iDenfy Identity Proofing Practice Statement

Introduction

Overview

iDenfy provides identity verification services to verify customers' identities online safely and quickly. ID verification is combined with identity document verification and face comparison. Identity verification is done by the automated system, but the final decision is made by iDenfy's registration officer.

Document Name and Identification

iDenfy Practice Statement, IDENTIFICATION iDenfy Trust Service Practice statement has been assigned the following OID: 1.3.6.1.4.1.59462.1.1.1.0.0

PKI Participants

No stipulation

Certificate Usage

No stipulation

Policy Administration

This practice statement is administrated by UAB "iDenfy", K. Barsausko 59, Kaunas, 51423, Lithuania, info@idenfy.com. This document is reviewed annually with approval from UAB "iDenfy" management board.

Definitions and Acronyms

Definitions:

- Identity verification: the process of verifying if the applicant of the identity document in indeed the rightful owner
- Applicant: New user that applies for identity verification of the document.
- Document verification: the process of verifying the authenticity of identity document.
- Identity document: An official and government-issued identity document such as passports, driving licenses, identity cards, and residence permits
- Selfie: biometric data provided by the applicant for facial verification purposes.
- Software as a service (SaaS): A software licensing and delivery model in which software is licensed on a

- subscription basis and is centrally hosted on a public cloud.
- Trust Service Provider: An entity that provides one or more electronic Trust Services.
- Supervisory Body: The authority which is designated by the member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state.
- Biometric verification provider: the party that provides biometric matching and liveness detection services for user verification purposes.
- Public cloud provider: the party that provides cloud services via the internet.

Acronyms:

- API Application Programming Interface
- CA Certification Authority
- CP Certificate Policy
- CRL Certificate Revocation List
- DG Datagroup
- DMZ Demilitarised Zone
- DPIA Data Protection Impact Assessment
- DPO Data Protection Officer
- ETSI European Telecommunications Standards Institute
- GDPR General Data Protection Regulation
- HSM Hardware Security Modules
- ISMS Information Security Management System
- PKI Public Key Infrastructure
- QSCD Qualified Signature Creation Device
- RA Registration Authority
- SaaS Software as a service
- TSA Time-Stamping Authority
- TSP Trust Service Provide
- TSPS Trust Service Poly / Trust Service Practice Statement
- TSU Time-Stamping Unit
- UTC Coordinated Universal Time
- NFC Near Field Communication
- MRZ Machine Readable Zone
- OCR Optical Character Recognition
- eMRTD electronic Machine Readable Travel Document
- eDL electronic Driving License
- ICAO International Civil Aviation Organization
- eID electronic Identity
- (Q)TSP (Qualified) Trust Service Provider
- SDK Software Development Kit
- SLA Service Level Agreement
- Partner - iDenfy's customer
- Company - iDenfy company
- Data subject - Partner's customer, identity holder
- Manual Verification - iDenfy's registration officer which review and confirm or deny identity verification manually
- NFC Verification - Verifying the authenticity of the presented Data Subject's identity document using electronic chip inside the ID document

Publication and Repository Responsibilities

Repositories

This document is published on the iDenfy official website. The official link to this document is www.idenfy.com/respository

This document identification number is: OID: 1.3.6.1.4.1.59462.1.1.1.0.0

This document has a grace period till 2023-01-01

This document came in force from 2023-01-01

Document's confidentiality: public document

Publication of certification information

iDenfy makes these documents publicly available:

- Practice statement
- Audit results
- Insurance certificate
- Other certificates
- Terms and conditions

Time or frequency of publication

iDenfy publishes updates of this information in the repository at least once per year or when significant changes are implemented.

All relying parties will be notified via the iDenfy public repository.

Access controls on repositories

Documents published in the Repository are for public information, and access is publicly available. The repository is protected against unauthorized changes. Only authorized employees of iDenfy to have writing/modifying/deleting permissions for the repository.

The documents must be signed by the iDenfy CEO with a qualified electronic signature and published in the official repository www.idenfy.com/security

Identification and Authentication (I&A)

Naming

No stipulation

Need for names to be meaningful

We're verifying the identity only of physical persons. The following information is collected during the identity verification process:

- Name, middle name (if applicable), and surname
- Date of birth
- Personal identification code (if applicable)
- Document identification number (if applicable)
- Document issuing date (if applicable)
- Document expiry date (if applicable)
- Document issuing authority (if applicable)
- Biometric picture and signature on ID Document
- ID document
- Issuing country
- Nationality (if applicable)

The maximum retention time is 8 years, it depends on identity verification context. The retention time is agreed upon with the Partner, the Partner should inform the applicants about retention time.

Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity is not accepted by iDenfy all names have to be real.

Rules for interpretation of name forms

The name for verification will always be taken from the identity document and compared with records we have got from verification initiator Partner.

Uniqueness of names

The uniqueness of each subject is ensured by providing the full name of the Data Subject with two unique identifiers:

- Personal identifier or ID document number
- Unique iDenfy number (ScanRef)
- Client id number (Data Subject unique identifier in Partner's system)

Recognition, authentication and role of trademarks

No stipulation

Initial identity validation

Method to prove possession of private key

No stipulation

Authentication of organization identity

No stipulation

Authentication of individual identity

The Data Subject's name, date of birth and other information (see - Need for names to be meaningful paragraph) will be verified. There will be two types of identity verification.

The first verification is based on 4 modules:

- Liveness detection
- Face comparison
- ID verification
- Manual Verification

The second verification is based on 5 modules:

- Liveness detection
- Face comparison
- ID verification
- NFC Verification
- Manual Verification

All automated system and manual verification actions and decisions are logged in the audit trail.

Non-verified subscriber information

No stipulation

Validation of authority

No stipulation

Criteria for interoperation

No stipulation

Identification and Authentication for Re-key Requests

No stipulation

Identification and Authentication for Revocation Requests

No stipulation

Certificate Life-Cycle Operational Requirements

No stipulation

Management, Operational, and Physical Controls

iDenfy has approved and implemented policies and procedures to assure data security for it’s trust service. iDenfy claims that it makes every sensible effort to detect and prevent material breaches, loss, damage or compromise of assets, and interruption to business activities.

iDenfy has implemented Information Security Policy, this policy specify security measures that are required and defines a set of practices specifying how security measures are implemented.

iDenfy executes risk assessment regularly to consider business risks, IT risks, and risks associated with the registration authority functions. This includes risks associated with physical facilities. These risk

assessments determine the necessary security requirements and operational procedures. iDenfy management approves risk assessment, oversees risk mitigation, and evaluates residual risks.

Physical Security Controls

Site location and construction

iDenfy main offices operates in Kaunas, Lithuania. iDenfy stores data in Amazon AWS datacenters and servers located in Dublin, Ireland.

Physical controls have been implemented for the main office and for datacenters and servers, which are used to process and store the personal data of the identity verification process in order to prevent unauthorized access to such premises.

Physical Access

Main office:
iDenfy provides physical access only to approved employees. Main office is protected with entry cards, welcome desk, 24-hours security officers, CCTV, fire and motion detectors, security alarms, access monitoring system.

AWS Datacenters and servers:

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification.

CCTV

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

DATA CENTER ENTRY POINTS

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

INTRUSION DETECTION

Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a

data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

Power and air conditioning;

Main office:

The main office is equipped with regular power connection and with additional power generators, the office has air conditioning systems.

AWS datacenters and servers:

Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Water exposures

Main office:
iDenfy has made reasonable efforts to ensure its secure facilities are protected from flood and water damage. iDenfy has personnel located on-site to reduce the extent of damage from a flood and any subsequent water exposure.

AWS:
In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

Fire prevention and protection

Main office:
The main office is equipted with fire and smoke detection systems to reduce the risk of damage or loss by fire.

AWS:
AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

Media storage

iDenfy has policy in place to ensure safe media usage. iDenfy avoid to use media storage, all sensitive data is stored in cloud storage.

Waste disposal

iDenfy has procedures in place to securely dispose of all media types.

Off-site backup.

iDenfy use cloud storage to backup it's data, to ensure availability of data, data is backed up in different AWS availability zones.

Procedural Controls

Trusted roles are assigned by management team who decide and assign permissions on the "principle of least privilege" basis. The list of personnel appointed to trusted roles is maintained. Inventorying is conducted when there is a new hire or termination. Access to systems is periodically reviewed by asset owners. The functions and duties performed by persons in trusted roles are distributed so that a lone person cannot subvert the security and trustworthiness of PKI operations.

Trusted roles

Trusted roles are executed mainly by iDenfy management team. Each individual has to fulfil all defined requirements for trusted roles before assignment to the trusted role.

- Security officers - overall responsibility for administering the implementation of the security practices.
- Registration officers - Performs the manual review procedures defined by the service procedure and approves or rejects Data Subjects.
- System administrator - Authorized to install, configure and maintain the systems for service management. Responsible for operating the systems on a day-to-day basis. Authorized to perform system backup.
- Compliance manager - Manages compliance, information security including risk management, quality
- System Auditors: Authorized to view archives and audit logs of the systems.

