Certification Practice Statement

of

identity Trust Management AG

for the identification procedures

identity Kurier Papier and identity Shop Papier,
identity Kurier Sign and identity Shop Sign,
identity Video and
identity eID

version 1.0
as of 2016-07-31

Table of Contents

Document History

Version	Date	Author / Editor	Change	Comment
1.0	31.07.2016	Meerloo Johannes/Jacobs Harald	Initial version	

1 Introduction

identity Trust Management AG is an identification services provider offering services in the field of verification of identities of natural persons and legal entities and obtaining signatures.

identity Trust Management AG resulted from a merger of the two companies formerly known as ID 8 GmbH and idvos GmbH. ID 8 was a company specialized in offline identifications services whereas idvos GmbH, a technology start-up, specialized in digital and online procedures for the verification of identities and documents.

The services identity Kurier Papier, identity Kurier Sign, identity Shop Papier, identity Shop Sign, identity Video and identity eID provided by identity Trust Management AG, have already been certified and confirmed as being compliant with the German Signature Act and the German Signature Ordinance. The modular confirmation allows certification services providers to use these services for identity verifications in the process of issuing qualified certificates.

This document is the CPS of identity Trust Management AG. It is not a full CPS according to RFC 3647, because identity Trust Management AG only covers the aspect of identity proofing, but does not offer other certification services.

The purpose of this document is to serve as a base for compliance with eIDAS, the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and the relevant ETSI standards, especially ETSI EN 319 411-2.

1.1 Overview

Identity verification can be conducted at the customer’s choice of address such as his domicile or workplace, in shops, in video conferences, or via the eID function of new ID cards. In addition, identity Trust Management AG offers professional contract management including but not limited to online signature of legally binding documents or contracts for the performance of a continuing obligation by qualified electronic signature (QES), obtains signatures, provides the results of identity verifications by electronic means and actively manages identities to support the recipients of electronic ID verifications.

The services of identity Trust Management AG are based on identity verifications in accordance with the German Geldwäschegesetz (prevention of money laundering act), the De-Mail act with its technical guidelines, and the German signature act and signature ordination.

identity Trust Management AG provides the following services.

- identity Kurier Papier
  Identification of the natural person to be identified by means of the physical presence of the person to be identified. The agent will visit the natural person at his home or any other agreed upon location and then performs the actual act of identification. Identity Kurier Papier is performed by regional couriers (Service Partner), connected by means of a proprietary, uniform and standardized software (identity Portal).

- identity Shop Papier
  Identification of the natural person to be identified by means of the physical presence of the person to be identified through visiting a special identification point, where the agent performs the actual act of identification. Identity Shop Papier is performed by contractually bound and affiliated ident partners or directly in shops.

- identity Kurier Sign
  Similar to identity Kurier Papier, but with additional verification of the signature performed by the identified person in presence of the agent.

- identity Shop Sign
  Similar to identity Shop Papier, but with additional verification of the signature performed by the identified person in presence of the agent.

- identity Video
  Identification via video session where the natural person has to be physically present in the same video session as the agent. identity Video is performed by trained and experienced identity Trust Management agents in accordance with procedures permitted by law. A video conference replaces the personal (physical) presence of the person to be identified.

- identity eID
  Identification of a natural person using the eID function of the German ID card.

identity Trust Management AG may use subcontractors in order to perform its services, but remains fully responsible for all aspects of the provided services. Contractual agreements are in place for all subcontractors. These include but are not limited to the obligation to comply with the requirements of the security concept.

1.2 Document Name and Identification

This document is the “Certification Practice Statement of identity Trust Management AG for the identification procedures identity Kurier, identity Shop Papier, identity Kurier Sign, identity Shop Sign, identity Video, and identity eID.”

Version: 1.0

Date: 2016-07-31

This document goes into effect when upon its publishing.

It loses its validity upon its replacement or when being succeeded by an updated version.

1.3 PKI Participants

No stipulation. identity Trust Management AG provides only identity verification.

