Vertrauensdienstrichtlinie für den eIDAS-konformen Zustelldienst E-POST

(Trust Service Practice Statement, TSPS)

1. Einführung

1.1 Name und Kennzeichnung des Dokuments

Dieses Dokument hat den Namen „Vertrauensdienstrichtlinie für den eIDAS-konformen Zustelldienst E-POST".

1.1.1 Verweise

1) 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
2) BSI-Standard 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz
3) ETSI EN 319 401 V2.1.1
4) Beendigungsplan

1.2 Übersicht

Deutsche Post AG bietet den Kommunikationsdienst E-POST an. E-POST ist als ein qualifizierter Dienst für die Zustellung elektronischer Einschreiben und nach der Verordnung (EU) Nr. 910/2014 (eIDAS) des Europäischen Parlaments notifiziert. Die bereitgestellten Dienste sind in der Leistungsbeschreibung auf der Produktseite ausführlich beschrieben.

Das hier vorliegende Dokument gilt ausschließlich für die Erbringung des Vertrauensdienstes E-POST nach der eIDAS-Verordnung.
Deutsche Post AG bietet den qualifizierten Vertrauensdienst „Zustelldienst" unter dem Markennamen „E-POST" an.
Dieses Dokument ist ein *Trust Service Practice Statement* (TSPS) nach ETSI EN 319 401[1].

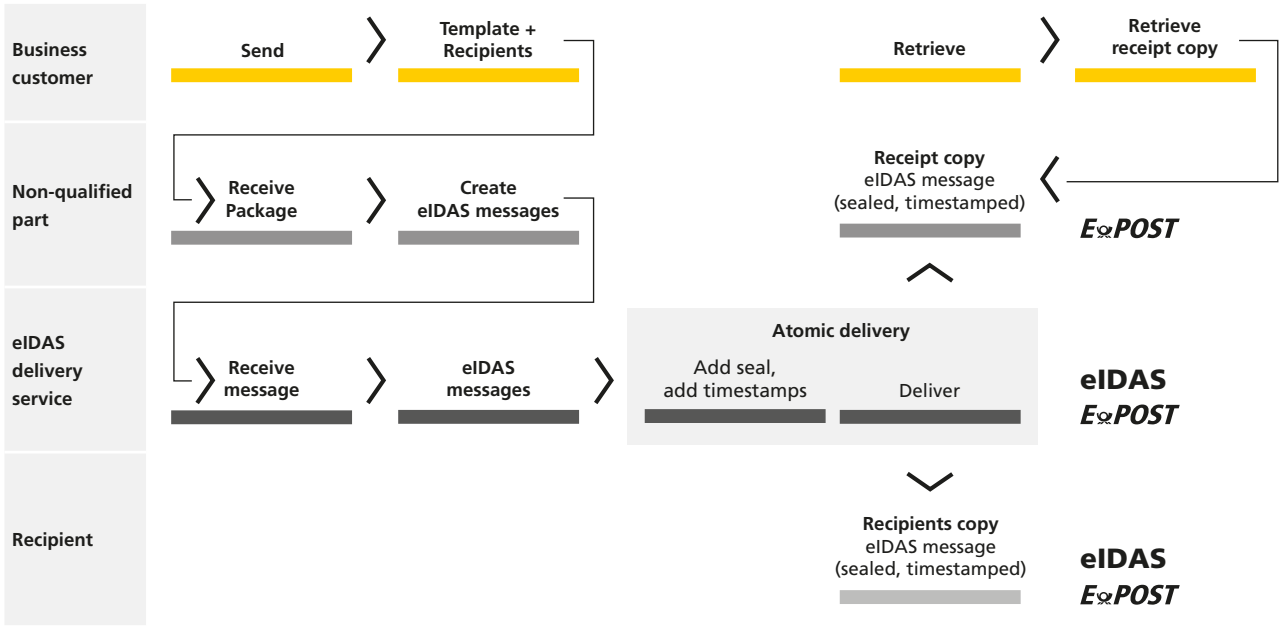
1.2.1 Identifizierung und Authentifizierung

Vertragspartner des Vertrauensdienstes sind als „substantiell" oder höher identifiziert (siehe 3.2).
Die Authentifizierung für das Versenden von eIDAS-konformen Nachrichten erfolgt mithilfe von zwei Faktoren (z.B. VPN + Kennwort/öffentlicher Schlüssel ODER feste Quell-IP Adresse + Kennwort/öffentlicher Schlüssel). Die Authentifizierung für das Empfangen von eIDAS-Nachrichten erfolgt mithilfe sicherer Kennwörter und optional einer zusätzlichen Zwei-Faktor-Authentifizierung (MTAN/SIMSme).

1.2.2 Leistungsübersicht

E-POST bietet einen elektronischen Zustelldienst für die Kommunikation zwischen zwei identifizierten Kunden. Ein Teil dieser Dienste ist als qualifizierter Zustelldienst registriert.