Administrative Accounts

All installation, configuration, management, and maintenance activities are carried out using **dedicated administrative accounts**, separate from normal user or registration officer accounts. These accounts are:

- Individually assigned to authorized personnel only.
- Protected with strong authentication, including multi-factor authentication.
- Restricted to the least privilege necessary for the assigned role.

- Logged and monitored to ensure full traceability of administrative actions.
  Shared or generic “admin” accounts are strictly prohibited.

Number of persons required per task

iDenfy ensures that the number of staff available for tasks to meet demand, but also to ensure that all security, risk and compliance regulation requirements are met.

Identification and authentication for each role

The background screening are done for employees in Trusted Roles, and all employees are verified and authenticated, including face-to-face checks and identification checks based on official national ID.

User accounts are created for personnel in specific roles that need access to the system. Only specific roles has full access to systems, other roles are limited with permissions. For critical systems two-factor authentication is required.

Roles requiring separation of duties

When assigning trusted roles, separation of duties is taking into account. Conflicting duties and areas of responsibility have been identified and are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of assets.

Conflict of Interest

All employees in trusted roles are free from conflict of interest that might prejudice the impartiality of iDenfy operations.

Personnel Security Controls

Qualifications, experience, and clearance requirements

Each applicant’s resume and compulsory identity document are verified. All employees sign a nondisclosure agreement as part of their employment contract.

Background Check Procedures

iDenfy proceeds following procedures to perform background checks:

- Identity verification
- Background checks as far as legally permitted in respective jurisdictions
- Reference taking from previous employers

Background checks are conducted on all candidates for employment and trusted sub contractors performing the Trust Service providing operations with access to production data. Checks are updated periodically, minimum once a two years.

Training requirements

Security training shall be followed by all personnel every year. The contents must be determined by Security Officers. Training depends on the role of the employee. Specific training can be organised via the personal yearly plan that each employee has.

Upon employment, all new employees follow a training plan. The training includes security awareness and other training-related training associated with their specific function, which includes (where applicable) software, hardware, office procedures, and security awareness.

Trusted roles has additional traninigs based on their functions.

iDenfy maintains records of who received training and what level of training was completed.

Retraining frequency and requirements

All employees are required to attend regular security awareness training sessions.

Job rotation frequency and sequence

No stipulation

Sanctions for unauthorized actions

iDenfy employees failing to comply with Company requirements such as being non-discriminatory policy, security requirements, data protection requirements and etc. are subject to disciplinary actions, up to and including termination of employment and legal sanctions.

Independent contractor requirements

Independent contractors must meet the same training requirements as iDenfy employees working in the same role.

Once the independent contractor completes the work for which it was hired or the independent contractor's employment is terminated, all access rights assigned to that contractor are removed as soon as possible.

Documentation supplied to personnel

Persons in Trusted Roles receive training and Trusted roles are documented and this documentation is provided as needed for the employee to perform job responsibilities.

Audit logging procedures

Types of events recorded

iDenfy Service logs at least the following events relating to the registration process:

General events	● Software installation, patches and updates ● Backup related information ● Boot and shutdown ● Boot and shutdown of logging (audit) function ● Time synchronization and detection of loss of synchronization ● All requests and reports relating to revocation, as well as the resulting actions. ● Availability and Capacity utilization
General Security events	● System account creation ● Access attempts ● Configuration changes to Firewalls, Switches, Intrusion detection systems, and load balancers ● System crashes or other anomalies ● Hardware failures ● Firewall and Switch activities ● Activities of system user with super admin rights ● Changes related to security policy

	● Changes in audit parameters ● Encryption key rotation
iDenfy events	Registration ● Backup ● Storage ● Archival ● Destruction ● Successful or unsuccessful processing of events ● Result ● Agent Name ● Identification time ● Transaction Number ● ID number ● Fraud reason ● Automated system actions and decisions ● NFC actions and decisions ● Timestamp Identification changes/decisions (whether data was edited by the agent and decision) ● Review of changes (whether the data change was reviewed by another agent) ● User data (birthday, birth name, birthplace, city, country, first name, last name, gender, nationality, address, personal number (or other serial number)) ● Identity document information (type, expiration date, country, number, issuing authority, date of issue) ● A result pdf (pdf that contains all results with pictures) ● Video of the ID document ● Pictures of ID documents ● Name of receiving TSP ● Agent's decision ● Timestamp

Log entries must also include:

- Date and Time
- Identity of the entry generator
- Attribute related to entry type

iDenfy logs of identifications include:

- Identifying document presented during application
- Personal data from accounts provided by trusted third parties
- Liveliness check output

- Data pertaining to session (e.g. smartphone type) at registration.

