Trust Service Practice Statement
D-TRUST AusweisIDent

ENGLISH

DEUTSCH

TSPS – Trust Service Practice Statement

D-TRUST AusweisIDent

Version 1.3

Copyright Notice and License

Please direct any inquiries regarding any other form of use of this TSPS of D-Trust GmbH not covered by the above-mentioned license to:

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin, Germany
Phone: +49 (0)30 259391 0
E-mail: info@d-trust.net

Document History

Version	Date	Description
1.0	2019-07-26	▪ Initial version ▪ Certification of the AusweisIDent service according to eIDAS
1.1	2020-09-28	▪ Amendments in section 5.5.2 ▪ Annual review of the entire CPS
1.2	2021-06-23	▪ Annual review of the entire CPS ▪ The on-site reading service is added to this "D-TRUST_AusweisIDent_TSPS" document. The identification service has now been renamed AusweisIDent Online (formerly AusweisIDent). This means that the document now includes the following services: "AusweisIDent OnSite" and "AusweisIDent Online".
1.3	2022-11-29	▪ Amendments in sections 1.1, 5.3.4, 5.3.5, 6.6.1, 6.6.3 ▪ Annual review of the entire CPS

Contents

1. Introduction

1.1 Overview

This document is the Trust Service Practice Statement (TSPS) of the AusweisIDent services operated by D-Trust GmbH:

a. AusweisIDent OnSite and
b. AusweisIDent Online.

AusweisIDent OnSite is a service provided by D-Trust GmbH to read out ID card data and transfer this data to an electronic form.

AusweisIDent Online is an identification service provided by D-Trust GmbH that is used to verify the identity of individuals. AusweisIDent Online can also be used in conjunction with trust services pursuant to Regulation (EU) No 910/2014 (eIDAS) of the European Parliament.

This document applies to identity verification pursuant to the eIDAS regulation and BSI TR-03128 (AusweisIDent Online) as well as to the rule for reading out ID card data to be transferred to electronic forms without any change in media (AusweisIDent OnSite) pursuant to BSI TR-03128. AusweisIDent OnSite is not identity verification within the meaning of eIDAS.

The structure of this document is based on the RFC 3647 Internet standard: "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework".

1.2 Document name and identification

This document is a Trust Service Practice Statement (TSPS) pursuant to ETSI EN 319 401 and BSI TR-03128.

Document name:	Trust Service Practice Statement for D-TRUST AusweisIDent
Version	1.3

1.3 PKI participants

D-Trust GmbH does not operate a certification authority within the scope of its AusweisIDent procedure, so that there is no PKI infrastructure with PKI entities.

AusweisIDent includes the services of both AusweisIDent Online and AusweisIDent OnSite.

The AusweisIDent Online service is used exclusively to identify individuals on the Internet with the help of the online ID function of the German ID card or the electronic residence permit. This service is operated by D-Trust GmbH which acts as an identification service provider within the meaning of sec. 2 (3a) in conjunction with sec. 18 of the German Act on Identity Cards and Electronic Identification (PAuswG, *Personalausweisgesetz*).

Companies and public authorities, as well as trust service providers (referred to here as service providers) can embed the AusweisIDent Online service in procedures that require online identification of customers or citizens at a high level of trust. Examples of this are opening a bank account or identification on the Internet (online) for a digital signature.

AusweisIDent OnSite is used exclusively for reading out ID card data from the ID card or electronic residence permit in order to transfer the ID card data to electronic forms without any change in media. This is not identity verification within the meaning of eIDAS. This service is operated by D-Trust GmbH which acts as a service provider for AusweisIDent OnSite within the meaning of sec. 18a PAuswG in conjunction with sec. 21a.

Companies and public authorities can embed the AusweisIDent OnSite service in procedures in order to transfer ID document data to electronic forms without any change in media. Opening a bank

account, signing a mobile phone contract or submitting an application to a public authority on-site are some examples.

1.3.1 Certification authorities (CAs)

D-Trust GmbH does not operate a certification authority within the scope of its AusweisIDent procedure.

1.3.2 Registration authorities (RAs)

No stipulation. See section 1.3.

D-Trust GmbH does not operate a registration authority (RA) within the scope of its AusweisIDent procedure. See section 1.3.

1.3.3 Subscriber

No stipulation. See section 1.3.

1.3.4 Relying parties

No stipulation. See section 1.3.

1.4 Certificate usage

No stipulation.

No certificates are issued as part of the AusweisIDent service.[1]

1.5 Policy administration

1.5.1 Responsibility for the document

This TSPS is maintained and updated by D-Trust GmbH. The representative of management is responsible for acceptance of the document.

This CPS is checked and, when necessary, updated annually by the TSP. A change is indicated by a new version number of this document.

Contact details:

D-Trust GmbH
Editorial unit
Kommandantenstr. 15
10969 Berlin, Germany

Phone: +49 (0)30 259391 0
E-mail: info@d-trust.net

1.6 Definitions and acronyms

1.6.1 Definitions and names

These rules are laid down in the CP.

1.6.2 Acronyms

These rules are laid down in the CP.

[1] AusweisIDent Online is a service for identifying individuals and AusweisIDent OnSite is a service for reading out ID card data for transfer to electronic forms without any change in media.

1.6.3 References

[AGB]	General Terms and Conditions of Business of D-Trust GmbH, latest version	https://www.bundesdruckerei.de/system/files/dokumente/pdf/AGB-der-bdr-fuer-Vertrauensdienste-und-Zertifizierungsdienste-der-D-TRUST.pdf
[CP]	Certificate Policy of D-Trust GmbH, latest version	http://www.d-trust.net/internet/files/D-TRUST_CP.pdf
BSI TR-03128	Service provider for the eID function	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03128/TR-03128_node.html
PAuswG (German abbreivation)	German Act on Identity Cards and Electronic Identification	https://www.gesetze-im-internet.de/pauswg/BJNR134610009.html

Additional rules are laid down in the CP.

2. Publication and Repository Responsibility

2.1 Repositories

The TSP publishes this TSPS and other process-relevant documents on the following website:

https://www.d-trust.net/en/support/repository

2.2 Publication of information concerning certificates

No stipulation.

No certificates are issued as part of the AusweisIDent service. This means that no certificate information is published.

2.3 Publication frequency

This TSPS is published and remains available for at least as long as AusweisIDent services are offered on the basis of this TSPS.

The websites of the TSP can be accessed publicly and free of charge 24/7.

2.4 Repository access control

This TSPS and other process-relevant documents can be publicly retrieved at no cost. Read access is unrestricted. Changes in repository and web contents are carried out exclusively by the TSP.

The relevant parts of other non-public documents can be issued on request against proof of a legitimate interest.

2.5 Access to and use of services

These rules are laid down in the CP.

3. Identification and Authentication

3.1 Naming

No stipulation.

No certificates are issued as part of the AusweisIDent service.

3.2 Initial identity verification

3.2.1 Proof of ownership of the private key

No stipulation.

No certificates are issued as part of the AusweisIDent service.

3.2.2 Identification and authentication of organizations

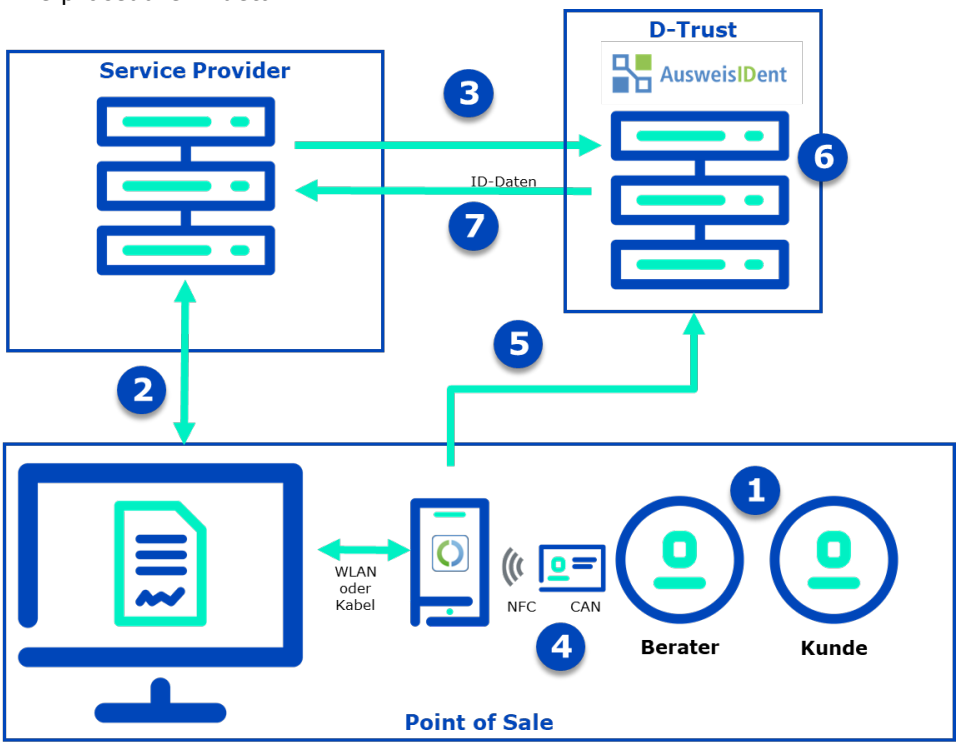
No stipulation.

