d.velop mobile services

# QERDS Public Policy
# d.velop eIDAS postbox

## Praxiserklärung zur Dienstleistungserbringung eines qualifizierten elektronischen Zustelldienstes

**Klassifizierung: Öffentlich**

**Version 1.0, 16.02.2026**

d.velop mobile services GmbH
Eggeroder Str. 6
48624 Schöppingen

# Hinweis zur Lesbarkeit

Aus Gründen der besseren Lesbarkeit wird im vorliegenden Dokument auf gendergerechte Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten jedoch gleichermaßen für alle Geschlechter.

# Version

Version 1.0
Datum 16.02.2026

# Änderungshistorie

Jede Änderung wird versioniert dokumentiert. Aktualisierte Versionen werden öffentlich bereitgestellt. Neufassungen gelten ab Veröffentlichungsdatum.

| Version | Datum | Bearbeiter | Bemerkung |
|---|---|---|---|
| 1.0 | 16.02.2026 | Iris Hagemann | Erstfassung |

### Policy Identifier (URI)

https://mobile-services.d-velop.de/policy/qerds/v1

### Veröffentlichung

Der Policy Identifier verweist immer auf die aktuell gültige Fassung dieser Public Policy. Frühere Versionen werden in einem Versionsarchiv derselben Repository-Seite vorgehalten.

Christian Gericke, Geschäftsführer
d.velop mobile services GmbH

Tim Gottschalk, Geschäftsführer
d.velop mobile services GmbH

# Inhaltsverzeichnis

# 1 Einleitung

Die *d.velop eIDAS postbox* stellt einen qualifizierten elektronischen Zustelldienst (QERDS) gemäß Art. 44 der Verordnung (EU) Nr. 910/2014 in der durch die Verordnung (EU) 2024/1183 geänderten Fassung (eIDAS-Verordnung) bereit. Der Dienst ermöglicht es Absendern, elektronische Dokumente rechtsverbindlich zuzustellen. Empfänger können diese Dokumente sicher entgegennehmen. Versand und Öffnung werden dabei durch elektronische Nachweise dokumentiert.

## 1.1 Zweck

Diese Public Policy beschreibt die öffentlich bereitzustellenden Informationen über den qualifizierten elektronischen Zustelldienst der d.velop mobile services GmbH gemäß Artikel 44 der Verordnung (EU) Nr. 910/2014 in der durch die Verordnung (EU) 2024/1183 geänderten Fassung (eIDAS-Verordnung). Sie dient Nutzern und Interessenten als verbindliche Informationsgrundlage über Funktionsumfang, Identifizierungs- und Zustellprozesse, die Bildung und Prüfung der Zustellnachweise sowie über wesentliche Pflichten der Beteiligten und die grundlegenden Datenschutz- und Sicherheitseigenschaften des Dienstes.

## 1.2 Geltungsbereich

Diese Public Policy gilt ausschließlich für den qualifizierten elektronischen Zustelldienst *d.velop eIDAS postbox*. Sie beschreibt die für den qualifizierten Zustelldienst relevanten Nutzungs-, Sicherheits- und Nachweisbedingungen. Kommerzielle Vertragsbedingungen werden in den jeweiligen Vertragsdokumenten geregelt. Soweit externe Dokumente für die Nutzung oder Nachweisführung maßgeblich sind, werden diese im Dokument referenziert.

## 1.3 Begriffsbestimmungen

In dieser Public Policy werden die folgenden Begriffe verwendet:

| | |
|---|---|
| Absender | Juristische Person, die eine qualifizierte Zustellung über den Dienst veranlasst haben und hierfür im Onboarding registriert wurde. |
| Beweisexport | Prüfbares Beweisobjekt als gesiegelter ASIC-Container, der die zu einer Zustellung gehörenden Evidenzen sowie die zugehörigen Prüf- und Validierungsinformationen bündelt. |
| Empfänger | Natürliche Person, der ein Dokument über den Dienst zugestellt wird und die dieses Dokument über ein registriertes Nutzerkonto entgegennimmt. |
| Evidenz | Elektronischer Nachweis über ein qualifiziertes Zustellereignis. |
| QERDS | Qualifizierter elektronischer Zustelldienst gemäß Art. 44 eIDAS-Verordnung – *d.velop eIDAS postbox*. |

| | |
|---|---|
| QTSP | Qualifizierter Vertrauensdiensteanbieter gemäß eIDAS-Verordnung – d.velop mobile services GmbH als Diensteanbieter des QERDS, sofern nicht ausdrücklich ein externer QTSP für qualifizierte Vertrauensdienste (z. B. Siegel) gemeint ist. |
| QWAC | Qualified Website Authentication Certificate (QWAC) gemäß eIDAS. Es dient der Identifizierung einer Organisation, hier Absender |
| Policy Identifier (URI) | Stabiler, eindeutiger Verweis (URI) auf die Repository-Seite der Public Policy, die die jeweils gültige Version sowie das Versionsarchiv bereitstellt. |
| Zustellmerkmal | Eindeutiges Zuordnungsmerkmal für die Zustellung im 1:1-Zustellmodell (Absender ↔ Empfänger), über das ein Empfänger eindeutig adressiert wird. |
| Zustellnachweis | Nachweisobjekt zur Dokumentation der qualifizierten Zustellung |
| Zustellprozess | Ablauf von der Übernahme der Verantwortlichkeit für ein eingeliefertes Dokument bis zum Ergebnis „geöffnet" oder „nicht geöffnet innerhalb der Frist". Der Zustellprozess umfasst auch die Erzeugung der zugehörigen Nachweise. |

## 1.4 Akteure

Am Dienst wirken folgende Akteure mit: Absender, Empfänger, Diensteanbieter sowie Vertrauens-diensteanbieter für qualifizierte Siegel und Zeitstempel. Zusätzlich tritt die d.velop AG im Produkt- und Vertriebskontext als Vertragspartner gegenüber Absendern und Empfängern auf.

Der qualifizierte Diensteanbieter betreibt den qualifizierten Vertrauensdienst. Die d.velop AG vertreibt den Dienst und tritt gegenüber Absendern und Empfängern als vertraglicher Ansprechpartner auf.