Copies of applications and identification documents are securely transferred right after successful identification to the QTSP as part of the evidence package. Logs are securely stored without the possibility of alteration/modification. Backups of logs are performed regularly. Logs can be accessed with permission via the iDenfy dashboard. The time used to record events as required in the audit log is synchronized with UTC at least once a day. The logs will be removed automatically after the agreed retention period, usually retention period is 8 years. The audit trail will not contain personal information.

CTO annually reviews key inventory on an annual basis and records this within ISMS Records.

Frequency of processing log

Processing of logs is scheduled at regular intervals depending on the type of log. Instructions related to frequency and work procedure related to a particular logs, is detailed in internal documentation.

Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

Retention period for audit log

Audit logs are retained for 10 years. Afterwards the logs are deleted, except for cases where it is legally required to keep logs for a longer period.

Protection of audit log

These media are accessible by iDenfy staff by viewing datacenters or logs reviewing platform. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction.

Audit log backup procedures

iDenfy performs regular backups of critical system data, audit log data, and other Sensitive Information. iDenfy has defined backup strategy and policies in internal documentation.

Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level.

Notifications to Event-Causing Subject

No stipulation

Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments are performed, reviewed, and revised. These assessments are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. Security officer will review logs

Records archival

Types of records

All data that can be relevant for the compliance audit is archived. Depending on contractual details with Partner the identification data, including personal data, can be archived or can be not archived.

For security and incident management purposes access and audit logs are recorded. Access and audit logs contain an IP address, username, email of the user.

Retention period for archive

Identification data and logs contained with it has retention period time depending on contractual details with a Partner.

Access and audit logs are archived for 12 months.

Protection of archive

Archive data associated with identification and related processes are subject to access restrictions and controls. Archives are secured against modification and deletion. To this end,

both organizational and technical controls are in place. The archives are stored on monitored, redundant cloud storage.

Archive backup procedures

Digital archive data is automatically generated via the internal systems processes. Backups of systems are made daily/weekly/monthly depending on media and in accordance with the iDenfy's backup procedures and policies.

Requirements for time-stamping of records

Records are timestamped (creation, execution).

Archive collection system (internal vs. external)

No stipulation

Procedures to obtain and verify archive information

Integrity and usability of archives shall be validated at least annually.

Key changeover

No stipulation.

Compromise and disaster recovery

In case of compromise or disaster, iDenfy executes according to a Bussiness Continuity Plan. It guarantees a robust set of procedures as well as physical and logical security measures to minimize the impact of disaster or compromise. All procedures have been developed to minimize potential impact and restore operations within a reasonable period of time. The Business Continuity Plan is tested annually to determine whether they meet requirements and continuity needs.

Incident and compromise handling procedures

Incidents or compromises are handled according to the iDenfy internal incident response procedure.

Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

In such cases where computing resources, software, and/or data have been identified as corrupt, appropriate steps are taken for incident investigation, appropriate escalation and incident response by internal procedures and policies.

Entity private key compromise procedures

No stipulation

Business continuity capabilities after a disaster

In order to ensure business continuity after a disaster iDenfy performs periodic crisis business continuity plan tests. iDenfy internal documentation defines how crisis management and communication take place in emergency situations. Backups are stored in different availability zones to minimize disaster impact.

CA or RA Termination

CA Termination

No stipulation

RA Termination

iDenfy has a documented Termination Plan which describes the process of service termination. Stakeholders affected by any termination will be informed according to the Termination Plan and Routine External Communication.

Technical security controls

iDenfy use dedicated workstations for the administration of the implementation of security policy. These workstations have access to a dedicated network segment that is used for administration only.

iDenfy has separated production and development environments.

Security officer will review the configurations at least every 2 months.

Key pair generation and installation

No stipulation

Private key protection and cryptographic module engineering controls

No stipulation

Other aspects of key pair management

No stipulation

Activation data

No stipulation

Computer security controls

Specific computer security technical requirements

iDenfy ensures that the identity verification system components are secure and correctly operated, with an acceptable risk of failure.

iDenfy has a variety of security controls in place:

- Multi-factor authentication for systems
- IP changes detection controls
- IP whitelisting controls
- Email confirmation controls
- Encrypted connections
- Encrypted storage
- Audit logs secured against alteration/modification/deletion
- Separated development and production environments
- Physical and logical access control
- Permissions based controls
- Time session based controls
- Firewall/antivirus controls
- Controls of software installation/removal
- Centralised device management system
- Physical controls against water, fire, flood, unauthorized access, CCTV monitoring
- Secure media removal/disposal
- Risk based logging, monitoring and alerting
- Trusted roles assigned and training for operating these systems
- Vulnerability scanning and penetration testing
- Controls to monitor/review accesses

- Passwords policy controls

Computer security rating

iDenfy uses standard computer systems.