1.4 Certificate Usage

No stipulation. identity Trust Management AG provides only identity verification.

1.5 Policy Administration

Changes to this document need to be approved by the management of identity Trust Management AG. After approval, the changed version is made available as stated in 2.1.3. The CPS is reviewed after major process changes or at least annually, as part of the internal audit and is adapted if necessary.

1.5.1 Organization administering the document

This CPS is administered by:

identity Trust Management AG
Lierenfelder Straße 51
40231 Düsseldorf
Deutschland

1.5.2 Contact Person

Security Officer

identity Trust Management AG
Lierenfelder Straße 51
40231 Düsseldorf
Deutschland

Phone: +49 211 68 77 3-0

E-Mail: kontakt@identity.tm

1.6 Definitions and Acronyms

TBD

2 Publication and Repository Responsibilities

2.1.1 Repositories

No stipulation. identity Trust Management AG provides only identity verification.

2.1.2 Publication of certificate information

No stipulation. identity Trust Management AG provides only identity verification.

2.1.3 Time or frequency of publication

The latest version of this CPS is available for download under www.identity.tm the official website of identity Trust Management AG. Previous versions of the CPS will be made available on that site as well.

New versions will be published whenever relevant modifications have been made.

The latest version of the terms and conditions (German document “AGB”) together with the data protection declaration (German document “Datenschutzerklärung”) are available under https://www.identity.tm/Impressum.

The websites of identity Trust Management AG are available to the public on 24 hours a day, 7 days per week. In case of system failure or any other kind of outages, identity Trust Management AG will undertake all efforts to ensure that the necessary information will be made available again as soon as possible.

3 Identification and Authentication

3.1 Naming

No stipulation. identity Trust Management AG does not issue certificates.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

No stipulation. identity Trust Management AG does not issue certificates.

3.2.2 Authentication of organization entity

No stipulation. identity Trust Management AG does not authenticate legal entities.

3.2.3 Authentication of individual identity.

The identity of the applicant is checked against an official identity document (ID). Either ID card or passport can be used.

For the Kurier and Shop processes, the applicant has to appear in person and a standard paper form is completed as evidence of the identification having been performed.

In case of the identity video process, the applicant has to be present in a video conference call and screenshots are recorded as evidence.

In case of identity eID process, the identification data is retrieved using the electronic identification processes provided by the official German eID solution. All data collected is securely stored within identity Trust Management AG's databases.

The information collected during the identification include, at least the full name (surname and given names) of the applicant, the date and place of birth, the type, validity period, and the reference number of the identity document presented. Further information of the applicant, like current address, may be collected, provided that this information has been validated during the identification.

All data exchanged electronically with the customers is protected and will be held confidential by encryption and integrity is protected by a qualified electronic signature. Data that is exchanged on paper, is transported inside of sealed transport boxes.

3.3 Identification and Authentication for Re-key Requests

No stipulation. identity Trust Management AG does not differentiate between identification requests for initial or re-key requests. All identifications are handled as described in section 3.2.3.

3.4 Identification and Authentication for Revocation Requests

No stipulation. identity Trust Management AG does not handle revocation requests.

4 Certificate Life-Cycle Operational Requirements

No stipulation. identity Trust Management AG is only performing identification services and does not issue certificates, does not process certificate applications, or provides CRL or OCSP services.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

All facilities concerned with the processing of identification data, including necessary infrastructural components like routers and firewalls are operated in an environment that physically protects the services against compromise through unauthorized access to systems or data. Facilities are surrounded by solid walls and access to these facilities is only possible to a limited number of authorised employees. Every entry of unauthorized persons to the secured premises is logged. Unauthorised persons are always accompanied by an authorised person whilst inside of the facility.

The premises of Service Partners and shops performing identity verification do not store any data outside of business-hours, neither in electronic nor in paper form. All locations are locked outside of business-hours. Keys are handed out to authorized personnel only.

