TSPS - Trust Service Practice Statement

POSTIDENT

version 1.1 – 29.03.2019

Version	Date	Description	Release
1.0	30.08.2018	First edition	S. Ferrari, 10.09.2018
1.1	29.03.2019	Review as part of the monitoring audit without changes in content	S. Ferrari, 01.04.2019

Inhalt

1. Introduction

1.1 Overview

POSTIDENT comprises various identity-proofing services offered by Deutsche Post AG to verify the identity of natural persons. POSTIDENT is a service component provided pursuant to Regulation (EU) No. 910/2014 (eIDAS) of the European Parliament.

This document only applies for verification of the identity of natural persons as an identity-proofing component offered by Deutsche Post AG in compliance with the eIDAS Regulation. Another component is the personal delivery of signature cards.

1.2 Document Name and Identification

This document is called “TSPS - Trust Service Practice Statement POSTIDENT”

This document is a Trust Service Practice Statement (TSPS) pursuant to ETSI EN 319 401[1].

1.3 PKI Participants

1.3.1 PKI Participants

A certificate authority (CA) is an organization that issues digital certificates. A certificate authority has mechanisms for the publication, distribution and revocation of certificates.

DPAG does not maintain a certificate authority (CA) in the context of POSTIDENT. POSTIDENT is an identity-proofing service available to certificate authorities to verify the identity of subscribers before issuing certificates.

1.3.2 Registration Authorities

A registration authority, as the authority upstream of the certificate authority, can assume responsibility for checking business data and personal data for subscriber data to be included in certificates.

This includes, in particular, operations such as submitting certificate applications to the certificate authority, confirming applications for the renewal of certificates, and the revocation of certificates.

DPAG does not operate a registration authority through its POSTIDENT process.

POSTIDENT is a service to verify the identity of natural persons, which can be used by certificate authorities or trust service providers as an identity-proofing component in the process for issuing certificates.

1.3.3 Subscribers

Subscribers are users of a trust service who are issued e.g. certificates by a certificate authority. When using POSTIDENT as an identity-proofing component, the subscriber is always a natural person.

DPAG verifies the identity of subscribers on behalf of its contractual partners, for example, certificate authorities.

1.3.4 Relying Parties

A relying party is a natural or legal person that relies on the correct identity of a contractual partner, e.g. the holder of a certificate, in a business transaction.

In the context of certification services, personal certificates issued on the basis of verification of identity via the POSTIDENT process are used to ensure the integrity of digitally signed documents and their clear allocation to the signatory.

1.4 Certificate Usage

Not applicable. POSTIDENT is an identity-proofing service for natural persons. It does not issue certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Deutsche Post AG
Produktmanagement Identitätsmanagement
Charles-de-Gaulle-Str. 20
53113 Bonn
Germany

www.postident.de

1.5.2 Contact Person

Information Security OfficerDeutsche Post AG
Identitätsmanagement
Charles-de-Gaulle-Str. 20
53113 Bonn
Germany

postident@deutschepost.de

www.postident.de

1.5.3 Person Determining CPS Suitability for the Policy

The suitability of this Practice Statement is assessed by the Information Security Officer for the business department.

1.5.4 TSPS Approval Procedures

The present TSPS has been approved by the management of the "Product Management Identity Management" department. The management of the Product Management Identity Management department is responsible for implementing the guidelines.

This document is approved by a written comment/signed email from the manager responsible for the trust service.

The TSPS is regularly reviewed and updated. New versions have to be approved by the management.

1.6 Definitions and Acronyms

1.6.1 Definitions

Terms requiring clarification are explained when they are first used in the document.

1.6.2 Acronyms

Abbreviation	Meaning
CA	Certificate Authority
CRL	Certificate Revocation List
CSP	Certification Service Provider
DPAG	Deutsche Post AG
eIDAS	Regulation (EU) No. 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ETSI	European Telecommunications Standards Institute
OCSP	Online Certificate Status Protocol
RA	Registration Authority
TSP	Trust Service Provider

1.6.3 References

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

2 Publication and Repository Responsibilities

2.1 Repositories

DPAG publishes this TSPS and other documents of relevance to the process such as General Terms and Conditions and descriptions of interfaces on http://www.postident.de/handbuch.

2.2 Publication of Certificate Information

DPAG's POSTIDENT service does not issue certificates. DPAG will notify users of POSTIDENT as an identity-proofing module within the context of eIDAS in advance of any significant changes to the format of the documentation used by the service.

