imID CJSC

PUB001 – Practice Statement

V1.0

Issue Status

Issue	Issue Date	Additions/Alterations
1.0	15/07/2026	1st issue of public version

Approval Details

Issue	Author: Role & Initials	Approval Date	Approved by: Role & Initials	Date Effective	Next Review
1.0	AH | CLRCO	15/07/2026	KM| CEO	15/07/2026	15/07/2027

Table of Contents

1. Introduction **8**

1.1 Overview 8

1.2 Document Name and Identification 10

1.3 PKI Participants 10

1.3.1 Certification authorities 10

1.3.2 Registration authorities 11

1.3.3 Subjects and Subscribers 11

1.3.4 Relying parties 11

1.3.5 Other participants 11

1.4 Certificate Usage 12

1.5 Policy Administration 12

1.5.1 Organization responsible for administrating the document 12

1.5.2 Contact 12

1.5.3 Entities determining the validity of the principles contained in the document 12

1.5.4 Approval procedures 12

1.6 Definitions and Acronyms 13

2. Publication and Repository Responsibilities **13**

2.1 Repository 13

2.2 Publication of Certification Information 13

2.3 Frequency of publication 13

2.4 Access to publication 14

3. Identification and Authentication **14**

3.1 Naming 14

3.2 Initial Identity Validation 14

3.3 Identification and Authentication for Re-key Requests 14

3.4 Identification and Authentication for Revocation Requests 14

4. Certificate Life-Cycle Operational Requirements **14**

4.1 Certificate Application 14

4.2 Certificate Application Processing 14

4.3 Certificate Issuance 15

4.4 Certificate Acceptance 15

4.5 Key Pair and Certificate Usage 15

4.6 Certificate Renewal 15

4.7 Certificate Re-key 15

4.8 Certificate Modification 15

4.9 Certificate Revocation and Suspension 15
4.10 Certificate Status Services 15
4.11 End of Subscription 15
4.12 Key Escrow and Recovery 15
5. Management, Operational, and Physical Controls 16
5.1 Physical Security Controls 16
5.1.1 Additional Physical and Environment Security Controls 16
5.2 Procedural Controls 18
5.2.1 Trusted roles 18
5.2.2 Four-eyes principle 18
5.2.3 Identification and authentication for each trusted role 18
5.2.4 Roles Requiring Separation of Duties 18
5.3 Personnel Controls 19
5.3.1 Qualifications, experience and clearances 19
5.3.2 Personnel verification procedures 19
5.3.3 Training requirements 19
5.3.4 Training frequency and requirements 20
5.3.5 Job rotation frequency and sequency 20
5.3.6 Sanctions for unauthorized actions 20
5.3.7 Independent contractor requirements 20
5.3.8 Documentation available to personnel 20
5.3.9 Cybersecurity measures for remote work 20
5.3.10 Remote Working Policy 20
5.3.11 Termination and Change of Employment 21
5.4 Audit logging procedures 21
5.4.1 Types of events recorded 21
5.4.2 Frequency of processing log 22
5.4.3 Retention time for records 22
5.4.4 Protection of records 22
5.4.5 Backups of records 23
5.4.6 Audit log accumulation system 23
5.4.7 Notification system to event-causing 23
5.4.8 Vulnerability assessment 24
5.5 Records Archival 25
5.5.1 Types of archives 25
5.5.2 Retention period of archives 25

5.5.3 Protection of archive 25
5.5.4 Backup archives procedures 25
5.5.5. Requirements for Time Stamping the archives 25
5.5.6 Archive storage 25
5.5.7 Archival information access and verification procedures 26
5.6 Key Changeover 26
5.7 Compromise and Disaster Recovery 26
5.7.1 Incident and compromise handling procedures 26
5.7.2 Incidents related to failures in hardware, software and/or data 26
5.7.3 Private key compromise or loss of calibration of a TSU clock procedures 27
5.7.4 Business Continuity Management 28
5.7.5 Use of Information from National CSIRT and Competent Authorities 28
5.8 CA or RA Termination 28
6. Technical security controls 29
6.1 Key Pair Generation and Installation 29
6.1.1 Supported Algorithms and Algorithm Identifiers 30
6.2 Private Key Protection and Cryptographic Module Engineering 30
6.3 Other Aspects of Key Pair Management 31
6.4 Activation Data 31
6.5 Computer Security Controls 31
6.5.1 Specific computer security technical requirements 31
6.5.2 Computer security rating 32
6.6 Life Cycle Security Controls 32
6.6.1 System development controls 32
6.6.2 Life cycle security controls 32
6.7 Network Security Controls 33
6.8 Time Synchronization 34
6.9 Time Stamping 34
7. Certificate, CRL, and OCSP Profiles 34
7.1 Certificate Profile 34
7.3 OCSP Profile 34
8. Compliance Audit and Other Assessment 35
8.1 Frequency or circumstances of assessment 35
8.2 Qualification of auditors 35
8.3 External auditor's relationship with imID CJSC 35
8.4 Audit scope 35

8.5 Actions taken as a result of deficiency 36
8.6 Communication of results 36
9. Other business and legal matters 36
9.1 Fees 36
9.1.1 Trust service prices 36
9.1.2 Prices for access to certificates 36
9.1.3 Prices for revocation or status information 36
9.1.4 Prices for other services 37
9.1.5 Rules for cost refunds 37
9.2 Financial responsibility 37
9.2.1 Insurance cover 37
9.2.2 Other resources for maintaining operations and compensation for damage 37
9.2.3 Insurance or warranty for end users 37
9.3 Confidentiality of business information 37
9.3.1 Definition of confidential business data 37
9.3.2 Business data not treated as confidential 37
9.3.3 Responsibilities for the protection of confidential business data 37
9.4 Privacy of personal information 38
9.5 Intellectual property rights 38
9.6 Representations and warranties 38
9.6.1 Certification Authority obligations and warranties 38
9.6.2 Registration Authority obligations and warranties 39
9.6.3 Time Stamp Authority obligations and warranties 39
9.6.4 Subjects and Subscribers obligations and warranties 39
9.6.5 Relying Party obligations and warranties 40
9.6.6 Representations and warranties of other participants 40
9.7 Warranty disclaimer 40
9.8 Limitation of liability 40
9.9 Indemnities 42
9.10 Term and Termination 42
9.11 Individual Notices and Communications 42
9.12 Amendments 42
9.12.1 Procedure for amendment 42
9.12.2 Notification mechanism 42
9.12.3 Circumstances under which OID must be changed 43
9.13 Dispute resolution procedures 43

9.14 Governing law 43
9.15 Compliance with applicable law 43
9.16 Miscellaneous provisions 43
9.16.1 Entire contract 43
9.16.2 Assignment 43
9.16.3 Severability 43
9.16.4 Enforcement 44
9.16.5 Force Majeure 44
9.16.6 Accessibility Clause 44
9.17 Other Provisions 44
10. Appendix 44
10.1 Definitions and Acronyms 44
10.1.1 Terminology 44
10.1.2 Acronyms 46

1. Introduction

imID CJSC was established in 2024 with the objective to provide electronic identification and related trust services. On December 9th, 2025 imID CJSC was granted accreditation as a Certification Authority in accordance with the laws of Republic of Armenia. imID CJSC operates under the regulatory oversight of the Ministry of High-Tech Industry of Republic of Armenia.

1.1 Overview

The Practice Statement outlines the rules for delivering trust services and carrying out Certification Authority activities in accordance with Armenian law. It ensures alignment with the requirements of the European Union Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). This document defines the roles, obligations, and responsibilities of all parties involved, and specifies the management, operational, and physical controls implemented by imID CJSC.

This document serves as a common framework for the provision of trust services and electronic identification services based on specific policies by imID CJSC. In particular, the Practice Statement covers the following services:

1. issuance and management of certificates for electronic signatures;
2. issuance of authentication certificates and provision of electronic means for electronic identification service;
3. issuance and management of certificates, including:
   a) provision of revocation service and publication of the certificate revocation lists (CRL);
   b) provision of online status information for certificates (OCSP);
4. management of remote signature creation device;
5. time stamping service.

The practices described in this document apply to the electronic trust services delivered by imID CJSC. Requirements specific to individual services are addressed in the respective service-specific policies. Where any inconsistency arises between this document and a service-specific policy, the service-specific policy shall prevail in respect of that service.

This document contains a declaration that the services provided under the Practice Statement comply with the following regulations:

1. Republic of Armenia Law on Electronic Document and Electronic Digital Signature (N HO-40-N adopted on December 14th, 2004, with subsequent revisions) and deriving government decrees;
2. 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, consolidated version: 18/10/2024.

Detailed requirements for provision of trust services and electronic identification services are described in separate policies. These policies are available in the public repository in accordance with Section 2.1.

