Domain-Name>.de-mail.de. Bspw. könnte sich die Firma „Dachdecker Müller“ die De-Mail-Subdomain „dachdecker-mueller.de-mail.de“ reservieren. Der lokale Teil einer De-Mail-Adresse, also der Teil vor dem @-Zeichen, ist von der juristischen Person im Prinzip frei wählbar. So kann die juristische Person Organisationspostfächer oder auch individuelle Postfächer mit den Namen der Mitarbeiter einrichten.

2.2. De-Ident

Im Rahmen der De-Mail-Dienste wird es eine einfache Möglichkeit zum Nachweis von Identitätsmerkmalen geben. Auf Anforderung des Nutzers erstellt der De-Mail-Provider eine Ident-Bestätigung, die anschließend per De-Mail an die De-Mail-Adresse des Empfängers gesendet wird. Damit sollen Bürger sich beispielsweise bei Online-Shops registrieren können oder nachweisen, dass Sie älter als 18 Jahre alt sind. Diese Inhalte werden vom De-Mail-Provider qualifiziert signiert, um die Korrektheit der übermittelten Daten zu bestätigen.



2.3. De-Safe

Eine häufige Anforderung ist, dass wichtige Dokumente sicher in elektronischer Form aufbewahrt werden können. Für diesen Fall sollen die De-Mail-Provider sog. Dokumentensafes bereitstellen, die eine langfristige Speicherung und den Schutz vor Verlust und Manipulation ermöglichen. Auch hier werden alle an den Safe übergebenen Dokumente unmittelbar nach der Entgegennahme verschlüsselt und integritätsgeschützt.

3. Authentisierungsniveaus zur Anmeldung am De-Mail-Konto

Grundlage für die Nutzung der De-Mail-Dienste ist die sichere Anmeldung an dem De-Mail-Konto des Nutzers. Grundsätzlich sind die Authentisierungsniveaus „Normal“ und „Hoch“ vorgesehen:

- „Normal“: entspricht Benutzername/Passwort
- „Hoch“: Besitz und Wissen (z.B. Mobiltelefon-basierte Verfahren (TAN), bestimmte Chipkarten oder der zukünftige elektronische Personalausweis als sog. Authentisierungstoken)

Das bei der Anmeldung am Account tatsächlich verwendete Authentisierungsniveau wirkt sich auf die weitere Nutzung der De-Mail-Dienste während des jeweiligen Anmeldezeitraums aus: So sind z. B. bestimmte Zugriffe auf Dokumente im De-Safe oder auf Nachrichten im Postfach sowie die Nutzung bestimmter Versandarten an ein Mindest-Authentisierungsniveau gekoppelt. Das jeweilige Authentisierungsniveau ist auch für die Kommunikationspartner ersichtlich, damit diese den Grad der Vertrauenswürdigkeit einstufen können.

4. Akkreditierte Diensteanbieter

Im Rahmen einer Akkreditierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) müssen die De-Mail-Provider die Umsetzung technischer und organisatorischer Maßnahmen nachweisen, die z.B. den internen oder externen Zugriff auf die Daten durch Unberechtigte verhindern.

Zudem müssen sie nachweisen, dass sie die De-Mail-Dienste interoperabel anbieten (d. h. auf technischer Ebene mit den anderen De-Mail-Providern nahtlos zusammenarbeiten). Dies ist wichtig, um der Entstehung von Insellösungen vorzubeugen. Erst nach erfolgreichem Durchlaufen des Akkreditierungsverfahrens dürfen sie am Markt als De-Mail-Provider auftreten. Detaillierte und aktuelle Information zum geplanten Zertifizierungs- und Akkreditierungsverfahren werden auf der Website des BSI veröffentlicht.

5. Technische Konzeption

5.1. Standardmäßige Transport-Sicherheit

Sowohl die Kommunikation der De-Mail-Nutzer mit ihren De-Mail-Provider als auch die Kommunikation von De-Mail-Providern untereinander verläuft grundsätzlich über gegenseitig authentifizierte und verschlüsselte Kommunikationskanäle. Alle Nachrichten (im Falle von De-Mail) und Dokumente (bei De-Safe) werden unmittelbar nach Entgegennahme durch den De-Mail-Provider des Nutzers integritätsgesichert und verschlüsselt. Bei Abruf der Nachrichten bzw. Dokumente werden die Daten vom De-Mail-Provider wieder entschlüsselt und die Integrität geprüft. Reicht einem Nutzer das dadurch realisierte Sicherheitsniveau nicht aus, kann er zusätzlich seine Nachrichten bzw. Dokumente Ende-zu-Ende-verschlüsseln und/oder Inhalte (qualifiziert) signieren.



5.2. Versand der Nachricht vom Absender an den De-Mail-Provider

Verwendet der Absender einen Webbrowser, um seine Nachrichten zu erstellen, so wird der Nachrichtentext über HTTP(S) (*Hypertext Transfer Protocol via TLS*) übertragen.

Im Falle eines E-Mail-Client wird die Nachricht mittels SMTP (*Simple Mail Transfer Protocol*) via TLS an den Provider gesendet. Von De-Mail-Providern können auch noch weitere Transportprotokolle unterstützt werden, wie z. B. OSCI (*Online Services Computer Interface*), welches insbesondere bei Fachverfahren der Verwaltung eingesetzt wird.

5.3. Prüfung und Ergänzung der Metadaten

Unmittelbar nach Entgegennahme der Nachricht vom Absender überprüft der De-Mail-Provider die mit der Nachricht übermittelten Metadaten. Z. B. muss die in der Nachricht als Absenderadresse angegebene De-Mail-Adresse dem De-Mail-Konto zugeordnet sein, von dem der Absender die Nachricht verschickt. Auch muss das Authentisierungsniveau des Absenders mindestens „Hoch“ sein, wenn er die De-Mail-spezifische Versandoption „Absender-bestätigt“ ausgewählt hat.