Delivery Service



1.2.2.1 Versenden

- Für eIDAS freigeschaltete Geschäftskunden liefern eine Empfängerliste und Vorlagen für Schreiben als Auftragspaket.
- E-POST empfängt und verarbeitet dieses Auftragspaket.
- Bei jeder Nachricht, die der Absender als eIDAS-Nachricht versenden möchte,
  - prüft E-POST in der Vorverarbeitung (MKG), ob der Empfänger für den Empfang von eIDAS-konformen Nachrichten berechtigt ist
  - erstellt die E-POST Vorverarbeitung (MKG) die eIDAS-Nachrichten im Rahmen eines individuellen Dienstleistungsvertrages mit dem Geschäftskunden
  - initiiert die E-POST Vorverarbeitung (MKG) die Zustellung der Mitteilung als eIDAS-konforme Nachricht
  - prüft E-POST, ob Absender und Empfänger zur Teilnahme am eIDAS-konformen Zustelldienst berechtigt sind
  - versiegelt E-POST die Nachricht kryptographisch mit einem eIDAS-konformen Siegel; den Nachrichten werden qualifizierte Zeitstempel zugeordnet. Im Anschluss daran kann die Nachricht nicht mehr geändert werden.
  - stellt E-POST die Nachricht dem Empfänger und dem Absender zu
- Absender und Empfänger können nach Zustellung auf eine bitidentische Kopie der Nachricht zugreifen.

1.2.2.2 Empfangen

Der Empfänger ist stets eine natürliche Person, der die Nachricht über eine Weboberfläche herunterlädt. Der Empfänger kann die Richtigkeit und Integrität der Nachricht auf der Weboberfläche überprüfen.

1.2.2.3 Empfangen der Belegkopie (Geschäftskunde)

Der Absender empfängt die Belegkopie in einem persönlichen Arbeitsraum. Der Absender lädt die Belegkopie über einen SFTP-Dienst herunter. Der Absender kann die Richtigkeit und Integrität der Nachricht unter Verwendung der technischen Beschreibung des Nachrichtenformats überprüfen.

1.3 PKI-Teilnehmer

Diese Unterkomponente beschreibt die Identitäten oder Arten von Instanzen, die im Rahmen des Vertrauensdienstes die Rolle der Teilnehmer übernehmen.

Zertifizierungsstellen	D-Trust (Bundesdruckerei GmbH) stellt Zertifikate aus, die die Integrität vertrauenswürdiger Kommunikation schützen.
Aussteller von Zeitstempeln	DGN GmbH stellt Zeitstempel aus, die das Datum und die Uhrzeit einer vertrauenswürdigen Kommunikation bescheinigen. Der Zeitstempeldienst wird als Zeitstempeldienst nach eIDAS erbracht.
Zulassungsstellen	Die Identifizierung und Authentifizierung der Vertragspartner wird von Deutsche Post AG geprüft.
Vertragspartner	Vertragspartner sind die Kunden des Vertrauensdienstes. Dies können natürliche oder juristische Personen sein. Ein Vertrag kann mehrere E-POST Adressen umschließen.
Vertrauende Beteiligte	Vertrauende Beteiligte sind aktive Vertragspartner und Vertragspartner, die ihr Konto gekündigt haben.

1.4 Verwaltung der Richtlinie

Deutsche Post AG hat ein Leitungsorgan ernannt, das für die Genehmigung dieser Richtlinie verantwortlich ist. Das Dokument wird durch eine schriftliche Stellungnahme/signierte E-Mail des für den Vertrauensdienst verantwortlichen Leiters genehmigt. Die Genehmigung wird in der Richtlinie durch den Hinweis in der Dokumentenhistorie dokumentiert, dass der Leiter das Dokument „freigegeben“ hat.
Die Richtlinie wird im Rahmen des externen Auditprozesses nach den Vorgaben der eIDAS-Verordnung regelmäßig aktualisiert, mindestens einmal im Jahr. Die Leitung ist letztlich für die Dokumentenprüfung verantwortlich. Während des Jahres stellt die Leitung sicher, dass alle Produkt- oder Prozessänderungen in Bezug auf ihre Auswirkungen auf die Richtlinie bewertet werden. Die geänderte Richtlinie wird auf der Website des Vertrauensdiensteanbieters veröffentlicht.
Der für das Produkt verantwortliche Produktmanager ist für die Pflege dieses Dokuments verantwortlich.

1.4.1 Informationssicherheitsrichtlinie

Die Umsetzung der Informationssicherheitsrichtlinie von E-POST erfolgt im Rahmen der Zertifizierung nach *ISO 27001 / IT-Grundschutz*. Deutsche Post AG ist für die Einhaltung der Informationssicherheitsrichtlinie verantwortlich, auch wenn ein Teil der Funktionalität durch externe Vertragspartner erbracht wird.
Externe Vertragspartner sind zur Einhaltung der konzernweiten Sicherheitsrichtlinie ISTM verpflichtet. Die Konformität wird von Deutsche Post mithilfe von Audits und/oder durch die Zertifizierung des Vertragspartners nach ISO 27001 überprüft.
Die Informationssicherheitsrichtlinie und die Anlagenaufstellung wird vom Leitungsorgan im Rahmen der E-POST Zertifizierung nach *ISO 27001 / IT-Grundschutz* genehmigt.

