Bundesamt
für Sicherheit in der
Informationstechnik

Erfüllung der Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben nach eIDAS-Verordnung durch De-Mail-Dienste

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

Die *VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG* (eIDAS-Verordnung) regelt u. a. Dienste zur Zustellung elektronischer Einschreiben. Bezüglich dieser Dienste tritt die eIDAS-Verordnung am 1. Juli 2016 in Kraft.

Ein *Dienst zur Zustellung elektronischer Einschreiben* ist nach der eIDAS-Verordnung „ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird", „der die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglicht und einen Nachweis der Handhabung der übermittelten Daten erbringt, darunter den Nachweis der Absendung und des Empfangs der Daten, und der die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung schützt".

Mit den Versandoptionen *Versandbestätigung* (§ 4 Abs. 7 De-Mail-G) und *Eingangsbestätigung* (§ 4 Abs. 8 De-Mail-G) erfüllt eine De-Mail diese Voraussetzungen und ist damit ein Dienst zur Zustellung elektronischer Einschreiben.

Für mittels *qualifizierter* Dienste zur Zustellung elektronischer Einschreiben versandte Nachrichten legt die eIDAS-Verordnung eine besondere Rechtswirkung fest. Für diese gilt nach Art. 43 Abs. 2 die Vermutung der Unversehrtheit der Daten, der Absendung dieser Daten durch den identifizierten Absender und des Empfangs der Daten durch den identifizierten Empfänger und der Korrektheit des Datum und der Uhrzeit der Absendung und des Empfangs, wie sie von dem qualifizierten Dienst angegeben werden. Anbieter entsprechender Dienste bekommen den Qualifikationsstatus von der zuständigen Behörde verliehen, nachdem sie die Konformität zu den entsprechenden Anforderungen aus der Verordnung nachgewiesen haben.

Die Anforderungen an qualifizierte Dienste zur Zustellung elektronischer Einschreiben durch De-Mails werden mit den Versandoptionen *Versandbestätigung*, *Eingangsbestätigung*, *absenderbestätigt* (§ 5 Abs. 5 De-Mail-G) und *persönlich* (§ 5 Abs. 4 De-Mail-G) erfüllt . Dies wird in nachfolgender Übersicht dargestellt. Insbesondere werden die für die Ausstellung der Testate gem. §§ 18 Abs. 1 Nr. 3, 2 S. 1 und 2, Abs. 3 Nr. 3 De-Mail-G wesentlichen Bestimmungen der BSI Technischen Richtlinie 01201 (TR) unter Hervorhebung der nach Teil 6 der TR „Sicherheit Modulübergreifend (dort Einleitung und Ziffer 3.4) einzuhaltenden Maßnahmen aus IT-Grundschutz sowie für Zertifizierungen nach ISO 27001 dargelegt.

Anforderung eIDAS-Verordnung	**Umsetzung bei De-Mail**
Art. 3 Nr. 36. „Dienst für die Zustellung elektronischer Einschreiben" ist ein Dienst, der die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglicht und einen Nachweis der Handhabung der übermittelten Daten erbringt, darunter den **Nachweis der Absendung und des Empfangs** der Daten, und der die übertragenen Daten **vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung schützt**."	Die geforderten Nachweise der Absendung und des Empfangs werden durch die Versandoptionen *Versandbestätigung* und *Eingangsbestätigung* erbracht. Durch die dabei angebrachten qualifizierten Signaturen nach §§ 4 Abs. 7 S. 3, Abs. 8 S. 4 De-Mail-G ist gleichzeitig der geforderte Schutz vor unbefugter Veränderung (bzw. genauer gesagt deren Erkennbarkeit) gegeben. Nachweis durch TR-Testat Interoperabilität (BSI TR 01201 Teil 3.4 Abschnitte 3.1, 3.5) i.S.v. §§ 4 Abs. 7, 8 i.V.m 18 Abs. 1 Nr. 3, Abs. 2 S. 1, 2 und Abs. 3 Nr. 3 De-Mail-G. Durch die organisatorischen und technischen Maßnahmen, die als Anforderungen im De-Mail-Gesetz und Technischer Richtlinie des BSI TR-01201 De-Mail (TR-01201) genannt sind, ist der geforderte Schutz vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung gegeben (Nachweise im Einzelnen s. u. zu Art. 24 Abs. 2 lit. e-g).

