TSPS - Trust Service Practice Statement

POSTIDENT

Version 1.1

Stand: 06.04.2021

Inhalt

1. Einleitung

1.1 Übersicht

Deutsche Post AG bietet mit POSTIDENT verschiedene Verfahren zur Identifizierung natürlicher Personen an. POSTIDENT steht als Komponente für Dienste gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS) des Europäischen Parlaments zur Verfügung.

Das hier vorliegende Dokument gilt ausschließlich für die Erbringung der Identitätsprüfung von natürlichen Personen als Identifizierungskomponente durch die Deutsche Post AG im Rahmen der eIDAS-Verordnung.

1.2 Dokumentenname und Identifikation

Dieses Dokument hat den Namen „Vertrauensdiensterichtlinie für die eIDAS-konforme Identifizierung POSTIDENT“.

Dieses Dokument ist ein Trust Service Practice Statement (TSPS) nach ETSI EN 319 401[1].

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

Eine Zertifizierungsstelle (CA) ist eine Organisation, die digitale Zertifikate ausgibt. Eine Zertifizierungsstelle unterhält Mechanismen für die Veröffentlichung, Verteilung und das Invalidieren von Zertifikaten.

Die DPAG unterhält im Kontext des POSTIDENT Verfahrens keine Zertifizierungsstelle (CA). POSTIDENT steht Zertifizierungsstellen als Identifizierungsdienst zur Verfügung, um vor der Ausgabe von Zertifikaten die Identität des Antragsstellers (subscriber) feststellen zu können.

1.3.2 Registrierungsstellen

Eine Registrierungsstelle kann als Vorinstanz einer Zertifizierungsstelle die Verantwortung für die Überprüfung der Geschäftsdaten und persönlichen Daten von Antragsdaten, welche in Zertifikate aufgenommen werden, übernehmen.

Hierzu gehören insbesondere Aufgaben wie das Einreichen von Zertifikatsanträgen bei der Zertifizierungsstelle, Bestätigung von Anträgen zur Erneuerung von Zertifikaten oder das Zurückziehen von Zertifikaten.

Die DPAG betreibt mit dem POSTIDENT Verfahren keine Registrierungsstelle.

Mit POSTIDENT wird ein Identifizierungsdienst für natürliche Personen zur Verfügung gestellt, welche von Zertifizierungsstellen oder Vertrauensdiensteanbietern für das Verfahren zur Ausstellung eines Zertifikats als Identifizierungskomponente genutzt werden kann.

1.3.3 Antragssteller

Antragssteller sind Nutzer eines Vertrauensdienstes, denen z.B. Zertifikate durch eine Zertifizierungsstelle ausgestellt werden. Bei der Nutzung von POSTIDENT als Identifizierungskomponente handelt es sich bei Antragsstellern immer um Natürliche Personen.

Die DPAG identifiziert Antragssteller im Auftrag ihrer Vertragspartner wie beispielsweise Zertifizierungsstellen.

1.3.4 Vertrauende Parteien

Eine vertrauende Partei (relying party) ist eine natürliche Person oder eine juristische Person, welche sich im Geschäftsverkehr auf die korrekte Identität eines Vertragspartners, z.B. einem Zertifikatsinhaber, verlässt.

Im Kontext von Zertifizierungsdiensten werden die auf Grundlage der Identifizierung mittels POSTIDENT Verfahren ausgestellten persönlichen Zertifikate genutzt, um die Unversehrtheit von digital signierten Dokumenten sowie die eindeutige Zuordnung zum Unterzeichner sicherzustellen.

1.4 Zertifikatsverwendung

Nicht zutreffend. Mit dem Service POSTIDENT wird die Identifizierung natürlicher Personen angeboten. Es werden keine Zertifikate ausgestellt.

1.5 Richtlinienverwaltung

1.5.1 Organisation - Verwaltung des Dokuments

Deutsche Post AG
Produktmanagement Identitätsmanagement
Friedrich-Ebert-Allee 37-39
53113 Bonn

www.postident.de

1.5.2 Kontaktperson

Information Security Officer Deutsche Post AG
Identitätsmanagement
Heinrich-Brüning-Str. 7
53113 Bonn
Deutschland

postident@deutschepost.de

www.postident.de

1.5.3 Person, die CPS-Eignung für die Richtlinie bestimmt

Eine Beurteilung der Eignung des Practice-Statement erfolgt durch den für den Geschäftsbereich zuständigen Information Security Officer.

1.5.4 TSPS-Genehmigungsverfahren

Das vorliegende TSPS wird durch das Management der Abteilung Produktmanagement Identitätsmanagement freigegeben. Das Management der Abteilung Produktmanagement Identitätsmanagement ist für die Umsetzung der Richtlinien verantwortlich.

Das Dokument wird durch eine schriftliche Stellungnahme/signierte E-Mail des für den Vertrauensdienst verantwortlichen Leiters genehmigt.

Das TSPS wird in regelmäßigen Abständen einem Review unterzogen und aktualisiert. Neu Versionen müssen durch das Management freigegeben werden.

1.6 Definitionen und Akronyme

1.6.1 Definitionen

Erklärungswürdige Begriffe werden bei Ihrer Einführung im Dokument näher erläutert.