The structure and contents of the Practice Statement are in accordance with the recommendation of RFC 3647, which is aligned to the following standards:

1. ETSI EN 319 401 v.3.1.1;
2. ETSI EN 319 411-1 v.1.5.1;
3. ETSI EN 319 411-2 v.2.6.1;
4. ETSI EN 319 421 v.1.3.1;
5. ETSI TS 119 431-1 v.1.3.1;
6. ETSI TS 119 431-2 v.1.2.1;
7. ETSI EN 319 412-1 V1.6.0;
8. ETSI EN 319 412-2 V2.4.1;
9. ETSI EN 319 412-3 V1.3.1;
10. ETSI EN 319 412-5 V2.5.0.

imID CJSC commits to operating in accordance with this Practice Statement. imID CJSC further commits to complying with all applicable service-specific policies, and to maintaining the currency of this Practice Statement so that it accurately reflects the operational practices of the organisation at all times.

imID CJSC commits that, upon production launch of its Smart Device Signing Applications (iOS and Android) and associated remote signing back-end services, the implementation will conform to EN 419 241-1 and the Protection Profile EN 419 241-2, and that remote-signing protocol exchanges and bindings will conform to ETSI TS 119 432. Until the Smart Device Signing Applications are publicly released, these controls shall be implemented, tested, and maintained in pre-production and shall be brought into production without material deviation at go-live.

The trust services are logically broken down into the following component services, to address requirements stated in clause 4.3 of ETSI EN 319 411-1 and 4.2 of ETSI EN 319 421:

- **Registration Services**
  - **Registration Authority** verifies the identity and, if applicable, any specific attributes of a Subject. Registration Authority provides registration for electronic identification and trust services, initiates and authorises certificate issuance/revocation following successful verification.

- **CA Services**
  - **Certificate generation service** issues certificates based on the identity and other attributes verified by the Registration service;
  - **Dissemination service** disseminates certificates to Subjects and makes them available to relying parties. This service also makes TSP's terms and conditions and any published policy and practice information available publicly;
  - **Revocation management service** processes requests and reports related to revocation to determine the necessary action. The results of this service are distributed through the revocation status service;
  - **Revocation status service** provides certificate revocation status information publicly.

- **RQSCD Service**
  - **Remote Qualified Signature Creation Device service** manages a Remote QSCD on behalf of the Subject, generates keys and creates signatures.

- **Electronic Identification Service**
  - The Authentication Service authenticates the Subject using authentication methods assigned through the Electronic Identification Means Provisioning Service.
  - The Electronic Identification Means Provisioning Service assigns authentication methods to the Subject and establishes their association with the Subject.

- **TSA Service**
  - The Time-Stamp Provisioning Service generates trusted timestamps in accordance with RFC 3161.
  - The Time-Stamp Management function monitors and controls the operation of the time-stamping services to ensure that the services are provided in accordance with the TSA policy.

This subdivision of services is only to clarify the trust services framework and does not restrict implementation of any further subdivision of the TSP's services.

imID CJSC defines and publishes terms and conditions for each of the trust services. Subscribers and parties relying on the trust service are informed of precise terms and conditions, before entering into a contractual relationship with imID CJSC.

imID CJSC makes terms and conditions available through a durable means of communication in Armenian and English languages. Terms and conditions are published electronically at https://imid.am/policies/ and retained in a form that preserves their integrity over time.

References to qualified certificates or services within imID CJSC documents entail adherence the specific requirements for qualified services established under to EU's eIDAS Regulation, applicable ETSI standards, compliance with which shall be subject to confirmation by qualified conformity assessment bodies. Such certificates and services are in conformity with the requirements set under the Law on Electronic Document and Electronic Signature of Republic of Armenia and deriving government decrees.

1.2 Document Name and Identification

The full name of this document is "imID CJSC Practice Statement". The document can be also referred to as Certificate Practice Statement (CPS), Practice Statement (PS) in imID CJSC documents - meaning the same document. The electronic version of this document is published and accessible at https://imid.am/policies/cps.

The Practice Statement can be identified by any party through the following OID: 1.3.6.1.4.1.63199.1.1

This Practice Statement supports other OIDs:

Document name	**OID number**
imID CJSC Trust Service Policy for Root and Subordinate Certification Authority	1.3.6.1.4.1.63199.1.2
imID CJSC Trust Service Policy for Personal CA	1.3.6.1.4.1.63199.1.4
imID CJSC Trust Service Policy for Time Stamp Authority	1.3.6.1.4.1.63199.1.5

1.3 PKI Participants

The Practice Statement regulates the most important roles between the following parties:

1.3.1 Certification authorities

The following Certification authorities (CAs) of imID CJSC issue certificates and revocation lists presently applicable.

Root CA(s):

- imID Root CA G1;

Policy CA(s):

- imID Policy CA G1;

Issuing CA(s):

- imID Personal CA G1;
- imID Mobile CA G1;
- imID TSA CA G1.

1.3.2 Registration authorities

The Registration Authority (RA) is an entity that is responsible for identification and authentication of Subjects of certificates.

imID CJSC as a RA has agreements with various entities performing RA services through Registration Points. The formally engaged Registration Points act on behalf of imID CJSC and are responsible to perform the following functions:

- identifying the Subject who submitted an electronic certificate request in accordance with the rules and procedures established by imID CJSC;
- verifying the Subject's identity at time of registration through applicable means, as defined in the rules and procedures;
- collecting and validating either direct evidence or an attestation from an authorized source regarding the identity and, if applicable, any specific attributes of Subjects to whom a certificate is issued;
- Accepting and maintaining certificate applications, checking the applications and/or forwarding the applications to the CA.
- verifying accuracy and completeness of an electronic certificate request.
- initiating and authorising certificate issuance/revocation following successful verification.

The final decision on certificate issuance is made by the CA.

1.3.3 Subjects and Subscribers

Subject means the natural person named in a certificate as the holder of the corresponding private key and on whose behalf the certificate is issued.

Subscriber means the entity that enters into a contractual relationship with imID CJSC under the Subscriber Agreement and/or the applicable Terms and Conditions governing the provision of electronic trust services.

Any natural person acting in their private capacity could become a Subscriber of imID CJSC for the purposes of electronic trust services.

1.3.4 Relying parties

A Relying Party is a natural person or legal person that relies on the trust services of imID CJSC.

1.3.5 Other participants

imID CJSC engages subcontractors, such as specialized data centres, for reliable and secure colocation and operation of server and network equipment, as well as providers of server signing solutions with the appropriate certifications, registration authority services and others.

imID CJSC maintains a Supply Chain Security Policy governing relations with all direct suppliers and service providers. These include security selection criteria for supplier selection, embedded security requirements in contracts, and monitoring of supplier cybersecurity practices.

The Supply Chain Security Policy identifies imID CJSC's role in the supply chain and defines criteria for selecting and contracting suppliers and service providers. Criteria address: availability of applicable certification, the ability of the supplier to meet imID CJSC's cybersecurity specifications; the risks and classification levels of the relevant services, systems, or products; the ability to diversify sources of supply and limit vendor lock-in; and the results of coordinated security risk assessments of critical supply chains. In the event such requirements cannot be satisfied by a single supplier, imID diversifies the supply through the engagement of additional suppliers.

Contracts with ICT service suppliers require those suppliers to propagate imID CJSC's security requirements throughout their own supply chains where they sub-contract parts of the ICT service, if and where such sub-contracting is

applicable. imID CJSC requests from ICT product suppliers a description of the software components and implemented security functions of their products or services, including configuration required for secure operation where applicable.

imID CJSC maintains a process for identifying and documenting product and service components critical to the continuity and integrity of its trust services. Assurance that critical components and their origin can be traced throughout the supply chain is obtained through one or more of the following: supplier declarations, certifications, contractual provisions, and integrity verification (e.g. hash verification or digital signatures upon receipt). Processes are in place to ensure components from suppliers are genuine and unaltered from their specification before deployment. Rules for sharing information on supply chain issues, vulnerabilities, and compromises between imID CJSC and its suppliers are defined in the Supply Chain Security Policy.

imID CJSC maintains a process for managing ICT components across their full lifecycle — covering procurement, deployment, maintenance, end-of-life, and replacement — including availability management and associated security risk controls at each phase. Supplier information security practices and service delivery are monitored, reviewed, and evaluated annually; any significant changes are assessed and managed accordingly. imID CJSC maintains a register of suppliers and their agreements that tracks where imID CJSC information is managed and archived; whilst this register is reviewed and validated annually to ensure agreements remain valid, fit for purpose and include relevant information security clauses.

1.4 Certificate Usage

The scope of this section is covered in a specific trust service policy.

1.5 Policy Administration

1.5.1 Organization responsible for administrating the document

This Practice Statement is administered by imID CJSC, headquartered at:

24/1 Azatutyan ave., Yerevan, 0014, Armenia

1.5.2 Contact

All inquiries and communication with respect to this document shall be directed to info@imid.am.

1.5.3 Entities determining the validity of the principles contained in the document

imID CJSC is responsible for assessing the completeness and accuracy of the Practice Statement and other documents related to trust services provided by imID CJSC, as well as ensuring their consistency. All inquiries and comments regarding the content of these documents should be directed to the address specified in Section 1.6.2.

1.5.4 Approval procedures

The Practice Statement remains in effect from its specified start date until a subsequent valid version is published.

The approval of the new version of the Practice Statement is decided by imID CJSC management. All changes are documented in the revision history. The approved document is then published.

imID CJSC management is responsible for enforcing the implementation of the practices defined in this Practice Statement across all operations and functions.

The review of the Practice Statement, certificate Policies and service specific practice statements is coordinated by the designated document owner. The process includes a formal review at least annually, documentation of all proposed changes in the revision history, approval by imID CJSC management (the CEO or the head of the functional division), versioning, and publication. Responsibility for maintaining the accuracy and currency of the documentrests with the document owner, as identified in imID CJSC's Document Management Procedure.