No certificates are issued as part of the AusweisIDent service.

3.2.3 Identification and authentication of Individuals

a) Reading out ID card data for transfer to electronic forms without any change in media using AusweisIDent OnSite.

The procedure in detail:



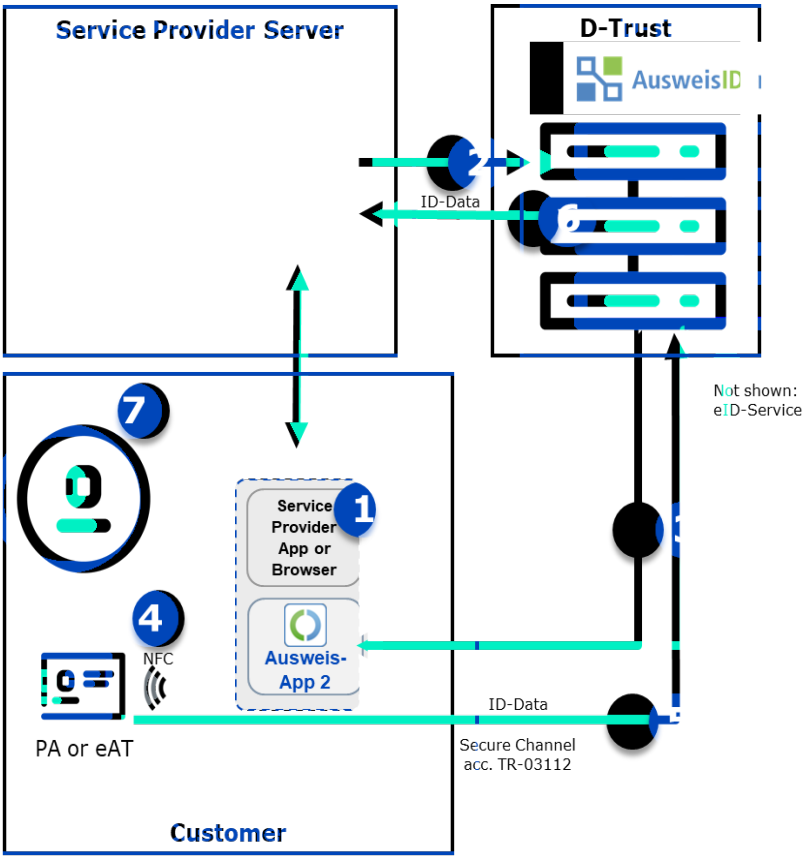
1. The sales consultant compares the photo with the customer's ID card.
2. The sales consultant starts the readout process on their terminal at the service provider.
3. The service provider sends an AuthorisationRequest to the AusweisIDent service. The readout process is started and controlled by the AusweisIDent service via the eID service.

4. The sales consultant holds the ID card up to the smartphone/terminal reader. The readout process is legitimised by entering the CAN.
5. The eID service reads the data from the ID card via the AusweisApp2 app.
6. AusweisIDent performs the read-out process and makes the data read out available via the interface.
7. The service provider takes the ID data from the interface and stores it in the system. The data is displayed to the sales consultant in the web form.

b) Identification and authentication of individuals with AusweisIDent Online

The AusweisIDent Online service is used to identify individuals on the Internet with the help of the online ID function of the German ID card or the electronic residence permit. Companies and public authorities, and even a trust service provider, can embed this service in procedures that require online identification of customers or citizens at a high level of trust. The AusweisIDent Online provider acts on behalf of the service provider. Opening a bank account, signing a mobile phone contract or submitting an application to a public authority are some examples.

The procedure in detail:



1. The customer calls the app (on the smartphone) or the service provider's website (with the browser) in order to use a service. To do this, he must identify himself and select AusweisIDent Online for legitimation.
2. The service provider server submits an *AuthorisationRequest* to AusweisIDent Online via the OAuth2/OpenID Connect interface of the service.

3. Via eID Server, AusweisIDent Online establishes a secure connection to AusweisApp2 on the customer's device (fully integrated as mobile SDK in the service provider's App or separately) according to TR-03113.
4. The customer places his ID card or or electronic residence permit on an NFC-enabled smartphone or a card reader on a PC and enters the secret PIN to confirm reading of the data.
5. The customer data is read from the ID card/electronic residence permit and temporarily stored by AusweisIDent Online until retrieved by the service provider. For the purpose checking the identity of an individual according to eIDAS, the following attributes must be read as a minimum as proof of identity and transferred to the service provider for storage.
    1. First name(s)
    2. Name
    3. Date of birth
    4. Place of birth
6. The service provider retrieves the customer's ID data signed by AusweisIDent Online. The customer's ID data is then deleted in AusweisIDent Online.
7. The customer is now legally identified.

3.2.4 Non-verified information concerning the subscriber

No stipulation.

No certificates are issued as part of the AusweisIDent service.

3.2.5 Verification of request authorization

No stipulation.

No certificates are issued as part of the AusweisIDent service.

3.2.6 Criteria for interoperability

Before AusweisIDent can be used, a contract must be entered into between the service provider and Bundesdruckerei or D-TRUST.

The interface between the service provider and AusweisIDent is described in the "AusweisIDent User Manual" (currently version 1.2.0). This document will be handed over to the service provider at the latest when the contract is concluded.

The interface between eID-Server and AusweisApp2 (eID client) is described in "Technical Guideline TR-03124-1 eID client – Part 1: Specifications".

No contractual relationship exists between the service provider's customer and Bundesdruckerei or D-TRUST, except when D-TRUST acts also as a service provider.

Interaction between the service provider, the service provider's customers and Bundesdruckerei or D-TRUST is described in "3.2.3 Identification and authentication of individuals".

3.3 Identification and authentication of applications for re-keying requests

No stipulation.

No certificates are issued as part of the AusweisIDent service. Therefore, identification and authentication are not carried out for re-keying requests.

3.4 Identification and authentication for revocation requests

No stipulation.

No certificates are issued as part of the AusweisIDent service. Therefore, identification and authentication are not carried out for revocation requests.

4. Operational Requirements for the Certificate Life Cycle

No stipulation.

No certificates are issued as part of the AusweisIDent service. Therefore, certificate applications are not processed within this framework and there is no service that checks the status or authenticity of certificates.

5. Facility, Management and Operational Controls

The descriptions in this chapter refer to AusweisIDent Online as an identification service for individuals and to AusweisIDent OnSite as a service for reading out ID card data to be transferred to electronic forms without any change in media, both of which are operated at D-Trust GmbH in accodance with ETSI EN 319 401 and BSI TR-03128.

D-Trust GmbH operates management systems accredited in accordance with both ISO/IEC 27001 and ISO 9001. Operation of the TSP is subject to this ISMS. An Information Security Policy regulates the binding requirements for operation. This was approved by the management of D-Trust GmbH and communicated to all employees of the TSP. The Security Policy is reviewed and updated each year, and also on an event basis.

If changes due to processes or operations lead to an update of the Security Policy, the resulting changes for TSP operation must be approved by management. The updated and approved Security Policy must be communicated promptly by the managers to all affected employees and, if necessary, the manager must initiate training measures.

With the exception of individual identification services, no other TSP activities are outsourced to external service providers. Where applicable, necessary aspects of the Security Policy will also become mandatory for service providers.

5.1 Physical security controls

Detailed documentation is available for physical security controls and the relevant parts of this can be made available for inspection to any party proving a justified interest in such disclosure. The documentation has been audited by a recognized conformity assessment body. Conformity assessment is regularly repeated in accordance with [EN 319 411-1] and [EN 319 411-2].
Furthermore, TÜV-IT has certified that the trust service provider of D-Trust GmbH applies and implements in its security area the "Infrastructure measures for high protection requirements – level 3" ["Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3"] (according to the catalogue of audit criteria for "Trusted Site Infrastructure"). This TÜV-IT certificate for a "Trusted Site Infrastructure" evaluates all infrastructure-relevant aspects. This audit is repeated every two years. The above-mentioned certificate confirms that D-Trust GmbH fulfils this demanding security standard for its facility, management and operational controls.

5.2 Procedural controls

5.2.1 Role concept

Documentation includes a role concept where TSP management assigns employees to one or more roles who then receive the corresponding authorizations in a managed process. The authorizations of the individual roles are limited to those authorizations which these roles need to fulfil their tasks. The assignment of authorizations is revised by security management on a regular basis, and authorizations are cancelled immediately when no longer needed.

Roles with security responsibility for TSP operation, known as "Trusted Roles" (including the tasks of security officer, system administrator, system operator, system auditor, registration officer, revocation officer and validation specialist) are defined in D-TRUST's authorization concepts. These roles may only be assumed by competent and reliable employees.