1.6.2 Akronyme

Abkürzung	Bedeutung
CA	Certificate Authority / Zertifizierungstelle
CRL	Certificate Revocation List
CSP	Certification Service Provider
DPAG	Deutsche Post AG
eIDAS	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
ETSI	European Telecommunications Standards Institute
OCSP	Online Certificate Status Protocol
RA	Registration Authority
TSP	Trust Service Provider / Vertrauensdiensteanbieter

1.6.3 Referenzen

Referenz	Quelle
eIDAS	http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910

2 Verantwortlichkeiten für Veröffentlichungen und Repositories

2.1 Repositories

DPAG veröffentlicht dieses TSPS und andere Verfahrens relevante Dokumente wie AGBs und Schnittstellenbeschreibungen auf http://www.postident.de/handbuch

2.2 Veröffentlichung von Zertifikatsinformationen

Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus. Die DPAG wird Nutzer von POSTIDENT als Identifizierungsmodul im Kontext eIDAS vorab informieren, sollten wesentliche Änderungen am Format der Dokumentation der Identifizierungsdienstleistung vorgenommen werden.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Nachfolgende TSPS Versionen werden ebenfalls nach deren Freigabe auf der Website der DPAG veröffentlicht. Wesentliche verfahrensrelevante Änderungen werden vor der Durchführung einer Änderung vorab angekündigt.

2.4 Zugriffskontrollen auf Repositories

Die veröffentlichten Dokumente sind frei über das Internet zugänglich. Es besteht ein reiner Lesezugriff.

Schreibende Zugriffe sind Administratoren vorbehalten. Hierzu sind technische Sicherungsmaßnahmen implementiert, welche das unbefugte Ändern des Inhalts verhindern.

3 Identifikation und Authentifizierung

3.1 Benennung

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus.

3.2 Initiale Identitätsvalidierung

3.2.1 Methode zum Nachweis des Besitzes eines privaten Schlüssels

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus.

3.2.2 Authentifizierung der Organisationseinheit

Nicht zutreffend. POSTIDENT stellt nur eine Möglichkeit zur Identifizierung von natürlichen Personen dar und nicht von juristischen Personen oder anderen Organisationsformen.

3.2.3 Authentifizierung der individuellen Identität

Identifizierung von natürlichen Personen - POSTIDENT durch Postfiliale

Bei der Identifizierung natürlicher Personen durch das Verfahren POSTIDENT durch Postfiliale wird die Identität der zu identifizierenden Person (iP) anhand eines amtlichen, gültigen Ausweisdokuments verifiziert. Es können alle natürlichen Personen, die in Besitz eines gültigen, für das Verfahren zulässigen Ausweisdokuments sind, identifiziert werden. Als zulässige Ausweisdokumente gelten gültige deutsche Personalausweise, andere gleichwertige deutsche Ausweisdokumente, ausländische dem deutschen Personalausweis entsprechende amtliche Identitätskarten sowie Reisepässe, soweit diese Dokumente ein Lichtbild des Inhabers enthalten und von der Deutschen Post zur Identifizierung akzeptiert werden.

Vorbereitung

- Für eine Identifizierung in der Filiale benötigt der Kunde:
  - **POSTIDENT Coupon**
  - **Gültiges Ausweisdokument**

Identifizierung

- Identitätsprüfung in einer Filiale
- **Auslesen** der Ausweisdaten mittels **Ausweisleser**
- **Automatische Übernahme der Daten** in unsere Erfassungsmaske

Datenprüfung und Bereitstellung

- **Datenprüfung** durch Mitarbeiter der DP
- Bestätigung der Daten durch **Unterschrift des Kunden** auf dem ZVT **und des Mitarbeiters** durch Eingabe seiner PIN

In der Filiale nimmt der Mitarbeiter von der zu identifizierenden Person einen Coupon mit den Daten des Auftraggebers entgegen, den sie zuvor vom Auftraggeber zur Verfügung gestellt bekommen hat.

Der Mitarbeiter der Filiale lässt sich ein o.g. Ausweisdokument vorlegen, identifiziert die Person durch einen Abgleich des Lichtbildes und erfasst unter Einbeziehung eines Ausweislesegerätes die personenbezogenen Daten mittels eines postspezifischen IT-Systems. Das Ausweislesegerät prüft wesentliche Sicherheitsmerkmale des vorgelegten Ausweisdokuments. Das Ergebnis der automatischen Prüfung wird dem Auftraggeber mitgeteilt.

Nach der Einholung der Unterschrift der zu identifizierenden Person mittels eines Zahlungsverkehrsterminals (ZVT) gibt der Mitarbeiter im System an, ob er einen Betrugsverdacht (z.B. aufgrund der Beeinflussung der identifizierten Person durch eine weitere Person hat und bestätigt anschließend durch Eingabe seiner individuellen PIN die ordnungsgemäße Durchführung der Identifikation und die Übereinstimmung der Daten.

Nach erfolgter Identifizierung werden dem Auftraggeber die Identifizierungsdaten übermittelt. Die Übermittlung erfolgt digital über das Auskunftsportal und/oder über digitale Datenschnittstellen.

Der POSTIDENT Datensatz mit den erhobenen Daten dient dem Auftraggeber als Nachweis der durchgeführten Identifikation und bestätigt die ihm

vorliegenden Angaben eines Antragstellers bei Übereinstimmung.