1.6 Definitions and Acronyms

Definitions and abbreviations used in this document are provided at the end.

2. Publication and Repository Responsibilities

2.1 Repository

imID CJSC has repository of:

- Publicly available documents along with previous versions (https://imid.am/policies);
- All published certificates (both active and revoked) and CRLs (http://pki.imid.am/).

The repository is intended for public use. The repository is available 24 hours a day, 7 days a week, subject to maintenance activities.

imID CJSC applies best endeavors to ensure that the repository is not unavailable for longer than 24 consecutive hours as a result of factors within its control. Planned maintenance windows are announced in advance via the imID CJSC website.

2.2 Publication of Certification Information

The repository contains the following documents and information:

- Practice Statement - current and previous versions;
- Trust Service Policies - current and previous versions;
- PKI Disclosure Statement
- Terms & Conditions for various trust services;
- Additional information, such as notifications about incidents;
- CA Certificates and profiles;
- Certificates Revocation Lists (CRLs).

The repository maintains both current and previous versions of these electronic documents.

2.3 Frequency of publication

Publications are issued with the following frequency:

- Practice Statement and specific trust service policies - see Section 9.12.1;
- certificates of all Certification Authorities operating trust services within imID CJSC - upon every issuance of new certificates;
- Certificate Revocation List (CRL) - according to specific Trust Service Policy and certificate profile.

2.4 Access to publication

imID CJSC has implemented logical and physical security mechanisms to prevent unauthorized creation, deletion, or modification of information published in the repository.

3. Identification and Authentication

The requirements for identification and authentication practices originate from ETSI EN 319 411-1 and ETSI EN 319 411-2. These practices apply to the registration of Subjects in terms of certificate issuance and the processing of revocation requests.

Their description is outlined in the Trust Service Policy, available publicly in the repository referred to in Section 2.1.

3.1 Naming

Requirements for distinguished name forms and name constraints are defined in the applicable Trust Service Policy (see section2.1 repository).

3.2 Initial Identity Validation

Requirements for identity proofing and validation of certificate applicants are defined in the applicable Trust Service Policy.

3.3 Identification and Authentication for Re-key Requests

Requirements for re-key identification and authentication are defined in the applicable Trust Service Policy.

3.4 Identification and Authentication for Revocation Requests

Requirements for identification and authentication of entities requesting revocation are defined in the applicable Trust Service Policy.

4. Certificate Life-Cycle Operational Requirements

The requirements for certificate life-cycle practices originate from ETSI EN 319 411-1 and ETSI EN 319 411-2. These practices apply to certificate management.

Their description is outlined in the Trust Service Policy, available publicly in the repository referred to in Section 2.1.

4.1 Certificate Application

Requirements for certificate application procedures are defined in the applicable Trust Service Policy.

4.2 Certificate Application Processing

Requirements for processing certificate applications are defined in the applicable Trust Service Policy.

4.3 Certificate Issuance

Requirements for certificate issuance and Subscriber notification are defined in the applicable Trust Service Policy.

4.4 Certificate Acceptance

Requirements for certificate acceptance by Subscribers are defined in the applicable Trust Service Policy.

4.5 Key Pair and Certificate Usage

Requirements for Subscriber and Relying Party obligations regarding key pair and certificate usage are defined in the applicable Trust Service Policy.

4.6 Certificate Renewal

Requirements for certificate renewal without re-keying are defined in the applicable Trust Service Policy.

4.7 Certificate Re-key

Requirements for certificate re-key (replacing the key pair) are defined in the applicable Trust Service Policy.

4.8 Certificate Modification

Requirements for certificate modification due to changes in Subscriber information are defined in the applicable Trust Service Policy.

4.9 Certificate Revocation and Suspension

Requirements for certificate revocation and suspension, are defined in the applicable Trust Service Policy.

4.10 Certificate Status Services

Requirements for CRL publication frequency and OCSP response are defined in the applicable Trust Service Policy.

4.11 End of Subscription

Requirements governing end of Subscriber relationship and associated certificate handling are defined in the applicable Trust Service Policy.

4.12 Key Escrow and Recovery

imID CJSC does not practice key escrow or key recovery for CA private keys.

CA private keys are not disclosed to third parties and are not made recoverable outside the controlled CA key management environment. Where CA private-key backup is implemented for service continuity or disaster recovery, it is performed under controlled key management procedures and does not constitute key escrow or key recovery.

5. Management, Operational, and Physical Controls

This section presents the general practices derived from ETSI EN 319 401 and ETSI EN 319 411-1 concerning the management, operational and physical controls implemented by imID CJSC.

A formal management process establishes the controls, ensuring regular reviews and updates. The imID CJSC management approves the risk assessment and accepts the identified residual risk.

imID CJSC has defined an Information Security Policy that is documented, approved by the Chief Executive Officer, implemented, maintained, and reviewed at least annually to ensure its continuing suitability, adequacy, and effectiveness. The policy sets out imID CJSC's approach to managing information security across its facilities, systems, and information assets. Changes to the Information Security Policy that affect the level of security provided are approved by CEO and communicated to subscribers, relying parties, assessment bodies, and Supervisory Body or other regulatory bodies as applicable.

5.1 Physical Security Controls

imID CJSC uses strong physical and environmental security measures to protect its data.

Regarding physical security, the following controls are in place:

- Advance request is required for entry to data centres and the imID CJSC office
- All access points are continuously monitored by CCTV
- Multiple secured doors protect access to sensitive areas
- Server racks are locked with cypher lockers at all times
- Security personnel are present at all times in data centres and the office
- All entries and exits are logged for traceability
- Facilities are protected against natural disasters through disaster recovery readiness with imID's 2nd Active data-centre
- Structural integrity is equally mitigated through disaster recovery readiness with imID's 2nd Active data-center
- Fire detection, suppression systems, and fire-rated enclosures are in place and regularly tested
- Utility failures are mitigated with redundant power, generators, UPS, cooling, telecoms, and environmental monitoring
- Assets are protected against theft, tampering, and break-ins using hardened structures and intrusion detection

A key element of protection is the establishment of the security zones, including a high-security perimeter. Within the most secure zone, imID CJSC stores Root CA systems and HSM devices, which are essential for services like certificate generation and revocation management. Access to this area is strictly controlled and requires dual control. The Root CA private key is stored in offline mode.

imID CJSC office has controlled remote access to the CA environment provided through a secure communication channel which is available only for authorized personnel in trusted roles.

5.1.1 Additional Physical and Environment Security Controls

- Staff privacy screen filters are utilized to secure visual on-screen access to authorized personnel
- Facilities are protected against natural disasters, including but not limited to floods, fire, and severe weather, through structural resilience measures and environmental safeguards by means of imID CJSC's 2nd data center in Active configuration.

- Fire safety measures are implemented, including automatic fire detection and suppression systems, fire-rated enclosures, and regular inspection and testing of fire-protection equipment;
- Risks arising from failure of supporting utilities—such as electrical power, telecommunications connectivity, cooling, and other essential services—are mitigated through redundant power supplies, UPS systems, backup generators, redundant network connections, and environmental monitoring;
- Protections are implemented to reduce risks of structural failure, including building integrity controls, preventive maintenance, and continuous monitoring of critical infrastructure components;
- Appropriate measures are in place to detect and prevent plumbing leaks and water intrusion, including leak-detection systems and segregation of sensitive equipment from high-risk areas;
- Assets and facilities are safeguarded against theft, tampering, and break-in attempts through physical hardening, intrusion detection mechanisms, and secure storage of sensitive devices;

imID CJSC's infrastructure is BCP-ready and provides redundancy and high availability of Trusted services across its data centers. imID is using a co-location model in enterprise-grade data center providers. imID CJSC data centers are equipped with logical and physical controls that make its CA and TSA operations inaccessible to non-trusted personnel. imID CJSC operates under a security policy designed to detect, deter, and prevent unauthorized access to imID CJSC's operations. A number of physical access controls are in place to ensure that access is monitored and strictly controlled.

A Service Level Agreement is in place between imID and the data center providers to guarantee uninterrupted and secure operation.

5.2 Procedural Controls

5.2.1 Trusted roles

The functions and tasks performed by personnel in Trusted Roles are distributed so that no single individual acting alone can circumvent security measures or subvert the security and reliability of imID's trust service operations.

The following Trusted Roles are established in imID CJSC's Trusted Roles documentation:

- **Security Officers:** responsible for supervising the implementation of imID's information security practices across all trust services; provides input in change management, initiates and oversees cryptographic key generation ceremonies; assigns security rights and supports annual risk assessment for trust services.
- **System Administrators:** install and configure hardware and software for operating systems; and maintain system and network resources.
- **System Operators:** handle standard system operations, including the creation of backup copies and the transfer of current copies and archives to offsite locations.
- **Registration Officers:** verify Subjects' identity, accept applications/requests for certificate issuance and verify the correctness of submitted requests; may initiate and authorise certificate issuance/revocation following successful verification.
- **System Auditors:** monitor services to ensure compliance with applicable policies and procedures; and review event logs and the incident management process.

5.2.2 Four-eyes principle

For highly security-critical operations, at least two individuals must be involved as a fundamental requirement. This is enforced through technical and organizational controls, including access permissions and knowledge verification.

