identity Management: Certification Practice Statement

Document information

Version	2.1
Version date	15.11.2024
Status	☐ In review since: July 2016 ☐ submitted on: ☒ approved/finalized
Confidentiality level	Public
Approved by	CTO
Owner of the document	ISO
Document name	identity Management: Certification Practice Statement
Distribution	

Table of Contents

1 Introduction

IDnow GmbH is an identification services provider offering services in the field of verification of identities of natural persons and legal entities and obtaining signatures.

The services identity Shop, identity PoS, identity Video, identity eID, identity autoID provided by IDnow GmbH, have already been certified and confirmed as being compliant with the eIDAS regulation and German Vertrauensdienstegesetz (VDG) and Vertrauensdiensteverordnung (VDV). The modular confirmation allowed certification services providers to use these services for identity verifications in the process of issuing qualified certificates.

In addition, IDnow GmbH offers the service identity e-Sign consisting of identity Video, the generation of a qualified certificate by a CA, and the qualified signature of a document using the qualified certificate provided by the CA.

This document is the CPS of IDnow GmbH. It is not a full CPS according to RFC 3647, because IDnow GmbH only covers the aspect of identity proofing, registration, and operations authority for the CA, 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 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 401.

This document is **public** information. Information owner is the *Security Officer*.

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, IDnow GmbH 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 IDnow GmbH 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 Trusted Service Provider Law (VDG).

IDnow GmbH provides the following services.

identity Shop: 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 is performed by contractually bound and affiliated ident partners or directly in identity`s shops.

identity PoS (Point of Sale): Identification of the natural person to be identified by means of the physical presence of the person to be identified. The person to be identified will visit the PoS partner shop and the agent then performs the actual act of identification at the point of sale in order to enable the natural person to sign documents with a qualified electronic signature. IDnow GmbH is responsible for the control of the identification software in the partners PoS system. Identity PoS is performed by partners, connected by means of a proprietary, uniform and standardized software (identity PoS).

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 IDnow 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 eSign: Identification of a natural person using the identity Video service and receipt of a document provided by the customer. The document and the identification data of the identity Video session are then delivered to the CA. The CA then issues a qualified certificate and signs the document with that certificate. The signed document and identification proofs are returned to the customer.

identity autoID: Identification of a natural person using an AI- and machine-learning based software that was developed by IDnow GmbH and which conformity has already been assessed (TUVIT.97174.TSP.06.2021).

IDnow GmbH 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 IDnow GmbH for the identification procedures identity Shop, identity PoS, identity Video, identity eID, identity autoID and identity e-Sign.”

This document goes into effect upon its publishing. It loses its validity upon its replacement or when being succeeded by an updated version.

1.3 PKI Participants

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA. IDnow GmbH provides identity verification. It serves as RA for the CA for short- or long-lived qualified certificates used for document signing.

1.4 Certificate Usage

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH provides several identity verification services which are not related to certificate issuance. Certificates issued by the CA in the context of identity e-Sign can be used for document signing only.

1.5 Policy Administration

Changes to this document need to be approved by the management of IDnow GmbH. As IDnow GmbH is also operating as registration authority for the CA this CPS must also be approved by the CA. After approval, the changed version is made available as stated. The CPS is reviewed after major process changes or at least annually, as part of the internal audit and is adapted if necessary.

This CPS is administered by:	Contact Person:
IDnow GmbH Auenstraße 100 80469 München Deutschland	Security Officer IDnow GmbH Lierenfelder Straße 51 40231 Düsseldorf hone: +49 211 68 77 3-0 E-Mail: sicherheit@identity.tm

1.6 Change log

Version	Date	Changes
1.0	31.07.2016	Initial version
1.1	31.10.2016	Inclusion of identity e-Sign
1.1.1	12.07.2017	Inclusion of identity Shop Papierlos and identity PoS
1.1.2	23.01.2018	Inclusion of D-Trust as CA
1.1.3	02.02.2018	Changes during and after TÜVIT audit
1.2	19.02.2018	Final Version
1.2.1	16.07.2018	Added identity Giro procedure and Trusted Role
1.2.2	30.07.2018	Minor corrections
1.3	30.07.2018	Final Version
1.3.1	02.12.2019	Added eSign with Namirial, removed DocuSign
1.3.2	07.08.2020	Removed TSP specific policies
1.3.3	19.08.2020	Revision Personnel Controls, Added Accessibility
1.4	20.08.2020	Minor clarification security officers
1.4.1	29.09.2020	Appointment procedure added to Personnel Controls
1.5	02.10.2020	Approved Version
1.6	04.11.2021	Added product identity autoID
1.6.1	16.11.2021	Minor corrections
1.6.2	01.02.2022	Updated document due to change of legal form from AG to GmbH
1.6.3	30.05.2022	Removal of identity Kurier and identiy Giro
1.7	28.07.2022	Approval
1.7.1	23.08.2022	Removed document version from chapter 1.2, approved
1.8	24.01.2023	Integration document for IDN merger, also rectified version to 1.8
1.8.1	03.01.2024	Review and Repository Update
1.9	04.01.2024	Approval
1.9.1	20.08.2024	Notification about termination extended from 2 to 3 months
2.0	20.08.2024	Approval
2.0.1	15.11.2024	Added reference to PRADO as ID card and passport register
2.1.	15.11.2024	Approval