1.5 Begriffsbestimmungen und Kurzbezeichnungen

eIDAS-Verordnung	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.
Kunde	Siehe „Vertragspartner“ unter PKI-Teilnehmer.
Kommunikationspartner	Die Kommunikation erfolgt zwischen zwei (oder mehreren) Kommunikationspartnern durch Austausch von Nachrichten. Ein Kommunikationspartner wird über seine E-POST-Adresse identifiziert. Ein Vertragspartner kann mehrere E-POST Adressen verwenden.
Vertrauenswürdige Nachricht	Ein E-POSTBRIEF, der nach den Vorschriften der eIDAS-Verordnung zwischen zwei Kommunikationspartnern ausgetauscht wird.
Vertrauender Beteiligter	Eine natürliche oder juristische Person, die sich auf den Vertrauensdienst verlässt.
Vertrauensdienst	Siehe Begriffsbestimmung in der eIDAS-Verordnung.
Zustelldienst	Ein Dienst, der eine sichere und zuverlässige Kommunikation nach eIDAS bietet.
Vertrauenswürdige Kommunikation	Kommunikation, die der Vertrauensdienst nach den Vorgaben der eIDAS-Verordnung ermöglicht.
E-POST	Der Markenname des Vertrauensdienstes gemäß dieser Erklärung.
TKG	Telekommunikationsgesetz. Deutsches Bundesgesetz, das den Bereich der Telekommunikation regelt.

2. Verantwortlichkeiten für Publikation und Repositorium

Diese Richtlinie wird auf der Website von E-POST frei verfügbar gemacht.
Alle Änderungen im hier vorliegenden Dokument werden vorab der Regulierungsbehörde (BNetzA) bekanntgeben und auf der Website von E-POST veröffentlicht.

3. Identifizierung und Authentifizierung

Vertragspartner des Vertrauensdienstes werden nach den Vorgaben der eIDAS-Verordnung identifiziert. Alle Identifizierungssysteme werden vor der Implementierung von der Konformitätsbewertungsstelle geprüft.

3.1 Benennung

Kommunikationspartner werden über ihre „E-POST-Adresse" identifiziert. Diese Adresse hat entweder das Format „<name.vorname[nummer]>@epost.de" oder „name@<unternehmen>.epost.de", wobei der in '<>' eingeschlossene Teil den Identifizierer bezeichnet. Beispiel: max.mustermann@epost.de bezeichnet Max Mustermann als eine Person. max.mustermann@deutschepost.epost.de bezeichnet Max Mustermann, der im Namen von Deutsche Post AG kommuniziert.

3.2 Erstmalige Identitätsprüfung

Vertragspartner des Vertrauensdienstes werden nach der eIDAS-Verordnung als „substanziell" oder höher identifiziert. Alle Identifizierungssysteme werden vor der Implementierung von der Konformitätsbewertungsstelle geprüft.

3.3 Kündigung

Vertragspartner können ihren Vertrag in Übereinstimmung mit den Allgemeinen Geschäftsbedingungen kündigen. Nach Kündigung kann der Vertragspartner nicht mehr an der Kommunikation teilnehmen. Der Vertragspartner hat die Möglichkeit, seine Nachrichten zu exportieren. Nach einer Nachfrist wird der Zugang auf alle Nachrichten gesperrt und die Nachrichten werden endgültig gelöscht.

4. Sicherheitskontrollen auf Management-, funktionaler und physischer Ebene

4.1 Physische Sicherheitskontrollen

Aufgrund des physischen Systemzugangs muss der Vertrauensdienst angemessen geschützt werden, um die Vertrauenswürdigkeit des Vertrauensdienstbetriebs sicherzustellen. Dies ist Teil der E-POST Zertifizierung nach *ISO 27001 / IT-Grundschutz*.
Alle Server sind in nach ISO 27001 zertifizierten Rechenzentren in verschlossenen Racks untergebracht. Der physische Zugang zu den Systemen ist durch eine mehrschichtige Zugangskontrolle geschützt.

4.2 Verfahrenskontrollen

Kollidierende Aufgaben und Verantwortungsbereiche werden voneinander getrennt, um die Möglichkeiten für unbefugte oder ungewollte Änderungen an den Anlagen des Vertrauensdiensteanbieters zu reduzieren. In Bereichen, wo eine strikte Trennung nicht direkt möglich ist, werden Vorbeuge- oder Gegenmaßnahmen getroffen.
Dazu gehören unter anderem ein unabhängiger Informationssicherheitsbeauftragter, ein unabhängiger Datenschutzbeauftragter, definierte Prozesse für den administrativen Zugang und Prüfpfade für kritische Interaktionen mit Anlagen. Die Aufgabentrennung und der Schutz der Anlagen erfolgen ebenfalls nach ISO 27001 / IT-Grundschutz sowie nach der E-POST Zertifizierung *„Trusted Site Privacy"*.