Anforderung eIDAS-Verordnung	Umsetzung bei De-Mail
Art. 15: „Soweit möglich werden Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte Personen mit Behinderungen zugänglich und nutzbar gemacht.“	Eine entsprechende Anforderung ergibt sich aus der TR-01201 (Abschnitt 7.3), wonach die Gestaltung der Weboberflächen entsprechend den Gesetzgebungen zur Barrierefreiheit (Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz) vorgenommen werden sollte.
Art. 19 Abs.1: „Qualifizierte und nichtqualifizierte Vertrauensdiensteanbieter ergreifen geeignete **technische und organisatorische Maßnahmen** zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit den von ihnen erbrachten Vertrauensdiensten. Diese Maßnahmen müssen unter Berücksichtigung des jeweils **neuesten Standes der Technik** gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen zu vermeiden bzw. so gering wie möglich zu halten und die Beteiligten über die nachteiligen Folgen solcher Vorfälle zu informieren.“	Umgesetzt durch Einhaltung der Voraussetzungen nach § 18 Abs. 2 S. 1 De-Mail-G, wonach die Diensteanbieter die technischen und organisatorischen Anforderungen nach den §§ 3 bis 13 sowie nach § 16 nach dem Stand der Technik zu erfüllen haben. Zudem sind nach § 18 Abs. 1 Nr. 3 De-Mail-G diese Anforderungen in der Art zu erfüllen, dass die Dienste sicher und zuverlässig erbracht werden. Nachweis wird durch Testat gem. § 18 Abs. 3 Nr. 3 i.V.m. Abs. 2 S. 2 De-Mail-G über die Einhaltung der TR-01201 erbracht Die Beherrschung von Sicherheitsrisiken nach dem Stand der Technik wird nach der TR-01201 Teil 6 „Sicherheit Modulübergreifend, (s. Einleitung und Ziffer 3.4) durch eine Zertifizierung entsprechend ISO/IEC 27001 auf Basis von IT-Grundschutz nachgewiesen
Art. 24 Abs. 2: „Für qualifizierte Vertrauensdiensteanbieter, die qualifizierte Vertrauensdienste erbringen, gilt Folgendes: [...] b) Sie beschäftigen Personal und gegebenenfalls Unterauftragnehmer, das bzw. die über das erforderliche Fachwissen, die erforderliche Zuverlässigkeit, die erforderliche Erfahrung und die erforderlichen Qualifikationen verfügt bzw. verfügen, in Bezug auf die Vorschriften für die Sicherheit und den Schutz personenbezogener Daten angemessen geschult worden ist und Verwaltungs- und Managementverfahren anwendet, die den anerkannten europäischen oder internationalen Normen entsprechen.	Die erforderlichen Nachweise von Fachkunde und Zuverlässigkeit werden im Rahmen der De-Mail-Akkreditierung nach § 18 Abs. 1 und 3 De-Mail-G erbracht durch Vorlage eines Testats nach § 18 Abs. 3 Nr. 3 De-Mail-G. Hierfür werden nach § 18 Abs. 3 S. 1 De-Mail-G „Nachweise über die persönlichen Eigenschaften, das Verhalten und die entsprechenden Fähigkeiten seiner oder der in seinem Betrieb tätigen Personen verlangt“. Zudem werden der Einsatz anerkannter Verwaltungs- und Managementverfahren sowie die Schulung im Umgang mit personenbezogenen Daten durch die für die Testatsausstellung im Rahmen der TR-01201 (Teil 6 „Sicherheit Modulübergreifend“ Ziffer 3.4) geforderten Audits analog ISO 27001 (hier: Abschnitt 7.2 sowie control A.7) auf Basis von IT-Grundschutz (konkret: Maßnahmen zu B 1.2, u. a. M 3.3., M 3.5, M 3.50) nachgewiesen.
c) Sie verfügen in Bezug auf das Haftungsrisiko für Schäden gemäß Artikel 13 über ausreichende Finanzmittel und/oder schließen eine angemessene Haftpflichtversicherung nach nationalem Recht ab.	Abgedeckt mit dem Nachweis einer Haftpflichtversicherung nach § 18 Absatz 3 Nr. 2 lit. a) De-Mail-G.