2.3 Time or Frequency of Publication

Subsequent version of the TSPS will also be published on the DPAG website after approval. Significant process-related changes will be announced before the change is made.

2.4 Access Controls on Repositories

The published documents are freely accessible via the internet. Access is read only.

Write access is for administrators only. To ensure this, technical security measures have been implemented to prevent unauthorized modification of the content.

3 Identification and Authentication

3.1 Naming

Not applicable. DPAG's POSTIDENT service does not issue certificates.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Not applicable. DPAG's POSTIDENT service does not issue certificates.

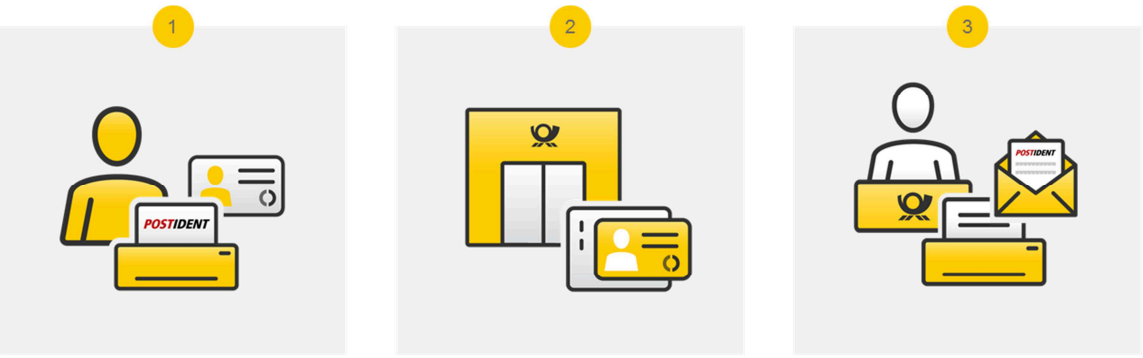
3.2.2 Authentication of Organization Entity

Not applicable. POSTIDENT only verifies the identity of natural persons, not of legal persons or other organizational forms.

3.2.3 Authentication of Individual Identity

Verification of the identity of natural persons in a post office - POSTIDENT durch Postfiliale

The "POSTIDENT durch Postfiliale" process comprises verifying the identity of a natural person in a post office on the basis of a valid official identity document. The identity of all natural persons in possession of a valid identity document authorized for the process can be verified. Authorized identity documents are valid German identity cards (*Personalausweise*), official foreign identity cards that are equivalent to a German identity card, and passports, provided that the documents contain a photograph of the holder and are accepted by Deutsche Post as identification.



Preparation

- The following **Documents** are **required** for an identification in your Post-Office:
  - **POSTIDENT Coupon** (in Paper or APP on your mobile device)
  - **A valid official Identification Document**

Identification

- **Automated** data processing ensures a speedy identification in the Post-Office
  - **Security-Checks** are performed by a **Document-Reader**
  - **Data** relevant for the identification process is **extracted from** the presented **ID-Document** and presented to the clerk for further approval

Data Verification and submission of the Result

- The clerk performs a **visual inspection on data** and compares it to the presented document
- To document the performed identification all Data is **printed** on a POSTIDENT Form
- The **signatures of the clerk and the person being identified** finalize the Form
- The Form is **mailed to the relying party**

In the post office, the person whose identity is to be verified presents the counter clerk with a coupon received from the relying party; this contains the relying party's data.

The clerk requests one of the above identity documents, verifies the identity of the person by comparison with the photograph and transfers the personal data to the POSTIDENT form available in the post office using an identity card reader and a Deutsche Post IT system. The card reader checks key security attributes in the identity document. The relying party is informed of the outcome of this automatic check.

When the person to be identified has signed the form, it is countersigned by the counter clerk to confirm that the identity-proofing process has been performed correctly and the data are correct.

The POSTIDENT form with the personal data of the person whose identity is to be verified is then sent to the relying party in a sealed envelope.

The POSTIDENT form with the data and security attributes collected provides the relying party with evidence that identity-proofing process has been performed and confirms the subscriber's data providing that they match.