4.2.1 Aufgabentrennung

Deutsche Post AG benennt die folgenden vertrauenswürdigen Rollen, um einen vertrauenswürdigen Betrieb des Zustelldienstes sicherzustellen:

- **Informationssicherheitsbeauftragter (ISB):** Verantwortlich für Sicherheitspraktiken; auch verantwortlich für Konformitätsbewertungen (Audit). Der ISB wird in Übereinstimmung mit dem Konzernregelwerk zur Informationssicherheit (ISTM) vom Management der Deutsche Post AG ernannt.
- **Systemadministrator:** Verantwortlich für die allgemeine Diensteverfügbarkeit. Er ist zur Installation und Aktualisierung des Systems berechtigt. Zudem ist er für Backup und Wiederherstellung verantwortlich. Der Systemadministrator wird vom Betriebsleiter und (in Vertretung) vom ISB bestätigt.
- **Telearbeiter (DevOps):** Verantwortlich für die Entwicklung und Pflege bestimmter Teile des Dienstes. Ein „Telearbeiter" wird vom Betriebsleiter und (in Vertretung) vom ISB bestätigt.
- **Datenschutzbeauftragter:** Verantwortlich für die Koordination aller Datenschutzaspekte des Dienstes. Wird im Rahmen des konzernweiten Datenschutzmanagements ernannt.
- **Systemauditor:** Der Systemauditor ist berechtigt, Archive und Auditprotokolle des vertrauenswürdigen TSP-Systems einzusehen. Diese Rolle ist in der Rolle des Informationssicherheitsbeauftragten enthalten.
- **Verantwortlicher Manager:** Der für den Vertrauensdienst verantwortliche Manager wird von einem Vorstandsmitglied des Unternehmensbereichs „Post - eCommerce - Parcel" oder einem bevollmächtigten Mitarbeiter ernannt.

4.2.2 Inzident-Management

E-POST implementiert ein Incident-Management nach *ISO 27001 / IT-Grundschutz*.
Die Systeme werden von IT-Sicherheitsexperten auf Sicherheitsstörungen überwacht. Zusätzlich werden zur Erkennung von Abweichungen Logfiles von Anwendungen erstellt und Maßnahmen auf Netzwerkebene getroffen. Dazu werden Tagesberichte an den ISB gesendet.
Erkannte Angriffe können an der Grenze des vertrauenswürdigen Systems blockiert werden.
Datenschutzfragen wird besondere Aufmerksamkeit gewidmet, um sicherzustellen, dass personenbezogene Daten nicht unerlaubt aufgezeichnet werden.
Es ist ein ISIRT-Team vorhanden, dass umgehend auf Störfälle reagiert. Ein Manager steht rund um die Uhr auf Abruf bereit.
Es ist ein Prozess vorhanden, mit dem die Überwachsungsstelle über einschlägige Sicherheitsverstöße/Integritätsverluste informiert wird. Deutsche Post AG hat Prozesse eingerichtet, mit denen im Störfall auch betroffene natürliche/juristische Personen informiert werden.
Kritische Sicherheitslücken werden innerhalb von 48 Stunden geschlossen.

4.2.2.1 Risikobewertung

E-POST ist nach ISO 27001 und IT-Grundschutz zertifiziert und implementiert ein Risikomanagementsystem nach BSI Standard 100-3 [2].

4.2.3 Prüfprozess und Verantwortlichkeiten

Prozesse und Risiken im Zusammenhang mit eIDAS werden regelmäßig überprüft. Diese Überprüfungen werden extern auditiert. Dies erfolgt einmal im Jahr im Rahmen der Auditierung nach *ISO 27001 / IT-Grundschutz* und alle zwei Jahre im Rahmen der eIDAS-spezifischen Auditierung durch die eIDAS-Konformitätsbewertungsstelle.

4.3 Sicherheitskontrollen des Personals

Deutsche Post AG stellt sicher, dass Mitarbeiter und Auftragnehmer die Vertrauenswürdigkeit des Vertrauensdienstes unterstützen. Dies ist Teil der E-POST Zertifizierung nach *ISO 27001 / IT-Grundschutz*.

Deutsche Post AG implementiert einen Prozess für Mitarbeiter, mit dem sichergestellt wird, dass alle Mitarbeiter über die erforderliche Expertise, Zuverlässigkeit, Erfahrung und Qualifikation für ihre Aufgaben verfügen. Deutsche Post AG stellt sicher, dass alle Mitarbeiter, die im E-POST-Betrieb personenbezogene Daten verarbeiten, regelmäßig (jährlich) in Bezug auf Datenschutz und Sicherheitsmaßnahmen geschult werden. Darüber hinaus wird ausschließlich Personen Zugang zu sensiblen Daten/Systemen gewährt, die von der Leitung und der IT-Sicherheit formal dafür zugelassen wurden. Verstöße gegen IT-Sicherheitsrichtlinien und/oder diese Richtlinie werden nach den Vorgaben im Rahmenwerk für Informationssicherheit (ISTM) von Deutsche Post AG behandelt.

Die Leitung von Deutsche Post AG hat nach den Vorgaben im Rahmenwerk für Informationssicherheit einen Informationssicherheitsbeauftragten ernannt. Der Informationssicherheitsbeauftragte hat die Rolle offiziell angenommen.