Die Datenerhebung beschränkt sich auf die Erhebung wesentlicher Daten, welche die Identifizierung eindeutig dokumentieren (i.d.R. Name, Vorname und Geburtsdatum, Geburtsort der identifizierten Person); hierbei werden zur Festlegung der im POSTIDENT-Prozess erhobenen Daten auch andere einschlägige Anforderungen an Identifizierungsverfahren, wie beispielsweise das Geldwäschegesetz herangezogen, um einen standarisierten Prozess in hoher Qualität zu gewährleisten.

3.2.4 Nicht verifizierte Teilnehmerinformationen

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus.

3.2.5 Bestätigung der Zertifizierungsstellen

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus. Die DPAG übernimmt für die Zertifizierungsstellen die Identifizierung ihrer Antragssteller/Teilnehmer.

3.2.6 Kriterien für die Zusammenarbeit

Grundlage für die Nutzung des POSTIDENT Verfahrens ist eine gültige Vertragsbeziehung des Auftraggebers mit der DPAG. Der POSTIDENT-Vertrag sowie die AGB-POSTIDENT bilden die Grundlage für die Zusammenarbeit zwischen dem Auftraggeber und der DPAG.
Die DPAG hat keine Vertragsbeziehung mit dem Antragssteller. Die Zusammenarbeit des Antragsstellers mit der DPAG ist in der Verfahrensbeschreibung in Kapitel 3.2.3 Authentifizierung der individuellen Identität beschrieben.

3.3 Identifizierung und Authentifizierung für erneute Schlüsselanfragen

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus. Aus diesem Grund gibt es im Verfahren POSTIDENT keine Unterscheidung hinsichtlich der Identifizierung für die Erstausstellung von Zertifikaten und erneuter Schlüsselanfragen.

3.4 Identifizierung und Authentifizierung für Sperranträge

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus. Dementsprechend werden auch keine Sperranträge verarbeitet.

4 Zertifikatslebenszyklus-Betriebsanforderungen

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus. Dementsprechend werden auch keine Anträge auf Zertifikate verarbeitet und es wird kein Service für die Prüfung des Zertifikatsstatus oder deren Echtheit bereitgestellt.

5 Anlagen-, Management- und Betriebskontrollen

Für das POSTIDENT Verfahren wird regelmäßig eine Risikoanalyse durchgeführt. Hierbei werden sowohl technische Systeme und Verfahren sowie manuelle Prozesse betrachtet. Es werden zu identifizierten Risiken, Maßnahmen definiert, welche dem Sicherheitsniveau des Identifizierungsverfahren angemessen sind. Es sind regelmäßige Qualitätskontrollen implementiert, welche durch interne Audits der Konzernrevision ergänzt werden.

5.1 Physikalische Kontrollen

5.1.1 Lage und Konstruktion des Standorts

Filialen sind so angelegt, dass es einen betrieblichen Bereich gibt, den nur Mitarbeiter betreten dürfen, und einen Bereich für die Kunden, die i.d.R. durch einen Schalter getrennt sind. Arbeits- und interne Informationsmaterialien liegen nicht für den allgemeinen Publikumsverkehr aus, sondern sind nur den Filialmitarbeitern zugänglich. Somit ist die allgemeine Sicherung einer Filiale zu betrachten (siehe 5.1.2 Physischer Zugang).

5.1.2 Physischer Zugang

Die Räume (Filialen) sind vor Zutritt Unbefugter zu schützen. Die Beschreibung der Sicherheitsmaßnahmen einer Filiale und von notwendigen Verhaltensweisen des Personals erfolgen in dem für den internen Gebrauch bestimmten Handbuch Security und einer entsprechenden Betriebsanweisung der Filiale. Folgende Sicherheitsmaßnahmen sind diesem zu entnehmen:

- unbekannten Personen ist der Zutritt zu den Diensträumen erst nach Prüfung der Berechtigung zu gewähren;
- eine Schließordnung muss existieren;
- Schlüssel sind in Sicherheitsbehältnissen aufzubewahren;
- alle Mitarbeiter haben ständig auf die Funktionsbereitschaft der Sicherungsmaßnahmen zu achten

Ebenso sind die Hintergrundsysteme entsprechend gegen unbefugten Zugriff geschützt und werden in zutrittsgesicherten Rechenzentren betrieben.

5.1.3 Stromversorgung und Klimaanlage

Nicht zutreffend.

5.1.4 Schutz vor Wasserschäden

Nicht zutreffend.

5.1.5 Brandschutz und -verhütung

Nicht zutreffend.

5.1.6 Medienspeicherung

Die erhobenen Daten werden entsprechend ihrem Schutzbedürfnis gesichert. DPAG stellt sicher, dass nur autorisierte Personen mit der entsprechenden Rolle Zugriff haben.

5.1.7 Entsorgung

Sensible Dokumente und Materialien werden datenschutzkonform vernichtet.

5.1.8 Off-Site-Backup

Nicht zutreffend.

5.2 Verfahrenskontrollen

5.2.1 Vertrauenswürdige Rollen

Folgende Rollen sind definiert, um eine Aufgabentrennung zu gewährleisten, bei der keine Interessenskonflikte bestehen:

- Information Security Officer (ISO): Verantwortlich für Sicherheitspraktiken; auch verantwortlich für Konformitätsbewertungen (Audit). Der ISO wird in Übereinstimmung mit dem Konzernregelwerk zur Informationssicherheit (ISTM) vom Management der Deutsche Post AG ernannt.