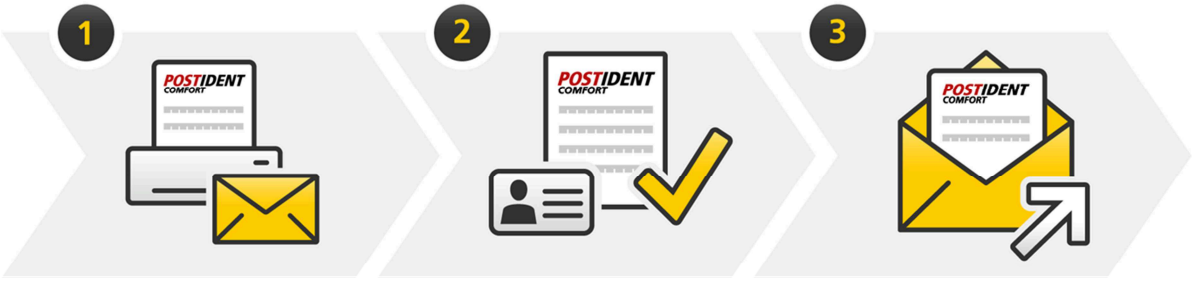
Data collection is limited to key data that document the person's identity (e.g. last name, first name and date of birth); the data collected on the POSTIDENT form are determined by the requirements for other identity-proofing processes such as money laundering legislation to ensure a standardized, high-quality process.

Delivery of identity-proofing documents after verification of the identity of a natural person by the mail carrier - POSTIDENT durch Postboten Individuell

The "POSTIDENT durch Postboten Individuell" service enables agents of Deutsche Post AG to verify the identity of natural persons on the basis of an authorized identity document when delivering letters.

On the one-page "POSTIDENT durch Postboten Individuell" form, the number of the identity document, date of birth, type of identity document and signature of the customer are entered beneath the part of the form defined by the relying party. When using this service, a sealed letter with identity-proofing documents prepared by the relying party can be attached to the POSTIDENT documents and delivered to the recipient after verification of his/her identity. Delivery is documented by the mail carrier on the form and countersigned by the recipient.

If the recipient is not present to accept delivery, he/she is notified that the item can be collected from the post office. Verification of identity is then performed by the counter staff in the post office.



Preparation and Mailing

- Print the filled in POSTIDENT Form; A customized text can be added to the Form
- Inform the customer about the Identification procedure
- Submit the Form and optionally the customer letter to Deutsche Post with "Einlieferungsliste" in a POSTIDENT envelope

Identification of the customer

- A Deutsche Post mail carrier performs the identification
- Hands the customer letter to the identified person after documenting the details of the presented ID-Document on the form
- Reciept of the customer letter is documented by the customer signature on the form under the customized text
- In case the mail carrier does not meet the customer, the customer may perform the process at his post office

Submission of the Result to the customer

- The POSTIDENT form containing the verification details and customer signature are sent to the relying party

3.2.4 Non-verified Subscriber

Not applicable. DPAG's POSTIDENT service does not issue certificates.

3.2.5 Validation of Authority

Not applicable. DPAG's POSTIDENT service does not issue certificates. DPAG verifies the identity of subscribers on behalf of certificate authorities.

3.2.6 Criteria for Interoperation

The basis for the use of the POSTIDENT process is a valid contractual relationship between the relying party and DPAG. The POSTIDENT contract and General Terms and Conditions for POSTIDENT form the basis for interoperation between the relying party and DPAG. DPAG does not have a contractual relationship with the subscriber. Interoperation between the subscriber and DPAG is set out in the process description in Chapter 3.2.3 Authentication of Individual Identity.

3.3 Identification and Authentication for Re-key Requests

Not applicable. DPAG's POSTIDENT service does not issue certificates. For this reason, the POSTIDENT process does not distinguish between identity-proofing for the initial issue of certificates and renewed requests for keys.

3.4 Identification and Authentication for Revocation Requests

Not applicable. DPAG's POSTIDENT service does not issue certificates. Therefore it does not process revocation requests.

4 Certificate Life-Cycle Operational Requirements

Not applicable. DPAG's POSTIDENT service does not issue certificates. Therefore, no applications for certificates are processed and there is no service to check the status or authenticity of the certificate.

5 Facility, Management, and Operational Controls

A risk analysis is performed regularly for the POSTIDENT process. This covers manual processes as well as technical systems and processes. The measures defined for the identified risks are appropriate for the security level of the identity-proofing process. Regular quality controls are performed; these are supplemented by internal audits by Corporate Auditing.