Alle Mitarbeiter von Deutsche Post AG und alle Auftragnehmer, die für den Vertrauensdienst tätig sind, sind an das Rahmenwerk für Informationssicherheit gebunden. Rollen sind voneinander getrennt, um Interessenskonflikte zu vermeiden. Bereiche, in denen das nicht möglich/machbar ist, werden streng kontrolliert.

Alle vertrauenswürdigen Rollen des Vertrauensdiensteanbieters werden in einem formalen Prozess formal durch die Leitung ernannt. Der Zugang zu sensiblen Daten wird im Vorfeld auf technische Weise verhindert. Der Zugang ist auf das erforderliche Maß beschränkt.

Das Leitungsorgan hat Prozesse und Experten eingesetzt, um sicherzustellen, dass Entscheidungen im Zusammenhang mit dem Vertrauensdienst mit der notwendigen Erfahrung, mit Kenntnis der Sicherheitsverfahren für Mitarbeiter und mit Erfahrung im Umgang mit Informationssystemen getroffen werden.

4.4 Verfahren zur Protokollierung von Audits

E-POST nutzt ein zentralisiertes Logging für Anwendungs- und Systemprotokolle. Administrative Aufgaben werden in einem separaten System in einer revisionssicheren Weise protokolliert. Mitteilungen werden ausschließlich im Rahmen der TKG-Vorgaben protokolliert.

4.5 Archivierung von Aufzeichnungen

Identifizierungsaufzeichnungen werden in einem externen System für mindestens fünf Jahre archiviert. Nachrichten im Rahmen des Zustelldienstes für elektronische Einschreiben werden nicht archiviert.

4.6 Beeinträchtigung und Wiederherstellung

Backup- und Wiederherstellungspläne sind vorhanden. Wiederherstellungstests sind vorhanden und werden regelmäßig durchgeführt.

Das Rechenzentrum verfügt über redundante Standorte, um „Single Point of Failure"-Ausfälle zu vermeiden. Die Beeinträchtigung und Wiederherstellung im Zusammenhang mit Zeitstempeln übernehmen die Zeitstempel- und Siegeldienste, die von secunet Security Networks AG bereitgestellt werden.

Für kryptographische Notfälle wie beeinträchtigte Schlüssel oder gebrochene Algorithmen stehen die folgenden Prozesse zur Verfügung:

- Der Empfang von Nachrichten wird deaktiviert.
- Bei beeinträchtigten privaten Schlüsseln wird die Regulierungsstelle informiert.
- Neue Siegel werden ausgestellt.
- Bei einem Integrationsverlust oder bei Verdacht auf manipulierte Nachrichten werden die betroffenen Kunden informiert.

4.7 Diensteinstellung

Wie unter [4] beschrieben, wird ein separates Dokument bereitgestellt, in dem die Einstellung des Dienstes beschrieben wird.

Vor einer Diensteinstellung trifft Deutsche Post AG die folgenden Maßnahmen:

1) Es werden alle Vertragspartner und alle sonstigen Einheiten informiert, die mit dem vertrauenswürdigen Dienst vertraglich in Verbindung stehen. Sonstige vertrauende Beteiligte werden zum Beispiel durch eine Einstellungsmitteilung auf der Website von Deutsche Post AG oder durch eine Pressemitteilung informiert.
2) Alle Verträge mit Sublieferanten werden gekündigt.
3) Geheime kryptographische Schlüssel werden zerstört oder widerrufen (z. B. Zertifikate).
4) Die Überwachsungsstelle wird nach den geltenden Vorschriften über die Einstellung informiert.
5) Im Falle einer Insolvenz des Diensteanbieters gehen alle Pflichten bezüglich der Diensteinstellung auf den Rechtsnachfolger über. Kann kein Rechtsnachfolger bestimmt werden, so werden die Identifikationsdaten im Rahmen der Gesetze digital der Aufsichtsstelle zur Verfügung gestellt.

5. Technische Sicherheitskontrollen

Zugang auf Systeme, die für die Bereitstellung des vertrauenswürdigen Dienstes erforderlich sind, werden in angemessener Weise geschützt, um die Vertrauenswürdigkeit des Zustelldienstes sicherzustellen. Deutsche Post AG stellt sicher, dass Mitarbeiter und Auftragnehmer die Vertrauenswürdigkeit des Zustelldienstes unterstützen. Dies ist Teil der E-POST Zertifizierung nach *ISO 27001 / IT-Grundschutz*.

5.1 Computersicherheitskontrollen

Zugriffsrechte, wie etwa Berechtigungen für Super User, werden auf ein für die Ausführung der Aufgabe angemessenes Maß begrenzt. Sind Nutzerberechtigungen erforderlich, wird mit revisionssicheren Auditprotokollen sichergestellt, dass ein unentdeckter Missbrauch unmöglich ist.

Die Systeme und die Netzwerkkonfiguration werden regelmäßig überprüft.

Zugriff auf die Systemkonfiguration des Vertrauensdienstes ist nur mit einer Zwei-Faktoren-Authentifizierung (2FA) möglich. Darüber hinaus ist der Systemzugriff durch eine zusätzliche Zugangskontrollschicht geschützt.