5.2 Procedural Controls

The paper-based identification protocols of the Kurier and Shop processes are collected by the digitization centre of identity Trust Management AG separated by co-operation or Service Partner in a dedicated transport box. Before shipping to the co-operation or Service Partner each transport box is sealed in order to prevent unauthorised access to or unnoticed modification of the boxes' content.

Electronic identification data of all identification processes is transmitted only through secured communication lines. All communication is encrypted; the authenticity and integrity of transmitted data is ensured through a qualified electronic signature.

identity Trust Management AG maintains a security concept which includes security controls and procedures for all its systems, facilities and assets providing the identification services. Risk assessment of the identification processes is performed as part of the security concept. Security measures to minimize risks have been implemented and are described within the security concept. The risk analysis is reviewed as part of the regular internal audit.

It is the security officer's duty to perform internal audits of the infrastructure and the used systems, processes, and documentations in order to ensure that the services are provided are consistent with this CPS and other policies and procedures defined by identity Trust Management AG. These internal audits are performed at least once a year. Results of the internal audit, including possible discrepancies or deficits, have to be reported to the general management of identity Trust Management AG. In such case the execution of corrective measures is initiated by the security officer in coordination with the data protection officer.

5.3 Personnel Controls

identity Trust Management AG employs staff and subcontractors, who possess the necessary expertise, reliability, experience, and qualifications.

All employees receive regular training with regards to security and personal data protection rules and measures.

Appropriate disciplinary actions and/or sanctions will be applied to personnel violating identity Trust Management AG’s policies or procedures.

Persons in trusted roles are selected by the company’s management and formally appointed to their roles.

Managerial personnel possess professional experience with the services provided and are familiar with security procedures for personnel with security responsibilities.

Personnel in trusted roles are to be held free from conflict of interest situations that might prejudice the impartiality of operations.

Trusted roles include roles that involve the following responsibilities:

- Security Officers: overall responsibility for administering the implementation of security practices.
- System Administrators: authorized to install, configure, and maintain systems.
- System Operators: responsible for operating systems on a day-to-day basis.
- System Auditors: authorized to review archives and audit logs of the systems.
- Identifier: Responsible for the identification of applicants and the documentation of the identification results.

Access to systems or applications is only granted after the appointment to a trusted role.

5.4 Audit Logging Procedures

System events are logged on a server dedicated for system logging. All attempts to access the IT infrastructure of identity Trust Management AG are logged to this server, indicating the type as well as the time of the event. Administrative access to the syslog server is only possible under dual control and only from within the internal network.

All systems, including the databases of the business software as well as the logging server, are backed up on a regular basis, twice per day, using a dedicated backup server. Backups are managed by the IT service and the hosting provider.

5.4.1 Types of events logged

All events regarding identification activities are logged in the business software of identity Trust Management AG.

5.4.2 Frequency of processing log

The correct operation of the logging functions is verified on a regular basis.

5.4.3 Retention period for audit log

Audit logs are retained for a period of 12 months and are securely deleted after that time.

5.4.4 Protection of audit log

Audit logs are only accessible under dual control and only from within the internal network.

5.4.5 Audit log backup procedures

Audit logs are covered by the routine backup procedures.

5.4.6 Audit collection system

System events are logged on a dedicated server.

5.4.7 Notification to event-causing subject

Depending on the severity and nature of the event, identity Trust Management AG will notify the event-causing subject (e.g. Service Partner who submitted data) of the event, the log-entry, and the result of investigations.

5.4.8 Vulnerability assessment

System events are logged on a server dedicated for system logging. All attempts to access the IT infrastructure of identity Trust Management AG are logged to this server, indicating the type as well as the time of the event.

5.5 Records Archival

All information regarding the performed identification is transmitted to the customer who issued the request for identification and who has to ensure proper archiving. The information will be made anonymous after three months and finally deleted from the systems of identity Trust Management AG after a maximum period of 12 months.