5.1 Physical Controls

5.1.1 Site Location and Construction

Post offices are designed with an area that only staff can enter and an area for customers, normally separated by a counter. The necessary working materials (forms) are not displayed for the general public; they are only accessible to branch staff. Therefore, the general security of the post office has to be taken into account (see 5.1.2 Physical Access).

Delivery offices are not open to the general public.

5.1.2 Physical Access

Facilities (post offices and delivery offices) must be protected from unauthorized access. A description of the security measures for post offices and delivery offices and the necessary staff conduct can be found in the internal security manual and a corresponding operating procedure at the branch. They set out the following security measures:

- Unknown persons may only be given access to business premises after checking their authorization
- There must be a lock-up procedure
- Keys must be kept in security containers
- All employees must ensure that the security measures are operational at all times

Similarly, background systems are protected against unauthorized access and are run from computer centers with access control.

5.1.3 Power and Air Conditioning

Not applicable.

5.1.4 Water Exposure

Not applicable.

5.1.5 Fire Prevention and Protection

Not applicable.

5.1.6 Media Storage

The POSTIDENT forms used have physical security attributes. They must always be stored in a safe place and only used for the identity-proofing process in accordance with the process description. In particular, after documentation of the identity-proofing process, the data collected are sent to the relying party in a sealed envelope and are therefore subject to postal secrecy.

5.1.7 Waste Disposal

Sensitive documents and materials are destroyed in conformance with data protection requirements.

5.1.8 Off-site backup

Not applicable.

5.2 Procedural Controls

5.2.1 Trusted Roles

The following roles have been defined to ensure that there are no conflicts of interest:

- Information Security Officer (ISO): Responsible for security practices; also responsible for conformity assessments (audits). The ISO is appointed by the management of Deutsche Post AG in accordance with the Group-wide Information Security Target Model (ISTM).
- Counter clerk: Responsible for identity-proofing in a post office.
- Mail carrier: Responsible for identity-proofing of recipients “at the front door” and for delivering the identity-proofing documents.
- Security team: Central team that deals with all suspected security breaches at DPAG.
- Data Protection Officer: Responsible for coordinating all data protection aspects of the service. Appointed in the context of Group-wide data protection management.
- Responsible manager: The manager responsible for the trust service is appointed by a member of the executive board of the Post - eCommerce - Parcel division or an authorized employee.

5.2.2 Number of Persons Required per Task

Not applicable.

5.2.3 Identification and Authentication for Each Role

The identity of all employees is checked at the start through personal discussions. Identity is then confirmed using the background check procedure outlined in section 5.3.2. Access authorization to the necessary IT system is via chip cards with a personal PIN.

5.2.4 Roles Requiring Separation of Duties

See 5.2.1

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Staff are trained to perform the POSTIDENT service and in use of the necessary applications; they receive personal training materials (e.g. an employee brochure) in which all workflows are described. This brochure can be used as reference manual for workflows. Knowledge is subsequently updated through appropriate training. Identity-proofing in post offices is supported by an IT system that guides staff step-by-step through the process and therefore ensures that all steps of the process are performed in a standardized manner.

5.3.2 Background Check Procedures

Through its recruitment process, hierarchical structure and quality assurance process, DPAG as the leading service-provider, ensures that only reliable staff are used. This includes, in particular, submission of a police clearance certificate in accordance with Section 30 of the Federal Central Criminal Records Act. The scope to perform background checks is limited by the applicable local legislation. Employees may not conduct the Postident process until their (onboarding) checks have been completed.

5.3.3 Training Requirements

During training, staff are instructed in how to perform the POSTIDENT process and in the use of the necessary applications. In this context, branch staff are instructed to inform their supervisor immediately of all relevant events (e.g. threats, coercion, damage and loss of materials) so that he or she can initiate the necessary steps. Instruction is given to new employees and repeated as necessary for experienced staff.

5.3.4 Retraining Frequency and Requirements

Further training is provided as required to maintain the necessary skills and standards. In addition, further training is provided if there are significant changes to systems or processes. At least once every year current information on important aspects of the identification process is provided to the clerks performing POSTIDENT.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

In the event of unauthorized actions, the management will take appropriate, defined administrative and disciplinary measures, which may result in the employee being excluded from the process.

5.3.7 Independent Contractor Requirements

DPAG uses contractors to verify identity. They are used in Postbank branches and post office branches in retail stores.