2 Publication and Repository Responsibilities

2.1 Repositories

Relevant documents, including this CPS and the General Terms and Conditions, of IDnow GmbH are available for download at https://www.idnow.io/certification-policies/.

Documents related to the qualified certificates issued by D-Trust for identity eSign and PoS are published by D-Trust. The underlying CP for sign-me are available as follows: https://www.bundesdruckerei.de/de/2833-repository

Documents related to the qualified certificates issued by Namirial S.p.A. for identity eSign and PoS are published by D-Trust. The underlying CP for sign-me are available as follows: https://support.namirial.com/en/docs/docs-tsp/#docs_compliance

Publication of certificate information: IDnow GmbH does not issue certificates. IDnow GmbH provides only identity verification and RA functionality for the CA.

2.2 Time and frequency of publications

The latest version of this CPS is available for download under www.idnow.io the official website of IDnow GmbH. 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.

The websites of IDnow GmbH 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, IDnow GmbH will undertake all efforts to ensure that the necessary information will be made available again as soon as possible.

2.3 Accountabilities and responsibilities

The contact person for questions regarding this document is the Chief Information Security Officer. Every employee of IDnow GmbH, as well as external personnel is responsible for working in accordance with this policy.

The management of the respective organisation is responsible for the implementation and validity of the security concept.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

3.1.2 Need for names to be meaningful

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

3.1.3 Anonymity and Pseudonymity of certificates

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

3.1.4 Rules of Interpreting various name forms

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

3.2 Initial identity validation

3.2.1 Methods to prove possession of private key

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

3.2.2 Authentication of organization entity or legal persons

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH does not authenticate organizations or 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. A register of widely accepted ID cards and passports can be found here:

https://www.consilium.europa.eu/en/documents-publications/

For the Shop processes, the applicant has to appear in person and a standard paper form or a completely digital data set (in cases of identity Shop papierlos and Identity PoS) 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 IDnow GmbH's databases.

In case of identity autoID process an OCR-Software automatically recognizes valid ID documents, capture images and extracts the identification data. The software is checking the authenticity of security features like holograms with real-time, video-based analysis and conducts biometric verification by comparing the user’s biometrics of the photo on their ID document with a selfie check.

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.

3.2.4 Non-verified subscriber information

IDnow does not submit non-verified data to the CA. Dual control ensures that data can be submitted only if approved by an identity proofing agent and a second person.

3.3 Identification and Authentication of Re-key Requests

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH 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

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

3.5 Accessibility

If possible IDnow GmbH provides its identification services to people with disabilities. The provision of end-user products for the use of the trust service is generally not required and is not offered by IDnow GmbH.

IDnow GmbH however offers the Trust Service Providers different kind of services (identity Video, identity eiD, identity Shop, identity autoID) that combined provides the necessary access required. The decision which kind of these services gets offered to the end user is made by the Trust Service Provider.

4 Certificate Life-Cycle Operational Requirements

Chapter 4 and subchapters are applicable only for the service identity e-Sign and identity PoS. There is no stipulation for other services because all other services provided by IDnow are not related to certificate issuance.

4.1 Certificate application

4.1.1 Who can submit a certificate application

From the perspective of the CA IDnow GmbH serves as RA and certificates can be requested by IDnow GmbH only after the identification and registration of the subscriber have been successfully completed.

From the perspective of IDnow GmbH everybody can submit an application.

4.1.2 Enrolment process and responsibilities

From the perspective of IDnow GmbH the typical application is not initiated by entering the applicant's personal data and the document to be signed in a web-frontend of IDnow GmbH.

Instead, the applicant logs into the website of one of IDnow GmbH's partners and initiates the identity e-Sign/PoS process at the partner's site or in a Point of Sale.

At the partner's website the applicant enters his/her personal data (first name, last name, date of birth, place of birth, nationality, address, phone number, e-mail address) and reads/prints/stores the document which is to be signed.

IDnow's partner includes the applicant's personal data in a pdf file and submits the pdf file together with the document to be signed to IDnow GmbH.