Die vorliegende Public Policy beschreibt die wesentlichen organisatorischen, technischen und sicherheitsrelevanten Rahmenbedingungen des qualifizierten elektronischen Zustelldienstes. Sie ersetzt keine vertraglichen Nutzungsbedingungen.

Vertragsbedingungen für Endnutzer werden durch die d.velop AG im Rahmen der jeweiligen Vertragsbeziehung bereitgestellt. Diese nehmen die für Sicherheit, Identifikation, Nutzung des Dienstes sowie für die Nachweisführung relevanten Pflichten von Absendern und Empfängern verbindlich auf.

## 1.5 Policy-Identifikation und Versionierung

Diese Public Policy wird unter einem stabilen Policy Identifier (URI) veröffentlicht. Der Policy Identifier verweist auf eine zentrale Repository-Seite, auf der die jeweils gültige Policy-Version mit Versionsnummer und Veröffentlichungsdatum bereitgestellt wird. Die Policy ist dort als PDF abrufbar. Frühere Versionen werden in einem Versionsarchiv derselben Repository-Seite vorgehalten, sodass die für eine Evidenz maßgebliche Policy-Version auch nachträglich eindeutig auffindbar ist.

Policy Identifier (URI): https://mobile-services.d-velop.de/policy/qerds/v1

# 2 Beschreibung des qualifizierten elektronischen Zustelldienstes

## 2.1 Überblick über den QERDS gemäß Art. 44 eIDAS

Der qualifizierte elektronische Zustelldienst des Diensteanbieters stellt eine digitale und rechtssichere Form der elektronischen Zustellung über die *d.velop eIDAS postbox* bereit. Versand und Öffnung werden durch elektronische Nachweise dokumentiert. Diese Nachweise werden mit qualifizierten elektronischen Siegeln und qualifizierten elektronischen Zeitstempeln geschützt, sodass Integrität, Unveränderbarkeit und ein belastbarer Zeitbezug nachprüfbar sind.

Wird ein Dokument innerhalb von vierzehn Tagen nicht geöffnet, wird der Zustellprozess systemseitig mit dem protokollierten Ergebnis „Frist abgelaufen, ungelesen" abgeschlossen. Der Fristablauf wird revisionssicher protokolliert und im Rahmen der Nachweisführung durch einen Fristablaufnachweis dokumentiert.

## 2.2 Funktion und Einsatzbereiche

Der QERDS *d.velop eIDAS postbox* unterstützt geschäftliche und organisatorische Anwendungsfälle, in denen eine rechtsverbindliche elektronische Zustellung erforderlich ist. Typische Einsatzbereiche sind die digitale Zustellung geschäfts- und vertragsrelevanter Dokumente, die Behördenkommunikation und öffentliche Verwaltungsprozesse sowie die digitale Kommunikation zwischen Unternehmen und Privatpersonen.

## 2.3 Abgrenzung zu nicht-qualifizierten Zustellungen

Neben der qualifizierten Zustellung stellt die d.velop postbox auch nicht-qualifizierte Standard-zustellungen bereit. Diese Public Policy beschreibt ausschließlich den qualifizierten elektronischen Zustell-dienst nach Art. 44 eIDAS. Nicht-qualifizierte Zustellverfahren sind nicht Gegenstand dieses Dokuments.

## 2.4 Rechtswirkungen gemäß Art. 43 eIDAS

Im Rahmen der qualifizierten Zustellung erzeugt der qualifizierte elektronische Zustelldienst elektronische Nachweise über den Versand eines Dokuments, nachdem die fachlichen und technischen Voraussetzungen für die Zustellung erfolgreich geprüft wurden, sowie über die Öffnung des Dokuments durch den Empfänger. Zusätzlich wird die Integrität der Nachweisobjekte kryptographisch abgesichert und prüfbar gemacht. Sämtliche Nachweise werden elektronisch gesiegelt und qualifiziert zeitgestempelt. Dadurch lassen sich die maßgeblichen Zustellereignisse nachvollziehbar und unabhängig verifizierbar belegen.

# 3 Registrierung, Identifizierung und Authentifizierung

Dieses Kapitel beschreibt, wie Absender und Empfänger im qualifizierten elektronischen Zustelldienst registriert, identifiziert und für die Nutzung des Dienstes authentifiziert werden. Ziel ist eine belastbare technische Zuordnung der Zustellereignisse zu den jeweils verantwortlichen Akteuren, sodass die erzeugten Nachweise rechtssicher zugeordnet und unabhängig überprüft werden können.

## 3.1 Registrierung von Absendern (juristische Personen)

Absenderorganisationen werden vor der Nutzung des qualifizierten Zustelldienstes im Rahmen eines Onboarding-Prozesses registriert. Dabei wird der Absender für die vorgesehenen Anlieferkanäle technisch freigeschaltet und es werden die für die spätere Zuordnung erforderlichen Referenzen und Zulassungen eingerichtet. Die Registrierung stellt sicher, dass nur zuvor erfasste und autorisierte Absender die qualifizierte Zustellung auslösen oder sicherheitsrelevante Konfigurationen verändern können.

## 3.2 Identifizierung und Authentifizierung von Absendern (juristische Personen)

Juristische Personen werden beim Onboarding über ein Qualified Website Authentication Certificate (QWAC) identifiziert. Das QWAC enthält geprüfte Organisationsinformationen und ermöglicht eine eindeutige Zuordnung der Absenderorganisation auf Basis der eIDAS-Vertrauensinfrastruktur.

Die Authentifizierung des Absenders erfolgt je Anlieferkanal mit den dafür vorgesehenen technischen Mechanismen. Sie baut auf der im Onboarding registrierten Absenderidentität und den dort eingerichteten Zulassungen und Referenzen auf. Dadurch können sicherheitsrelevante Aktionen und Einlieferungen eindeutig einem registrierten Absender zugeordnet werden.

Für die systemgestützte Nutzung stellt der Dienst zusätzlich sicher, dass ein für die Einlieferung verwendeter Konfigurations- oder Credential-Stand nachvollziehbar referenziert und gegen Manipulation abgesichert ist. Die konkrete technische Ausprägung ist kanalabhängig und umfasst je nach Anlieferweg insbesondere die Verwendung von zertifikatsbasierten Nachweisen, kanalgebundenen Credentials sowie integritätsgesicherten Konfigurationsständen. Dadurch kann der Dienst belegen, dass Einlieferungen und Zustellvorgänge nur auf Basis zulässiger und unveränderter Voraussetzungen durchgeführt wurden.