Anforderung eIDAS-Verordnung	Umsetzung bei De-Mail
d) Sie unterrichten Personen, die einen qualifizierten Vertrauensdienst nutzen wollen, klar und umfassend über die genauen Bedingungen für die Nutzung des Dienstes, einschließlich Nutzungsbeschränkungen, bevor sie vertragliche Beziehungen zu dieser Person eingehen.	Nachweis durch Datenschutzzertifikat der BfDI (Erfüllung der Aufklärungs- und Informationspflichten nach § 9 De-Mail-G).
e) Sie verwenden vertrauenswürdige Systeme und Produkte, die vor Veränderungen geschützt sind und die technische Sicherheit und Zuverlässigkeit der von ihnen unterstützten Prozesse sicherstellen.	Nachweis durch Testat gemäß §§ 18 Abs. 1 Nr. 3, 2 S. 1 und 2, Abs. 3 Nr. 3 De-Mail-G auf Grundlage der Zertifizierung nach ISO/IEC 27001 (hier: control A.14) auf Basis von IT-Grundschutz (z. B. M 2.80) und TR-01201 Teil 6.1 Abschnitte 5.2.2 und 6.3 sowie Durchführung von IS-Revision und Penetrationstests vor Erstzertifizierung.
f) Sie verwenden vertrauenswürdige Systeme für die Speicherung der ihnen übermittelten Daten in einer überprüfbaren Form, so dass i) diese nur mit Zustimmung der Person, auf die sich die Daten beziehen, öffentlich abrufbar sind, ii) nur befugte Personen Daten eingeben und gespeicherte Daten ändern können, iii) die Daten auf ihre Echtheit hin überprüft werden können.	Nachweis der Verwendung vertrauenswürdiger Systeme für die Speicherung von Daten durch Testat gemäß §§ 18 Abs. 1 Nr. 3, 2 S. 1 und 2, Abs. 3 Nr. 3 De-Mail-G auf Grundlage der Zertifizierung nach ISO/IEC 27001 (hier: u. a. control A.14) auf Basis von IT-Grundschutz (u. a. M 2.80). Im Einzelnen: zu i): Nachweis durch Datenschutzzertifikat des BfDI zu ii): Rollenkonzept gemäß TR-01201 Teil 6.1: Sicherheit übergeordnete Komponenten und ISO/IEC 27001 control A.9. zu iii): Anforderungen an Integritätsschutz und Integritätssicherung gemäß TR-01201 Teile 6.1.
g) Sie ergreifen geeignete Maßnahmen gegen Fälschung und Diebstahl von Daten.	Nachweis durch Testat gemäß §§ 18 Abs. 1 Nr. 3, 2 S. 1 und 2, Abs. 3 Nr. 3 De-Mail-G auf Grundlage der Zertifizierung nach ISO/IEC 27001 (hier: controls A.9, A.12, A.13) auf Basis von IT-Grundschutz (u. a. M 4.93, M 2.220) inkl. zusätzlicher Anforderungen an Integritätsschutz und Integritätssicherung gemäß TR-01201 Teil 6.1, durch Datenschutzzertifikat des BfDI und TR-Testate Funktionalität und Interoperabilität (BSI TR 01201 Teil 1.4 Abschnitte 2 und 3 sowie Teil 3.1 Abschnitt 3) sowie Durchführung von IS-Revision und Penetrationstests vor Erstzertifizierung.