In the PoS procedure the collection of the applicant's data and the document to be signed can also be handled by the agent in the Point of Sale.

4.2 Certificate application processing

After IDnow has received the applicant's data and the document to be signed the applicant initiates the session for the identity Video or PoS process.

After verification of the applicant's personal data in the identity Video or identity PoS process IDnow GmbH submits all data, including the proofs for identity verification and the document, to the CA.

4.2.1 Performing identification and authentication functions

By starting the video session for eSign the applicant and an identification agent enter into a video conference. The agent conducts a video identification which is compliant with the German Trusted Service Provider Law (VDG) and with the eIDAS regulation 910/2014. The agent verifies that the applicant presents a valid ID document and that the personal data of the ID document match with the data collected by the partner organization in 4.1.2.

In the PoS procedure the agent conducts an identification which is also compliant with the German Trusted Service Provider Law (VDG) and with the eIDAS regulation 910/2014. The agent verifies that the applicant presents a valid ID document and that the personal data of the ID document match with the data collected by the partner organization in 4.1.2.

In a second step a second agent repeats the identification. Only if both agents approve the positive identification of the applicant the identification is considered successful.

After the identification has been successfully completed all data collected is submitted to the CA.

4.3 Certificate issuance

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow does not issue certificates. Certificates are issued by the CA.

4.4 Certificate acceptance

4.4.1 Conducting certificate acceptance

After the certificate has been issued and the document has been signed the certificate owner can download the signed document. Alternatively, the signed document can be sent by e-mail. The signature on the document includes the certificate.

The certificate owner is responsible to check the certificate for correctness.

If the certificate owner does not want to accept the certificate he/she may request revocation of the certificate after the certificate has been issued. If the certificate owner does not revoke the certificate it is considered as accepted.

4.4.2 Publication of the certificate

Neither CA nor IDnow publish the certificate. The certificate is contained in the signed document and can be made available by the certificate owner.

4.4.3 Notification of certificate issuance

IDnow and the certificate owner are notified of the certificate issuance. No other entities are notified.

4.5 Key pair and certificate usage

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

4.6 Certificate renewal

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

4.7 Certificate re-key

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

4.8 Certificate modification

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

4.9 Certificate revocation and suspension

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

4.10 Certificate status service

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA. Certificate status service is operated by the given CA.

4.11 End of subscription

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

4.12 Key escrow and recovery

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

At no point in time is IDnow in possession of private keys associated with the customer's certificates. Key escrow or recovery is not possible.

Private EE keys are generally and exclusively generated and stored by the TSP. A specific procedure for key depositing is not offered.

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

Electronic identification data of all identification processes as well as the electronic document submitted during the identity e-Sign process 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.

IDnow GmbH 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 IDnow GmbH. 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 IDnow GmbH. 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

IDnow GmbH 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 IDnow GmbH'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
- Registration Officers: responsible for verifying information that is necessary for certificate issuance and approval of certification requests
- System Auditors: authorized to review archives and audit logs of the systems.

Access to systems or applications is only granted after the appointment to a trusted role. The roles according to the security concept of IDnow are mapped as follows.

- Security Officers = Security Officer. Additionally, the Head of QA serves as deputy Security Officer. Security Officers are personally appointed by the CEO.
- System Administrators = System Administrators ("IT-Dienst" and the less privileged role "Prozessmanagement"). System Administrators are personally appointed by the CEO.
- System Operators = All operational roles such as Identifiers (Responsible for the identification of applicants and the documentation of the identification results) and Verifiers (HUB-Prüfer; Responsible for the verification of applicants from another

Identifier and the documentation of the identification results). The appointment of System Operators is done by signing an employment contract that contains the role's responsibilities. The appointment of System Operators who are not employed by IDnow GmbH is done by providing and revoking the system access of the identifiers. Authorized to provide and revoke access are according to the security concept the roles "IT-Dienst", "Geschäftsführung", all Head Of Departments, "Qualitätsmanagement" and "Digitalisierungszentrum".

- Registration Officers = All operational roles such as Identifiers (Responsible for the identification of applicants and the documentation of the identification results) and Verifiers (HUB-Prüfer; Responsible for the verification of applicants from another Identifier and the documentation of the identification results). The appointment of Registration Officers is done by signing an employment contract that contains the role's responsibilities. The appointment of System Operators who are not employed by IDnow GmbH is done by providing and revoking the system access of the identifiers. Authorized to provide and revoke access are according to the security concept the roles "IT-Dienst", "Geschäftsführung", all Head Of Departments, "Qualitätsmanagement" and "Digitalisierungszentrum".
- System Auditors = CTO ("IT-Dienst"). The CTO is the only one granted administrative access to audit logging procedures as described in chapter 5.4.