Employees are regularly trained to fulfill their roles and related responsibilities, and are made aware of compliance with applicable security regulations. The requirements for the respective roles are documented and can be viewed by employees at any time. Before employees can perform their assigned roles, they must agree to these roles. In the case of mutually exclusive roles, a person can assume only one of these roles (four-eyes principle). A risk assessment is carried out on a regular basis.

Employees working in the area of certification and revocation services act independent and are free from commercial/financial constraints that could influence their decisions and acts. The organization structure of the TSP considers and supports employees in the independence of their decisions.

5.2.2 Four-eyes principle

The four-eyes principle is the minimum requirement for particularly security-critical operations. This is ensured by technical and organizational measures, such as access authorization and verification of knowledge.

5.2.3 Identification and authentication (I&A) for individual roles

The role concept is ensured by technical and organizational measures, such as access authorization and verification of knowledge. Before being allowed to access any security-critical applications, the employee concerned must have been successfully authenticated. Event logs enable the identification of employees who performed past actions; the employees are accountable for their acts.

5.2.4 Role exclusions

The role concept includes various role exclusions in order to prevent any conflict of interests, to ensure the four-eyes principle and avoid any harmful acts.

5.3 Personnel controls

The TSP meets the requirements concerning personnel as laid down in [EN 319 411-1] and [EN 319 411-2].

5.3.1 Requirements in terms of qualification, experience and reliability

The TSP ensures that persons employed in the area of the trust service have the required knowledge, experience and skills.

The identity, reliability and professional qualifications of employees are verified before they commence work. Regular and demand-driven training ensures competency in the respective fields of activity as well as general information security. Training and proficiency checks are documented.

Line managers, in particular, are selected according to special criteria. They must demonstrate that they have knowledge of security procedures for staff with security responsibility and that they have sufficient experience of information security and risk assessment in relation to the trust service provided. Evidence can be provided in the form of certificates and CVs. If the required qualification cannot be proven sufficiently, it must be acquired through appropriate training before the employee can take over management functions in TSP operations.

5.3.2 Security screening

Individuals who work in security-relevant areas of the TSP are also regularly required to present clearance certificates.

The TSP also operates a management system certified according to ISO 27001 and ISO 9001 that provides employees with security-relevant requirements and/or rules of conduct.

5.3.3 Training

The TSP trains trust service personnel.

5.3.4 Frequency of training and information

The TSP trains trust service personnel at the beginning of their employment, annually and as required.

5.3.5 Frequency and sequence of job rotation

Role changes are documented. The corresponding employees are trained annually.

5.3.6 Measures in the case of unlawful acts

The TSP does not employ any unreliable persons in the trust service.

Violations by employees of the policies or processes of TSP operations are analyzed and evaluated. If the relationship of trust cannot be ensured, these employees are excluded from security-relevant activities.

5.3.7 Requirements for freelance staff

No stipulation; no freelance staff are employed.

5.3.8 Documentation handed over

Comprehensive process instructions and procedures for all production steps define the relevant employee roles and rights as well as the corresponding manual and automated checks. The technical security infrastructure of D-Trust GmbH ensures that deviations from these defined processes are not possible in the production process.

5.4 Audit logging procedures

5.4.1 Monitoring access

The TSP implements comprehensive surveillance measures (for instance, video surveillance) in order to warrant the security of its trust services and the underlying IT systems and documents.

The audit logging procedures are supplemented by organizational rules. Visitor rules, for instance, require that visitors be announced and registered by name at least 24 hours before their visit. While in the area of the trust service provider's premises, visitors must be accompanied at all times by an employee of the TSP.

5.4.2 Monitoring organizational measures

Monitoring organizational measures is another part of the security concept.

This includes a regular risk analysis that provides a comprehensive analysis of threats to the TSP's operations and defines requirements and counter-measures. It also includes an analysis of the residual risk where the appropriateness of the residual risk is identified and, if reasonable, accepted.

Furthermore, all relevant assets are correctly identified, and the corresponding changes to these assets are checked or, if applicable, released by the TSP staff commissioned by management.

5.5 Records archived

5.5.1 Types of records archived

The personal data is deleted in AusweisIDent after it has been transferred to the service provider, but at the latest after 10 minutes, and is not archived.

System logs with access data (date/time, incoming IP address, client ID, the name of the read fields, redirect URI) are deleted on the server after 90 days.

5.5.2 Archiving times for data

The personal data is deleted in AusweisIdent after it has been received by the service provider (both in the case of AusweisIDent Online and AusweisIDent OnSite). The personal data is not archived.

No archiving is carried out within the scope of identification using the AusweisIDent Online service or within the scope of AusweisIdent OnSite.

Event logs of IT systems are stored for at least six months. Recordings of administrative activities are stored for a period of 90 days.

For the archiving system, the system time is synchronized daily with the official time via DCF77.

5.5.3 Archive protection

There is no need to back up the archive, since no personal data is archived within the framework of the AusweisIDent service.

5.5.4 Archive data backup

No stipulation.

No personal data is archived within the framework of the AusweisIDent service.

5.5.5 Request for time stamping of records

No stipulation.

5.5.6 Archiving (internally/externally)

No stipulation.

No personal data is archived within the framework of the AusweisIDent service.

5.5.7 Procedure for obtaining and verifying archive information

No stipulation.

No personal data is archived within the framework of the AusweisIDent service.

5.6 Key change at the TSP

No stipulation.

No certificates are issued as part of the AusweisIDent service.

5.7 Compromising and continuation of business on the part of the TSP

The security concept describes the implementation of recovery procedures for restoring the operability of the TSP. Backups are made on a daily basis and after changes. Backups are stored in a different fire zone.

5.7.1 Treatment of incidents and cases of compromise

The TSP has a contingency concept and a restart plan which are known to the roles involved and which can be implemented by these when necessary. Responsibilities are clearly distributed and are known.

Should a system recovery be necessary, the responsibilities and corresponding "Trusted Roles" are laid down in D-TRUST's authorization concept and are known to the respective employees. See section 5.2.1.

5.7.2 Recovery after resources have been compromised

The security concept describes the implementation of recovery procedures for restoring the operability of the TSP.

5.7.3 Compromising of the private CA key

No stipulation.

5.7.4 Ways of continuing business following compromise and disaster

In the event of an emergency and depending on the nature of the incident, the TSP decides whether recovery is to be carried out and then takes measures to avoid recurrence.

5.8 Termination of AusweisIDent services

The personal data read out is signed and only temporarily stored until it is transferred to the service provider. AusweisIDent itself does not archive any personal data.

When the signed personal data has been transferred, the process is legally completed.

In the event of termination of AusweisIDent services, the related services will no longer be offered. Any obligations to archive information regarding business transactions will be assumed by the customer.

6. Technical Security Controls

6.1 Key pair generation and installation

No stipulation.

No certificates are issued as part of the AusweisIDent service.

6.2 Private key and protection and cryptographic module engineering controls

No stipulation.

No certificates are issued as part of the AusweisIDent service.

6.3 Other aspects of key pair management

No stipulation.

No certificates are issued as part of the AusweisIDent service.

6.4 Activation data

No stipulation.

No certificates are issued as part of the AusweisIDent service.

6.5 Computer security controls

D-TRUST operates an information security management system (ISMS) in accordance with ISO/IEC 27001. Operation of the TSP is subject to this ISMS. A Security Policy regulates the binding requirements for IT operations. This was approved by the management of D-Trust GmbH and communicated to all employees of the TSP. The Security Policy is reviewed and updated each year, and also on an event basis.

Evaluation and, if necessary, elimination of identified vulnerabilities takes place within 48 hours. If it is not possible to resolve the problem within 48 hours, the assessment will include a concrete action plan.

6.5.1 Specific technical security requirements for the computer systems

The computers, networks and other components used by the TSP ensure in their given configuration that only those actions can be carried out which are not in conflict with this TSPS and [EN 319 411-1] or [EN 319 411-2], respectively.

The TSP's computer security for exposed systems is ensured, amongst other things, by multi-level security systems providing perimetric virus protection, end-point protection and integrity-protecting tools.

It is ensured that security-relevant software updates are installed at the appropriate point in time on the relevant systems. Any deviations are suitably documented by the TSP and, if necessary, addressed in the TSP's risk management.

6.5.2 Assessment of computer security

The computers, networks and other components used for this procedure are subject to appropriate monitoring in accordance with [EN 319 401].

6.5.3 Monitoring

The relevant systems are continuously monitored in order to ensure the availability of the AusweisIDent system. Each failure is recorded, documented, classified according to its severity and prioritized. The handling of critical notifications is part of the incident management process. Notifications on security-relevant events are sent to a central place and assessed according to their criticality.

In case of failures where a service is no longer available, the parties affected will be informed every 24 hours on the current status of trouble-shooting.

6.6 Life cycle security controls

The requirements of section 5 [BRG] are already adequately considered during the planning of all systems operated by the TSP or on behalf of the TSP.