- Filialmitarbeiter: Verantwortlich für die Durchführung der Identifizierung in einer Filiale.
- Security-Team: Zentralen Stelle zur Aufarbeitung aller Verdachtsfälle im Bereich Security DPAG.
- Datenschutzbeauftragter: Verantwortlich für die Koordination aller Datenschutzaspekte des Dienstes. Wird im Rahmen des konzernweiten Datenschutzmanagements ernannt.
- Verantwortlicher Manager: Der für den Vertrauensdienst verantwortliche Manager wird von einem Vorstandsmitglied des Unternehmensbereichs „Post & Paket“ oder einem bevollmächtigten Mitarbeiter ernannt.

5.2.2 Anzahl der benötigten Personen pro Aufgabe

Nicht zutreffend.

5.2.3 Identifikation und Authentifizierung für jede Rolle

Zu Beginn wird die Identität aller Mitarbeiter in persönlichen Gesprächen überprüft. Die Identität wird weiter bestätigt durch die Hintergrundprüfverfahren in Abschnitt 5.3.2. Die Zugriffsberechtigung für das notwendige IT-System erfolgt über Chipkarten mit einer persönlichen PIN.

5.2.4 Rollen, die eine Trennung der Aufgaben erfordern

Siehe 5.2.1

5.3 Personalkontrollen

5.3.1 Qualifikationen, Erfahrung und Freigabeanforderungen

Die Mitarbeiter werden zur Durchführung von POSTIDENT im Umgang mit den erforderlichen Anwendungen geschult und verfügen persönlich über Schulungsmaterial (z.B. Mitarbeiterbroschüre), in dem alle Abläufe beschrieben sind. Diese Broschüre dient direkt vor Ort ebenso dazu, Arbeitshandlungen nachzuschlagen. In der Folgezeit werden die jeweiligen Fachkenntnisse durch angemessene Schulungsmaßnahmen auf dem Laufenden gehalten. Bei der Identifizierung in der Filiale wird der Identifizierungsprozess durch ein IT-System gestützt, welches den durchführenden Mitarbeiter Schrittweise durch den Identifizierungsprozess führt und somit eine standardisierte Durchführung gewährleistet.

5.3.2 Zuverlässigkeitsprüfung

Die DPAG als führender Dienstleister stellt durch das Einstellungsverfahren, den hierarchischen Aufbau und Qualitätssicherungsverfahren sicher, dass nur zuverlässige Mitarbeiter zum Einsatz kommen. Hierzu zählt u.a. auch die Vorlage eines polizeilichen Führungszeugnisses gemäß § 30 Bundeszentralregistergesetz. Das Ausmaß, in dem diese Untersuchungen durchgeführt werden, ist durch die anwendbare lokale Gesetzgebung beschränkt. Mitarbeiter dürfen das Postident nicht durchführen, so lange ihre (Einstellungs-)Überprüfung noch nicht abgeschlossen ist.

5.3.3 Schulungsanforderungen

Im Rahmen der Schulung erfolgt die Qualifizierung im POSTIDENT-Prozess, sowie im Umgang mit den erforderlichen Anwendungen. Hier werden die Filialmitarbeiter darauf hingewiesen, dass sie bei allen sicherheitsrelevanten Vorkommnissen (z. B. Bedrohungen, Nötigungen, Beschädigung und Verlust von Materialien) unverzüglich ihren Vorgesetzten informieren müssen, der dann die erforderlichen Schritte veranlasst. Die Unterrichtung wird bei neuen Mitarbeitern durchgeführt und bei erfahrenen Mitarbeitern im Bedarfsfall zielgerichtet wiederholt.

5.3.4 Häufigkeit und Umfang von Nachschulungen

Nachschulungen werden je nach Erfordernis durchgeführt, um das erforderliche Niveau sicherzustellen und die Kompetenz beizubehalten. Darüber hinaus erfolgen Nachschulungen bei signifikanten Änderungen an Systemen oder Prozessen. Mindestens einmal jährlich werden die Mitarbeiter mit Informationen zu wichtigen Aspekten des Identifizierungsprozesses versorgt und damit auf dem aktuellen Stand gehalten.

5.3.5 Jobrotationsfrequenz und Sequenz

Nicht zutreffend.

5.3.6 Sanktionen für unerlaubte Handlungen

Bei unerlaubten Handlungen werden durch das Management angemessene administrative und disziplinarische Maßnahmen ergriffen, die definiert sind und zum Ausschluss der Mitarbeiter vom Verfahren führen können.

5.3.7 Anforderungen an unabhängige Auftragnehmer

DPAG setzt Vertragspartner für die Durchführung von Identifizierungen ein. Diese sind in Postbank Filialen sowie Postfiliale des Einzelhandels eingesetzt.

Vertragspartner sind verpflichtet die vertraglich definierten Anforderungen zu erfüllen, insbesondere die Teilnahme an den vorgenannten Schulungsmaßnahmen und Erfüllung der vorgenannten Qualifikations- und Zuverlässigkeitsanforderungen. Dies gilt auch für beim Vertragspartner angestellte Mitarbeiter.

5.3.8 Dokumentation für das Personal

Schulungsmaterial (Mitarbeiterbroschüre) und alle für die Ausübung der Arbeit erforderlichen Dokumente werden den Mitarbeitern zur Verfügung gestellt.