Die Systeme des Vertrauensdiensteanbieters werden laufend in Bezug auf Angriffe oder Informationssicherheitsstörfälle überwacht. Eigens dafür vorgesehene Mitarbeiter prüfen, ob Viren, Schadware und unerlaubte Software erkannt werden.

Sicherheitspatches werden in einem dokumentierten Freigabezyklus installiert. Erforderliche „Out of band"-Patches werden von Experten evaluiert.

5.2 Lebenszyklus-Sicherheitskontrollen

Alle Anlagen, die zur Erbringung des Vertrauensdienstes erforderlich sind, werden in angemessener Weise geschützt, um die Vertrauenswürdigkeit des Zustelldienstes sicherzustellen. Deutsche Post AG stellt sicher, dass Mitarbeiter und Auftragnehmer die Vertrauenswürdigkeit des Zustelldienstes unterstützen. Dies erfolgt im Rahmen der Zertifizierung nach *ISO 27001* / *IT-Grundschutz* von E-POST.

Die Softwareentwicklung erfolgt auf sichere Weise und umfasst unter anderem Sicherheitsprüfungen und Penetrationstests. Neue Software wird nach einem dokumentierten und revisionsfähigem Freigabeprozess eingeführt.

Datenträger dürfen aus der Installation des Vertrauensdienstanbieters nicht entfernt werden, es sei denn, der ISB hat den Prozess schriftlich genehmigt. Wenn nicht sichergestellt werden kann, dass alle Daten in verschlüsselter Form auf Speichermedien abgelegt sind, werden die Speichermedien in Übereinstimmung mit ISO 66399 Schutzklasse 2 oder höher entsorgt.

Daten werden auf redundanten Systemen gespeichert, in unterschiedlichen Brandabschnitten. Das schützt gleichzeitig vor einem Datenverlust aufgrund eines Defekts einzelner Datenträger.

Ein dokumentierter Prozess für die Zugangssteuerung stellt sicher, dass Berechtigungen für neue, abgehende und wechselnde Mitarbeiter rechtzeitig bearbeitet werden und dass unnötige Berechtigungen vermieden werden. Zugriffsrechte werden regelmäßig überprüft. Neue/gelöschte Nutzerkonten werden dem ISB monatlich gemeldet.

5.3 Netzwerksicherheitskontrollen

Das Netzwerk wird mit einer „Default deny all"-Regel durch Firewalls sowie durch separate Netzwerke für Anwendungen, Verwaltung, Protokollierung in Zonen partitioniert. Prozesse zur Erstellung und Überprüfung von Firewall-Regeln sind vorhanden.

Alle im Rahmen der Systemkonfiguration vorhandenen Netzwerkmitteilungen befinden sich in einem Rechenzentrum ODER sie werden für die Übertragung zwischen Rechenzentren verschlüsselt.

Bei einer Kommunikation zwischen den vertrauenswürdigen Systemen und anderen Systemen wird mit kryptographischen Maßnahmen die Identität, Integrität und Vertrauenswürdigkeit auf dem entfernten System sichergestellt. Das Gleiche gilt für kritische Kommunikationspfade innerhalb der Systemkonfiguration.

Die externe (Internet-) Kommunikation ist redundant ausgelegt.

Alle externen IP-Adressen werden laufend auf Anfälligkeiten oder andere Sicherheitsprobleme („Penetrationstest") getestet. Ebenso werden alle externen Zugriffsmöglichkeiten über eine Firewall auf Anwendungsebene überwacht.

Alle internen IP-Adressen werden laufend auf Anfälligkeiten oder andere Sicherheitsprobleme („Penetrationstest") getestet.

5.4 Zeitstempel

Das Zeitstempeln operativer Daten erfolgt mithilfe einer Stratum-2-Maschine als Zeitquelle.

Vertrauenswürdige Mitteilungen werden mit eIDAS-konformen Zeitstempeln versehen. Diese eIDAS-konformen Zeitstempel werden beim Vertrauensdienst für die Ausstellung von Zeitstempeln nach eIDAS bezogen. Dabei werden ausschließlich die Hash-Werte der Nachricht übertragen.

5.5 Konformitätsprüfung und andere Bewertungen

Neben Überprüfungen durch die Konformitätsbewertungsstelle nach der eIDAS-Verordnung wird die Ordnungsmäßigkeit mindestens einmal im Jahr durch Aufrechterhaltung der Zertifizierung nach ISO 27001 hergestellt.

5.6 Kryptographische Kontrollen

Mit kryptographischen Protokollen wird die Vertrauenswürdigkeit des Zustelldienstes sichergestellt. Dies ist Teil der E-POST Zertifizierung nach *ISO 27001* / *IT-Grundschutz*.

Elektronische Siegel werden von einem Dienst erworben, der von einer Drittpartei gehostet wird. Der Dienst verwendet Smartcards für Siegel nach eIDAS. Der Zugriff auf den Dienst erfolgt über eine gesicherte Verbindung. Dabei werden ausschließlich die Hash-Werte der Nachricht übertragen.

5.7 Operative Sicherheit

E-POST verwendet vertrauenswürdige Systeme und Produkte. Sofern speziell entwickelte Software zum Einsatz kommt, wird die Vertrauenswürdigkeit der Software mit geeigneten Prozessen validiert.