5.2.3 Identification and authentication for each trusted role

imID CJSC has implemented an onboarding procedure for each trusted role, which includes issuing personal authentication credentials to the IT systems and physical premises. Personnel are not allowed to have access to the trusted functions until the necessary checks are completed.

Every account is unique and assigned to one specific person, ensuring accountability.

Each person assigned to a trusted role formally accepts the responsibilities associated with it.

Access rights assigned to each trusted role are reviewed at regular intervals, and at a minimum annually, to verify that they remain appropriate and consistent with the principle of least privilege. Any access rights that are no longer required are revoked without delay.

Formal appointments to trusted roles within imID are made by the CEO. Such appointments are documented and retained as part of imID CJSC's personnel records.

5.2.4 Roles Requiring Separation of Duties

All personnel assigned to trusted roles shall be free from conflicts of interest that could compromise the impartiality or integrity of trust service operations.

Each trusted role is granted only the permissions necessary for the assigned responsibilities. Some roles may be combined or modified within a limited scope. The role of System Auditor remains strictly separated from all other trusted roles.

imID CJSC has a substitution system in place that ensures continuity of operations while maintaining compliance with the required separation of duties.

imID CJSC enforces the separation of security administration functions from operational functions through role-based access controls. The use of system utility programs -including diagnostic tools, configuration management utilities, and privileged system management software- is restricted to authorised administrators, requires documented justification, and is subject to logging and periodic review.

5.3 Personnel Controls

5.3.1 Qualifications, experience and clearances

imID CJSC ensures the trustworthiness and competence of all personnel involved in the management and operation of trust services through rigorous vetting and specific qualification standards.

- **Identity Verification**: Every individual must appear in person before an authorized imID CJSC representative to verify their identity using government-issued photo identification prior to assignment.
- **Background Vetting**: Personnel assigned to Trusted Roles shall undergo a formal background check encompassing one or more of the following: identity verification, reference checks, verification of criminal records and were deemed necessary other verification means as determined by imID CJSC.
- **Technical Competency**: Candidates for Trusted Roles must demonstrate professional proficiency in Certification Authority, Public Key Infrastructure (PKI) and digital signature technology.
- **TSA Specialization**: Personnel involved in Time-Stamping operations must possess documented knowledge of time-stamping technology, mechanisms for the calibration of clocks with UTC, and associated security procedures.
- **Clearance and Refresh**: Background checks are refreshed, and personnel suitability is re-adjudicated at least once every **five (5) years**.
- **Confidentiality**: All personnel are contractually bound by professional secrecy and confidentiality obligations that persist even after the termination of their employment or contract.
- **Supplier Compliance**: These requirements are binding for all third-party contractors and service providers who perform critical trust service functions

5.3.2 Personnel verification procedures

For Personnel assigned to Trusted Roles, imID CJSC verifies information in accordance with relevant laws, regulations and principles of ethics. The checks are proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

imID CJSC ensures that personnel will not have access to the Trusted functions until the necessary checks are completed.

5.3.3 Training requirements

Managerial personnel responsible for trust services shall possess proven experience or dedicated training in trust service operations, information security, and risk management appropriate to their responsibilities.

In addition, imID CJSC requires trusted roles to meet strict competence and experience criteria at hiring and provides regular training to maintain their qualifications. Training covers at least:

- national and EU regulations;

- role responsibilities and tasks;
- disaster recovery procedures;
- information security policies;
- security controls and procedures based on this document and other policies;
- personal data protection.

5.3.4 Training frequency and requirements

All personnel shall receive security and cybersecurity awareness training, including updates on new threats and current security practices, at least once every 12 months. Items described in Section 5.3.3 must be repeated regularly or whenever significant changes are made to the Practice Statement or other policies.

5.3.5 Job rotation frequency and sequency

Not applicable.

5.3.6 Sanctions for unauthorized actions

Personnel are contractually bound to perform their duties in accordance with applicable internal rules and policies. Failure to comply with such obligations may result in disciplinary or other responsibility measures pursuant to the terms of the employment contract and in accordance with the labour legislation of the Republic of Armenia.

5.3.7 Independent contractor requirements

Independent contractors are subject to privacy protection and confidentiality conditions. Under a signed contract, the persons or consultants are subject to the same verification procedure as those defined under the HR policy.

5.3.8 Documentation available to personnel

Personnel of imID CJSC has access to the following documents:

- ImID CJSC Practice Statement;
- imID CJSC Trust Service Policy for Root CA;
- imID CJSC Trust Service Policy for the issuance of authentication certificates, qualified certificates for electronic signatures and for the management of remote signature creation devices;
- imID Trust Service Policy for Time Stamp Authority;
- imID CJSC Trust Service Policy for the Issuance of Certificates for Authentication and Advanced Electronic Signatures of the imID MobileID System.

5.3.9 Cybersecurity measures for remote work

When personnel perform duties remotely, imID CJSC shall apply cybersecurity measures ensuring the protection of all information accessed, processed, or stored outside imID premises.

5.3.10 Remote Working Policy

imID CJSC permits remote work only for authorized personnel under strict security conditions to protect information accessed, processed, or stored outside imID premises.

- **Secure Connectivity**: All remote access to internal systems is conducted exclusively via encrypted channels that provide assured identification of endpoints and protection against data modification.
- **Authentication**: Multi-factor authentication (MFA) is mandatory for all remote administrative and operational access to trust service components.
- **Data Protection**: Sensitive information is not stored on personal or unauthorized media; all work is performed within secure, managed sessions.

5.3.11 Termination and Change of Employment

Upon termination of employment or a contractual relationship, imID CJSC ensures that all organisational assets including equipment, access tokens, cryptographic devices, documentation, and any other items issued to the individual, are returned before or on the day of departure. Access rights to all IT systems, physical premises, and trust-service infrastructure are revoked on or before the effective date of termination, in accordance with imID CJSC's established access management procedures and ETSI. The same requirements apply upon a change of role that results in a reduction of access privileges, with rights adjusted to reflect the new responsibilities without delay.

5.4 Audit logging procedures

5.4.1 Types of events recorded

imID CJSC generates and records events related to trust services and electronic identification services which can be provided as evidence for legal proceedings. All logs are stored locally and transmitted to centralized log servers. The centralized log servers enforce the logging policy, including retention and archiving requirements. Logs contain, at a minimum, the following information:

1. Life Cycle of Keys and Certificates

- CA - related keys & certificates (e.g. OCSP, TSU) lifecycle management
- Subscriber key pairs lifecycle management
- Events relating to certificate generation, issuance, publication, and dissemination

2. Registration and Revocation Information

- Registration events & information gathered by Registration Authority
- Identity proofing records (type of documents, identification numbers, and validation methods)
- Identity of the Registration Authority employee accepting the application
- Storage location of copies of applications
- Name of Registration Authority processing the subscriber application
- Requests and reports relating to revocation and resulting actions

3. Significant Security, System, and Clock Synchronization Events

- Changes in the security policy settings
- System start-up and shutdown
- System crashes and hardware failures
- Changes in firewall configuration and rule base

- PKI system access attempts
- Activities of system users with superuser rights
- Synchronization of the clock to UTC
- Detection of loss of synchronization
- Inbound and outbound network traffic;
- Activities regarding user administration and permission management, and access (including privileged access) to systems and applications;
- Activities performed with administrator accounts;
- Access or changes to critical configuration files and backups;
- Physical access to facilities, where appropriate;
- Access and use of network equipment and devices;
- Environmental events, where appropriate.

4. Audit Log Metadata (Per Record Requirements)

- Type of event
- Event identifiers
- Date and time of the event
- Source of the event
- Identity of the person or the service generating the entry
- Status
- Description of the entry

Only authorized persons from the imID CJSC staff have access to the information in the records.

The primary sources of logs are applications and systems related to trust services and electronic identification systems.

The time used to record all logged events is synchronised with Coordinated Universal Time (UTC) at least once every 24 hours using trusted GNSS-based NTP time sources. Synchronisation events and any detected loss of synchronisation are recorded in the audit logs.

5.4.2 Frequency of processing log

The logs and monitoring are regularly checked for discrepancies. Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3 Retention time for records

All events related to certificates are maintained for 7 years after the certificate has expired or has been revoked. Logs regarding security events and events related to the clock synchronisation are kept according to internal risk assessment for time period necessary for legal proceedings.

5.4.4 Protection of records

imID CJSC stores logs on dedicated storage. To ensure integrity and confidentiality, imID has implemented security controls, including monitored access that requires authorization to prevent unauthorized access.

After the retention period, all records are securely transferred to archival media, and this process is monitored and traced.

In the event of legal proceedings, imID CJSC can restore and provide evidence as required through its 7-year eIDAS Regulation compliant retention period.

Audit logs and archived records shall be protected against unauthorized deletion or destruction, ensuring they remain intact for the full duration of their required retention period.

Storage media is protected against theft through physical security controls including locked storage facilities and asset tracking. At the end of the required retention period, storage media containing sensitive or personal data is securely sanitised or physically destroyed in accordance with imID CJSC's internal document defining media management and secure disposal policy, ensuring that data cannot be recovered from deleted files or reallocated storage objects. Each disposal event is documented and verified.