6.6.1 Security controls during development

Security requirements are already analyzed during the draft design phase for all system development projects carried out by or on behalf of the TSP. The results are defined as requirements for development.

D-Trust’s test environment for development, testing and staging systems is separate from its production systems.

6.6.2 Security controls in conjunction with computer management

Administration of computers, networks and other components is strictly limited to personnel authorized according to the role concept. Log files are regularly analyzed with a view to rule violations, attempted attacks and other incidents. Audit logging procedures begin when a device is set into operation and end when it is disposed of.

6.6.3 Life cycle security controls

Any devices used are operated in accordance with their manufacturers' instructions. Prior to being set into operation, they are meticulously checked and inspected. They are only set into operation if it is clear beyond any doubt that they were not manipulated. Hardware and software checks, for instance, are sealed in order to be able to detect manipulation and attempted manipulation during any activity or inspection. In the case of suspected manipulation of a component, any action planned will not be carried out and the incident is reported to the TSP manager. In order to enable an immediate and co-ordinated response to any security-relevant incidents, the TSP defines clear-cut escalation rules for the individual roles.

Capacity requirements and utilization as well as the suitability of the systems involved are monitored and adapted as required. Devices exchanged or obsolete data media are taken out of service and disposed of in such a manner that any misuse of functionalities or data is ruled out. Changes in systems, software or processes are subject to a documented change management process. Security-critical modifications are checked by the security officer.

The company's media are safely protected against damage, theft, loss or compromising depending on their respective classification within the scope of the TSP's documentation guideline.

Penetration tests are carried out at least once a year by an independent and competent body. Furthermore, vulnerability scans are initiated at least once every three months. The results of the penetration test report are archived internally.

6.7 Network security controls

A network concept is implemented in trust service operations that ensures that the relevant systems are operated in particularly well-protected network zones. The network architecture of the TSP features a multi-level concept of network security zones. Detailed documentation is available for the network concept and the relevant parts of this can be made available for inspection to any party proving a relevant interest in such disclosure.

In order to protect the processes of the TSP, firewalls and intrusion detection/prevention mechanisms are used, for instance, that only allow expressly permitted connections. The TSP operates network segments with different protection requirements and separates networks for employees and Internet uses on the one hand from server networks on the other. The systems are subject to regular inspection and revision, the employees in charge are accountable. Anomalies are reported by technical systems and organizational processes and addressed by a defined incident handling procedure as well as related processes.

Redundancy ensures the availability of the Internet connection. There are two permanent connections to the provider on two different routes. If the provider's access point fails, the system automatically switches to the second connection.

Cryptographic mechanisms are used to protect data traffic with a high protection demand outside the networks protected by the TSP for which integrity or confidentiality must be ensured.

The physical security of the networks operated and used by the TSP is ensured and adapted to the structural conditions and any changes therein.

6.8 Time stamps

The TSP operates a time stamp service. However, time stamps are not offered within the scope of this TSPS.

7. Profiles of Certificates, Revocation Lists and OCSP

No stipulation.

No certificates are issued as part of the AusweisIDent service. Therefore, AusweisIDent does not operate CRLs or OCSPs to check the revocation status of certificates.

8. Checks and Other Evaluations

Revisions, revision objects and processes are described in detail in D-Trust GmbH's documentation. The role concept documents the qualification and position of the internal auditor.

Documentation is regularly audited by an independent conformity assessment body. Relevant parts of these documents can be inspected against proof of a legitimate interest.

The TSPS meets the requirements for services laid down in ETSI EN 319 401 and BSI TR-03128. A regular assessment by a qualified and independent third party proves conformity. This audit takes place annually. Regular internal audits are additionally carried out.

9. Other Business and Legal Matters

With regard to the corresponding provisions, see section 9 in the CP as well as additionally the General Terms and Conditions [AGB].

TSPS – Trust Service Practice Statement

D-TRUST AusweisIDent

Version 1.3

Copyright UND NUTZUNGSLIZENZ

Anfragen zu einer sonstigen, in der vorgenannten Lizenz nicht enthaltenen Nutzungsart dieses TSPS der D-Trust GmbH sind zu richten an:

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin, Germany
Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	26.07.2019	▪ Initialversion ▪ Zertifizierung des AusweisIDent-Dienstes nach eIDAS
1.1	28.09.2020	▪ Ergänzung in Abschnitt 5.5.2 ▪ Jährliches Review des gesamten CPS
1.2	23.06.2021	▪ Jährliches Review des gesamten CPS ▪ Dieses Dokument „D-TRUST_AusweisIDent_TSPS" wird erweitert um den Dienst des Vor-Ort-Auslesens. Eine Abgrenzung erfolgt durch die Umbenennung des Identifizierungsdienstes von AusweisIDent in AusweisIDent Online. Damit umfasst das Dokument die Dienste: „AusweisIDent Vor-Ort" und „AusweisIDent Online".
1.3	29.11.2022	▪ Ergänzungen in den Abschnitten 1.1, 5.3.4, 5.3.5, 6.6.1, 6.6.3 ▪ Jährliches Review des gesamten CPS

Inhaltsverzeichnis

1. Einleitung

1.1 Überblick

Dieses Dokument ist das Trust Service Practice Statement (TSPS) der von D-Trust GmbH betriebenen AusweisIDent-Dienste:

a. AusweisIDent Vor-Ort und
b. AusweisIDent Online.

AusweisIDent Vor-Ort ist ein Dienst der D-Trust GmbH zum Auslesen von Ausweisdaten zur Übernahme in ein elektronisches Formular.

AusweisIDent Online ist ein Identifizierungsdienst der D-Trust GmbH zur Überprüfung der Identität natürlicher Personen. AusweisIDent Online kann auch in Verbindung mit Vertrauensdiensten gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS) des Europäischen Parlaments eingesetzt werden.

Dieses Dokument gilt für die Überprüfung der Identität natürlicher Personen gemäß der eIDAS-Verordnung sowie gemäß BSI TR-03128 (AusweisIDent Online) und zur Regelung vom Auslesen von Ausweisdaten zur medienbruchfreien Übernahme in elektronische Formulare (AusweisIDent Vor-Ort) gemäß BSI TR-03128. AusweisIDent Vor-Ort ist keine Identifizierung natürlicher Personen nach eIDAS.

Die Struktur dieses Dokuments folgt dem Internet-Standard RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework".

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument ist ein Trust Service Practice Statement (TSPS) gemäß ETSI EN 319 401 und BSI TR-03128.

Dokumentname:	Trust Service Practice Statement zum D-TRUST AusweisIDent
Version	1.3

1.3 PKI-Teilnehmer

Die D-Trust GmbH betreibt im Rahmen ihres AusweisIDent-Verfahrens keine Zertifizierungsstelle und daher gibt es keine PKI-Infrastruktur mit PKI-Teilnehmern.

AusweisIDent umfasst die Dienste AusweisIDent Online und AusweisIDent Vor-Ort.

AusweisIDent Online dient ausschließlich der Identifizierung natürlicher Personen über das Internet mit der Online-Ausweisfunktion des Personalausweises oder des elektronischen Aufenthaltstitels. Diesen Dienst betreibt die D-Trust GmbH und agiert dabei als Identifizierungsdiensteanbieter im Sinne des §2 Absatz 3a des PAuswG i.V. mit §18 PAuswG.

AusweisIDent Online kann von Unternehmen und Behörden, aber auch von einem Trust Service Provider, im Folgenden Service Provider genannt, in Verfahren eingebettet werden, die eine Identifizierung des Kunden oder Bürgers mittels eID auf einem hohen Vertrauensniveau erfordern. Beispiele sind die Eröffnung eines Bankkontos oder das Identifizieren über das Internet (online) für eine digitale Signatur.

AusweisIDent Vor-Ort dient ausschließlich zum Auslesen von Ausweisdaten des Personalausweises oder des elektronischen Aufenthaltstitels zur medienbruchfreien Übernahme der Ausweisdaten in elektronische Formulare. Es ist keine Identifizierung natürlicher Personen nach eIDAS. Diesen Dienst betreibt die D-Trust GmbH und agiert als Diensteanbieter für AusweisIDent Vor-Ort im Sinne des §18a des PAuswG i.V. mit § 21a.

AusweisIDent Vor-Ort kann von Unternehmen und Behörden in Verfahren zur medienbruchfreien Übernahme der Ausweisdaten in elektronische Formulare eingebunden werden. Beispiele sind die

Eröffnung eines Bankkontos, das Abschließen eines Mobilfunkvertrags oder das Einreichen eines Antrages bei einer Behörde vor Ort.

1.3.1 Certification authorities (CA)

Die D-Trust GmbH betreibt im Rahmen ihres AusweisIDent-Verfahrens keine Zertifizierungsstelle.

1.3.2 Registrierungsstellen (RA)

Keine Vorgaben. Siehe Abschnitt 1.3.

Die D-Trust GmbH betreibt im Rahmen ihres AusweisIDent-Verfahrens keine Registrierungsstelle (RA). Siehe Abschnitt 1.3.