Life cycle technical controls

System development controls

The software development process adheres to common practices to limit the risk of bugs and vulnerabilities:

- iDenfy has implemented the software development policy, best practices, and standards. Training is executed for Company's developers.
- Version control is applied to all code to ensure control over what code is to be released and what is in development, and it also provides an audit trail of all changes to our code.
- Code changes have to be approved by several departments before being deployed to the production environment.
- New code is tested using automated and manual tests before the software is released to production.
- Analysis is applied to detect vulnerabilities and deficits in code automatically
- External penetration testing is performed on annual basis

Security management controls

All operational systems of iDenfy are monitored, managed, and controlled to ensure safe operation. Additional to manual monitoring, it is also an automated process where the relevant, trusted personnel are alerted upon any activity which is out of the expected behavior.

The systems configurations are regularly reviewed. The maximum interval for checking system configuration is two months.

Life cycle security controls

No stipulation

Network security controls

iDenfy has a variety of security controls in place:

- Frontend, backend, datacenters are in separate logical servers
- All network traffic is encrypted with TLS
- Firewalls block unallowed traffic
- WAF is implemented
- Vulnerability scanning is performed on regular basis
- Penetration tests are performed by the external party on yearly basis
- The transfer of data to Partner is always encrypted
- There is no physical transfer of data
- Additional controls (see Specific computer security technical requirements)

Time-stamping

All systems time with timezone is synchronized through NTP daily.

Certificate, CRL, and OCSP profiles

No stipulation

Compliance audit and other assessments

Frequency or circumstances of assessment

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards, including ETSI standards for Trust Service Providers, and other industry standards related to the operation of CAs. An independent external auditor to assess iDenfy's compliance with eIDAS and ETSI perform a regular audit.

Identity/qualifications of assessor

iDenfys CAB is accredited according to ISO/IEC 17065 and ETSI EN 319 403. The CAB is competent to carry out conformity assessments of Qualified Trust Service Providers and its services.

Assessor's relationship to assessed entity

The auditor of the CAB is independent from iDenfy and iDenfy assessed systems. The internal auditor shall not audit his/her own areas of responsibility.

Topics covered by assessment

The conformity assessment covers the conformity of information system, policies and practices, facilities, personnel, and assets with eIDAS regulation, respective legislation and standards.

The CAB audits all parts of the information system used to provide Trust Services. Activities subject to internal auditing are the following:

- TSPS, Service Definition, Terms & Conditions, Subscriber Agreement
- TRA Service and systems
- TRA Process Description and TRA Operational Guide
- ISMS (Routines, Policies, Controls and Records).

The CAB audits iDenfy protection of subscriber data, accuracy and implementation of security policy, performance of work procedures and contractual obligations, as well as compliance with TSPS.

Actions taken as a result of deficiency

Depending on the severity of the deficiency the following actions may be taken:

- Auditor may note the deficiency in the report
- An action plan can be developed and steps taken to remedy the deficiency. This could include a revision to the iDenfy TSPS or to applied procedures
- If the deficiency is judged to have risks for the operation of the iDenfy TRA Service actions has to be taken without any delay

Communication of results

Certificate(s) for trust service(s) resulting from conformity assessment audits conducted pursuant to the eIDAS regulation, corresponding legislation and standards, are published on iDenfy's website https://www.idenfy.com/security/.

iDenfy submits the resulting conformity assessment report to the Supervisory Body within three working days.

Other business and legal matters

Fees

Users do not pay any fees using iDenfy services. Partners are paying fees according to the contract.

Financial responsibility

To cover the liabilities of art. 13 of the eIDAS regulation, iDenfy has a full liability insurance policy which provides coverage of €500.000. More details about liability can be found in the repository https://www.idenfy.com/cyber-insurance/ and in the insurance agreement.

Confidentiality of business information

Scope of confidential information

Confidential information includes any information provided by Data Subject for purposes of identification. iDenfy considers all data provided within the framework of the trust service as confidential.

Information not within the scope of confidential information

Any information not listed as confidential or intended for internal use only is public information.

Responsibility to protect confidential information

iDenfy's personnelhandle confidential information in strict confidence and are required to sign confidentiality agreements before being employed. All confidential information will be protected

against unauthorized access, modification, or removal using physical, logical, and/or procedural security.

Privacy of personal information

iDenfy Service processes Personal Data in accordance with applicable national legislation of Republic of Lithuania and European Union General Data Protection Regulation (GDPR) requirements.