Nach Prüfung der Metadaten wird der Nachrichteninhalt auf Malware untersucht. Anschließend ergänzt der De-Mail-Providers des Absenders weitere Metadaten, wie z. B. die aktuelle Zeit, versieht anschließend die Nachricht inklusive Metadaten mit einer Integritätssicherung und verschlüsselt sie. Erst mit der Integritätssicherung wird die Nachricht zu einer De-Mail mit allen integrierten Sicherheitsmerkmalen.

5.4. Integritätssicherung und Verschlüsselung

Grundsätzlich besteht die vom De-Mail-Provider des Absenders angebrachte Integritätssicherung aus einer Prüfsumme (Hashwert) über die Metadaten und den Nachrichteninhalt. Bei Nachrichten, die mit der Versandoption „Absender-bestätigt“ versendet werden, wird der Hashwert vom Provider noch zusätzlich qualifiziert signiert und die Signatur zusätzlich in den Metadaten der Nachricht gespeichert. Die Signatur bestätigt, dass der De-Mail-Provider die Metadaten korrekt erfasst hat und er den angegebenen Nachrichteninhalt vom Absender unverändert entgegengenommen hat.

Nach der Integritätssicherung verschlüsselt der De-Mail-Provider den Nachrichteninhalt mit einem hybriden Verfahren sowohl für sich selbst als auch für den oder die De-Mail-Provider des/der Empfänger.



5.5. Versandbestätigung

Unmittelbar vor der Übertragung der integritätsgeschützten und verschlüsselten Nachricht an den oder die Empfänger, stellt der De-Mail-Provider des Absenders – falls vom Absender angefordert – eine qualifiziert signierte Versandbestätigung aus. Die Versandbestätigung wird dem Absender als Anhang einer De-Mail zugestellt.

Die Versandbestätigung enthält unter anderem den Hashwert der ursprünglichen Nachricht und den Zeitpunkt der Übermittlung. Damit kann der Absender gegenüber Dritten nachweisen, dass er zu einem bestimmten Zeitpunkt eine bestimmte Nachricht versendet hat.

5.6. Übertragung der transportgesicherten Nachrichten an De-Mail-Provider

Die integritätsgeschützte und verschlüsselte De-Mail wird vom De-Mail-Provider des Absenders mittels SMTP über einen mit SSL/TLS gegenseitig authentisierten und verschlüsselten Kommunikationskanal an den De-Mail-Provider des Empfängers übertragen.

Nach Entgegennahme der transportgesicherten Nachrichten wird eine Kopie der Nachricht temporär entschlüsselt und die Integrität der Nachricht bzw. der Inhalt beispielsweise auf Malware geprüft. Anschließend verwirft der Provider des Empfängers die entschlüsselte Nachrichten-Kopie und legt die transportgesicherte Nachricht in das Postfach des Empfängers ab.

5.7. Zugangsbestätigung

Unmittelbar nach Ablage der Nachricht in das Postfach des Empfängers stellt der De-Mail-Provider des Empfängers eine Zugangsbestätigung für den Absender der Nachricht aus – sofern vom Absender gewünscht. Der De-Mail-Provider signiert die Bestätigung qualifiziert und sendet sie dem Absender als Anhang einer De-Mail zurück.

Die Zugangsbestätigung enthält unter anderem den Hashwert der ursprünglichen Nachricht sowie den Zeitpunkt der Ablage der Nachricht in das Postfach des Empfängers. Der Absender der ursprünglichen Nachricht kann mit der Zugangsbestätigung gegenüber Dritten nachweisen, dass der Empfänger ab einem bestimmten Zeitpunkt Zugang zu einer bestimmten Nachricht hatte.

5.8. Protokolle und Datenformate von De-Mail

Für die De-Mail-Kommunikation sind zwei Kommunikationsstrecken relevant. Zum einem die Strecke zwischen Nutzer und seinem De-Mail-Provider; und zum anderen die „interne“ Strecke zwischen zwei De-Mail-Providern.

Für den Kommunikationskanal zwischen Nutzer und seinem Provider gibt es die sicherheitstechnische Anforderung, dass die Kommunikation über einen gegenseitig authentisierten und vertraulichen Kanal erfolgen muss (wie z. B. SSL/TLS; dies kann aber auch über OSCl-Transport realisiert werden). Die technische Umsetzung und damit die Wahl des Transportprotokolls und auch der verwendeten Datenformate können individuell zwischen De-Mail-Provider und Nutzer erfolgen. Auch können Absender und Empfänger prinzipiell unterschiedliche Protokolle / Datenformate und damit auch Client-Anwendungen nutzen. De-Mail-Provider müssen als Client-Anwendungen mindestens Webbrowser mit HTTP(S) unterstützen. Darüber hinaus sind auch E-Mail-Clients mit SMTP für den Versand und POP3 bzw. IMAP für den Empfang von Nachrichten jeweils über einen sicheren Kommunikationskanal eingesetzt möglich.

Im Gegensatz zum Kommunikationskanal zwischen Nutzer und De-Mail-Provider sind die Protokolle und Datenformate zwischen zwei De-Mail-Providern genau spezifiziert, so dass alle Provider einheitlich (interoperabel) untereinander kommunizieren können.

Zur Absicherung des Kommunikationskanals zwischen zwei De-Mail-Providern kommt SSL/TLS zum Einsatz. Über diesen sicheren Kommunikationskanal wird SMTP zum Übermitteln der Nachrichten und als Datenformat das Standard-E-Mail-Format (*Internet Message Format*) eingesetzt.