1.3.3 Zertifikatsnehmer (ZNE)

Keine Vorgaben. Siehe Abschnitt 1.3.

1.3.4 Zertifikatsnutzer (ZNU)

Keine Vorgaben. Siehe Abschnitt 1.3.

1.4 Verwendung von Zertifikaten

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.[1]

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument

Dieses TSPS wird durch die D-Trust GmbH gepflegt. Der Beauftragte der Geschäftsführung übernimmt die Abnahme des Dokuments.

Dieses TSPS wird jährlich durch den TSP überprüft und ggf. aktualisiert. Eine Änderung wird durch eine neue Versionsnummer dieses Dokumentes kenntlich gemacht.

Kontaktdaten:

D-Trust GmbH
Redaktion
Kommandantenstr. 15
10969 Berlin, Germany

Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Diese Regelungen sind in der CP festgehalten.

1.6.2 Abkürzungen

Diese Regelungen sind in der CP festgehalten.

[1] AusweisIDent Online ist ein Identifizierungsdienst für natürliche Personen und AusweisIDent Vor-Ort ist ein Dienst zum Auslesen von Ausweisdaten zur medienbruchfreien Übernahme in elektronische Formulare.

1.6.3 Referenzen

[AGB]	Allgemeine Geschäftsbedingungen der D-Trust GmbH, aktuelle Version	https://www.bundesdruckerei.de/system/files/dokumente/pdf/AGB-der-bdr-fuer-Vertrauensdienste-und-Zertifizierungsdienste-der-D-TRUST.pdf
[CP]	Certificate Policy – Zertifikatsrichtlinie der D-Trust GmbH, aktuelle Version	http://www.d-trust.net/internet/files/D-TRUST_CP.pdf
BSI TR-03128	Diensteanbieter für die eID-Funktion	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03128/TR-03128_node.html
PAuswG	Personalausweisgesetz	https://www.gesetze-im-internet.de/pauswg/BJNR134610009.html

Weitere Regelungen sind in der CP festgehalten.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der TSP veröffentlicht diese TSPS und weitere prozessrelevante Dokumente auf der folgenden Webseite:

https://www.d-trust.net/de/support/repository

2.2 Veröffentlichung von Informationen zu Zertifikaten

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt. Daher entfällt eine Veröffentlichung von Informationen zu Zertifikaten.

2.3 Häufigkeit von Veröffentlichungen

Dieses TSPS wird veröffentlicht und bleibt mindestens so lange abrufbar wie die Dienste des AusweisIDents auf Basis dieses TSPS angeboten werden.

Die Webseiten des TSP können öffentlich und unentgeltlich 24x7 abgerufen werden.

2.4 Zugriffskontrollen auf Verzeichnisse

Dieses TSPS und weitere prozessrelevante Dokumente können öffentlich und unentgeltlich abgerufen werden. Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom TSP vorgenommen.

Weitere, nicht öffentliche Dokumente, können bei begründetem Interesse auf Nachfrage in den relevanten Teilen ausgegeben werden.

2.5 Zugang und Nutzung von Diensten

Diese Regelungen sind in der CP festgehalten.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

3.2.2 Identifizierung und Authentifizierung von Organisationen

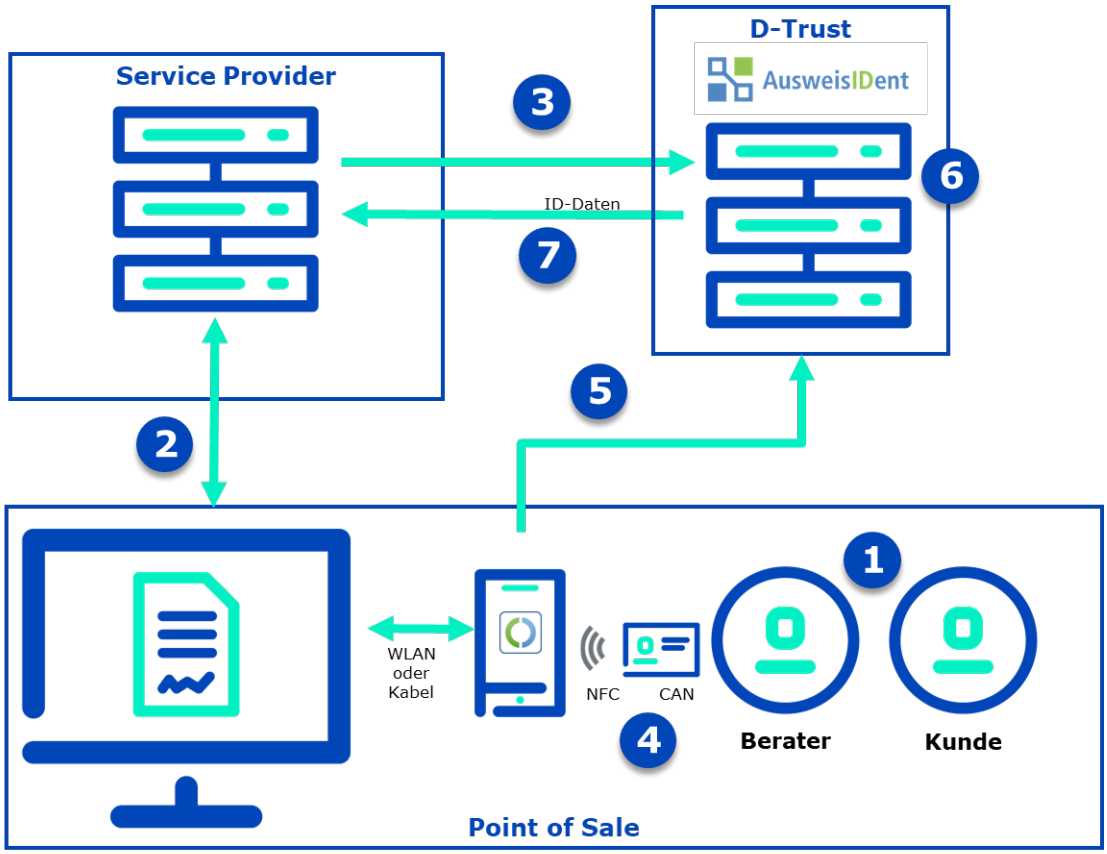
Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen für AusweisIDent

a) Auslesen von Ausweisdaten zur medienbruchfreien Übernahme in elektronische Formulare mit AusweisIDent Vor-Ort

Der Ablauf im Einzelnen:



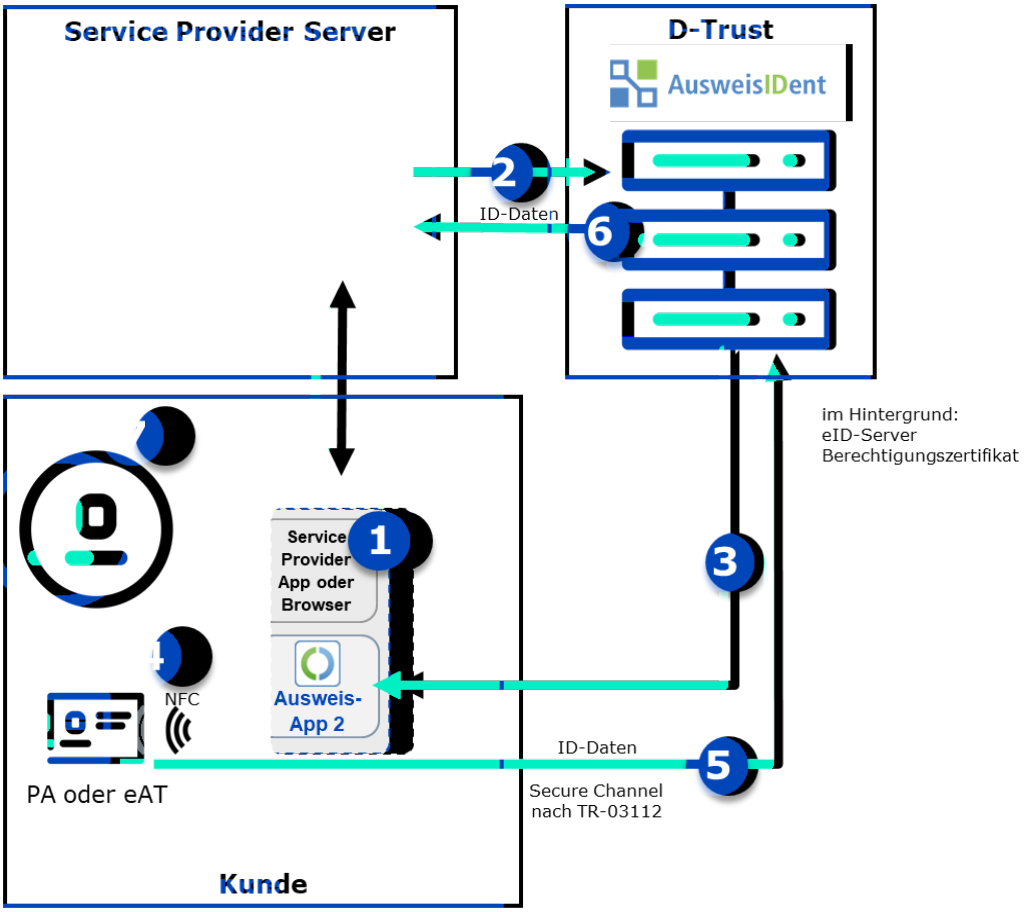
1. Der Berater führt den Lichtbildabgleich mit dem Ausweis des Kunden durch.
2. Der Berater startet den Auslese-Vorgang über sein Terminal beim Service Provider.