Mit Ausnahme der Softwareentwicklung ist die operative Sicherheit Teil der Zertifizierung nach *ISO 27001* / *IT-Grundschutz* von E-POST.

6. Sonstige geschäftliche und rechtliche Angelegenheiten

6.1 Entgelte

Entgelte werden nach den Allgemeinen Geschäftsbedingungen erhoben.

6.2 Diskriminierungsfreie Nutzung

E-POST bietet seinen Vertragspartnern einen diskriminierungsfreien Zugang durch Umsetzung von Best-Practice-Lösungen beim Webdesign. E-POST ist ein dokumentenorientierter Dienst, bei dem Dokumentformate (PDF) eingesetzt werden, die möglicherweise nicht für alle Nutzer lesbar sind. Bei der ausschließlicher Nutzung über die Tastatur muss mit Einschränkungen gerechnet werden.

6.3 Finanzielle Verantwortung

Deutsche Post AG gewährleistet, dass für den Betrieb und für Verpflichtungen, die sich aus der Erbringung des eIDAS-konformen Dienstes E-POST ergeben, Finanzmittel in ausreichender Höhe vorgehalten werden.

Verfahren zur Behebung von Streitigkeiten und Ansprüchen von Kunden oder anderen vertrauenden Beteiligten sind in separaten Richtlinien beschrieben, die von der Konformitätsbewertungsstelle verifiziert werden.

Alle Vereinbarungen mit Subunternehmen, Outsourcing-Diensten und Dritten, die zur Erbringung des eIDAS-konformen Dienstes erforderlich sind, unterliegen Verträgen und dem Verhaltenskodex von Deutsche Post AG.

6.4 Vertraulichkeit betrieblicher Informationen

Sofern nicht anders zwischen dem Vertragspartner und Deutsche Post AG schriftlich vereinbart wird, wird die Vertraulichkeit betrieblicher Informationen von Deutsche Post AG nach deutschem Recht gewährleistet.

6.5 Schutz personenbezogener Daten

Personenbezogene Daten von Vertragspartnern werden nach dem deutschen Bundesdatenschutzgesetz (BDSG) und dem Telekommunikationsgesetz (TKG) geschützt.

6.6 Haftungsbeschränkungen

Deutsche Post AG ist für die Erfüllung seiner Pflichten nach deutschem Recht und nach ETSI EN319 401 verantwortlich. Deutsche Post AG stellt sicher, dass Finanzmittel in ausreichender Höhe für Entschädigungen zur Verfügung stehen, die sich aus einer absichtlichen oder fahrlässigen Verletzung der eIDAS-Verordnung durch Deutsche Post AG ergeben.

Deutsche Post AG haftet nicht für
- Schäden, die dadurch entstehen, dass Vertragspartner ihre Zugangsdaten für E-POST nicht geheim halten.
- die Nichterfüllung seiner Pflichten aufgrund von Fehlern oder Sicherheitsproblemen öffentlicher Stellen.
- die Nichterfüllung seiner Pflichten aufgrund höherer Gewalt.

6.7 Schadensersatz

Deutsche Post AG erbringt den vertrauenswürdigen „Zustelldienst" nach den Vorschriften und Verfahren, die in dieser Richtlinie beschrieben sind. Deutsche Post AG stellt sicher, dass alle in dieser Richtlinie beschrieben Vorschriften vom Vertrauensdienst erfüllt werden.
Deutsche Post AG erfüllt darüber hinaus die Sicherheitsvorschriften für Zustelldienste nach den Vorgaben der eIDAS-Verordnung.
Die Erbringung des Vertrauensdienstes unterliegt zwei jährlichen Audits, die von der Konformitätsbewertungsstelle durchgeführt werden.
Deutsche Post AG hält darüber hinaus die E-POST Zertifizierung nach ISO 27001 aufrecht.
Aufzeichnungen zum Betrieb des Vertrauensdienstes werden dem vertrauenden Beteiligten für Gerichtsverfahren zur Verfügung gestellt (siehe 6.10.4).
Darüber hinaus übernimmt Deutsche Post AG keine weitere Haftung.

6.8 Verfahren zur Beilegung von Streitigkeiten

Für alle Streitigkeiten, die sich aus oder im Zusammenhang mit den Vorschriften für den Vertrauensdienst für Deutsche Post AG ergeben, ist das Gericht in Bonn (Deutschland) zuständig.

6.9 Geltendes Recht

Diese Vereinbarung beruht auf und unterliegt dem jeweils geltenden materiellen Recht in Deutschland.

6.10 Sonstige Bestimmungen

6.10.1 Pflichten der Nutzer

Vertragspartner sind verpflichtet, ihre Zugangsdaten jederzeit geheim zu halten. Vertragspartner sind ferner verpflichtet, den Zustelldienst in Übereinstimmung mit den Allgemeinen Geschäftsbedingungen auf neue Nachrichten hin zu überprüfen. Vertragspartner sind verpflichtet, ihre Kopie der versendeten und empfangenen Nachrichten zu sichern.