5.4 Audit-Logging-Verfahren

5.4.1 Arten der protokollierten Ereignisse

In der Filiale durchgeführte Identifikationen werden elektronisch protokolliert.

Hierbei werden folgende Daten im Durchführungsprotokoll erfasst:

- Zeitpunkt der Identifizierung
- Journalsatznummer
- Mitarbeiterkennung der Person welche die Identifizierung durchgeführt hat
- Name, Vorname und Geburtsdatum der identifizierten Person

5.4.2 Häufigkeit der Protokollverarbeitung

Durchführungsprotokolle werden in begründeten Verdachtsfällen zur Klärung von Unregelmäßigkeiten von Identifizierungsergebnissen herangezogen.

5.4.3 Aufbewahrungsfrist für Audit Log

Die Durchführungsprotokolle werden 10 Jahre lang aufbewahrt.

5.4.4 Schutz des Audit Logs

Es sind Sicherungsmaßnahmen zum Schutz der Durchführungsprotokolle vor Veränderung oder Verlust über die gesamte Aufbewahrungsfrist implementiert. Durchführungsprotokolle werden in einem gesicherten Archiv, welches getrennt vom Entstehungssystem ist, aufbewahrt. Der Zugriff auf die Durchführungsprotokolle ist speziell autorisiertem Personal vorbehalten.

5.4.5 Prüfprotokoll-Sicherungsverfahren

Durchführungsprotokolle werden redundant gesichert.

5.4.6 Audit-Sammelsystem (intern oder extern)

Durchführungsprotokolle werden bei der Identifizierung in der Filiale automatisiert erstellt.

5.4.7 Benachrichtigung an das Ereignis verursachende Subjekt

Nicht zutreffend.

5.4.8 Schwachstellenbewertung

Sollten bei der Bewertung von Durchführungsprotokollen Schwachstellen entdeckt werden, initiiert das Security-Team geeignete Maßnahmen zur Behebung.

5.5 Aufzeichnungen Archival

5.5.1 Archivierte Datentypen

- Dieses TSPS
- Vertragsunterlagen
- Durchführungsprotokolle gemäß Abschnitt 5.4

5.5.2 Aufbewahrungsfrist für Archiv

Die Aufbewahrungsfrist beträgt mindestens 10 Jahre.

Identifikationsdaten werden nicht archiviert. Die Archivierung der im Rahmen des POSTIDENT Verfahrens erzeugten Identifikationsdaten obliegt dem Auftraggeber.

5.5.3 Archivschutz

Die archivierten Daten werden entsprechend ihrem Schutzbedürfnis angepasst gesichert. DPAG stellt sicher, dass nur autorisierte Personen mit der entsprechenden Rolle Zugriff haben. Es kommen redundante Systeme zur zuverlässigen Archivierung der Durchführungsprotokolle gemäß Abschnitt 5.4 zum Einsatz.

5.5.4 Archivsicherungsverfahren

Das Archiv wird regelmäßig gesichert.

5.5.5 Anforderungen für das Zeitstempeln von Datensätzen

Nicht zutreffend.

5.5.6 Archiv-Sammelsystem (intern oder extern)

Die Archivsammelsysteme werden im DPAG IT-Verbund betrieben.

5.5.7 Verfahren zum Abrufen und Überprüfen von Archivinformationen

Die Archivzugriffsmöglichkeiten sind so gestaltet, dass ein Zugriff nur für befugtes Personal mit entsprechender Rolle vgl. 5.2.1 Zugriff nehmen kann.

5.6 Schlüsselumschaltung

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus und verwaltet demnach keine Schlüssel.

5.7 Entschädigung und Notfallwiederherstellung

5.7.1 Unfall- und Kompromittierungsverfahren

Nicht zutreffend.

5.7.2 Rechenressourcen, Software und / oder Daten sind beschädigt

Nicht zutreffend.

5.7.3 Verfahren bei der Kompromittierung von privaten Schlüssel

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus.
Die Schlüsselverwaltung obliegt der CA.

5.7.4 Business Continuity-Funktionen nach einer Katastrophe

Durch die dezentrale Filialstruktur kann das Identifizierungsverfahren in der Filiale auch beim Ausfall einzelner Filialen in benachbarten Filialen durchgeführt werden.

5.8 CA- oder RA-Kündigung

Nicht zutreffend. Mit dem Service POSTIDENT wird keine CA oder RA betrieben.

5.8.1 Kündigung des Identifizierungsangebotes POSTIDENT

Mit der Übergabe der POSTIDENT-Daten an den Auftraggeber (relying party) als Nachweis der durchgeführten Identifizierung sind die Verpflichtungen erfüllt und anhand des POSTIDENT-Datensatzes bzw. Ergebnis-PDFs jederzeit für den Auftraggeber nachvollziehbar. Im Falle einer anstehenden Beendigung des Identifizierungsdienstes POSTIDENT werden bestehende Vertragsbeziehungen selbstverständlich ordnungsgemäß zu Ende geführt und die Kündigungen gemäß der vertraglich vereinbarten Fristen rechtszeitig ausgesprochen, so dass der Auftraggeber (relying party) sich darauf einstellen und die Datensätze entsprechend abrufen kann. Nachweise etc. werden entsprechend den gesetzlichen Regelungen sicher aufbewahrt.