3. Der Service Provider stellt einen AuthorisationRequest an den AusweisIDent-Service. Der Auslesevorgang wird durch AusweisIDent über den eID-Service gestartet und gesteuert.
4. Der Berater hält den Ausweis an das Smartphone/Lesegerät des Terminals. Durch Eingabe der CAN wird der Auslesevorgang legitimiert.
5. Der eID-Service liest die Daten via AusweisApp2 aus dem Ausweis aus.
6. AusweisIDent übernimmt den Auslesevorgang und stellt die ausgelesenen Daten über die Schnittstelle bereit.
7. Der Service Provider übernimmt die Ausweisdaten von der Schnittstelle und speichert diese im System. Die Daten werden dem Kundenberater im Webformular angezeigt.

b) Identifizierung und Authentifizierung natürlicher Personen mit AusweisIDent Online

AusweisIDent Online dient der Identifizierung natürlicher Personen über das Internet mit der Online-Ausweisfunktion des Personalausweises oder des elektronischen Aufenthaltstitels. Dieser kann von Unternehmen und Behörden, aber auch von einem Trust Service Provider in Verfahren eingebettet werden, die eine Identifikation des Kunden oder Bürgers mittels eID auf einem hohen Vertrauensniveau erfordern. Der Anbieter von AusweisIDent Online handelt im Auftrag des Service Providers. Beispiele sind die Eröffnung eines Bankkontos, das Abschließen eines Mobilfunkvertrags oder das Einreichen eines Antrages bei einer Behörde.

Der Ablauf im Einzelnen:



1. Der Kunde ruft die App (auf dem Smartphone) oder Webseite (mit dem Browser) des Service Providers auf und will einen Service nutzen. Dazu muss er sich identifizieren und wählt AusweisIDent Online zur Legitimation aus.
2. Der Service Provider Server stellt einen *AuthorisationRequest* an AusweisIDent Online über die OAuth2 / OpenID Connect-Schnittstelle des Dienstes.
3. Der AusweisIDent Online etabliert via eID Server eine nach TR-03113 abgesicherte Verbindung zur AusweisApp2 auf dem Gerät des Kunden (vollintegriert als mobile SDK in Service Provider App oder separat).
4. Der Kunde hält seinen PA oder eAT an ein NFC-fähiges Smartphone oder den Kartenleser am PC und bestätigt das Auslesen der Daten durch Eingabe der geheimen PIN.
5. Die Kundendaten werden vom PA / eAT gelesen und von AusweisIDent Online temporär bis zum Abruf durch den Service Provider gespeichert. Für den Zweck der Identifizierungsprüfung einer natürlichen Person nach eIDAS müssen mindestens die folgenden Attribute für den Identitätsnachweis ausgelesen werden und zur Speicherung an den Service Provider übergeben.
    1. Vorname (n)
    2. Name
    3. Geburtsdatum
    4. Geburtsort
6. Der Service Provider ruft die von AusweisIDent Online signierten personenbezogenen Daten des Kunden ab. Anschließend werden die personenbezogenen Daten des Kunden in AusweisIDent Online gelöscht.
7. Der Kunde ist rechtsicher identifiziert.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

3.2.6 Kriterien für die Interoperabilität

Die Nutzung von AusweisIDent setzt einen Vertrag zwischen Service Provider und Bundesdruckerei bzw. D-TRUST voraus.

Die Schnittstelle zwischen dem Service Provider und AusweisIDent ist in dem „AusweisIDent–Anwenderhandbuch" (aktuelle Verion 1.2.0) beschrieben. Dieses Dokument wird dem Service-Provider spätestens bei Vertragsabschluss ausgehändigt.

Die Schnittstelle zwischen eID-Server und AusweisApp2 (eID-Client) ist in der „Technical Guideline TR-03124-1 eID-Client – Part 1: Specifications" festgelegt.

Zwischen dem Kunden des Service Providers und der Bundesdruckerei bzw. D-TRUST besteht kein Vertragsverhältnis, außer D-TRUST agiert auch als Service Provider.

Das Zusammenspiel von Service Provider, Kunden des Service Providers und der Bundesdruckerei bzw. D-TRUST ist in „3.2.3 Identifizierung und Authentifizierung natürlicher Personen" beschrieben.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying)

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt. Daher findet eine Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung nicht statt.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt. Daher findet eine Identifizierung und Authentifizierung von Sperranträgen nicht statt.

4. Betriebsanforderungen zum Zertifikatslebenszyklus

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt. Daher werden in dem Rahmen auch keine Zertifikatsanträge bearbeitet und es gibt keinen Dienst, der den Status oder die Echtheit von Zertifikaten überprüft.

5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf den AusweisIDent Online als ein Identifizierungsdienst für natürliche Personen und den AusweisIDent Vor-Ort als ein Dienst zum Auslesen von Ausweisdaten zur medienbruchfreien Übernahme in elektronische Formulare, die bei der D-Trust GmbH gemäß ETSI EN 319 401 und BSI TR-03128 betrieben werden.

Die D-Trust GmbH betreibt zertifizierte Managementsysteme gemäß ISO/IEC 27001 sowie ISO 9001. Der Betrieb des TSP unterliegt diesem ISMS. Eine Information Security Policy regelt die verbindlichen Vorgaben für den Betrieb. Diese wurde von der Geschäftsführung der D-Trust GmbH freigegeben und an alle Mitarbeiter des TSP kommuniziert. Es erfolgt ein jährliches als auch anlassbezogenes Review und Update der Security Policy.

Führen prozess- bzw. betriebsbedingte Änderungen zu einem Update der Security Policy, sind die daraus resultierenden Änderungen für den TSP Betrieb von der Geschäftsführung zu genehmigen. Die aktualisierte und genehmigte Security Policy ist zeitnah durch die Führungskräfte an alle davon betroffenen Mitarbeiter zu kommunizieren bzw. bei Bedarf muss die Führungskraft Schulungsmaßnahmen einleiten.

Bis auf vereinzelte Identifizierungsdienstleistungen findet eine Auslagerung von Tätigkeiten an externe Dienstleister im Anwendungsbereich nicht statt. Soweit anwendbar werden notwendige Aspekte der Security Policy für Dienstleister ebenfalls verpflichtend.

5.1 Bauliche Sicherheitsmaßnahmen

Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Die Dokumentation wurde durch eine anerkannte Konformitätsbewertungsstelle geprüft. Die Konformitätsbewertung wird gemäß [EN 319 411-1] und [EN 319 411-2] regelmäßig wiederholt.
Ferner wurde dem Sicherheitsbereich des Trustcenters der D-Trust GmbH durch den TÜV-IT die Anwendung und Umsetzung der „Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3" beurkundet (gemäß Prüfkriterienkatalog für „Trusted Site Infrastructure"). Mit diesem TÜV-IT-Zertifikat „Trusted Site Infrastructure" werden alle Infrastruktur-relevanten Aspekte bewertet. Diese Prüfung wird alle zwei Jahre wiederholt. Das genannte Zertifikat bestätigt der D-Trust GmbH diesen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Teil der Dokumentation ist ein Rollenkonzept, in dem Mitarbeiter einer oder mehrere Rollen durch das Management des TSP zugeordnet werden und entsprechende Berechtigungen durch einen gesteuerten Prozess erhalten. Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Zuordnung der Berechtigungen wird regelmäßig durch das Sicherheitsmanagement revisioniert und umgehend nach Entfall des Bedarfs entzogen.

Rollen mit Sicherheitsverantwortung für den Betrieb des TSP, genannt „Trusted Roles", (mit unter anderem den Aufgaben des Sicherheitsbeauftragten, System Administrator, System Operator, System Auditor, Registration Officer, Revocation Officer und Validation Specialist) werden in den Berechtigungskonzepten der D-TRUST festgelegt. Diese Rollen dürfen nur von fachkundigen und zuverlässigen Mitarbeitern übernommen werden.

Mitarbeiter werden regelmäßig geschult, um ihre Rollen und damit verbundenen Verantwortlichkeiten zu erfüllen und bezüglich der Einhaltung geltender Sicherheitsvorgaben sensibilisiert. Die Anforderungen an die jeweiligen Rollen sind dokumentiert und können von den Mitarbeitern jederzeit eingesehen werden. Bevor Mitarbeiter ihre zugewiesenen Rollen ausüben, müssen sie diesen zustimmen. Im Falle von sich ausschließenden Rollen, kann eine Person nur eine dieser Rollen übernehmen (Vier-Augen-Prinzip). Eine Risikobewertung findet regelmäßig statt.