Privacy plan

iDenfy has a GDPR Policy at www.idenfy.com/privacy-policy and a data protection officer (DPO) appointed and registered with the Lithuanian Data Protection Agency. The DPO can be contacted at dpo@idenfy..com

Information treated as private

GDPR define what information shall be treated as private.

Information not deemed private

All information which is not by GDPR required as private could be public.

Responsibility to protect private information

iDenfy and all personnel respect private information, controls as per requirements are implemented to protect private information. All iDenfy personnel must protect private information from disclosure to non-authorized parties.

Notice and consent to use private information

iDenfy will only use confidential information in accordance with the Privacy Policy

Disclosure pursuant to judicial or administrative process

iDenfy reserves the right to disclose personal information if iDenfy reasonably believes that disclosure is required by law or regulation, or disclosure is necessary in response to judicial, administrative, or other legal process.

Other information disclosure circumstances

No stipulation.

Intellectual property rights

iDenfy commits to protect it’s intellectual property rights.

Representations and warranties

CA representations and warranties

No stipulation.

RA representations and warranties

This Practice Statement shall form representations and warranties from iDenfy.

iDenfy shall:

- Provide its services consistent with the requirements and the procedures and policies defined in this Practice Statement
- Identify, analyse and evaluate risks, and take appropriate measures of treatment accordingly to the results of assessment, ensuring appropriate level of security
- Review and revise risk assessment at least annually.
- Be responsible for the effective compliance with the procedures defined in this Practice statement
- Provide the service in compliance eIDAS regulation and related legal acts and standards
- Provide publicly published repositories of all practice statements
- Protect the integrity and confidentiality of personal data and information acquired as part of service

- Within 24 hours after having become aware of it, notify the Supervisory Body of any breach of security or loss of integrity that has a significant impact on the Trust Service provided
- Within 24 hours after initial discovery, notify the Lithuanian Data Protection Authority of any personal data breach
- Where the breach of security or loss of integrity or personal data breach is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach without undue delay
- Preserve all the documentation, records and logs related to Trust Service
- Ensure a conformity assessment with a CAB on a recurring basis according to requirements.
- Present the conclusions of the CAB to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- Have the financial stability and resources required to operate in conformity with this Practice Stement;
- Publish the terms of the compulsory insurance policy and the conclusion of CAB in the iDenfy website
- Secure that employees do not have criminal records of intentional crime
- Ensure that suppliers are safe and follow safety requirements by iDenfy

Subscriber representations and warranties

Data Subject of service warrant that all documents, representations and information provided in the registration process are accurate, complete and truthful.

Relying party representations and warranties

No stipulation

Representations and warranties of other participants

No stipulation

Disclaimers of warranties

No stipulation

Limitations of liability

Limitations of Liability for Data Subjects are stated in terms and conditions. Limitations of Liability for Partners are stated in agreements between iDenfy and Partners.

Indemnities

No stipulation.

Term and termination

Term

This Practice Statement is effective immediately after publication in the public repository and remains effective until a new version or replacement is published at https://www.idenfy.com/security/

Termination

By publishing a new version of the Practice Statement, the previous version of the Practice Statement is terminated or when it is terminated due to Trust Service or iDenfy's termination. iDenfy has the termination plan in place. The end users will be announced about termination at least 3 months before in case of scheduled termination. The termination plan is regularly maintained.

Effect of Termination and survival

Despite the fact that this Practice Statement may eventually no longer be in effect, the following obligations and limitations of this Practic Statement should survive, sections: Representations and Warranties, Financial Responsibility, Confidentiality of Business Information.

Individual notices and communications with participants

No stipulation.

Amendments

Procedure for amendment

iDenfy Management can amend this Practice Statement. Only changes that do not affect the acceptance of the service and security level of the described procedures and regulations can be made to this iDenfy Practice Statement without notice. Changes that do not affect security include linguistic changes and minor rearrangements. Changes can be in the form of an amendment or a new version of the Practice Statement should be published immediately to the repository https://www.idenfy.com/security/.

Notification mechanism and period

Practice Statement changes that require notification will be made 14 days after notification. Notification will be published on https://www.idenfy.com/security/. Changes that affect the terms of an agreement will be notified to the appropriate Partner or signatory of the agreement.

Circumstances under which OID must be changed

No stipulation.

Dispute resolution provisions

All disputes between the parties will initially be settled by negotiations. If the parties fail to reach and friendly agreement, the conflict will be resolved at the court of the location of iDenfy or its Partner. Other parties will be informed of any claim or compliant not later than 30 calendar days after the detection of the basis of the claim, unless otherwise provided by law.