These contractual partners have a contractually defined obligation to meet defined requirements, especially taking part in the training outlined above and meeting the above qualification and reliability requirements. This also applies for staff employed by contractors.

5.3.8 Documentation Supplied to Personnel

Staff receive training materials (employee brochure) and all documents required to perform their work.

5.4 Audit Logging Procedures

5.4.1 Types of Events Logged

Identity-proofing in post offices is logged electronically.

The following data are logged:

- Time of verification of identity
- Log serial no.
- Employee ID of the person who performed the identity verification process
- Last name, first name and date of birth of the person verified

5.4.2 Frequency of Processing Log

Logs are used in the event of justified suspicions in order to clarify irregularities in the outcome of the identity-proofing process.

5.4.3 Retention Period for Audit Log

The logs are kept for 10 years.

5.4.4 Protection of Audit Log

Security measures are implemented throughout the retention period to prevent alteration or loss of audit logs. They are stored in a secure archive that is separate from the system used to generate them. Only specially authorized personnel have access to the audit logs.

5.4.5 Audit Log Backup Procedures

Redundant back-up is used for audit logs.

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are generated automatically when identity is verified in a post office.

5.4.7 Notification to Event-Causing Subject

Not applicable.

5.4.8 Vulnerability Assessments

If the assessment of the audit logs identifies vulnerabilities, the Security Team shall initiate suitable steps to eliminate them.

5.5 Records Archival

5.5.1 Types of Records Archived

- This TSPS
- Contractual documents
- Audit log as described in section 5.4

5.5.2 Retention Period for Archive

The retention period is at least 10 years.

The identity verification data are not archived. The relying party is responsible for archiving the data generated during the POSTIDENT process.

5.5.3 Protection of Archive

The archived data are secured on the basis of the protection required. DPAG ensures that only authorized personnel with the relevant roles have access. Redundant systems are used for reliable archiving of audit logs in accordance with section 5.4.

5.5.4 Archive Backup Procedures

The archive is backed up regularly.

5.5.5 Requirements for Time-Stamping of Records

Not applicable.

5.5.6 Archive Collection System (Internal or External)

The archive collection systems are operated within the DPAG IT network.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to archives is structured to ensure that archives can only be accessed by authorized personnel with the corresponding role as defined in 5.2.1.

5.6 Key Changeover

Not applicable. DPAG's POSTIDENT service does not issue certificates, nor does it manage keys.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Not applicable.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

Not applicable.

5.7.3 Entity Private Key Compromise Procedures

Not applicable. DPAG's POSTIDENT service does not issue certificates.
The CA is responsible for key management.

5.7.4 Business Continuity Capabilities after a Disaster

Thanks to the decentralized branch structure, identity-proofing can be performed in neighboring post offices if individual branches are unavailable.

5.8 CA or RA Termination

Not applicable. The POSTIDENT service does not operate a CA or an RA.

5.8.1 Termination of Identity Proofing Service

The contractual obligation is fulfilled when the POSTIDENT form is delivered to the relying party as evidence that the identity-proofing process has been performed, and this can be traced by the relying party at all times via the POSTIDENT form. Consequently, there are no further precautions for termination of the service. In the event of upcoming termination of the POSTIDENT identity-proofing service, existing contractual relationships will naturally be completed correctly and timely notice of termination will be served, observing the contractual notice periods, so that the relying party can adjust. Evidence, etc. is archived securely in compliance with the statutory requirements.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Not applicable. DPAG's POSTIDENT service does not generate keys.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Not applicable. DPAG's POSTIDENT service does not generate or manage keys.

6.3 Other Aspects of Key Pair Management

Not applicable. DPAG's POSTIDENT service does not generate or manage keys.

6.4 Activation Data

Not applicable. DPAG's POSTIDENT service does not generate or manage keys.

6.5 Computer Security Controls

All IT systems involved in the process are subject to the Group-wide Information Security Target Model (ISTM) adopted by the Board of Management of DPAG. This contains extensive rules on information security. Software can only be installed by authorized personnel. Software installation or other administrative changes to the IT system used to perform the Postident process are not possible.

6.5.1 Specific Computer Security Technical Requirements

The equipment used to provide this service ensures that only authorized personnel and subcontractors have access to areas where personal data and other sensitive information are processed. Access authorization is altered immediately if an employee transfers to a different position or leaves the company.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Information Security Control Standards, which are part of the Group-wide Information Security Target Model (ISTM), determine the system development controls to be implemented as defined in Chapter 14 "System Acquisition, Development and Maintenance".