5.4 Audit Logging Procedures

System events are logged on a server dedicated for system logging. All attempts to access the IT infrastructure of IDnow GmbH 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 and document signing activities are logged in the business software of IDnow GmbH.

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, IDnow GmbH 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 IDnow GmbH are logged to this server, indicating the type as well as the time of the event.

5.5 Records Archival

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

5.6 Key Changeover

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH 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 IDnow GmbH informs the relevant supervisory authority, the CA, and other customers at least three months in advance about this fact.

All documentation relevant for the CA and the customers will be provided for collection at designated interfaces. The CA and 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

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH is only performing identification services and document signing services. IDnow GmbH does not issue certificates on its own.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH is only performing identification services and document signing services. IDnow GmbH does not issue certificates on its own.

6.3 Other Aspects of Key Pair Management

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH is only performing identification services and document signing services. IDnow GmbH does not issue certificates on its own.

6.4 Activation Data

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow GmbH is only performing identification services and document signing services. IDnow GmbH does not issue certificates on its own and does not handle customer’s activation data.

6.5 Computer Security Controls

- IDnow GmbH 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 IDnow'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 IDnow GmbH, is only possible for authorized employees after successful authentication. Every authorized user is allocated to a role that defines the rights that are granted to the user. Each user has its own credentials to authenticate to the systems.

- 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 IDnow GmbH. 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.

IDnow GmbH 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 IDnow GmbH 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 IDnow's security concept.

All infrastructural components are permanently monitored for correct function.

6.8 Timestamping

No stipulation. IDnow GmbH does not issue time-stamps

7 Certificate, CRL, and OCSP Profiles

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

IDnow Services GmbH is only performing identification services and document signing services. IDnow Services GmbH does not issue certificates or provide CRL or OCSP services.

8 Compliance Audit and Other Assessment

8.1 Frequency and circumstances of compliance audit

- Audits for compliance with the German Geldwäschegesetz (prevention of money laundering act), the De-Mail act with its technical guidelines, the German Trusted Service Provider Law (VDG) and eIDAS are performed on a regular basis. Some customers may perform additional, annual third-party audits in order to fulfil their outsourcing responsibilities.
- In addition, as IDnow GmbH is operating as RA for the CA, IDnow GmbH undergoes regular audits in order to prove compliance with CA´s CP/CPS, ETSI EN 319 401, 319 411-1 and 319 411-2.

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 Trusted Service Provider 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) or European equivalents to perform such audits and certifications. They are independent from IDnow GmbH.

8.4 Topics covered by audit

This chapter relates to the services of the Certificate Authority as Trusted Service Provider and is specified in relevant service-based Policy and/or Practice Statement of the CA.

8.4.1 Actions taken as a result of deficiency

In case of identified deficiencies, an action and remediation plan will be agreed between IDnow GmbH and the auditors.

8.5 Communication of results

Audit results are communicated to the responsible supervisory bodies. Audit results related to the RA functionality are communicated to the respective CA.

9 Other Business and Legal Matters

9.1 Fees

Fees will be negotiated individually between IDnow GmbH and the cooperation partners.

9.2 Financial Responsibility

IDnow GmbH 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

IDnow GmbH 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

IDnow GmbH has committed itself to the principle of acquiring, processing or using as little personal data as possible. IDnow GmbH 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 IDnow GmbH 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.

Personal data collected during the identification and registration for identity e-Sign is processed only for

i) enabling the RA to identify and authenticate the applicant if required
ii) conducting the identity checks required for the issuance or revocation of a qualified certificate

iii) including the applicant's name in the certificate.

9.4.2 Principles on data acquisition and disclosure

For 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 are 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.

IDnow GmbH 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.

IDnow GmbH 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 must 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, IDnow GmbH 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.

IDnow GmbH 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

IDnow GmbH 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.

9.6 Representations and warranties

- IDnow ensures that each subscriber for which a certificate application is submitted to the CA has been identified and authenticated properly and that certificate requests are accurate, complete, and duly authorized.
- IDnow informs subscribers about the general terms and conditions regarding the use of a certificate before submitting a certificate request to the CA. The subscriber must confirm this by clicking on a check box on the screen.
- IDnow supports the audit teams in a constructive way and makes any reasonable effort needed to complete an audit and to communicate the results.
- IDnow alerts the CA in case of a security incident related to RA functionality.
- IDnow protects its information systems and guarantees the security of the data transmitted to the PKI.

IDnow.

Signed by: Armin Bauer

EMail: armin.bauer@idnow.io
Signing time: 18-11-2024 12:17:08

IDnow.