5.4.5 Backups of records

Records are regularly backed up and securely stored in accordance with established procedures including specific schedule. Integrity checks are performed after the completion of each backup task.

Backup arrangements are tested at least annually to verify that essential information and software can be successfully restored, and that recovery capabilities meet the requirements defined in the Business Continuity Plan.

Adequate backup facilities are maintained to ensure that all essential information and software can be fully recovered in the event of a disaster or media failure.

5.4.6 Audit log accumulation system

Each application automatically collects and transmits log entries to the logging system.

The logging functions are initiated automatically when the system starts and are continuously maintained throughout the entire operational period of the system.

5.4.7 Notification system to event-causing

IT systems are continuously monitored using monitoring tools.

ImID CJSC maintains a monitoring team that oversees the system, ensuring real-time tracking of performance metrics and security events.

In the event of activities impacting system security, the system is configured to automatically generate alerts that are sent via communication channels. These alerts are immediately directed to the Security Officer and the System Administrator.

In the event of identifying a significant incident, the incident management procedure is activated, which includes notification to the supervisory body and, on a per need basis, to the users of imID services.

Monitoring activities are designed and operated with consideration to the sensitivity of any information collected or analysed adhering to the data minimisation concept limited to only necessary data. Access to monitoring data and system alerts is restricted to authorised personnel.

imID CJSC has established and maintains an incident communication plan that defines: incident categorisation levels; well-defined escalation procedures specifying roles and responsibilities at each level; and standardised reporting protocols for internal notifications and external communications to supervisory bodies, affected parties, and other stakeholders as applicable.

A reporting procedure is available for staff, contractors, and customers to report possible network and information security incidents. This reporting channel (including a dedicated support email and hotline) is communicated to contractors through contractual provisions and to customers through the imID Operations Center portal and Terms and Conditions. imID CJSC staff are trained on the reporting procedure and directed to address reports to the appropriate point of contact.

5.4.8 Vulnerability assessment

imID CJSC has implemented a vulnerability management procedure and a risk management procedure. In accordance with these procedures, imID CJSC systems are subject to vulnerability scanning at least monthly. If any vulnerabilities are detected, the vulnerability management procedure is activated to address and mitigate the identified risks within set timelines based on the triaging for applicability and criticality of the discovered vulnerability.

Critical vulnerabilities (CVSS 9.0–10.0) are addressed within 48 hours while noncritical vulnerabilities are subject to timeframes determined by the security zone of the affected asset, ranging from under 12 hours to under 7 days . For each identified vulnerability, imID CJSC either remediates within the applicable SLA, or — where remediation is not feasible within the SLA — formally documents a risk acceptance and treatment plan to mitigate vulnerability in accordance with imID Risk Management Policy, including mitigating controls, an expiry date, and approval by the relevant authority. Where a vulnerability is architecturally non-exploitable in imID's environment, a technical exemption is documented in the internal portal with approval from the CTO and Head of Information Security, without requiring full risk acceptance governance.

imID CJSC carries out a risk assessment to identify threats to and vulnerabilities of the assets supporting the provision of trust services, encompassing operational, financial, legal/compliance, information security and other risks. The risk assessment is reviewed at least annually and whenever significant changes to the operating environment occur or an incident involving assets is identified.

5.5 Records Archival

5.5.1 Types of archives

imID CJSC archives all data related to:

- physical or digital records about certificate applications, signed Subscriber agreements and documents, registration information (including evidence of Subject identity verification) and requests or applications for revocation;
- all requests submitted by users of imID CJSC services including certificate application;
- all events relating to the life cycle of keys managed by the CA, including any Subject key pairs generated by the CA;
- other documents related to the trust service and electronic identification service provision.

5.5.2 Retention period of archives

Archived data (paper and electronic) is stored for a minimum 7 years after any certificate based on these records ceases to be valid.

5.5.3 Protection of archive

imID CJSC stores archives on dedicated storage. To ensure integrity and confidentiality, imID has implemented security controls, including monitored access that requires authorization and encryption of media storage to prevent unauthorized access.

During the preservation period, imID CJSC monitors the media on which archived data is stored to ensure data availability throughout the required retention period.

To protect against media obsolescence and deterioration, imID CJSC maintains a media refresh cycle and migrates archived data to new media before existing media reaches end of service life or shows signs of degradation. The condition of archive media is checked via live monitoring which logs and generates alerts delivered to imID CJSC's IT Engineering team for remediation.

Archive media containing sensitive data is protected against theft through physical access controls and asset tracking. At the end of the required retention period, archive media is securely sanitised or physically destroyed. Sensitive data cannot be recovered from deleted files or reallocated storage objects after disposal. Disposal events are documented.

5.5.4 Backup archives procedures

imID CJSC has implemented a backup process for archives to ensure data recovery in the event of primary media failure. This mechanism guarantees the ability to restore archives from backup copies.

Detailed procedures for archiving, backup creation, and data recovery are outlined in the internal documentation.

5.5.5. Requirements for Time Stamping the archives

Electronic archives are time stamped by imID CJSC qualified time stamp service.

5.5.6 Archive storage

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction.

5.5.7 Archival information access and verification procedures

Access to the archive is granted only to individuals holding trusted roles and is possible only after successful authorization.

To verify the integrity of archived data, periodic tests are conducted. This process may be carried out under the supervision of the system administrator and the security officer and must be documented in the event log.

5.6 Key Changeover

The key changeover procedure applies to the keys of certification authorities (Root CA, Policy CA, subordinate CAs). The key exchange process is conducted in a manner that ensures the maintenance of the agreed minimum certificate validity period.

Before the expiration of any Certification Authority certificate, a new PKI is established. As part of this process, a new pair of keys and a certificate for the new Certification Authority are generated.

During the transition period, both the old and new certification authorities operate concurrently until the old authority's certificate expires. The new certification authority assumes the role of the expiring one and handles all certificate-related activities, including issuance, suspension, revocation, and CRL generation.

The expiring Certification Authority continues to process only the revocation of certificates issued under its own infrastructure and generates CRLs until its operational activity ceases upon certificate expiration.

The new Certification Authority's certificate is promptly published in the repository to ensure business and trust continuity.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

ImID CJSC maintains internal procedures to guide its staff in response to security incidents, natural disasters and similar events that may give rise to system outages or compromise. These include but are not limited to the following internally maintained documents: Business Continuity Plan, Disaster Recovery Plan and Incident Management Procedure.

imID CJSC tests the effectiveness of its Business Continuity and Disaster Recovery at least annually to ensure their reliability and adequacy.

imID CJSC's incident communication plan contained within its Incident Management Policy & Standard Operating Procedure defines the process for informing stakeholders about incidents that may affect the provisioning of trust services. Notification obligations include: the Supervisory Body or other Regulatory body, notified within 24 hours of a significant security breach or loss of integrity — and within 30 minutes in the event of a key compromise; subscribers and relying parties, notified of the incident; and law enforcement, where criminal activity is suspected.

5.7.2 Incidents related to failures in hardware, software and/or data

In the event of a failure or corruption of hardware, software, or data integrity, imID CJSC prioritizes the immediate restoration of secure operations and the preservation of evidence.

- **Reporting**: Any disruption to critical computing resources or suspected data corruption must be reported immediately to the **Incident Control Team (ICT)** and the **Security Officer**.

- **Assessment**: An immediate investigation is conducted to determine the severity of the incident and whether any Trust Service Tokens or private keys have been compromised.

- **Restoration**: System administrators shall restore services using the last known good configuration and verified backup media to ensure the integrity of the operational environment.

- **Integrity Verification**: Before returning a system to production, its integrity and configuration must be verified against the authorized security baseline.

- **Post-Incident Analysis**: Every significant failure requires a formal root-cause analysis to implement corrective actions and prevent recurrence.

The incident response procedure includes mechanisms for reassessing and reclassifying events as new information becomes available during an investigation. Events initially categorised at a lower severity level may be escalated upon identification of additional indicators of compromise, broader impact, or changes in the nature of the incident.

5.7.3 Private key compromise or loss of calibration of a TSU clock procedures

Key compromise is handled according to Incident Management documentation. If the particular key compromise is qualified as a disaster, the business continuity plan may be triggered.

In the event of a compromise or a suspected compromise of the private key of imID CJSC Certification Authority, the following actions are taken:

- the operating authority is immediately terminated;
- if time stamp authority is compromised, suspected compromise, or loss of TSU clock calibration, the imID CJSC will immediately cease issuing time stamps until corrective measures are implemented to restore secure and accurate operation;
- the Certification Authority generates a new key pair;
- all Subjects and Relying Parties are immediately informed;
- the certificate, corresponding to the compromised key is revoked with the appropriate reason for revocation;
- all Subject's certificates issued under the compromised CAs are revoked with the appropriate reason for revocation;
- new CA certificate is issued;
- new certificates are issued to affected Subjects;
- the new certificates are issued at the expense of imID CJSC;
- an instant analysis is made, and a report is prepared on the cause of compromise.

In the event of a compromise or suspected compromise of time stamp unit (TSU) keys imID CJSC will provide Subscribers with all necessary information to identify improperly issued time stamps. The information provided will include, among other details, the name of the qualified time stamp authority and the time during which the improper issuance of time stamps occurred.