6.6.2 Security Management Controls

The Information Security Control Standards, which are part of the Group-wide Information Security Target Model (ISTM), determine the internal security management controls to be implemented as defined in Chapter 12 “Operations Security”. The control processes within the meaning of the information security management system are defined in the Information Security Process Standards – which are part of the Group-wide Information Security Target Model (ISTM) – see Chapter 4 “Information Security Management System, Compliance Assessment and Governance, and Reporting”. Security-related patches are installed promptly by authorized employees via a standardized software rollout process.

6.6.3 Life Cycle Security Controls

The Information Security Control Standards – which are part of the Group-wide Information Security Target Model (ISTM) – determine the security controls to be implemented for the entire life cycle of IT systems as defined in Chapter 14.2.2 “System Change Control Procedures”.

Information values are classified for every processing IT system and suitable security measures are implemented on the basis of a risk evaluation. In the Postident process, this applies in particular to the IT system used in the identity-proofing process.

6.6.4 Network security controls

The control requirements for information security – which is part of the Group-wide Information Security Target Model (ISTM) – determine the network security controls to be implemented as defined in Chapter 13.1 “Network Security Management”. The network is partitioned into separate zones by firewalls so that all systems are protected from external access. There is also logic separation of backend and frontend systems.

6.7 Time-Stamping

Cryptographic time-stamping is not used in the POSTIDENT process.
For time stamps that document when the identity-proofing process was performed, the NTP log for the time synchronization of the process-support IT systems is used. The counter clerk signs the POSTIDENT form to confirm that the data are correct.

7 Certificate, CRL, and OCSP Profiles

Not applicable. DPAG's POSTIDENT process does not issue certificates or CRLs, nor does it operate OCSP responders.

8 Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

In accordance with Article 20(1) eIDAS, so-called conformity assessments have to be performed at least every 24 months. Additional assessments are required if significant changes are made to the audited processes. In addition, audits are performed by internal units.

8.2 Identity/Qualifications of Assessor

The conformity assessment required by eIDAS is performed by an accredited conformity assessment body.

8.3 Assessor's Relationship to Assessed Entity

The conformity assessment is always performed by a conformity assessment body that is independent of DPAG.

8.4 Topics Covered by Assessment

The purpose of the assessment is to check whether the components used by DPAG in the context of POSTIDENT meet the requirements of this TSPS.

This audit is confined to the following two processes: “POSTIDENT durch Postfiliale (Basic)” for identity-proofing of a natural person, and “POSTIDENT durch Postboten Individuell (Special)” for the delivery of a sealed letter provided by the relying party with the identity-proofing documents. The outcome of identity proofing using the “POSTIDENT durch Postfiliale (Basic)” process is the POSTIDENT form. This contains the data on the person whose identity has been verified and his/her signature. In addition, since the form contains further details of the post office and the employee’s signature, all necessary information is available to track the identity-proofing process.

8.5 Actions Taken as a Result of Deficiency

Should any deficiencies be identified by the TSP, these can be notified to the Postident back office. An evaluation will be performed and the TSP will be consulted on any action to be taken. If deficiencies are established, they are reported to the department responsible for the post offices or for delivery, with a request to provide the relevant information and to draw attention to the problems during training. Depending on the deficiencies established, those responsible will decide whether technical or process adjustments are necessary.

If DPAG establishes irregularities in the course of the identity-proofing process (suspected fraud/security breaches), this will be notified to the TSP so that action can be taken by the TSP.

8.6 Communications of Results

DPAG will communicate the outcome to the relevant organizational units and, in particular, take suitable action to address the deficiencies identified.

9 Other Business and Legal Matters

9.1 Fees

Identity-proofing via the POSTIDENT process is free of charge to the person whose identity is verified because the contract with DAPG is concluded by the relying party.

The relying party must pay the fees set out in the valid POSTIDENT price list for the identity-proofing service, plus any postal charges.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DPAG has business liability insurance.

9.2.2 Other Assets

DPAG guarantees that sufficient funding is available for the operations and obligations arising from the performance of the eIDAS-compliant components of the POSTIDENT service.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All data collected in connection with the identity-proofing process must be kept confidential and may not be disclosed to third parties.

The outcome of the identity-proofing process is communicated by letter post on the POSTIDENT form in a sealed envelope.