The Data Subject or any other party can submit their claim or complaint on the following email: info@idenfy.com

Governing law

iDenfy provides identity verification services to Trust Service Provider (TSP) as defined in EU Regulation 910/2014 also known as eIDAS. This requires iDenfy to be respectful to the applicable requirements of the following standards, requirements and regulations:

- eIDAS - 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.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) effective from 2018-05-25

Identity Proofing Service Requirements

Handling of Attribute Encoding Differences

In order to ensure consistent comparison of identity attributes across different types of evidence and sources, iDenfy applies the following rules:

- **Character encoding**: All attributes are normalized to Latin (ASCII) characters before comparison. For example, diacritical characters (ø, å, č, ü) are converted to their nearest Latin equivalent (o, a, c, u).

- **Cross-language consistency**: Attributes collected from partners (e.g., in Chinese, Cyrillic, or other scripts) are converted to Latin characters and compared with the normalized attributes extracted from identity documents.

- **Name structure differences**:

    - Missing middle names do not affect verification if first and last names match.

    - Prefixes and suffixes (Dr., Jr., Mr., etc.) are disregarded.

    - Truncations due to document field length are accepted if consistent.

    - Initials-only names (e.g., “J. S.”) are not accepted.

- **Evidence priority**: In case of differences between multiple sources of evidence, authoritative government-issued document data shall prevail.

- **Audit trail**: All normalization and resolution decisions are logged in the audit trail, with the Registration Officer’s final decision recorded.

Handling of Discrepancies with Trusted Register Data

If the attributes obtained from trusted registers (e.g., lost and stolen document databases, government identity registries) differ from those obtained from identity documents or other authoritative evidence, the following procedure applies:

1. **Immediate rejection** – The identity proofing request is rejected, and no identity assertion is issued.

2. **Audit trail** – The discrepancy is logged in the audit trail with details of the conflicting attributes and the source of evidence.

3. **Registration Officer review** – A Registration Officer reviews the case to confirm that the discrepancy is genuine and not due to technical errors (e.g., encoding or data format issues).

4. **Notification** – The relying party (Partner) is informed via the secure API response that verification failed due to evidence inconsistency.

5. **No override** – Discrepancies with trusted registers cannot be overridden by manual decision; trusted register data prevails.

Goals for Presentation Attack Detection (PAD) Performance

iDenfy applies Presentation Attack Detection (PAD) measures in compliance with ISO/IEC 30107-3. The following goals are established for PAD performance, in line with industry best practice benchmarks (e.g., iBeta certified testing):

- **APCER (Attack Presentation Classification Error Rate): ≤ 1%**

- **BPCER (Bona Fide Presentation Classification Error Rate): ≤ 5%**

These goals represent the maximum acceptable error rates. iDenfy's current PAD system (FaceTec Inc.) has achieved **0% APCER and 1–2% BPCER** under iBeta Level 1 and Level 2 evaluations, which exceeds these goals.

The service is continuously monitored and tested to maintain or improve performance against these targets. Results are reviewed at least annually, and corrective actions are taken if performance deviates from the stated objectives.

Updating of PAD Goals Based on Threat Intelligence

iDenfy maintains a threat intelligence process that monitors developments in presentation attack methods (e.g., deepfakes, synthetic identities, advanced spoofing techniques). As part of this process:

- PAD goals (APCER/BPCER) are reviewed at least annually, and more frequently if new threats or attack techniques emerge.
- Updates are based on external threat intelligence sources, results of bounty programs, incident reports, and industry research (e.g., ISO/IEC 30107-3 evaluations, iBeta testing).
- If threat intelligence indicates that existing PAD thresholds are insufficient to mitigate emerging risks, new performance goals will be set and published in the updated Practice Statement.
- All changes are subject to management review and approval, and are documented in the annual review cycle of this Practice Statement.

iDenfy applies PAD means that have been evaluated by iBeta against ISO/IEC 30107-3 standards. While ISO/IEC 19989-3 evaluations are not yet available for this PAD solution, iDenfy commits to undergoing accredited laboratory re-evaluation in line with ISO/IEC 19989-3 as soon as such accredited testing services become available. Evaluations will be repeated at least every second year, and updated results will be reflected in this Practice Statement.

Quality and Security Goals in Identity Proofing

Objectives

iDenfy defines measurable quality and security objectives for its Identity Proofing Service to ensure resilience against both false acceptance and false rejection of applicants. These objectives are established in line with ETSI TS 119 461, ISO/IEC 30107-3, and industry best practices.

- **False Acceptance Rate (FAR / APCER)**: Target ≤ **1%**
- **False Rejection Rate (FRR / BPCER)**: Target ≤ **5%**

These thresholds are considered acceptable to balance usability and fraud prevention.