The security concept including all its historic versions, evidences for technical qualification of the employees, the role list including history and information regarding service partners and subcontractors, are archived on electronic data storage media and / or paper-based for the complete time of business activity of identity Trust Management AG.

As long as a business relationship continues to exist, this information is to be made available for the TSP upon request. In case of termination of the business relationship, identity Trust

Management AG makes all necessary information available to its customer. In such case the customer is obligated to retrieve and properly archive the information.

5.6 Key Changeover

No stipulation. identity Trust Management AG does not issue certificates and does not handle CA keys.

5.7 Compromise and Disaster Recovery

The hosting provider maintains an ISO 27001 compliant Information Security Management System which includes a disaster recovery plan. According to that plan, services will be restored as soon as possible.

5.8 CA or RA Termination

In case of termination of services, the management of identity Trust Management AG informs the relevant supervisory authority and other customers at least two months in advance about this fact.

All documentation relevant for the customers will be provided for collection at designated interfaces. Customers will be requested to collect all documentation necessary to fulfill their legal requirements on retention periods.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

No stipulation. identity Trust Management AG is only performing identification services and does not issue certificates on its own.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

No stipulation. identity Trust Management AG is only performing identification services and does not issue certificates on its own.

6.3 Other Aspects of Key Pair Management

No stipulation. identity Trust Management AG is only performing identification services and does not issue certificates on its own.

6.4 Activation Data

No stipulation. identity Trust Management AG is only performing identification services and does not issue certificates on its own.

6.5 Computer Security Controls

identity Trust Management AG has taken appropriate technical and organizational measures to protect systems and data against unauthorized access and to ensure the integrity and authenticity of systems and data.

The servers for the administration of identity Trust Management's local offices are physically separated from the servers providing the business functionality.

Local servers do neither store nor process personal data collected during the identity verification process. The servers for business functionality (i.e. those that process and store personal data) are operated and hosted by a service provider.

All systems are access controlled and protected by firewalls. Access to the business software of identity Trust Management AG, is only possible for authorized employees after successful authentication. All systems and networks are configured according to "DENY ALL by Default", which means, that only explicitly necessary connections, services and access rights are configured. Security patches for systems are installed if necessary.

Administrative access to the systems is only possible for authorized employees in the role of system administrator after successful authentication.

The systems are permanently monitored with regards to processing power and storage capacity. In case of the configured thresholds being reached, IT service, security officer and management will be notified automatically.

6.6 Life Cycle Security Controls

Development of the business software is performed by the IT service of identity Trust Management AG. Development is performed in a separated development environment and includes definition and testing of security requirements. Releases must be approved by the management. Approval and releases are completely documented.

identity Trust Management AG maintains a list of all its assets which defines the necessary security level for each asset. The list is reviewed regularly as part of the annual internal audit.

6.7 Network Security Controls

The internal networks of identity Trust Management AG are separated from each other and from external networks by firewalls which are configured to allow only the necessary data connections.

Network accessible components provide continuous service (except, when necessary, for brief periods of maintenance or backup).

All components have appropriate security measures implemented to ensure protection against denial of service and intrusion attacks.

Unused network ports and services are deactivated. Any boundary control devices, used to protect the network, are configured to accept only explicitly allowed connections.

All security principles and measures that apply are identified in identity Trust Management's security concept.

All infrastructural components are permanently monitored for correct function.

6.8 Timestamping

No stipulation. identity Trust Management AG does not issue time-stamps.

7 Certificate, CRL, and OCSP Profiles

No stipulation. identity Trust Services AG is only performing identification services and does not issue certificates or provide CRL or OCSP services.

8 Compliance Audit and Other Assessment

8.1 Frequency of compliance audit

Audits for eIDAS compliance are performed on a regular basis.. Some customers may perform additional, annual third-party audits in order to fulfil their outsourcing responsibilities.

8.2 Identity/qualifications of auditor

Compliance auditors have competence in the field of compliance audits.