## 3.3 Registrierung von Empfängern (natürliche Personen)

Empfänger registrieren sich durch die Erstellung eines Nutzerkontos. Die Registrierung dient der Anlage eines eindeutigen Empfängerkontos als Grundlage für die spätere qualifizierte Zustellung. Ein qualifizierter Empfängerstatus wird dabei erst dann erreicht, wenn zusätzlich die Identifizierung erfolgreich abgeschlossen wurde und die für die starke Authentifizierung erforderlichen Zugangsmittel eingerichtet sind.

## 3.4 Identifizierung von Empfängern (natürliche Personen)

Empfänger werden als natürliche Personen mittels staatlicher elektronischer Identität (eID) identifiziert. Die eID-Identifizierung liefert amtlich verifizierte Identitätsattribute und adressbezogene Daten, die für die eindeutige Zustellung erforderlich sind. Die Identifizierung erfolgt kontrolliert und so, dass die ausgelesenen Identitätsdaten im Empfängerkonto als verifizierte Grundlage für die qualifizierte Nutzung herangezogen werden.

## 3.5 Authentifizierungsmethoden von Empfängern

Für sicherheitsrelevante Empfängeraktionen wird eine starke Authentifizierung über Passkey (WebAuthn) eingesetzt. Der Passkey ist ein gerätegebundenes Authentifizierungsmittel auf Basis asymmetrischer Kryptographie. Er wird so verwendet, dass insbesondere das erstmalige Öffnen eines zugestellten Dokuments mittels *d.velop eIDAS postbox* eine erfolgreiche Passkey-Authentifizierung voraussetzt.

Die Passkey-basierte Authentifizierung ist phishing-resistent und reduziert Risiken, die bei passwort-basierten Verfahren typischerweise entstehen. Sie ermöglicht eine starke Authentifizierung ohne die Speicherung oder Übertragung geheimer Passwörter durch den Dienst.

## 3.6 Anforderungen an die Identitätsbindung

Die Identität des Absenders und des Empfängers muss eindeutig an die jeweilige Nutzung des Dienstes gebunden sein, sodass Zustellnachweise rechtssicher den beteiligten Akteuren zugerechnet werden können. Diese Identitätsbindung wird im Dienst wie folgt hergestellt:

- Juristische Personen: QWAC ⇄ Sendersystem ⇄ gesiegeltes Konfigurationsprofil
- Natürliche Personen: eID ⇄ Nutzerkonto ⇄ Passkey

Damit ist sichergestellt, dass Zustellereignisse und Nachweise eindeutig identifizierten natürlichen oder juristischen Personen zugeordnet werden können. Die Bindung wird so umgesetzt, dass spätere sicherheitsrelevante Aktionen und die Nachweisbildung auf nachvollziehbaren, überprüfbaren Referenzen beruhen.

# 4 Ablauf der qualifizierten elektronischen Zustellung

Dieses Kapitel beschreibt den Ablauf der qualifizierten elektronischen Zustellung über die *d.velop eIDAS postbox*. Der Prozess umfasst die Einlieferung durch den Absender, die Annahme und Validierung durch den Dienst, die Bereitstellung im Postfach des Empfängers sowie das Öffnen durch den Empfänger. Der Dienst dokumentiert die für die Nachweisführung relevanten Ereignisse und erzeugt darauf basierend elektronische Nachweise gemäß den Anforderungen des Art. 44 eIDAS.

## 4.1 Einlieferung durch den Absender

Der Absender übermittelt ein Dokument über ein angebundenes Sendersystem oder über bereitgestellte Schnittstellen an den qualifizierten elektronischen Zustelldienst. Die Einlieferung erfolgt so, dass sie einem registrierten Absender eindeutig zugeordnet werden kann. Der Dienst nimmt die Einlieferung nur an, wenn die erforderlichen Voraussetzungen für die qualifizierte Verarbeitung erfüllt sind.

## 4.2 Eingang und Validierung der Dokumente

Nach Eingang prüft der Dienst automatisiert, ob die Einlieferung des Dokuments fachlich und technisch zulässig ist. Der Dienst prüft, ob die Einlieferung über einen für den Absender freigeschalteten und zertifizierten Anlieferkanal erfolgt. Er prüft außerdem, ob ein gültiges eIDAS-Zustellprofil für den Absender vorliegt. Der verwendete Profilstand muss dem zuvor legitimierten Konfigurationsstand entsprechen. Er darf nicht verändert sein. Die Prüfung erfolgt über einen Integritätsabgleich gegen den gespeicherten Profilstand.

Zusätzlich werden die formalen Anforderungen an die Einlieferung geprüft. Dazu gehören das zulässige Dokumentformat (PDF) und technische Rahmenbedingungen wie das maximale Dokumentvolumen von 20 MB. Der Dienst prüft außerdem, ob eine Zustellung an einen eindeutig identifizierten Empfänger möglich ist. Die Zustellbarkeit wird je nach Zustellmodell entweder über ein Zustellmerkmal (1:1-Beziehung) oder über einen Adressabgleich ermittelt.

Nur wenn alle Prüfungen erfolgreich sind, wird die Einlieferung angenommen. Erst ab diesem Zeitpunkt wird der qualifizierte Zustellprozess gestartet und der Einlieferungsnachweis erzeugt. Wenn eine Voraussetzung nicht erfüllt ist, wird die Einlieferung kontrolliert abgebrochen. Eine qualifizierte Zustellung wird nicht eingeleitet. Der Absender erhält eine ablehnende Rückmeldung über den jeweils genutzten Anlieferkanal. Die Rückmeldung enthält eine sprechende Fehlerbeschreibung, aus der der Ablehnungsgrund hervorgeht (z. B. Anlieferkanal nicht freigeschaltet, ungültiger Profilstand, Empfänger nicht zustellbar, Format/Größenlimit verletzt). Die genaue Ausprägung der Fehlerdarstellung ist schnittstellenabhängig.

## 4.3 Zustellung des Dokuments an den Empfänger

Nach erfolgreicher Validierung wird das Dokument dem Empfänger in seinem Postfach bereitgestellt. Die Bereitstellung erfolgt so, dass sie dem Empfängerkonto eindeutig zugeordnet ist und die Grundlage für eine qualifizierte Öffnung und Nachweisführung bildet.