Mitarbeiter, die im Bereich der Zertifizierungs- und Sperrdienste tätig sind, agieren unabhängig und sind frei von kommerziellen/finanziellen Zwängen, die ihre Entscheidungen und Handlungen beeinflussen könnten. Die organisatorische Struktur des TSP berücksichtigt und unterstützt die Mitarbeiter in der Unabhängigkeit ihrer Entscheidungen.

5.2.2 Mehraugenprinzip

Besonders sicherheitskritische Vorgänge müssen mindestens im Vier-Augen-Prinzip durchgeführt werden. Dies wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen durchgesetzt.

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen, wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen, durchgesetzt. Die durchführende Person muss sich, bevor sie Zugriff auf sicherheitskritische Anwendungen erhält, erfolgreich authentifizieren. Über Event-Logs kann die durchführende Person nachträglich einer Aktion zugeordnet werden; sie ist rechenschaftspflichtig.

5.2.4 Rollenausschlüsse

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern, das Mehraugenprinzip zu erzwingen und schädliches Handeln vorzubeugen.

5.3 Eingesetztes Personal

Der TSP erfüllt die Anforderungen an das Personal aus [EN 319 411-1] und [EN 319 411-2].

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Der TSP gewährleistet, dass die im Bereich des Vertrauensdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen.

Die Identität, Zuverlässigkeit und Fachkunde des Personals wird vor Aufnahme der Tätigkeit überprüft. Regelmäßige und anlassbezogene Schulungen gewährleisten die Kompetenz in den Tätigkeitsbereichen sowie die allgemeine Informationssicherheit. Schulungen und Leistungsnachweise werden dokumentiert.

Insbesondere Führungskräfte werden nach speziellen Kriterien ausgewählt. Sie müssen nachweisen, dass sie in Bezug auf den bereitgestellten Vertrauensdienst über Kenntnisse der Sicherheitsverfahren für Mitarbeiter mit Sicherheitsverantwortung und über ausreichende Erfahrung in Bezug auf Informationssicherheit und Risikobewertung verfügen. Nachweise können in Form von Zertifikaten und Lebensläufen erbracht werden. Kann die erforderliche Qualifikation nicht ausreichend nachgewiesen werden, muss diese durch eine entsprechende Schulungsmaßnahme erworben werden bevor der Mitarbeiter im TSP Betrieb Managementfunktionen übernehmen darf.

5.3.2 Sicherheitsprüfungen

Personen, die in sicherheitsrelevanten Bereichen des TSP tätig sind, müssen unter anderem regelmäßig polizeiliche Führungszeugnisse vorlegen.

Übergreifend betreibt der TSP ein nach ISO 27001 sowie ein ISO 9001 zertifiziertes Managementsystem. Hierdurch werden den Mitarbeitern entsprechend sicherheitsrelevante Vorgaben bzw. Verhaltensregeln zugänglich gemacht.

5.3.3 Schulungen

Der TSP schult Personen, die im Vertrauensdienst tätig sind.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Der TSP schult Personen, die im Vertrauensdienst tätig sind zu Beginn ihres Einsatzes, jährlich und bei Bedarf.

5.3.5 Häufigkeit und Folge von Job-Rotation

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden jährlich geschult.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Der TSP schließt unzuverlässige Mitarbeiter von den Tätigkeiten im Vertrauensdienst aus.

Verstöße von Mitarbeitern gegen die Richtlinien oder die Prozesse des TSP-Betriebs werden analysiert und bewertet. Kann das Vertrauensverhältnis nicht sichergestellt werden, werden diese Mitarbeiter von sicherheitsrelevanten Tätigkeiten ausgeschlossen.

5.3.7 Anforderungen an freie Mitarbeiter

Entfällt; freie Mitarbeiter werden nicht eingesetzt.

5.3.8 Ausgehändigte Dokumentation

Umfangreiche Verfahrensanweisungen definieren für alle Produktionsschritte die zuständigen Mitarbeiterrollen und -rechte sowie entsprechende manuelle und maschinelle Prüfungen. Durch die sicherheitstechnische Infrastruktur der D-Trust GmbH ist gewährleistet, dass von diesen definierten Verfahren im Produktionsbetrieb nicht abgewichen werden kann.

5.4 Überwachungsmaßnahmen

5.4.1 Überwachung des Zutritts

Der TSP betreibt umfangreiche Überwachungsmaßnahmen (beispielsweise durch Videoüberwachung) zur Absicherung der Vertrauensdienstleistungen und deren zugrundeliegenden IT-Systemen und Dokumenten.

Die Überwachungsmaßnahmen werden durch organisatorische Regelungen ergänzt. Beispielsweise sieht die Besucherregelung unter anderem vor, dass Besucher mindestens 24 Stunden vor dem Besuch namentlich angemeldet sein müssen. Im Bereich des Trustcenters müssen Besucher stets in Begleitung eines Mitarbeiters des TSP sein.

5.4.2 Überwachung von organisatorischen Maßnahmen

Ein weiterer Bestandteil ist die Überwachung von organisatorischen Maßnahmen.

Hierzu gehört eine regelmäßige Risikoanalyse, die die Bedrohung für den Betrieb des TSP umfassend analysiert sowie Anforderungen und Gegenmaßnahmen definiert. Ferner ist eine Restrisikoanalyse enthalten, in der die Vertretbarkeit des Restrisikos aufgezeigt und ggf. akzeptiert wird.

Weiterhin werden relevante Assets angemessen erfasst, sowie entsprechende Änderungen dieser Assets überprüft bzw. wenn anwendbar durch das vom Management beauftragte Personal des TSP freigegeben.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Personenbezogene Daten werden nach Übernahme durch den Service Provider in AusweisIDent gelöscht, spätestens aber nach 10 Minuten, und nicht archiviert.

System-Logs mit Zugriffsdaten (Datum/Uhrzeit, Ankommender IP-Adresse, Client-ID, den Namen der ausgelesenen Felder, Redirect-URI) werden auf dem Server nach 90 Tagen gelöscht.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Die personenbezogenen Daten werden nach Übernahme durch den Service Provider in AusweisIDent (sowohl in AusweisIDent Online als auch AusweisIDent Vor-Ort) gelöscht. Eine Archivierung von personenbezogenen Daten findet nicht statt

Eine Archivierung findet weder im Rahmen des Identifizierungsdienstes durch das AusweisIDent Online noch im Rahmen des AusweisIDent Vor-Ort statt.

Event-Logs der IT-Systeme werden mindestens 6 Monate gespeichert. Die Speicherdauer von Aufzeichnungen der administrativen Tätigkeiten beträgt 90 Tage.

Für das Archivierungssystem wird die Systemzeit über DCF77 täglich gegen die offizielle Zeit synchronisiert.

5.5.3 Sicherung des Archivs

Eine Sicherung des Archivs entfällt, da personenbezogene Daten im Rahmen des AusweisIDent nicht archiviert werden.

5.5.4 Datensicherung des Archivs

Keine Vorgaben.

Es erfolgt keine Archivierung von personenbezogenen Daten im Rahmen des AusweisIDent.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Keine Vorgaben.

5.5.6 Archivierung (intern / extern)

Keine Vorgaben.

Es erfolgt keine Archivierung von personenbezogenen Daten im Rahmen des AusweisIDent.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Keine Vorgaben.

Es erfolgt keine Archivierung von personenbezogenen Daten im Rahmen AusweisIDent.

5.6 Schlüsselwechsel beim TSP

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

5.7 Kompromittierung und Geschäftsweiterführung beim TSP

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren für die Wiederherstellung der Betriebsfähigkeit des TSP. Es erfolgt ein tägliches Backup und ein Backup nach Veränderungen. Backups werden in einem anderen Brandabschnitt aufbewahrt.

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Der TSP verfügt über ein Notfallkonzept sowie einen Wiederanlaufplan, die den beteiligten Rollen bekannt sind und von ihnen im Bedarfsfall umgesetzt werden. Die Verantwortlichkeiten sind klar verteilt und bekannt.

Sollte eine System Recovery erforderlich sein, sind die Verantwortlichkeiten und entsprechenden „Trusted Roles" im Berechtigungskonzept der D-TRUST deklariert und den jeweiligen Mitarbeitern bekannt. Siehe Abschnitt 5.2.1.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren für die Wiederherstellung der Betriebsfähigkeit des TSP.

5.7.3 Kompromittierung des privaten CA-Schlüssels

Keine Vorgaben.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach Kompromittierung und Desaster

In einem Notfall entscheidet der TSP je nach Art des Vorfalls, ob ein Recovery durchgeführt wird und ergreift Maßnahmen, um eine Wiederholung zu vermeiden.

5.8 Beendigung der AusweisIDent Dienste

Die ausgelesenen personenbezogenen Daten werden signiert und nur bis zur Übergabe an den Service Provider temporär zwischengespeichert. AusweisIDent selbst archiviert keine personenbezogenen Daten.