6.10.2 Pflichten externer Organisationen

Deutsche Post AG arbeitet zur Erbringung der E-POST-Funktionalität nach eIDAS mit mehreren Organisationen zusammen.
- **noris networks AG:** Hosting, Betriebssystemverwaltung und Internet-Konnektivität werden von noris networks AG erbracht. Der Hosting-Anbieter ist zur Aufrechterhaltung der Zertifizierung nach *ISO 27001 / IT-Grundschutz* verpflichtet. Alle Prozesse in Bezug auf Verfügbarkeit, Sicherheit und Risikomanagement sind in der E-POST Zertifizierung nach *ISO 27001 / IT-Grundschutz* oder der Zertifizierung des Hosting-Anbieters enthalten.
- **E-POST Development GmbH (DPEPD):** DPEPD ist eine Tochtergesellschaft von Deutsche Post AG und für die Entwicklung, den Betrieb und die Wartung von E-POST verantwortlich. Betriebs- und Wartungsaufgaben sind in der E-POST Zertifizierung nach *ISO 27001 / IT-Grundschutz enthalten*.
- **secunet Security Networks AG (secunet):** Secunet bindet einen dritten eIDAS-konformen Zeitstempeldienst an und betreibt eine eIDAS-konforme Versiegelung von Briefen durch fortgeschrittene Siegelkarten der DPAG. Bei der Erbringung des Zeitstempeldienstes unterliegt das anbietende Unternehmen den Vorschriften der eIDAS-Verordnung.
- **DGN GmbH:** Anbieter des eIDAS konformen qualifizierten Zeitstempeldienstes. Unterliegt in diesem Sinne der eIDAS-Norm.
- **D-Trust:** Bereitstellung der fortgeschrittenen Siegelkarten und der dazugehörigen Infrastruktur.
- **DPCSC:** Überprüfung der Geschäftskunden-Registrierung und -Identifizierung sowie Kundendienst für alle Vertragspartner.

Auftragnehmer, deren Leistungen für E-POST nicht der eIDAS-Verordnung unterliegen, werden hier nicht beschrieben, sind aber in der E-POST Zertifizierung nach *ISO 27001 / IT-Grundschutz* einbezogen.

6.10.3 Geschäftsbedingungen

In den Allgemeinen Geschäftsbedingungen von E-POST sind die Bedingungen beschrieben, nach denen Kunden die Zustellung eIDAS-konformer Mitteilungen nutzen können. Die allgemeinen Bedingungen basieren auf deutschem Recht und sind ein rechtsverbindlicher Bestandteil des Vertrages zwischen den Kunden und Deutsche Post.
Sie enthalten Angaben zu folgenden Aspekten:
a. Angewandte Richtlinie für den Vertrauensdienst,
b. Einschränkungen bei der Nutzung des Dienstes,
c. Pflichten des Nutzer, soweit zutreffend,
d. Informationen für Beteiligte, die sich auf den Vertrauensdienst verlassen,
e. Aufbewahrungszeitraum für die Ereignisprotokolle des Vertrauensdiensteanbieters,
f. Haftungsbeschränkungen,
g. Beschränkungen bei der Verwendung der erbrachten Dienste einschließlich Beschränkungen für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstehen,
h. Anzuwendendes Rechtssystem,
i. Verfahren zur Beilegung von Beschwerden und Streitigkeiten,
j. Angaben, ob der Vertrauensdienst des Vertrauensdiensteanbieters in Bezug auf seine Konformität mit der Vertrauensdienstrichtlinie als konform bewertet wurde; im positiven Fall ist anzugeben, nach welchem Konformitätsbewertungsprogramm vorgegangen wurde,
k. die Kontaktangaben des Vertrauensdienstes und
l. Verpflichtungen in Bezug auf die Verfügbarkeit.

6.10.4 Nachweisführung

Deutsche Post AG führt Aufzeichnungen über den Betrieb des Vertrauensdienstes, um den ordnungsgemäßen Betrieb des Vertrauensdienstes nachweisen zu können. Diese Aufzeichnungen werden ausschließlich Strafverfolgungsbehörden auf Gerichtsbeschluss und Personen offengelegt, die bei berechtigtem Interesse darauf zugreifen dürfen.
Aufzeichnungen im Zusammenhang mit der Identifizierung von Kommunikationspartnern werden für einen Zeitraum von mindestens fünf Jahren aufbewahrt.
Aufzeichnungen der Kommunikation werden nicht aufbewahrt. Absender und Empfänger erhalten jeweils eine vollständige Kopie der Kommunikation, die unabhängig von der Verfügbarkeit des Vertrauensdiensts validiert werden kann.
Aufzeichnungen einer vertrauenswürdigen Kommunikation werden dadurch geführt, dass den Kommunikationspartnern kryptographisch signierte (mit einem Siegel nach eIDAS-Verordnung) und mit einem Zeitstempel versehene Kopien zugestellt werden. Durch Validierung des Siegels und des Zeitstempels auf den entsprechenden Kopien können beide Teilnehmer die Richtigkeit der Kommunikation unabhängig voneinander validieren.
Alle weiteren Aufzeichnungen unterliegen dem deutschen Telekommunikationsgesetz.

Stand: 01.07.2017