## 4.4 Öffnung durch den Empfänger

Der Empfänger kann das Dokument nach erfolgreicher Authentifizierung mittels Passkey öffnen. Das Öffnen ist ein wesentliches Ereignis für die Nachweisführung. Das erstmalige Öffnen eines zugestellten Dokuments erfolgt derzeit ausschließlich über die Mobile App. Im Webclient ist der Zugriff auf vorher freigeschaltete Dokumente möglich.

## 4.5 Umgang mit Nichtöffnung innerhalb einer definierten Frist

Wird ein bereitgestelltes Dokument innerhalb von sieben Tagen nicht geöffnet, erhält der Absender als Komfortfunktion eine entsprechende Information. Diese Information wird als protokollierter Servicehinweis geführt. Sie ist kein Evidenztyp und nicht Bestandteil des gesiegelten Zustellnachweises.

Wird das Dokument innerhalb von vierzehn Tagen nicht geöffnet, wird der Zustellprozess mit dem Ergebnis „Frist abgelaufen, ungelesen" abgeschlossen. Hierzu wird ein Fristablaufnachweis erzeugt. Der Fristablaufnachweis ist Teil der Nachweisführung und wird wie die übrigen Nachweise qualifiziert gesiegelt.

## 4.6 Abschluss des Zustellprozesses

Die Zustellung gilt als abgeschlossen, wenn der Empfänger das Dokument geöffnet hat. Sie gilt ebenfalls als abgeschlossen, wenn seit der Bereitstellung vierzehn Tage verstrichen sind, ohne dass eine Öffnung erfolgt ist. In diesem Fall ist die Zustellung abgeschlossen, jedoch ungelesen. Der Zustellnachweis dokumentiert den Abschluss der Zustellung anhand der maßgeblichen qualifizierten Ereignisse. Er umfasst insbesondere den Versand sowie die Öffnung oder den Ablauf der Frist ohne Öffnung.

# 5 Evidenz- und Nachweisbildung

## 5.1 Art der erzeugten Nachweise

Der qualifizierte elektronische Zustelldienst erzeugt zu den maßgeblichen Ereignissen des qualifizierten Zustellprozesses elektronische Nachweise (Evidenzen). Diese Evidenzen werden nach ihrer Erstellung kryptografisch abgesichert und dienen als überprüfbare Belege für Absender und Empfänger.

Für jede qualifizierte Zustellung gilt folgende Nachweislogik:

- Es wird immer ein Einlieferungsnachweis erzeugt. Er dokumentiert die erfolgreiche Annahme der Einlieferung nach Abschluss der fachlichen und technischen Eingangskontrollen. Mit diesem Zeitpunkt startet der qualifizierte Zustellprozess.
- Als Ergebnisnachweis wird entweder ein Öffnungsnachweis oder ein Fristablaufnachweis erzeugt. Der Öffnungsnachweis dokumentiert die erstmalige Öffnung des Dokuments durch den Empfänger. Der Fristablaufnachweis dokumentiert, dass das Dokument innerhalb der definierten Frist nicht geöffnet und der Zustellprozess mit dem entsprechenden Endergebnis abgeschlossen wurde.

Zusätzlich stellt der Dienst einen Zustellnachweis bereit. Er führt die für die Zustellung relevanten Ereignisse in einem zusammenhängenden Nachweisobjekt zusammen und bildet das Ergebnis der Zustellung (Öffnung oder Fristablauf) nachvollziehbar ab. Evidenzen werden ausschließlich erzeugt, wenn der qualifizierte Zustellprozess gestartet wurde. Wird eine Einlieferung vor der Annahme abgebrochen, entstehen keine Evidenzen.

**Policy-Identifier in Evidenzen**
Die vom Dienst erzeugten Evidenzen und der Zustellnachweis enthalten eine Referenz auf diese Public Policy (Policy Identifier). Dadurch ist nachvollziehbar, nach welchen Vorgaben die Evidenz erzeugt wurde.

## 5.2 Integrität, Unveränderbarkeit, Zuverlässigkeit des Zeitbezugs

Für die kryptographisch abgesicherte Nachweisführung werden Evidenzen und Nachweise mit einem qualifizierten elektronischen Zeitstempel versehen. Dadurch sind Integrität, Unveränderbarkeit und ein belastbarer Zeitbezug nachprüfbar. Jede nachträgliche Manipulation wäre an Siegel oder Zeitstempel erkennbar. Siegel und Zeitstempel können unabhängig verifiziert werden.

**Uhrensynchronisation (betrieblicher Zeitbezug)**
Die qualifizierten Zeitstempel in den Evidenzen werden durch einen externen qualifizierten Vertrauensdienst erbracht und sind maßgeblich für den beweiskräftigen Zeitbezug der Nachweise. Unabhängig davon stellt der Diensteanbieter für Protokollierung, Korrelation und Betriebsüberwachung eine konsistente Systemzeit sicher. Dazu werden die für den Betrieb relevanten Systeme zentral per NTP synchronisiert und die Synchronisation wird überwacht. Diese Systemzeit dient der technischen Nachvollziehbarkeit (z. B. Audit-Logs, Monitoring, Fehleranalyse), ersetzt jedoch nicht den qualifizierten Zeitstempel der Evidenzen.

## 5.3 Aufbewahrung der Evidenzen

Evidenzen werden für die Dauer von sieben Jahren aufbewahrt. Während der Aufbewahrungsfrist stellt der Dienst sicher, dass Evidenzen vollständig, unverändert und abrufbar bleiben. Nach Ablauf der Aufbewahrungsfrist werden Evidenzen gemäß den definierten Lösch- und Aufbewahrungsregeln entfernt, sofern keine abweichenden gesetzlichen Pflichten bestehen.

## 5.4 Abrufbarkeit der Nachweise durch Nutzer

Absender und Empfänger können Nachweise zu ihren jeweiligen Zustellungen über ihre Nutzerzugänge abrufen. Der Zugriff ist rollen- und berechtigungsgebunden. Der Dienst stellt die Nachweise in zwei Formen bereit:

**Zustellnachweis (Anzeige-/Abrufformat)**

- Empfänger erhalten den Zustellnachweis in einem menschenlesbaren Format als PDF.
- Absender erhalten den Zustellnachweis als maschinenlesbare Evidenz in einem strukturierten Format (JSON oder XML).