6 Technische Sicherheitskontrollen

6.1 Generierung und Installation von Schlüsselpaaren

Nicht zutreffend. Mit dem Service POSTIDENT erzeugt die DPAG keine Schlüssel.

6.2. Schutzmechanismen für private Schlüssel und kryptografische Module

Nicht zutreffend. Mit dem Service POSTIDENT erzeugt und verwaltet die DPAG keine Schlüssel.

6.3 Weitere Aspekte der Verwaltung von Schlüsselpaaren

Nicht zutreffend. Mit dem Service POSTIDENT erzeugt und verwaltet die DPAG keine Schlüssel.

6.4 Aktivierungsdaten

Nicht zutreffend. Mit dem Service POSTIDENT erzeugt und verwaltet die DPAG keine Schlüssel.

6.5 Computersicherheitskontrollen

Alle am Verfahren beteiligten IT-Systems unterliegen dem konzernweit geltenden Information Security Target Model (ISTM), welches durch den Vorstand der DPAG verabschiedet wurde. Es regelt die Aspekte zur Informationssicherheit umfassend. Eine Installation von Software ist nur durch autorisiertes Personal möglich. Eine Softwareinstallation oder sonstige administrative Veränderungen des zur Durchführung von Postident genutzten IT-Systems sind ausgeschlossen.

6.5.1 Spezifische Computersicherheitstechnische Anforderungen

Die zur Bereitstellung des Dienstes genutzten Einrichtungen gewährleisten, dass nur befugte Mitarbeiter und Unterauftragnehmer Zugang zu Bereichen haben, in denen personenbezogene Daten oder andere sensible Informationen verarbeitet werden. Die Zugangsberechtigungen werden unmittelbar angepasst, wenn ein Mitarbeiter seine Stelle wechselt oder das Unternehmen verlässt.

6.6 Lebenszyklus technische Kontrollen

6.6.1 Systementwicklungskontrollen

Die Kontrollanforderungen für die Informationssicherheit - Bestandteil des konzernweit geltenden Information Security Target Model (ISTM) - definieren in Kapitel 14 "Anschaffung, Entwicklung und Instandhaltung von Systemen" die umzusetzenden Systementwicklungskontrollen.

6.6.2 Sicherheitsmanagementkontrollen

Die Kontrollanforderungen der Informationssicherheit, Bestandteil des konzernweit geltenden Information Security Target Model (ISTM), definieren in Kapitel 12 "Betriebssicherheit" die umzusetzenden betrieblichen Sicherheitsmanagementkontrollen. Die Kontrollprozesse im Sinne eines Informationssicherheits-Managementsystems sind in der Richtlinie Prozesse für die Informationssicherheit - Bestandteil des konzernweit geltenden Information Security Target Model (ISTM) - in Kapitel 4 "Informationssicherheits-Managementsystem, Compliance-Assessment und Governance sowie Berichtswesen" definiert. Sicherheitsrelevante Patches werden zeitnah über einen standardisierten Software-Rollout-Prozess von autorisierten Mitarbeitern durchgeführt.

6.6.3 Lebenszyklus-Sicherheitskontrollen

Die Kontrollanforderungen für die Informationssicherheit - Bestandteil des konzernweit geltenden Information Security Target Model (ISTM) - definieren in Kapitel 14.2.2 "Änderungskontrollverfahren" für den gesamten Lebenszyklus von IT-Systemen die umzusetzenden Sicherheitskontrollen.

Informationswerte werden für jedes verarbeitende IT-System klassifiziert und entsprechend einer Risikobewertung geeignete Maßnahmen zur Sicherung dieser etabliert. Dies betrifft im Rahmen von Postident

insbesondere das Kassensystem, an dem die Identifizierung durchgeführt wird.

6.6.4 Netzwerksicherheitskontrollen

Die Kontrollanforderungen für die Informationssicherheit - Bestandteil des konzernweit geltenden Information Security Target Model (ISTM) - definieren in Kapitel 13.1 "Netzwerksicherheitsmanagement" die umzusetzenden Netzwerksicherheitskontrollen. Das Netzwerk wird durch Firewalls in getrennte Zonen partitioniert, so sind insbesondere alle Systeme vor externen Zugriffen geschützt. Ebenso findet eine logische Trennung zwischen Backend- und Frontend-Systemen statt.

6.7 Zeitstempel

Kryptographische-Zeitstempel finden im POSTIDENT Verfahren keine Anwendung.
Bei Zeitstempeln, welche den Durchführungszeitpunkt einer Identifizierung dokumentieren, kommt das NTP Protokoll zur Zeitsynchronisation der Prozessunterstützenden IT-System zum Einsatz.

7 Zertifikat-, CRL- und OCSP-Profile

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate oder CRLs aus und betreibt keine OCSP-Responder.

8 Compliance-Audit und andere Bewertungen

8.1 Häufigkeit und Umstände der Bewertung

Gemäß eIDAS Artikel 20 (1) müssen Compliance-Audits mindestens alle 24 Monate durchgeführt. Zusätzliche Audits sind erforderlich, wenn wesentliche Änderungen an den auditierten Prozessen vorgenommen werden. Darüber hinaus finden Audits durch interne Einheiten statt.

8.2 Identität / Qualifikation des Prüfers

Die von eIDAS geforderte Konformitätsbewertung wird durch eine akkreditierte Konformitätsbewertungsstelle durchgeführt.