Mit der Übergabe der signierten personenbezogenen Daten ist der Vorgang rechtlich abgeschlossen.

Im Fall einer Beendigung von AusweisIDent werden damit in Verbindung stehende Dienste nicht mehr angeboten. Etwaige Verpflichtungen zur Archivierung von Informationen zu Geschäftsvorfällen übernimmt der Kunde.

6. Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

6.4 Aktivierungsdaten

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

Die D-TRUST betreibt ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001. Der Betrieb des TSP unterliegt diesem ISMS. Eine Security Policy regelt die verbindlichen Vorgaben für den IT Betrieb. Diese wurde von der Geschäftsführung der D-Trust GmbH freigegeben und an alle Mitarbeiter des TSP kommuniziert. Es erfolgt ein jährliches als auch anlassbezogenes Review und Update der Security Policy.

Die Bewertung und ggf. die Behebung von identifizierten Schwachstellen erfolgt innerhalb von 48 Stunden. Ist die Behebung innerhalb von 48 Stunden nicht möglich, so enthält die Bewertung einen konkreten Behandlungsplan.

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die vom TSP eingesetzten Computer, Netze und andere Komponenten stellen in der eingesetzten Konfiguration sicher, dass nur Aktionen durchgeführt werden können, die nicht im Widerspruch zu diesem TSPS und [EN 319 411-1] bzw. [EN 319 411-2] stehen.

Die Computersicherheit des TSP wird für exponierte Systeme u.a. durch mehrstufige Sicherheitssysteme zum Zwecke des perimetrischen Virenschutzes, Endpoint-Protection und integritätssichernde Werkzeuge sichergestellt.

Es wird sichergestellt, dass sicherheitsrelevante Softwareupdates in angemessener Zeit auf den relevanten Systemen installiert werden. Abweichungen hiervon werden vom TSP angemessen dokumentiert und ggf. im Risikomanagement des TSP adressiert.

6.5.2 Beurteilung von Computersicherheit

Die für dieses Verfahren eingesetzten Computer, Netze und andere Komponenten unterliegen gemäß [EN 319 401] einem entsprechenden Monitoring.

6.5.3 Monitoring

Zur Sicherstellung der Verfügbarkeit des AusweisIdents erfolgt ein kontinuierliches Monitoring der relevanten Systeme. Jede Störung wird erfasst, dokumentiert und gemäß ihrer Auswirkung mit einem Schweregrad gekennzeichnet und daraufhin priorisiert. Die Behandlung von kritischen Meldungen erfolgt im Rahmen des Prozesses Incident Management. Meldungen zu sicherheitsrelevanten Ereignissen werden an eine zentrale Stelle übermittelt und gemäß Kritikalität ausgewertet.

Bei Störungen mit Verfügbarkeitsverlust eines Services werden die betroffenen Parteien mindestens alle 24 Stunden über einen aktuellen Status zur Störungsbeseitigung informiert.

6.6 Technische Maßnahmen während des Life Cycles

Bereits bei der Planung aller vom TSP oder im Auftrag des TSP betriebener Systeme werden die Anforderungen aus Abschnitt 5 [BRG] angemessen berücksichtigt.

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Bei der Entwicklung aller vom TSP oder im Auftrag des TSP durchgeführter Systementwicklungsprojekte werden Sicherheitsanforderungen im Entwurfsstadium analysiert. Die gewonnenen Erkenntnisse werden als Anforderungen bei der Entwicklung festgelegt.

Die Testumgebung der D-Trust für Entwicklungs-, Test- und Staging-Systeme ist getrennt von ihren Produktionssystemen.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Ausschließlich entsprechend dem Rollenkonzept autorisiertes Personal darf Computer, Netze und andere Komponenten administrieren. Es findet eine regelmäßige Auswertung von Logfiles auf Regelverletzungen, Angriffsversuche und andere Vorfälle statt. Überwachungsmaßnahmen beginnen mit Inbetriebnahme eines Gerätes und enden mit dessen Entsorgung.

6.6.3 Sicherheitsmaßnahmen während des Life Cycles

Eingesetzte Geräte werden gemäß Herstellerangaben betrieben. Vor Inbetriebnahme werden sie eingehend geprüft und kommen nur zum Einsatz, wenn zweifelsfrei feststeht, dass sie nicht manipuliert wurden. Durch Versiegelung der Hardware und Softwarechecks beispielsweise werden Manipulationen und Manipulationsversuche bei jeder Aktion oder Revision erkennbar. Bei Verdacht auf Manipulation einer Komponente, wird eine ggf. geplante Aktion an der Komponente nicht durchgeführt und der Vorfall dem TSP-Leiter gemeldet. Um kurzfristig und koordiniert auf eventuelle sicherheitsrelevante Vorfälle reagieren zu können, definiert der TSP klare Eskalationsrichtlinien für die einzelnen Rollen.

Kapazitätsanforderungen und -auslastungen sowie Eignung der beteiligten Systeme werden überwacht und bei Bedarf angeglichen. Ausgetauschte Geräte oder obsolete Datenträger werden derart außer Betrieb genommen und entsorgt, dass Funktionalitäts- oder Datenmissbrauch ausgeschlossen wird. Änderungen an Systemen, Software oder Prozessen durchlaufen einen dokumentierten Change-Management-Prozess. Sicherheitskritische Änderungen werden durch den Sicherheitsbeauftragten geprüft.

Die Medien des Unternehmens werden entsprechend ihrer Klassifizierung im Rahmen der Dokumentationsrichtlinie des TSP zuverlässig vor Schaden, Entwendung, Verlust oder Kompromittierung geschützt.

Penetrationstests werden durch eine unabhängige und fachkundige Stelle mindestens einmal pro Jahr durchgeführt. Weiterhin werden mindestens einmal pro Quartal Schwachstellenscans veranlasst. Die Ergebnisse des Penetrationstestberichts werden intern archiviert.

6.7 Sicherheitsmaßnahmen für Netze

Im Betrieb des Vertrauensdienstes wird ein Netzkonzept realisiert, welches sicherstellt, dass die relevanten Systeme in gesicherten Netzwerkzonen betrieben werden. Die Netzwerkarchitektur des TSP beinhaltet ein mehrstufiges Konzept der Netzwerksicherheitszonen. Für das Netzkonzept liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Zum Schutz der Prozesse des TSP werden beispielsweise Firewall und Intrusion Detection / Prevention Mechanismen eingesetzt, die nur explizit erlaubte Verbindungen zulassen. Der TSP betreibt Netzsegmente unterschiedlichen Schutzbedarfs und trennt dabei Mitarbeiter- und Internet-nahe Netze sorgfältig von Servernetzwerken. Die Systeme unterliegen regelmäßigen Revisionen, die Verantwortlichen sind berichtspflichtig. Auffälligkeiten werden durch technische Systeme und organisatorische Prozesse gemeldet und in einem definierten Incidentverfahren und daran ansetzenden Prozessen behandelt.

Die Verfügbarkeit der Internetanbindung ist durch Redundanz abgesichert. Es bestehen zwei ständige Verbindungen zum Provider auf zwei unterschiedlichen Streckenführungen. Beim Ausfall des Zugangspunktes des Providers erfolgt die automatische Umschaltung auf die zweite Anbindung.

Datenverkehr mit hohem Schutzbedarf außerhalb der durch den TSP geschützten Netzwerke, für den Integrität oder Vertraulichkeit sichergestellt werden muss, wird durch kryptographische Mechanismen geschützt.

Die physische Sicherheit der durch den TSP betriebenen und genutzten Netze ist sichergestellt und wird den baulichen Gegebenheiten und ihren Veränderungen angepasst.

6.8 Zeitstempel

Der TSP betreibt einen Zeitstempeldienst. Zeitstempel werden im Rahmen dieses TSPS jedoch nicht angeboten.

7. Profile von Zertifikaten, Sperrlisten und OCSP

Keine Vorgaben.

Im Rahmen des AusweisIDents werden keine Zertifikate ausgestellt. Daher betreibt der AusweisIDent weder CRLs noch OCSPs zur Überprüfung des Sperrstatus von Zertifikaten.

8. Überprüfungen und andere Bewertungen

Revisionen, Revisionsgegenstände und Prozesse sind detailliert in der Dokumentation der D Trust GmbH beschrieben. Das Rollenkonzept dokumentiert die Qualifikation und die Stellung des Revisors.

Die Dokumentation wird regelmäßig durch eine unabhängige Konformitätsbewertungsstelle geprüft. Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden.

Die TSPS erfüllt für Dienste die Anforderungen gemäß ETSI EN 319 401 und BSI TR-03128. Ein regelmäßiges Assessment durch einen qualifizierten und unabhängigen Dritten belegt die Konformität. Diese Auditierung findet jährlich statt. Darüber hinaus finden regelmäßig interne Audits statt.

9. Sonstige finanzielle und rechtliche Regelungen

Bezüglich der entsprechenden Regelungen wird auf Kapitel 9 in der CP sowie ergänzend die [AGB] verwiesen.