If the cryptographic algorithms (or their parameters) used by imID CJSC certification authorities become insufficient to ensure an adequate level of trust services, imID CJSC will inform all certificate Subjects of this fact through public announcements.

imID CJSC shall clearly indicate that any certificates and revocation status information issued using the compromised CA key may no longer be valid or trustworthy. This is performed through the CRL publication on the imID CJSC website (http://pki.imid.am/) and OCSP service.

imID CJSC shall schedule and perform the mass revocation of all certificates affected by the use of insufficient or weakened cryptographic algorithms or parameters, ensuring timely mitigation of associated security risks through

reissuing of affected certificates via a new Certification Authority that fulfils updated cryptographic security requirements.

5.7.4 Business Continuity Management

To maintain the integrity of its services, imID CJSC implements data backup and recovery procedures as part of its Business Continuity Plan (BCP). Stated goals are to ensure the resilience of imID's Trust Services and the continuous availability of revocation status information.

imID CJSC's systems are redundantly configured at its primary facility and are mirrored at a separate, location for failover in the event of a disaster. If a disaster causes imID's primary CA or TSA operations to become inoperative, imID will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

5.7.5 Use of Information from National CSIRT and Competent Authorities

imID CJSC maintains a process for receiving, reviewing, and applying information provided by the National CSIRT or other competent authorities. The Security Officer evaluates such information and, where relevant, initiates preventive, corrective, or crisis-management actions in accordance with imID CJSC's Incident Management Procedure and Business Continuity Plan.

imID CJSC has established a Crisis Management Plan, maintained as part of its Business Continuity and Incident Management documentation. The plan addresses the following elements:

- Roles and responsibilities: In a crisis situation, a Crisis Management Team is activated. Defined roles include Crisis Coordinator, Communications Officer, Technical Lead, and Legal/Compliance, each with documented responsibilities for decision-making, escalation, and communication.
- Communications with competent authorities: Procedures exist for both mandatory and voluntary communications with relevant competent authorities during a crisis, including the Supervisory Body, the national CSIRT, and data protection authorities as applicable, in compliance with regulatory timelines and formats.
- Security controls in crisis: Appropriate controls for maintaining network and information security during a crisis are defined, including degraded-mode operation procedures, temporary access restrictions, and emergency key management measures.
- Testing and review: The Crisis Management Plan is tested at planned intervals (at minimum annually) and is reviewed following any significant incident as part of the post-incident review process. Test outcomes and review findings are documented and used to improve the plan.

5.8 CA or RA Termination

imID CJSC maintains an up-to-date termination plan in case of cessation of its trust services that outlines all necessary steps to minimize disruptions to Subscribers and Relying Parties.

Prior to service termination, imID CJSC will inform all affected entities, including Subscribers, other TSPs, and relevant authorities such as supervisory bodies. Information about the termination will also be made publicly available to other relying parties.

All subcontractors authorized to act on behalf of imID CJSC will have their authorization revoked before service termination.

If applicable, imID CJSC will transfer obligations to a reliable party for maintaining necessary records to provide evidence of the TSP's operations for a reasonable period (including revocation information and PKI infrastructure certificates). If no such information is held, imID CJSC will provide justification.

Before terminating services, imID CJSC will securely destroy or withdraw from use all private keys, including backup copies, ensuring they cannot be retrieved.

When feasible, imID CJSC will arrange the transfer of trust services for existing customers to another TSP.

imID CJSC identifies and documents all records subject to hand-over during service termination, including audit logs, registration information, certificate and key life-cycle records, and archived evidence retained under Sections 5.4 and 5.5, ensuring they remain available for the duration of their required retention period.

imID CJSC has arrangements to cover the costs to fulfil these minimum requirements in case the TSP goes bankrupt, or for other reasons, is unable to cover the costs by itself.

6. Technical security controls

This section describes practices derived from ETSI EN 319 411-1, ETSI EN 319 411-2, and ETSI EN 319 421. The requirements comprehensively cover the description of technical security controls, including primarily:

1. The management and protection of cryptographic material (private key generation, dissemination, activation, deletion etc).
2. IT security management and the lifecycle of security mechanisms.

Practices common to all services are specified in the following subsections, starting from Section 6.4.

imID CJSC uses a RQSCD certified under the requirements of Annex II of EU eIDAS Regulation within the scope of the services delivered my the means of imID App and imID Personal CA.

Separate trust service policies provide practices implemented by imID CJSC for each trust service.

6.1 Key Pair Generation and Installation

imID CJSC ensures that all cryptographic keys are generated in a secure manner that prevents compromise and ensures the integrity of the Public Key Infrastructure.

- **Key Generation Ceremony**: All Certification Authority (CA) keys must be generated during a formal, documented key ceremony.
- **Independent Oversight**: An independent, qualified auditor shall witness the ceremony for Root and Subordinate CAs to verify compliance with the stated procedures.
- **Hardware Security**: Generation must occur within a Hardware Security Module (HSM) certified to **FIPS 140-3 Level 3** or equivalent Common Criteria standards.
- **Trusted Roles**: A minimum of two individuals in Trusted Roles is required to perform the generation, ensuring no single person can access the private key material.

For imID Root CA and its subordinate Policy and Issuing CAs, as well as the end-user certificates refer to the documents describing the policies on the key management and certificate profiles:

Document name	**OID number**

imID CJSC Trust Service Policy for Root CA and Subordinate Certification Authority	1.3.6.1.4.1.63199.1.2
imID CJSC Trust Service Policy for the Issuance of Certificates for Authentication, Electronic Signatures and for the Management of Remote Signature Creation Devices (also referred to as Trust Service Policy for Personal CA)	1.3.6.1.4.1.63199.1.4

6.1.1 Supported Algorithms and Algorithm Identifiers

imID CJSC uses only cryptographic algorithms that are considered secure and suitable for the intended trust service.

For the RSA cryptography family, imID CJSC uses or permits, as defined in the applicable Certificate Profile, RSA with a minimum key length of 2048 bits, used together with at least the SHA-256 hash algorithm.

For the elliptic curve cryptography family, imID CJSC uses or permits, as defined in the applicable Certificate Profile, ECDSA with named curves providing a security strength at least equivalent to NIST P-256, used together with at least the SHA-256 hash algorithm.

Certificates encode the subject public key algorithm in the subjectPublicKeyInfo.algorithm field and the certificate signature algorithm in the tbsCertificate.signature and signatureAlgorithm fields, using AlgorithmIdentifier values in accordance with RFC 5280. The specific algorithm object identifiers and parameters are defined in the applicable Certificate Profile; see section7.1.

The suitability of approved cryptographic algorithms, key sizes, hash functions and certificate lifetimes is reviewed at least annually, and additionally when ETSI TS 119 312, SOG-IS guidance, or the applicable certificate profiles are updated. Algorithms or parameters that no longer remain suitable are phased out through controlled certificate profile updates.

6.2 Private Key Protection and Cryptographic Module Engineering

imID CJSC employs multi-layered physical and logical controls to safeguard the private keys used for providing trust services.

- **Multi-Person Control**: Access to CA private keys is strictly controlled through an **M-of-N** multi-person authentication scheme, requiring the presence of at least two authorized individuals.
- **Hardware Integrity**: Private keys are stored exclusively in HSMs that are physically protected within high-security perimeters and monitored 24/7 via CCTV and intrusion detection.
- **Root CA Isolation**: The Root CA private key is maintained in an **offline state** (air-gapped) and is only activated within the secure zone for specific signing operations.
- **Secure Destruction**: Upon expiration or revocation, all copies of the private key shall be destroyed in a manner that ensures they cannot be retrieved or reconstructed.

6.3 Other Aspects of Key Pair Management

Requirements for key archival, key deactivation, key destruction, and other aspects of key pair management are governed by the HSM management procedures and the applicable Trust Service Policy.

6.4 Activation Data

The data required to activate CA private keys is managed with the same level of security as the keys themselves to prevent unauthorized use.

- **Creation and Distribution**: Activation data (such as PINs or passwords) is generated by the individuals in Trusted Roles during the key ceremony.
- **Separation of Knowledge**: No single individual shall possess the full set of data required to activate a private key.
- **Secure Storage**: Activation data must be stored on secure, tamper-evident media and kept in physically separate safes from the hardware modules they activate.
- **Protection from Disclosure**: Personnel is strictly prohibited from sharing, recording, or disclosing activation data to unauthorized parties.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

imID CJSC ensures that the TSP's system components are secure and correctly operated. The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The TSP's components include the following security mechanisms:

- require authenticated logins for trusted roles;
- provide access control with least privilege;
- provide security audit capability;
- require use of strong password policy;
- require use of cryptography for session communication;
- provide means to maintain software and firmware integrity and up to date;
- multi-factor authentication;
- IT monitoring systems and alerting;
- clean-desk policy and auto-locking screen.

Only system administrators can access the server infrastructure and always through encrypted connections.

Certificates and CRLs are digitally signed by the applicable Certification Authority, allowing relying parties to verify their authenticity and integrity. All administrative actions affecting dissemination and revocation services are recorded and retained in accordance with the applicable audit logging requirements.

imID CJSC protects certificate dissemination services and revocation status services through technical and organizational access controls. Only authorized personnel acting in approved trusted roles are permitted to create, publish, update, or remove certificates, CRLs, revocation status information, and associated repository data. Access to the relevant systems is restricted through strong authentication, role-based access control, segregation of duties, and least-privilege principles.