Evidenzen werden in einem Format bereitgestellt, das eine unabhängige Prüfung der kryptographischen Absicherung (Siegel, Zeitstempel) ermöglicht.

**Beweisexport (prüfbares Beweisobjekt)**
Zusätzlich kann ein Beweisexport als gesiegelter ASIC-Container angefragt werden. Der Beweisexport enthält die zugehörigen Evidenzen, die Validierungsreports sowie die zugehörigen Siegelartefakte. Dadurch kann die Nachweisführung unabhängig vom Produkt geprüft und archiviert werden. Der Beweisexport ist insbesondere für die externe Beweisführung vorgesehen, zum Beispiel für die Vorlage bei Gerichten oder gegenüber Dritten.

# 6 Pflichten und Verantwortlichkeiten der Nutzer

Absender und Empfänger tragen Mitverantwortung dafür, dass qualifizierte Zustellungen sicher durchgeführt werden können und die erzeugten Nachweise belastbar bleiben. Dazu gehört insbesondere der Schutz von Authentifizierungsmitteln, die Einhaltung der vorgesehenen Verfahren sowie die Nutzung geeigneter und vertrauenswürdiger Systeme.

## 6.1 Pflichten des Absenders

Der Absender ist dafür verantwortlich, den Dienst ausschließlich im Rahmen der vorgesehenen Prozesse zu nutzen und die Voraussetzungen für eine qualifizierte Zustellung sicherzustellen. Dazu gehören insbesondere:

**Eindeutige Adressierung und korrekte Bereitstellung von Zustellinformationen**
Der Absender stellt sicher, dass er bei der Einlieferung das richtige Zustellmerkmal für den vorgesehenen Empfänger verwendet.

Sofern die Adressierung über vorbereitete Konten oder Zustellbeziehungen erfolgt, liegt es in der Verantwortung des Absenders, die dafür erforderlichen Informationen dem richtigen Empfänger korrekt und sicher bereitzustellen. Dazu zählen insbesondere Einladungs- oder Freischaltinformationen sowie sonstige Zugangsdaten, sofern diese im jeweiligen Verfahren vorgesehen sind.

Sofern die Adressierung auf Basis der Empfängeradresse erfolgt und diese im Rahmen der Übermittlung als Metadaten mitgegeben wird, stellt der Absender sicher, dass die verwendete Adresse dem vorgesehenen Empfänger zuzuordnen ist.

**QWAC als Voraussetzung für Onboarding und Anlieferkanäle**
Der Absender ist für die Beantragung und Bereitstellung eines gültigen Qualified Website Authentication Certificate (QWAC) verantwortlich. Das QWAC ist Voraussetzung für das technische Onboarding. Ohne QWAC erfolgt kein Onboarding. Ohne Onboarding werden keine Anlieferkanäle konfiguriert und freigeschaltet.

Der Absender stellt außerdem sicher, dass das QWAC während der Nutzung gültig bleibt. Dazu gehört insbesondere die rechtzeitige Erneuerung vor Ablauf sowie die Bereitstellung des aktualisierten Zertifikats zur erneuten Prüfung und Aktualisierung der hinterlegten Referenzen.

**Schutz technischer Zugangsdaten**
Der Absender schützt alle technischen Zugangsdaten und Credentials, die im Kontext der Anlieferung eingesetzt werden. Dazu zählen insbesondere Zertifikate, Schlüsselmaterial, Secrets und vergleichbare Artefakte. Der Absender stellt sicher, dass nur berechtigte Personen und Systeme Zugriff erhalten.

**Organisatorische Zugriffskontrolle und Administration**
Die Verantwortung für Rollen- und Zugriffskontrolle im Absenderbereich liegt beim Absender. Der Absender stellt sicher, dass ausschließlich berechtigte Personen administrative Tätigkeiten ausführen. Rollenwechsel, Austritte und Berechtigungsänderungen werden so umgesetzt, dass unberechtigte Zugriffe ausgeschlossen sind. Soweit hierfür eine Mitwirkung des Anbieters erforderlich ist, veranlasst der Absender die notwendigen Maßnahmen unverzüglich.

**Sicherer Dokumenteninhalt**
Der Absender stellt sicher, dass zur Zustellung eingereichte Dokumente frei von Schadsoftware sind. Er stellt außerdem sicher, dass die Inhalte nicht gegen geltendes Recht oder die zulässigen Nutzungsbedingungen verstoßen.

**Unterlassung missbräuchlicher Nutzung**
Der Absender unterlässt missbräuchliche Nutzung des Dienstes. Dazu gehören insbesondere der Versuch, Sicherheitsmechanismen zu umgehen, die Übermittlung unzulässiger Inhalte oder die Nutzung nicht freigegebener Clients und Integrationswege.

## 6.2 Pflichten des Empfängers

Der Empfänger ist verpflichtet, die Voraussetzungen für eine sichere Nutzung des Dienstes einzuhalten und sein Authentifizierungsmittel vor Missbrauch zu schützen. Dazu gehören insbesondere:

**Schutz des Authentifizierungsmittels**
Der Empfänger schützt sein Authentifizierungsmittel, insbesondere Passkey und Geräteschutzmechanismen wie PIN oder Biometrie, vor unbefugter Nutzung. Er verwendet geeignete Gerätesperren. Bei Verdacht auf Missbrauch oder bei Verlust des Endgeräts ergreift der Empfänger angemessene Gegenmaßnahmen, zum Beispiel Gerätesicherung und Kontoschutzmaßnahmen.

**Sorgfalt bei der Nutzung und regelmäßige Kenntnisnahme**
Der Empfänger prüft eingehende Zustellungen regelmäßig. Er öffnet Dokumente nur in einer vertrauenswürdigen Umgebung. Er führt erforderliche Sicherheits- und Bestätigungsschritte ordnungsgemäß durch, sofern diese im jeweiligen Prozess vorgesehen sind.

**Korrekte Angaben im Rahmen der Registrierung/Identifizierung**
Soweit im Prozess Angaben durch den Empfänger erforderlich sind, macht der Empfänger diese vollständig und wahrheitsgemäß. Identitäts- und Adressdaten, die aus der eID-Identifizierung übernommen werden, sind systemseitig führend.