Performance Testing

To ensure compliance with the defined objectives, iDenfy implements the following testing framework:

1. **Baseline Certification Tests**

    - Liveness detection technology has been tested by iBeta to ISO/IEC 30107-3 standards with results of **0% APCER** and **1–2% BPCER**, establishing a certified performance baseline.

2. **Internal Testing and Monitoring**

    - **Quarterly statistical sampling** of completed verifications is performed to measure false acceptance and rejection rates against defined thresholds.
    - Results are documented in KPI reports and reviewed by the IT team.

3. **External Independent Testing**

    - Annual revalidation is performed by accredited external laboratories or through re-certification audits.
    - Where applicable, updated PAD conformance test reports are obtained.

4. **Continuous Monitoring**

    - All verification sessions are logged with outcome codes.
    - Error cases (e.g., user complaints about wrongful rejections) are reviewed.

Review and Improvement

- If testing identifies performance degradation outside the defined thresholds, corrective actions are initiated (e.g., contacting the supplier with a request to retrain AI models, improving operator training, adjusting document verification rules).

- Goals are reviewed at least **annually** by iDenfy's management and adjusted if stricter industry benchmarks or regulatory requirements apply.

Transparency

- High-level results of performance testing will be published in iDenfy's public repository alongside this Practice Statement.

- Partners are informed of current FAR/FRR ranges in the technical documentation and may request detailed KPI reports under NDA.

Use Cases for Which Compliance is Claimed

iDenfy claims compliance with ETSI TS 119 461 V1.1.1 for the following identity proofing use cases, as defined in clause 9 of the standard:

1. **Unattended Remote Identity Proofing of Natural Persons**

    - Covered by the *Identity Verification Procedure* (hybrid manual/automated).
    - Evidence collected: government-issued ID (physical or digital), face biometrics, liveness detection, optional trusted register checks.
    - Compliance claimed: **Yes**.

2. **Hybrid Manual and Automated Operation**

    - Automated document and biometric checks are supplemented by manual review by trained Registration Officers.
    - Compliance claimed: **Yes**.

3. **Manual Operation**

    - Document authenticity and face comparison performed entirely by Registration Officer with supporting tools.
    - Compliance claimed: **Yes**.

4. **Automated Operation**

    - Automated identity verification with biometric and document validation systems. Final decision still confirmed by Registration Officer.
    - Compliance claimed: **Yes** (within scope of ETSI, decision safeguarded by manual override).

5. **Use of Physical and Digital Identity Documents as Evidence**

    - Accepted documents: passport, national ID, residence permit, driving license (as listed in the supported-documents repository).
    - Compliance claimed: **Yes**.

6. **Use of Trusted Registers as Supplementary Evidence**

    - Implemented where allowed by national legislation (e.g., lost/stolen document registers in Lithuania).
    - Compliance claimed: **Yes** (limited to jurisdictions where registers are available).

7. **Use Cases *Not* Supported**

    - Identity proofing of legal persons.

- Identity proofing of natural persons representing legal persons.
- Use of eID means or digital signature as primary evidence.
- These use cases are **Out of Scope / Not Applicable**.

Miscellaneous provisions

Entire agreement

No stipulation

Assignment

No stipulation

Severability

If parts of any of the provisions in this Practice Statement are incorrect or invalid, this shall not affect the validity of the remaining provisions until the Practice Statement is updated. The process for updating this Practice Statement is described in section Amendments.

Enforcement (attorneys' fees and waiver of rights)

No stipulation

Force Majeure

iDenfy and other parties cannot be responsible for any outcomes caused by events beyond it's reasonable control, including but without limitation to:

- War and/or nature disaster and/or pandemic
- Acts of government or the European Union
- Export or import prohibitions
- Breakdown or general unavailability of public telecommunications networks and logistics infrastructure
- General shortages of energy, fire, explosions, accidents, strikes or other concerted actions of workmen, lockouts, sabotage, civil commotion and riots.

Other provisions

All associated policies must be published and communicated to employees and external parties as relevant. The documents must be reviewed, approved, and signed by the iDenfy board member with a qualified electronic signature and published in the official repository www.idenfy.com/security. The official repository should include versioning history, other associated documents, and security and compliance documents.

This document is reviewed during yearly management reviews or on significant changes. Any changes, corrections, or updates will be applied only following this document's procedures.

Document History

2022-12-06 Document drafted;
2023-03-12 Approved by iDenfy's management board.
2024-05-08 Approved by iDenfy's management board.
2025-09-09 Document updated by iDenfy's management board.
2025-09-09 Approved by iDenfy's management board.