Revocation status information may only be modified through authorized certificate lifecycle and revocation management processes. Unauthorized attempts to add, delete, modify, or otherwise manipulate certificates, CRLs, revocation status information, or associated repository data are prevented through access control mechanisms and are subject to monitoring and audit logging.

6.5.2 Computer security rating

Not applicable.

6.6 Life Cycle Security Controls

6.6.1 System development controls

imID CJSC follows a documented development methodology where all software and configurations including scripts and control files, are treated as formal code under change control.

- Security by Design: Every project requires a formal security requirements analysis and impact assessment before development.
- Isolation: All development and testing occur in environments logically or physically isolated from production.
- Validation: The software will be approved by the Security Officer and will originate from a trusted source. New versions of software are tested in a testing environment of the appropriate service, and their deployment is conducted according to documented change management procedures. Changes to systems are documented.
- Continuous Audit: System configurations are monitored and verified against the authorized baseline at least once per quarter.

Current configurations and changes of imID CJSC systems are documented through imID CJSC's Change Management practices.

The configuration of the TSP systems is checked and verified on a quarterly basis. One of the control mechanisms supporting this process is the internal audit, conducted in accordance with the approved schedule.

6.6.2 Life cycle security controls

imID CJSC ensures the continuing suitability and effectiveness of its security controls through planned maintenance and evaluation cycles.

- **Security Reviews**: imID CJSC policies, assets, and practices—including this Practice Statement—are formally reviewed at least annually, or upon significant infrastructure changes, to ensure ongoing adequacy.

- **Asset Management**: All information assets critical to trust service operations are registered and classified into security classes based on a formal risk assessment. A responsible person is appointed for every identified asset.

- **Patch Management**: Security patches for certification systems and supporting infrastructure are applied within a reasonable period, and in no event later than six months after becoming available. Reasons for delayed application of any patch must be formally documented.

Each entry in the asset inventory shall contain, where applicable: a unique asset identifier; a description of the asset; the designated asset owner; the asset location; the asset type (e.g. hardware, software, service, facility, personnel, or physical records); the type and classification level of information processed or stored; the date and version of the last update or patch; the overall classification level; and the asset's end-of-life or planned replacement date.

Rules for the acceptable use of information assets and associated handling procedures are documented in imID CJSC's Acceptable Use Policy. This policy is referenced in relevant agreements and supplier contracts, where applicable, and is reviewed at least annually, consistent with the guidance in ISO/IEC 27002:2022 clause 5.10.

6.7 Network Security Controls

imID CJSC ensures the following network security controls:

- Network segmentation;
  - high security zone (HSM and PKI) with no direct Internet access;
  - communication between network zones is restricted;
  - RootCA is kept offline
- Access control;
  - restricted physical and logical access to network devices;
  - secure Internet communication through encrypted transport to protect data transmission.
  - ensures that only personnel in Trusted Roles have access to its data center secure zone
  - the certificate dissemination application and revocation status application (OCSP/CRL) enforce access control; only authorised CA system accounts may publish certificates or update revocation status information; all access attempts are logged.
- Network separation;
  - physically segregated and air-gapped administrative network from operational activities to isolate TSP functions
  - clear separation between corporate IT, production and non-production environments.
- Hardening;
  - configuration hardening through the deactivation of unnecessary ports and services to minimize attack surfaces.
- Monitoring;
  - implementation of firewalls to control incoming and outgoing network traffic;
  - firewalls are configured to deny all inbound and outbound protocols and access not required for the operation of imID CJSC, implementing a default-deny posture;
  - NOC team is responsible for monitoring and detection of abnormal events.
- Configuration audits;
  - regular internal audits of network configurations to ensure compliance with security policies and best practices.
- Encryption
  - Hardware supported & enforced encryption on Trusted estate devices
  - Inter-site communication secured via cryptographic securing of data traffic
  - Split-key technology for physical hardening of cryptographic ciphers & user protections
- Pro-active security testing
  - Monthly and ad-hoc vulnerability scans of public and private IP addresses identified by imID CJSC; scans are performed by or on behalf of qualified personnel with appropriate skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report;
  - At least annual external penetration testing of certification systems, and after infrastructure or application upgrades or modifications that imID CJSC determines are significant;
  - Penetration testing is performed by an independent organisation, adherent to the highest standards of proficiency, code of ethics and independence necessary to provide a reliable report during a) initial set-up, b) after significant infrastructure or application changes and c) at least annually.

- Deployment of anti-virus and anti-malware protection providing both detection and removal capabilities, deployed across network and information systems; definitions and signatures are updated at least daily.

6.8 Time Synchronization

The systems supporting certificate revocation and status information services synchronize their clocks with UTC using trusted GNSS-based time synchronization sources. Synchronization is performed automatically and at least once every 24 hours. Time synchronization status is monitored, and relevant synchronization events and failures are recorded in audit logs.

All audit events are timestamped using the synchronised system time, ensuring the integrity and non-repudiation of the audit trail. Accurate time synchronisation is also used to support certificate status validation, signature authorisation processes, security monitoring and other trust service operations requiring reliable time information.

6.9 Time Stamping

imID CJSC uses a Time Stamp service for archiving purposes.

7. Certificate, CRL, and OCSP Profiles

imID CJSC issues certificates and revocation information in strict accordance with ITU X.509 v3 standards and the specific profiles mandated by the ETSI EN 319 412 series.

7.1 Certificate Profile

All certificates are generated as X.509 v3 certificates. Each issued certificate includes a unique serial number containing at least 64 bits of output from a cryptographically secure random number generator. Profiles adhere to the following standards:

- **ETSI EN 319 412-1**
- **ETSI EN 319 412-2**
- **ETSI EN 319 412-3**
- **ETSI EN 319 412-5**

7.2 CRL Profile

Certificate Revocation Lists are issued as X.509 v2 CRLs. Each entry must include a reasonCode extension utilizing the standard reason codes defined in RFC 5280 (e.g., keyCompromise, affiliationChanged, superseded).

7.3 OCSP Profile

Online Certificate Status Protocol responses conform to RFC 6960. Responses are signed by the issuing CA or a dedicated OCSP responder whose certificate is issued by the relevant CA.

8. Compliance Audit and Other Assessment

imID CJSC maintains continuous compliance through a multi-layered audit framework comprising external conformity assessments and internal technical self-audits.

- **External Audit Frequency**: A conformity assessment is conducted by an independent external auditor — a Conformity Assessment Body (hereinafter also referred to as a CAB or external auditor) accredited in the European Union — once every two years, with an interim check conducted in the period between assessments. The scope of each assessment is determined in accordance with the applicable requirements and standards, and will include but is not limited to the evaluation of information systems, policies, facilities, and assets.
- **Audit Schemes**: Assessments are performed in accordance with the specific requirements of **ETSI EN 319 401 v.3.1.1, ETSI EN 319 411-1 v.1.5.1**, **ETSI EN 319 411-2 v.2.6.1.**, and **ETSI EN 319 421 v1.3.1, ETSI EN 431-1 v. 1.3.1**.
- **Auditor Qualifications**: External audits are exclusively performed by a Conformity Assessment Body (CAB) accredited to **ISO/IEC 17065** and **ETSI EN 319 403**.
- **Internal Self-Audits**: On at least an annual basis, imID CJSC performs internal self-audits against a randomly selected sample of at least **three percent** of all certificates issued since the previous internal audit.
- **Deficiency Remediation**: If an audit reports a non-compliance, imID CJSC shall develop a formal corrective action plan within reasonable timeline. Remediation must be completed within the time limit set by the Supervisory Body or as mandated by the relevant ETSI standard.
- **Publication**: Conformity certificates and audit conclusions are published in the public repository.

8.1 Frequency or circumstances of assessment

The conformity of information systems, policies, practices, facilities, personnel and assets of imID CJSC are assessed by a CAB pursuant to the Armenian Law, eIDAS Regulation, ETSI standards.

Conformity is assessed at least every 2 years and when any major change is made to Trust Service operations.

imID CJSC has appointed system auditor who conducts internal reviews and audits in accordance with its audit program.

8.2 Qualification of auditors

External audits are conducted by a CAB accredited according to ISO/IEC 17065, as outlined by ETSI EN 319 403, with a focus on meeting the requirements specified in the eIDAS Regulation (EU) No 910/2014. The CAB is authorized to perform conformity assessments of Qualified Trust Service Providers and their services.

The internal audit is performed by imID CJSC employees with the necessary experience and qualification.

8.3 External auditor's relationship with imID CJSC

imID CJSC has chosen an external auditor who is entirely independent from the organization.

8.4 Audit scope

The CAB audits all parts of the information system used to provide Trust Services.

The audit by the Conformity Assessment Body covers the entire imID CJSC operations for the provision of qualified certification services under consideration of all standard and standardization documents related to the Armenian Law and Regulation (EU) No 910/2014:

- documentation;
- Archives, as fully defined in section "5.5.1 Types of Archives" of this document;
- information data related to the issuance and management of qualified certificates;
- physical and information security and reliability of the technological system and management.

The scope of internal audits includes:

- verification of the TSP's activity and its compliance with the Trust Service Policies and Practice Statement;
- comparison of the practices and procedures outlined in this document with their practical implementation during operation;
- verification of the processes performed by the Registration Authority.