**Meldung von Sicherheitsvorfällen**
Der Empfänger meldet Sicherheitsvorfälle, Verdachtsfälle oder den Verlust des Endgeräts unverzüglich über die vorgesehenen Kontaktwege. Dies gilt insbesondere dann, wenn die Sicherheit des Kontos oder die Nachweisführung betroffen sein kann.

## 6.3 Externe Abhängigkeiten (Geräte, Software, Konnektivität)

Die Nutzung des Dienstes setzt geeignete Endgeräte, eine stabile Internetverbindung und kompatible Software voraus. Einschränkungen ergeben sich insbesondere aus Betriebssystemversionen, Browser- und App-Unterstützung sowie verfügbaren Sicherheitsfunktionen des Endgeräts.

Für Störungen oder Sicherheitsrisiken in Netzen, Endgeräten oder Software der Nutzer und Dritter außerhalb des Einflussbereichs des Diensteanbieters kann keine Verantwortung übernommen werden.

Der Dienst kann den Zugriff ablehnen, einschränken oder zusätzliche Authentifizierung verlangen, wenn technische Indikatoren auf ein erhöhtes Sicherheitsrisiko hindeuten. Dies gilt insbesondere bei

erkennbaren Manipulations- oder Integritätsrisiken oder bei fehlenden Voraussetzungen für eine sichere Authentifizierung.

# 7 Verantwortlichkeiten des Diensteanbieters

## 7.1 Allgemeine Dienstverantwortung

Der Diensteanbieter betreibt den qualifizierten elektronischen Zustelldienst gemäß eIDAS-Verordnung und den einschlägigen ETSI-Spezifikationen. Er stellt sicher, dass die zustellrelevanten Prozesse sowie die Erzeugung, Integrität, Nachvollziehbarkeit und Aufbewahrung der Zustellnachweise durch geeignete technische und organisatorische Maßnahmen abgesichert sind.

Der Dienst wird auf einer cloudbasierten Betriebsplattform innerhalb der Europäischen Union betrieben. Eine lokale Verarbeitung oder Speicherung dienstrelevanter Daten auf Arbeitsplatzsystemen ist ausgeschlossen.

## 7.2 Schutz der Inhalte

Der Diensteanbieter schützt die Vertraulichkeit und Integrität der verarbeiteten Dokumente sowie der zustellrelevanten Informationen während Transport und Speicherung durch kryptographische Maßnahmen nach dem Stand der Technik. Die Absicherung der Datenübertragung erfolgt über gesicherte Schnittstellen und Transportverschlüsselung.

Qualifizierte elektronische Siegel und qualifizierte elektronische Zeitstempel werden nicht in der eigenen Infrastruktur erzeugt, sondern über einen externen qualifizierten Vertrauensdiensteanbieter bezogen. Der Betrieb der zugrunde liegenden kryptographischen Infrastruktur, einschließlich der Schlüssel, liegt dabei im Verantwortungsbereich des jeweiligen QTSP.

## 7.3 Verfügbarkeit

Der Dienst ist auf hohe Verfügbarkeit und Resilienz ausgelegt. Die produktiven Komponenten werden georedundant in den Cloud-Regionen EU-01 (Deutschland) und EU-02 (Österreich) betrieben. Ergänzend werden Sicherungs- und Wiederanlaufkomponenten in einer weiteren Cloud-Umgebung für Backup-, Wiederherstellungs- und Ausweichszenarien (Cold-Standby) genutzt. Die Verfügbarkeit wird durch Monitoring, Kapazitäts- und Skalierungsmanagement sowie definierte Betriebs-, Wiederanlauf- und Wiederherstellungsprozesse unterstützt.

## 7.4 Umgang mit Störungen und Sicherheitsvorfällen

Störungen und sicherheitsrelevante Ereignisse werden zeitnah erkannt, bewertet, dokumentiert und behandelt. Sicherheitsereignisse werden sowohl automatisiert (Monitoring und Alerting, Anomalien, Integritätsfehler) als auch manuell (Betrieb, Entwicklung, Support, Kundenmeldungen) erkannt. Ereignisse werden unverzüglich gemeldet und in Ticketsystemen nachvollziehbar dokumentiert.

Für die Incident-Bearbeitung gelten definierte Schritte zur Erstbewertung und Klassifikation einschließlich Impact-Regeln. Bei Hinweisen auf Beeinträchtigungen von Kernprozessen, Evidenzerzeugung, Auditketten oder Zustellprozessen wird der Impact als hoch eingestuft. Abhängig von der Einstufung wird ein Incident Response Team (IRT) aktiviert, dass Analyse, Eindämmung, forensische Sicherung, Maßnahmen und Wiederherstellung koordiniert.

Sicherheits- und Systemereignisse werden an angebundene SIEM-Systeme übertragen. Bei Störungen dieser Anbindung werden Ereignisse lokal zwischengespeichert und nach Wiederverfügbarkeit nachgeliefert.

## 7.5 Beschwerdemanagement

Für Beschwerden im Zusammenhang mit dem qualifizierten elektronischen Zustelldienst steht ein strukturiertes Beschwerdeverfahren zur Verfügung. Vertragspartner von Absendern und Empfängern ist die d.velop AG. Beschwerden können über die veröffentlichten Kontaktwege eingereicht werden. Der Eingang wird bestätigt und die Beschwerde einer sachgerechten Bearbeitung zugeführt. Der Beschwerdeführer wird über das Ergebnis informiert. Betrifft eine Beschwerde den Betrieb oder sicherheitsrelevante Eigenschaften des qualifizierten elektronischen Zustelldienstes, erfolgt die Bearbeitung unter Einbindung des Diensteanbieters. Kann eine Beschwerde nicht einvernehmlich geklärt werden, besteht die Möglichkeit, sich an die zuständige Aufsichtsbehörde gemäß eIDAS-Verordnung zu wenden. Beschwerden und deren Bearbeitung werden dokumentiert und zur kontinuierlichen Verbesserung des Dienstes genutzt.