9.3.2 Information Not Within the Scope of Confidential Information

Basic product information, General Terms and Conditions, etc. that are published without special protected access on http://postident.de/handbuch/ do not constitute confidential information.

9.3.3 Responsibility to Protect Confidential Information

All persons used by DPAG to provide the identity-proofing service are responsible for protecting confidential information in accordance with this TSPS, contractual provisions, the Federal Data Protection Act and the EU General Data Protection Regulation.

9.4 Privacy of personal information

9.4.1 Privacy Plan

All information relating to identity-proofing of customers is protected from unauthorized access.

9.4.2 Information Treated as Private

The German and European data protection laws define which information is to be treated as private.

9.4.3 Information not Deemed Private

All information relating to identity-proofing must be treated as private.

9.4.4 Responsibility to Protect Private Information

Deutsche Post is subject to the applicable legal provisions. All staff and agents are obligated to respect data privacy pursuant to Section 5 BDSG and the EU GDPR.

9.4.5 Notice and Consent to Use Private Information

The contractual parties shall respect the privacy of all information that they and/or third parties used by them to perform the contract obtain directly or indirectly from each other in the course of their contractual collaboration, even after the end of the contractual relationship, and shall not disclose it to third parties.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The conditions set forth in 9.4.5 shall not apply to statutory disclosure obligations or disclosure obligations imposed lawfully by authorities or courts of law; in such cases the contractual partner will be informed and the procedure will be agreed.

9.4.7 Other Information Disclosure Circumstances

DPAG will refrain from using the information and data for purposes other than the performance of this contract.

9.5 Intellectual Property Rights

Not applicable.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Not applicable.

9.6.2 RA Representations and Warranties

Not applicable.

9.6.3 Subscriber Representations and Warranties

Not applicable.

9.6.4 Relying Party Representations and Warranties

Not applicable.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of Warranties

Disclaimers of warranties are governed by the contractual agreements between DPAG and the relying party.

If the customer receives an incorrect or incomplete Postident form, it can be sent to the POSTIDENT back office. The relevant POSTIDENT process will then be remedied or repeated.

9.8 Limitations of Liability

Limitations of liability are subject to the contractual agreements between DPAG and the relying party. DPAG carries the overall responsibility that the identification process conforms to this policy, even if individual parts are executed by subcontractors.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

Claims for damages are based on the contractual agreements between DPAG and the relying party.

9.10 Term and Termination

9.10.1 Term

This TSPS comes into force when published on the DPAG website. Amendments to this TSPS shall come into effect when they are published.

9.10.2 Termination

This TSPS shall remain in force until it is replaced by a new one.

9.10.3 Effect of Termination and Survival

Even if this TSPS should no longer be in force, the following obligations and restrictions pursuant to this TSPS shall remain in force: Section 9.6 (Representations and Warranties), section 9.2 (Financial Responsibility) and section 9.3 (Confidentiality of Business Information).

9.11 Individual notices and communications with participants

Not applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

Not applicable.

9.12.2 Notification Mechanism and Period

Timely notification of process-related changes that affect the overall outcome of the identity-proofing service will be provided for all contractual parties via the individually agreed channels.

9.12.3 Circumstances under Which OID Must be Changed

Not applicable. DPAG's POSTIDENT service does not issue certificates.

9.13 Dispute Resolution Provisions

DPAG only offers identity-proofing services to support the registration authorities of certificate authorities that issue certificates. DPAG does not have any contractual agreements with end-users or relying parties. In the event of disputes with end-users and relying parties, the issuing CA's dispute resolution procedures shall apply. All persons are treated equally in the defined standardized Postident identification process. For all cases that are not covered by

the process, the relying party has a contractual obligation to offer an alternative identification option. Complaints about the DPAG service can be submitted to postident@deutschepost.de.

9.14 Governing Law

This TSPS is subject to the law of the Federal Republic of Germany.

9.15 Compliance with Applicable Law

This TSPS is subject to national law and the eIDAS Regulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement - Vollständige Vereinbarung

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

If a provision in this TSPS should be partially incorrect or invalid, this shall not affect the validity of the remaining provisions until the TSPS is updated. The update process is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Not applicable.

9.16.5 Force Majeure

DPAG is not liable for delays or errors in the service underlying this TSPS that result from events beyond its control such as strikes, acts of war, uprisings, epidemics, power outages, fire, earthquakes and other catastrophes.

9.17 Other provisions

Not applicable.