Anforderung eIDAS-Verordnung	Umsetzung bei De-Mail
h) Sie zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten auf und bewahren sie so auf, dass sie über einen angemessenen Zeitraum, auch über den Zeitpunkt der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters hinaus, verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und die Kontinuität des Dienstes sicherzustellen. Die Aufzeichnung kann in elektronischer Form erfolgen.	Sichergestellt nach § 13 De-Mail-G, durch die darin enthaltenen Dokumentationspflichten, sowie hinsichtlich der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters insbesondere durch §§ 11, 12 De-Mail-G. Nachweis durch TR-Testat Funktionalität (BSI TR 01201 Teil 2.1 Abschnitt 5).
i) Sie verfügen über einen fortlaufend aktualisierten Beendigungsplan, um die Dienstleistungskontinuität nach den von der Aufsichtsstelle gemäß Artikel 17 Absatz 4 Buchstabe i geprüften Vorgaben sicherzustellen.	Die Kontinuität ist nach § 11 De-Mail-G durch die Regelungen im Falle einer Einstellung der Tätigkeit sichergestellt.
j) Sie stellen eine rechtmäßige Verarbeitung personenbezogener Daten gemäß der Richtlinie 95/46/EG sicher.	Eine rechtmäßige Verarbeitung wird durch Einhaltung der nationalen Umsetzungsnormen der Richtlinie durch DMDA sichergestellt. Der Nachweis über die Erfüllung der datenschutzrechtlichen Anforderungen erfolgt durch Datenschutzzertifikat des BfDI (s. § 18 Abs. 3 Nr. 4 De-Mail-G).
k) Sie erstellen im Falle qualifizierter Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, eine Zertifikatsdatenbank und halten sie auf dem neuesten Stand.“	- nicht anwendbar, da DMDA nicht Aussteller qualifizierter Zertifikate sind -
Art. 44 Abs. 1 b): „Sie stellen die **Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit** sicher.	Die für den Versand von De-Mails mit der Versandoption *absenderbestätigt* benötigte sichere Anmeldung stellt die Authentifizierung des Absenders auf hohem Niveau sicher. Die Erstidentifizierung nach § 3 Abs. 3 S. 1 Nr. 1 De-Mail-G erfüllt die Anforderungen nach Art. 24 Abs. 3 eIDAS-VO und ist damit als geeignet auch für diesen qualifizierten Vertrauensdienst anzusehen. Nachweis durch TR-Testat Funktionalität (BSI TR 01201 Teil 2.1 Abschnitte 2, 3).

Anforderung eIDAS-Verordnung	Umsetzung bei De-Mail
c) Sie stellen die **Identifizierung des Empfängers vor der Zustellung der Daten** sicher.	Die für den Empfang von De-Mails mit der Versandoption *persönlich* benötigte sichere Anmeldung stellt die Authentifizierung des Empfängers auf hohem Niveau sicher. Erstidentifizierung und Authentifizierung erfolgen in jedem Fall vor dem Abruf der Daten. Die Erstidentifizierung erfüllt die Anforderungen nach Art. 24 eIDAS-VO nach § 3 Abs. 3 S. 1 Nr. 1 eIDAS-VO und ist damit als geeignet auch für diesen qualifizierten Vertrauensdienst anzusehen. Nachweis durch TR-Testat Funktionalität (BSI TR 01201 Teil 2.1 Abschnitte 2, 3).
d) Das **Absenden und Empfangen** der Daten ist **durch** eine **fortgeschrittene elektronische Signatur** oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten Vertrauensdiensteanbieters auf eine Weise **gesichert**, die die Möglichkeit einer unbemerkten Veränderung der Daten ausschließt.	Die Sicherung erfolgt durch die qualifizierte Signatur der *Versandbestätigung* bzw. *Eingangsbestätigung* durch den De-Mail-Diensteanbieter. Nachweis durch TR-Testat Interoperabilität (BSI TR 01201 Teil 3.4 Abschnitte 3.1, 3.5).
e) Jede **Veränderung** der Daten, die zum Absenden oder Empfangen der Daten nötig ist, **wird** dem Absender und dem Empfänger der Daten **deutlich angezeigt**.	Im De-Mail-System werden übersandte Daten grundsätzlich nicht verändert. Die erstellten Hash-Codes, die auch signiert werden, enthalten nur solche Informationen, die beim Versand einer De-Mail unverändert bleiben. Dadurch bleiben die Hash-Codes unverändert und die entsprechenden Signaturen können von allen Beteiligten geprüft werden. Nachweis durch TR-Testat Interoperabilität (BSI TR 01201 Teil 3.4 Abschnitt 3.1).
f) Das Datum und die Zeit des Absendens, Empfangens oder einer Änderung der Daten werden durch einen **qualifizierten elektronischen Zeitstempel** angezeigt.“	Die geforderten Zeitstempel sind in der durch den DMDA ausgestellten *Versandbestätigung* bzw. *Eingangsbestätigung* enthalten. Die technischen und organisatorischen Anforderungen an qualifizierte Zeitstempel (Art. 42 der eIDAS-VO) werden durch die Anforderungen aus der TR-01201 abgedeckt. Nachweis durch TR-Testat Interoperabilität (BSI TR 01201 Teil 3.4 Abschnitte 3.1, 3.5) und Zertifizierung ISO/IEC 27001 auf Basis von IT-Grundschutz und BSI TR 01201 Teil 1.3 Abschnitt 5.1.1.