## 7.6 Beendigung des Dienstes und Fortführung der Nachweisprüfung

Der Diensteanbieter trifft organisatorische und technische Vorkehrungen für den Fall einer Beendigung des qualifizierten elektronischen Zustelldienstes. Ziel ist es, Auswirkungen für Absender, Empfänger und sonstige berechtigte Parteien zu minimieren und insbesondere sicherzustellen, dass Informationen zur Prüfung der Korrektheit bereits erzeugter Nachweise für einen angemessenen Zeitraum weiterhin verfügbar bleiben. Hierzu hält der Diensteanbieter einen aktuellen Beendigungsplan vor. Vor einer Beendigung werden betroffene Parteien und zuständige Stellen rechtzeitig informiert. Soweit möglich, wird eine Übertragung der für die Fortführung erforderlichen Pflichten und Informationen an eine geeignete, verlässliche Stelle vorgesehen, damit die Überprüfbarkeit von Siegeln/Zeitstempeln und Nachweisen fortbesteht. Kryptographische Schlüssel, die im Verantwortungsbereich des Diensteanbieters liegen, werden im Beendigungsfall ordnungsgemäß außer Betrieb genommen und vor unbefugter Wiederverwendung geschützt.

Unabhängig von einer Beendigung des Dienstes regeln Löschung und Offboarding-Prozesse die Beendigung der Teilnahme einzelner Absender oder Empfänger. Operative Daten werden nach den geltenden Löschkonzepten entfernt, ohne die Unveränderbarkeit und Aufbewahrung qualifizierter Nachweise zu beeinträchtigen. Bereits erzeugte Zustellnachweise und Evidenzen bleiben entsprechend der festgelegten Aufbewahrungsfristen unverändert erhalten.

## 7.7 Verantwortungsabgrenzung zu Infrastruktur- und Vertrauensdiensteanbietern

Der qualifizierte elektronische Zustelldienst wird in einer arbeitsteiligen Betriebs- und Lieferkette erbracht. Der Diensteanbieter verantwortet die End-to-End-Prozesse der qualifizierten Zustellung innerhalb der *d.velop eIDAS postbox*, einschließlich der fachlichen Steuerung, der sicherheitsrelevanten Kontrollen, der Erzeugung und Aufbewahrung von Zustellnachweisen sowie der Überwachung der Dienstkomponenten.

Die zugrunde liegende Cloud-Infrastruktur (Compute, Storage, Netzwerk, Rechenzentrumsbetrieb) wird durch externe Infrastrukturbetreiber bereitgestellt. Der Diensteanbieter verantwortet in diesem Modell die sichere Konfiguration und den sicheren Betrieb der darauf betriebenen Dienstkomponenten (z. B. Härtung, Zugriffssteuerung, Überwachung, Patch- und Änderungsprozesse) sowie die Umsetzung der für den QERDS erforderlichen technischen und organisatorischen Maßnahmen.

Qualifizierte elektronische Siegel und qualifizierte elektronische Zeitstempel werden über einen externen qualifizierten Vertrauensdiensteanbieter bezogen. Die Verantwortlichkeiten zur Erzeugung dieser Vertrauensdienste liegen beim jeweiligen QTSP. Der Diensteanbieter verantwortet die korrekte Anforderung, Einbindung und Verwendung im Rahmen der Evidenz- und Nachweisbildung (siehe Kapitel 7.2 Schutz der Inhalte).

Unabhängig von der Aufgabenteilung stellt der Diensteanbieter durch geeignete Kontrollen sicher, dass die Dienstleistungserbringung auch bei Einbindung externer Dienstleister nachvollziehbar, überprüfbar und im Rahmen der qualifizierten Prozesse abgesichert bleibt.

# 8 Datenschutz und Datensicherheit

Für die Nutzung des qualifizierten elektronischen Zustelldienstes werden personenbezogene Daten verarbeitet, soweit dies für Registrierung, Identifizierung, Zustellung, Nachweisbildung, Support und die Erfüllung gesetzlicher Pflichten erforderlich ist. Der Dienst wird durch die d.velop mobile services GmbH als Diensteanbieter betrieben.

Informationen zur Datenverarbeitung für Endnutzer (z. B. Transparenzhinweise und Betroffenenrechte) werden durch die d.velop AG als Vertragspartner gegenüber Absendern und Empfängern bereitgestellt. Ergänzende dienstspezifische Informationen des Diensteanbieters werden, soweit erforderlich, zusätzlich veröffentlicht. Die Datenschutzinformationen der d.velop AG sind unter https://www.d-velop.de/datenschutz abrufbar.

## 8.1 Grundsätze der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt nach den Grundsätzen der DSGVO, insbesondere:

- **Rechtmäßigkeit und Transparenz:** Die Verarbeitung erfolgt auf einer gültigen Rechtsgrundlage und wird gegenüber Endnutzerinformationen durch die d.velop AG bereitgestellt. Betriebs- und dienstbezogene Pflichten liegen beim Diensteanbieter.

- **Zweckbindung:** Daten werden ausschließlich für die definierten Zwecke verarbeitet, insbesondere für den Betrieb des Zustelldienstes, die Nachweisbildung und die Erfüllung regulatorischer Anforderungen.
- **Datenminimierung:** Es werden nur solche Daten verarbeitet, die für die Durchführung der qualifizierten Zustellung und die Erzeugung bzw. Prüfbarkeit der Nachweise erforderlich sind.
- **Integrität und Vertraulichkeit:** Durch technische und organisatorische Maßnahmen wird ein angemessenes Schutzniveau für personenbezogene Daten und zustellrelevante Informationen gewährleistet (z. B. Zugriffsbeschränkungen, Protokollierung, Verschlüsselung und Transportabsicherung gemäß Stand der Technik).

## 8.2 Speicherfristen

Zustell- und Nachweisdaten werden nur so lange gespeichert, wie es für den jeweiligen Zweck und zur Erfüllung gesetzlicher bzw. regulatorischer Anforderungen erforderlich ist. Für die qualifizierte Zustellnachweise gilt eine Aufbewahrungsfrist von sieben Jahren, sofern keine abweichenden gesetzlichen Aufbewahrungs- oder Nachweispflichten bestehen. Die Aufbewahrung und Löschung der Evidenzen erfolgt im Verantwortungsbereich des Diensteanbieters, während Abruf und Darstellung gegenüber Endnutzern über die durch die d.velop AG bereitgestellten Endnutzerzugänge erfolgt. Nach Ablauf der jeweiligen Frist werden Daten gemäß den definierten Lösch- und Aufbewahrungsregeln entfernt bzw. anonymisiert, soweit keine fortbestehenden Pflichten oder berechtigten Gründe entgegenstehen (z. B. laufende Streitfälle oder gesetzliche Aufbewahrungspflichten).