8.3 Das Verhältnis des Prüfers zur bewerteten Entität

Die Konformitätsbewertung wird stets durch eine von der DPAG unabhängigen Konformitätsbewertungsstelle durchgeführt.

8.4 Von der Bewertung erfasste Themen

Der Zweck des Audits besteht darin, zu überprüfen, ob die von DPAG im Rahmen POSTIDENT eingesetzten Komponenten den Anforderungen dieses TSPS entsprechen.

Dieses Audit ist beschränkt auf das Verfahren "POSTIDENT durch Postfiliale (Basic)" für die Identifizierung einer natürlichen Person. Das Ergebnis der Identifizierung bei POSTIDENT durch Postfiliale (Basic) ist der POSTIDENT-Datensatz bzw. das Ergebnis-PDF. Im Datensatz bzw. auf dem Ergebnis-PDF sind die Daten der zu identifizierenden Person sowie deren Unterschrift vorhanden. Darüber hinaus sind durch weitere Angaben zur entsprechenden Filiale alle entsprechenden Informationen vorhanden, um die Identifizierung nachvollziehbar machen zu können.

8.5 Maßnahmen auf Grund festgestellter Mängel

Sollten Mängel durch den TSP festgestellt werden, können diese durch ihn an die Serviceeinheit Postident gemeldet werden. Hier findet eine Bewertung statt, sowie eine Abstimmung mit dem TSP über ggf. durch diesen durchzuführende Maßnahmen. Festgestellte Mängel werden der verantwortlichen Abteilung für die Filialen gemeldet und diese wird aufgefordert, entsprechende Informationen herauszugeben und in Schulungen auf die Vorkommnisse hinzuweisen. Abhängig von den festgestellten Mängeln wird zwischen den Verantwortlichen festgelegt, ob und welche prozessualen oder technischen Anpassungen erforderlich sind. Sollten seitens der DPAG im Rahmen der Identifizierung Unregelmäßigkeiten (Betrugsverdacht/Sicherheitsmängel) festgestellt werden, wird sie den TSP hierüber informieren, so dass dieser seinerseits Maßnahmen einleiten kann.

8.6 Übermittlung der Ergebnisse

DPAG wird die Ergebnisse mit den relevanten Organisationseinheiten teilen und insbesondere festgestellte Mängel durch geeignete Maßnahmen adressieren.

9 Weitere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

Die Durchführung einer Identifizierung mittels POSTIDENT ist für die zu identifizierende Person kostenfrei, da der Vertrag der DPAG mit dem Auftraggeber geschlossen wird.

Der Auftraggeber hat für das jeweilige Identifizierungsverfahren die in der aktuellen Preisliste POSTIDENT für die einzelnen Produkte ausgewiesenen Entgelte zu entrichten.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungsschutz

Die DPAG unterhält eine Betriebshaftpflichtversicherung.

9.2.2 Sonstige Vermögenswerte

DPAG gewährleistet, dass für den Betrieb und für Verpflichtungen, die sich aus der Erbringung des eIDAS-konformen Komponenten-Dienstes POSTIDENT ergeben, Finanzmittel in ausreichender Höhe vorhanden sind.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang der vertraulichen Informationen

Alle im Rahmen einer Identifizierung erhoben Daten werden geheim gehalten und Dritten nicht offenbart.

Die Übermittlung des Identifizierungsergebnisses erfolgt elektronisch über eine gesicherte Schnittstelle oder durch Abruf über ein gesichertes Portal.

9.3.2 Informationen, die nicht zu vertraulichen Informationen gehören

Grundsätzliche Produktinformationen, AGB, etc. welche ohne einen gesonderten Zugriffsschutz auf http://www.postident.de/handbuch/ veröffentlicht sind gelten nicht als vertrauliche Informationen.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Alle von der DPAG zur Erbringung der Identifizierungsdienstleistung eingesetzten Personen sind verantwortlich für den Schutz vertraulicher Informationen gemäß dieses TSPS, vertraglicher Regelungen, dem Bundesdatenschutzgesetz und nach der EU DSGVO.

9.4 Datenschutz persönlicher Daten

9.4.1 Datenschutzplan

Alle Informationen, die die Identifizierung von Kunden betreffen, sind vor unbefugtem Zugriff geschützt.

9.4.2 Informationen, die als privat behandelt werden

Die deutschen und europäischen Datenschutzgesetze definieren, welche Informationen als privat zu behandeln sind.

9.4.3 Informationen, die nicht als privat gelten

Alle die Identifizierung betreffenden Informationen sind als privat zu behandeln.

9.4.4 Verantwortung zum Schutz privater Informationen

Die Deutsche Post unterliegt den einschlägigen gesetzlichen Bestimmungen. Sämtliche Mitarbeiter und Erfüllungsgehilfen sind auf das Datengeheimnis gemäß § 5 BDSG und der EU DSGVO verpflichtet.

9.4.5 Hinweis und Zustimmung zur Verwendung privater Informationen

Die Vertragsparteien werden alle Informationen, die sie und/ oder von ihnen zur Vertragserfüllung herangezogene Dritte im Rahmen der

vertragsgegenständlichen Zusammenarbeit voneinander direkt oder indirekt erhalten, auch nach Beendigung des Vertragsverhältnisses geheim halten und Dritten nicht offenbaren.