Auditors are ETSI “lead auditors” qualified and trained for Information Security Management System assessment, in particular qualified to conduct audits for compliance with eIDAS relevant ETSI standards (e.g. ETSI EN 319 411-2) and for compliance with local signature laws.

Compliance auditors perform such compliance audits as a primary responsibility on behalf of the applicable certification body.

8.3 Auditor’s relationship to audited party

The certification body and compliance auditors are accredited by the German accreditation body (DAkkS – Deutsche Akkreditierungsstelle) to perform such audits and certifications. They are independent from identity Trust Management AG.

8.4 Topics covered by audit

The auditors choose the control objectives to be covered in the assessment in accordance with eIDAS, ETSI requirements and the German Signature Law.

8.5 Actions taken as a result of deficiency

In case of identified deficiencies, an action and remediation plan will be agreed between identity Trust Management AG and the auditors.

8.6 Communication of results

Audit results are communicated to the responsible supervisory bodies.

9 Other Business and Legal Matters

9.1 Fees

Fees will be negotiated individually between identity Trust Management AG and the cooperation partners.

9.2 Financial Responsibility

identity Trust Management AG maintains financial stability as required for the provision of the services and as shown in its annual reports. It has public liability insurance as well as pecuniary damage liability insurance to cover liabilities arising from its business operation.

9.3 Confidentiality of Business Information

identity Trust Management AG treats all business information obtained from its business partners as confidential, unless otherwise agreed upon.

9.4 Privacy of Personal Information

9.4.1 Purpose of data acquisition, processing and usage

identity Trust Management AG has committed itself to the principle of acquiring, processing or using as little personal data as possible. identity Trust Management AG acquires data on employees, subcontractors, customers and suppliers in its IT systems only for the purpose of enabling cooperation as effective as possible. In case identity Trust Management AG receives note about the invalidity of data, these data will either be deleted or marked invalid.

Personnel data acquired, processed or used on behalf of the customer is treated according to the same principles. Provided address data will only be used for the provision of the services according to the orders.

9.4.2 Principles on data acquisition and disclosure

All personnel assigned and engaged in data processing, it is prohibited to acquire, process or use any data without authorization or in any unlawful manner. All personnel is bound by the principles of data secrecy before being assigned to any job involving the processing of personal data. The requirements on data secrecy continue after cessation of the job assignment.

identity Trust Management AG acquires personal data only directly from the affected person and only up to the amount required for the purpose of a legally conformant identification. With an exception for the initial identification request from the TSP, data acquisition from third parties does not take place. Personal data is only acquired for performing identifications and is not used for any other purposes.

identity Trust Management AG may surrender and transmit personnel data to legal institutions only upon their explicit written request citing case and purpose and only as far as it is necessary for the purpose of prosecution of criminal and administrative misconduct or offense, in order to prevent threats to public safety and order, in order to comply with the duties and responsibilities of agencies involved in the protection of the constitution, the federal intelligence service, the military intelligence service or the tax authorities or as far as an official court order dictates.

All information is disclosed only by the data security officer and every disclosure is documented. It is the data security officer’s responsibility, to validate if the requesting authority is legally authorised to do so and if the request is in accordance with applicable legal requirements. The requesting authority has to inform the person whose data has been requested as soon as possible, under the condition that this act of information, does not endanger or impede the authority’s duties to a higher degree, then those interests of said person concerned, who’s data is being disclosed.

9.4.3 Technical and organizational controls

According to the legal requirements, identity Trust Management AG has implemented technical and organizational controls for the protection of personal information, in a way that the unauthorized access is prevented and that the immutability and authenticity of the data is guaranteed.

identity Trust Management AG has implemented proper data security measures for all security systems that are required by law.

The data security officer documents all data security measures in a data security concept.

9.5 Dispute Resolution Procedures

identity Trust Management AG has established procedures for the resolution of disputes and complaints. Customers can place their complaints directly in the identity Portal. Other parties can submit their complaints in writing, by email or by phone.

All complaints will be analysed and handled as soon as possible.