# 9 Serviceverfügbarkeit und Support

Der Diensteanbieter stellt den Betrieb des qualifizierten elektronischen Zustelldienstes sicher, überwacht kritische Komponenten zur frühzeitigen Störungserkennung und führt Wiederherstellungsmaßnahmen nach definierten Betriebsprozessen durch. Die Kommunikation und Supportannahme gegenüber Absendern und Empfängern erfolgt grundsätzlich über die d.velop AG als Vertragspartner, sofern in diesem Dokument nicht ausdrücklich abweichend beschrieben.

## 9.1 Verfügbarkeitsangaben

Soweit Verfügbarkeit, Servicefenster oder Servicelevels gegenüber Absendern und Empfängern vereinbart werden, werden diese durch die d.velop AG als Vertragspartner bereitgestellt bzw. vertraglich geregelt.

Unabhängig davon stellt der Diensteanbieter die technischen und organisatorischen Grundlagen für einen stabilen Betrieb bereit. Dazu gehören insbesondere Monitoring, Betriebsprozesse und definierte Wiederanlaufverfahren.

## 9.2 Kommunikationskanäle

Dienstbezogene Hinweise, die direkt die Nutzung des Dienstes betreffen (z. B. Wartungsinformationen oder bekannte Einschränkungen), können im Produkt über Hinweise in der Mobile App und im Webclient bereitgestellt werden (In-Produkt-Kommunikation). Supportanfragen, vertragliche Kommunikation und

weitergehende Informationen gegenüber Absendern und Empfängern erfolgen über die von der d.velop AG bereitgestellten Kontaktwege. Diese sind in Kapitel 10 ausgewiesen.

## 9.3 Supportzeiten

Supportzeiten und Reaktionsmodalitäten werden durch die d.velop AG gegenüber Absendern und Empfängern bereitgestellt. Sicherheitsrelevante Meldungen werden über die in Kapitel 10 genannten Wege angenommen und gemäß den festgelegten Prozessen bearbeitet. Sofern zur Bearbeitung eine technische Analyse oder Maßnahme erforderlich ist, erfolgt eine Eskalation an den Diensteanbieter.

## 9.4 Wartungsfenster

Geplante Wartungsfenster werden angekündigt. Wartungen werden so geplant und durchgeführt, dass Auswirkungen auf Nutzer minimiert werden. Während Wartungsfenstern kann die Verfügbarkeit eingeschränkt sein. Nach Wartungen werden definierte Prüf- und Wiederanlaufmaßnahmen durchgeführt. Die Durchführung der Wartungen, die betriebliche Umsetzung sowie die technische Wiederherstellung liegen im Verantwortungsbereich des Diensteanbieters.

Die Ankündigung geplanter Wartungsfenster erfolgt im Produkt über Hinweise in der Mobile App und im Webclient (In-Produkt-Kommunikation). Sofern darüber hinaus eine externe Kommunikation erforderlich ist, erfolgt diese durch die d.velop AG als Vertragspartner gegenüber Absendern und Empfängern.

# 10 Kontaktinformationen

**Diensteanbieter (Betreiber des qualifizierten elektronischen Zustelldienstes)**
Der qualifizierte elektronische Zustelldienst *d.velop eIDAS postbox* wird durch die d.velop mobile services GmbH betrieben. Der Diensteanbieter ist verantwortlich für den Betrieb des Dienstes, die technische Umsetzung der qualifizierten Zustellprozesse sowie die Erzeugung und Aufbewahrung der Nachweise im Rahmen des qualifizierten Dienstes.

d.velop mobile services GmbH
Adresse: Eggeroder Straße 6, 48624 Schöppingen
E-Mail: postbox.trustbox@d-velop.de

**Vertragspartner und Support (Absender- und Empfängerkommunikation)**
Gegenüber Absendern und Empfängern tritt die d.velop AG als Vertragspartner auf und stellt die Kontaktwege für Supportanfragen und vertragliche Kommunikation bereit. Supportanfragen werden über die von der d.velop AG bereitgestellten Kanäle entgegengenommen und bei Bedarf gemäß definierten Eskalationsprozessen an den Diensteanbieter überführt.

d.velop AG
Adresse: Schildarpstraße 6-8, 48712 Gescher
Support-/Helpdesk-Portal für Absender: https://serviceportal.d-velop.de
Support-/Helpdesk-Portal für Empfänger: https://help.d-velop.de/postbox

**Aufsichtsbehörde**

Die Aufsicht im Zusammenhang mit der Qualifikation und den Aufsichtsaufgaben für qualifizierte Vertrauensdiensteanbieter in Deutschland erfolgt durch die Bundesnetzagentur.

Bundesnetzagentur – Referat IS15
Canisiusstraße 21, 55122 Mainz, Deutschland
E-Mail: eidas@bnetza.de

# 11 Anwendbares Recht und Streitbeilegung

Diese Public Policy beschreibt die öffentlich bereitzustellenden Informationen zum qualifizierten elektronischen Zustelldienst und dessen Nachweisführung. Vertragliche Regelungen (einschließlich Preis-/Leistungsvereinbarungen, Servicelevels, Supportzeiten, Haftung sowie anwendbarem Recht und Gerichtsstand) werden – soweit einschlägig – durch die d.velop AG als Vertragspartner gegenüber Absendern und Empfängern in den jeweiligen Vertragsdokumenten festgelegt.

Unbeschadet davon können Nutzer Beschwerden, über die in dieser Public Policy beschriebenen Kontaktwege einreichen. Beschwerden werden angenommen, dokumentiert, bewertet und nach definierten Prozessen bearbeitet. Sofern Beschwerden oder Streitfälle den qualifizierten Vertrauensdienst, die Nachweisführung oder sicherheitsrelevante Aspekte betreffen, erfolgt die erforderliche fachliche Einbindung des Diensteanbieters im Rahmen der vereinbarten Zusammenarbeit.