9.4.6 Offenlegung nach Gerichts- oder Verwaltungsverfahren

Von den unter 9.4.5 genannten Bedingungen unberührt sind gesetzliche oder durch Behörden oder Gerichte rechtmäßig verfügte Offenbarungspflichten; in entsprechenden Fällen wird der Vertragspartner informiert und das Vorgehen insoweit mit ihm abgestimmt.

9.4.7 Sonstige Angaben zu Offenlegungsbedingungen

Die DPAG wird Informationen nicht für andere Zwecke als zur Abwicklung dieses Vertrages verwenden.

9.5 Rechte an geistigem Eigentum

Nicht zutreffend.

9.6 Zusicherungen und Gewährleistungen

9.6.1 CA-Zusicherungen und Gewährleistungen

Nicht zutreffend.

9.6.2 RA-Erklärungen und Garantien

Nicht zutreffend.

9.6.3 Zusicherungen und Garantien des Antragssteller

Nicht zutreffend.

9.6.4 Relying Party Vertretungen und Garantien

Nicht zutreffend.

9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Nicht zutreffend.

9.7 Gewährleistungsausschluss

Gewährleistungsausschlüsse richten sich nach den vertraglichen Vereinbarungen zwischen der DPAG und dem Auftraggeber.

9.8 Haftungsbeschränkungen

Haftungsbeschränkungen unterliegen den vertraglichen Vereinbarungen zwischen DPAG und dem Auftraggeber. DPAG ist Gesamtverantwortlicher für die korrekte Durchführung der Identifizierung, auch wenn Teilleistungen durch Unterauftragnehmer erfüllt werden.

9.9 Schadenersatz

9.9.1 Entschädigung

Entschädigungsansprüche richten sich nach den vertraglichen Vereinbarungen zwischen DPAG und dem Auftraggeber.

9.10 Laufzeit und Kündigung

9.10.1 Laufzeit

Das TSPS tritt mit Veröffentlichung auf der Website von DPAG in Kraft. Änderungen zu diesem TSPS werden bei Veröffentlichung wirksam.

9.10.2 Beendigung

Dieses TSPS bleibt in Kraft, bis es durch ein neues ersetzt wird.

9.10.3 Auswirkung der Beendigung

Auch in dem Falle, dass dieses TSPS möglicherweise nicht mehr in Kraft sein sollte, bestehen folgende Verpflichtungen und Beschränkungen dieses TSPS fort: Abschnitt 9.6 (Zusicherungen und Gewährleistungen), Abschnitt 9.2 (Finanzielle Verantwortung) und Abschnitt 9.3 (Vertraulichkeit von Geschäftsinformationen).

9.11 Individuelle Mitteilungen und Mitteilungen an die Teilnehmer

Nicht zutreffend.

9.12 Änderungen

9.12.1 Verfahren für den Änderungsantrag

Nicht zutreffend.

9.12.2 Benachrichtigungsmechanismus und -zeitraum

Verfahrensrelevante Änderungen, welche Einfluss auf das Gesamtergebnis der Identifizierungsleistung haben, werden allen Vertragspartnern basierend auf den individuell vereinbarten Kanälen fristgerecht mitgeteilt.

9.12.3 Umstände, unter denen OID geändert werden muss

Nicht zutreffend. Mit dem Service POSTIDENT stellt die DPAG keine Zertifikate aus.

9.13 Streitbeilegungsbestimmungen

DPAG bietet nur Identitätsüberprüfungsdienste an, um die Registrierungsstellen der Zertifizierungsstellen, die die Zertifikate ausstellen zu unterstützen. DPAG hat keine vertragliche Vereinbarungen mit Endnutzern oder relying parties. Bei Streitigkeiten mit Endnutzern und relying parties gelten die Streitbeilegungsverfahren der ausstellenden CAs. Im Rahmen des festgelegten standardisierten Identifikationsverfahren POSTIDENT werden alle Personen gleich behandelt. Für alle nicht über das Verfahren abgedeckten Fälle ist der Auftraggeber vertraglich dazu verpflichtet, eine alternative Identifizierungsmöglichkeit anzubieten. Beschwerden über die Dienste von DPAG können eingereicht werden bei postident@deutschepost.de .

9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland.

9.15 Einhaltung des anwendbaren Rechts

Dieses TSPS unterliegt nationalem Recht sowie der eIDAS Verordnung.

9.16 Verschiedene Bestimmungen

9.16.1 Vollständige Vereinbarung

Nicht zutreffend.

9.16.2 Zuordnung

Nicht zutreffend.

9.16.3 Salvatorische Klausel

Wenn Teile einer der Bestimmungen in diesem TSPS falsch oder ungültig sind, berührt dies nicht die Gültigkeit der verbleibenden Bestimmungen bis zur Aktualisierung des TSPS. Der Prozess zur Aktualisierung ist in Abschnitt 9.12 beschrieben.

9.16.4 Vollstreckung (Anwaltskosten und Verzicht auf Rechte)

Nicht zutreffend.

9.16.5 Höhere Gewalt

Die DPAG haftet nicht für die Verzögerungen oder Fehler in der diesem TSPS unterliegenden Leistung, die von Ereignissen außerhalb ihrer Kontrolle, wie z.B. Streiks, Kriegshandlungen, Aufstände, Epidemien, Stromausfälle, Feuer, Erdbeben und andere Katastrophen, ausgelöst werden.

9.17 Sonstige Bestimmungen

Nicht zutreffend.