8.5 Actions taken as a result of deficiency

The reports of internal and external audits are submitted to the imID CJSC management.

Where the CAB identifies deviations or non-compliance in the assessment, the Supervisory Body requires from TSP to remedy these to fulfil requirements within a time limit set by the Supervisory Body.

imID CJSC aims for full compliance and timely correction of non-conformities.

8.6 Communication of results

The results of the performed internal and external audits are not published.

The certification document received by the Conformity Assessment Body may be published on imID's website.

9. Other business and legal matters

9.1 Fees

9.1.1 Trust service prices

Specified in relevant Terms and Conditions or agreement with Subscriber.

9.1.2 Prices for access to certificates

Specified in relevant Terms and Conditions or agreement with Subscriber.

9.1.3 Prices for revocation or status information

imID CJSC does not charge a fee for certificates revocation, publishing certificates in CRLs and making CRLs published in the repository (or elsewhere) accessible to relying parties.

9.1.4 Prices for other services

Specified in relevant Terms and Conditions or agreement with Subscriber.

9.1.5 Rules for cost refunds

imID CJSC handles refund requests case-by-case. Further details are set forth in the relevant terms and conditions.

9.2 Financial responsibility

9.2.1 Insurance cover

imID maintains appropriate insurance policy to ensure compliance with the requirements of Republic of Armenia Government Decree 1015-N, as well as with Article 24(2)(c) of the eIDAS Regulation and to cover potential liabilities arising from its relevant activities, ensuring continuity and compensation capacity.

9.2.2 Other resources for maintaining operations and compensation for damage

Not applicable

9.2.3 Insurance or warranty for end users

Equally covered in section 9.2.1.

9.3 Confidentiality of business information

9.3.1 Definition of confidential business data

All personal data and information processed under the imID CJSC Information Security Policy are classified as non-public.

9.3.2 Business data not treated as confidential

Information considered public is listed in section 2.2 of this document.

9.3.3 Responsibilities for the protection of confidential business data

imID CJSC has implemented the Information Security Policy in terms of protection of any confidential business data.

imID CJSC's Information Security Policy is documented, implemented, maintained, and reviewed at least annually to ensure its continuing suitability, adequacy, and effectiveness. The policy is approved by the relevant management body in accordance with the governance system and covers security controls and operating procedures for imID CJSC's facilities, systems, and information assets providing trust services.

Changes to the Information Security Policy that affect the level of security provided are approved by the CEO of imID CJSC. Where such changes are relevant to subscribers, relying parties, assessment bodies, or supervisory bodies and other regulatory bodies, they are communicated through the appropriate channels, including publication on the imID CJSC website.

9.4 Privacy of personal information

With respect to the relations pertaining to the processing of personal data imID is governed by the Constitution of the Republic of Armenia, international treaties of the Republic of Armenia, the Law on Personal Data Protection (adopted on 15.05.2015),applicable government decrees and ImID CJSC Privacy Policy.

The Law of Republic of Armenia on Protection of Personal Data guarantees the rights of natural persons (data subjects) and imposes mandatory requirements on personal data processors, controllers, authorised persons, and third parties.

9.5 Intellectual property rights

The trust services operated by imID CJSC are owned by imID CJSC. All trademarks, patents, trade names, service marks, logos, and other intellectual property rights used in connection with the services are the property of imID CJSC or their respective legal owners and are protected under applicable intellectual property laws.

9.6 Representations and warranties

9.6.1 Certification Authority obligations and warranties

imID CJSC shall:

- provide its services consistently with the requirements and the procedures defined in this Practice Statement and in accordance with the rules under which this Practice Statement is established;
- provide services in compliance with Armenian Law, eIDAS Regulation and related technical standards;
- maintain a publicly available repository of relevant documents and information;
- adhere to and implement the procedures outlined in this document;
- issue certificates containing accurate data at the time of the registration;
- ensure that certificates do not contain any mistakes resulting from negligence or procedural violations by individuals confirming applications for certificate issuance or issuing certificates;
- not copy or store private keys of Subjects outside of HSM devices;
- protect the integrity and confidentiality of personal data;
- inform the Conformity Assessment Body and National Supervisory Body of any changes to a public key used for the provided Trust Services;
- notify the Supervisory Body within 24 hours of becoming aware of any security breaches or loss of integrity that significantly impacts the Trust Service provided;
- inform affected natural or legal persons without undue delay if a breach of security, loss of integrity, or personal data breach is likely to adversely affect them;
- preserve all documentation, records and logs related to Trust Services as outlined in section 5.4 for logs and section 5.5 for archival;
- maintain the financial stability and resources necessary to operate in accordance with this Practice Statement;
- ensure its employees receive adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

imID CJSC further warrants that it has documented agreements with its subcontracting parties. These contracts include defined liabilities, ensuring that agreements with critical service providers, including cloud service providers, contain service level commitments and/or audit provisions requiring them to implement security measures aligned with imID CJSC's information security requirements and risk assessment.

imID CJSC establishes and maintains a register of suppliers and their agreements to track where imID CJSC information is managed and archived. This register identifies all direct suppliers and sub-processors, the services or products provided, and the information security obligations contained in each agreement. The register is reviewed and validated annually to ensure agreements remain valid, fit for purpose and include information security clauses where applicable.

9.6.2 Registration Authority obligations and warranties

imID CJSC, as a Registration Authority (RA), maintains formal agreements with entities performing registration authority services through their Registration Points.

imID CJSC is accountable for authorizing and supervising these Registration Points, ensuring they operate in accordance with contractual obligations, applicable laws and regulations.

Each agreement includes specific provisions that:

- impose strict obligations regarding the confidentiality of all processed information, including personal data;
- define responsibilities for the secure processing, storage, archival, and destruction of data;
- ensure that identity verification services are delivered in accordance with the procedures aligned with this Practice Statement, internal operational policies, and applicable legal requirements;
- require the transmission of verified Subject identity data to the Certification Authority in a secure and controlled manner;
- subject the Registration Points to regular audits conducted by imID CJSC or by third parties commissioned by imID CJSC;
- mandate regular training of personnel, either internally or through training provided directly by imID CJSC.

Agreements with Registration Point operators are maintained in imID CJSC's supplier register and reviewed at defined intervals to verify they remain current, fit for purpose, and incorporate the applicable information security requirements.

9.6.3 Time Stamp Authority obligations and warranties

imID CJSC warrants to all Subscribers and Relying Parties that its Time-Stamping Service is operated in strict accordance with the following technical and legal mandates:

- **Time Accuracy**: Each electronic time-stamp token is issued with an accuracy not exceeding one second from Coordinated Universal Time (UTC).
- **Service Availability**: imID CJSC commits to fulfilling revocation requests within 24 hours of the receipt of the request.
- **Standards Compliance**: All tokens are issued in accordance with **ETSI EN 319 422** and utilize cryptographic suites that conform to **ETSI TS 119 312**.
- **Evidence Preservation**: imID CJSC warrants the preservation of all electronic records, logs, and evidence related to the issuance of time-stamp tokens for a minimum period of **seven (7) years** to support future legal verification.
- **Manipulation Prevention**: The Authority utilizes synchronized hardware clocks and audited operational procedures to prevent any unauthorized modification or manipulation of time data.
- **Risk Management**: imID CJSC warrants that a dedicated risk assessment is conducted and maintained in accordance with **ETSI EN 319 401 (Clause 5)** as part of the overall governance framework.

9.6.4 Subjects and Subscribers obligations and warranties

Subjects and Subscribers shall:

- Comply with the terms and conditions of the trust services provided by imID CJSC;
- Provide truthful data in applications submitted to the Registration Authority;
- Immediately inform imID CJSC about any errors, defects, or changes in the certificate;
- Protect the credentials necessary for the use of imID CJSC authentication services and for signature creation against misuse, loss, disclosure, manipulation, or unauthorized use; neither communicating nor disclosing them to third parties, and maintaining sole control of them;
- Not use revoked or expired certificates;
- Halt the use of imID CJSC services as soon imID CJSC notifies about the system being compromised;
- Initiate the revocation in case of a potential or actual security violation (or suspicion of a security violation) regarding their private keys;
- Use the certificates and the corresponding private keys only for the purposes stated in the certificate and in accordance with the aims and restrictions stated in the Practice Statement and specific trust service policy.

9.6.5 Relying Party obligations and warranties

If the Relying Party verifies qualified signatures, it is obligated to use compliant software or services and follow these requirements:

- Verify if the certificate that supports the given signature was issued according to the present document and imID CJSC Trust Service Policy;
- Verify if a trust service provider issued the qualified certificate and if the certificate was valid at the time of signing;
- Verify if the signature validation data corresponds to the data provided to the Relying Party;
- Verify if the integrity of the signed data has not been compromised.

The Relying Party should refrain from using unknown or unprotected systems provided by a third party for validation.

If the Relying Party verifies the Time Stamp, a Relying Party must:

- Ensure that the Time Stamping Unit's certificate was valid and had not been revoked at the time of issuance;
- Verify if Time Stamp Unit was issued by imID CJSC;
- Consider any limitations indicated in the certificate.

9.6.6 Representations and warranties of other participants

Specified in relevant service-based Policies.

9.7 Warranty disclaimer

imID CJSC:

- Is liable for the performance of all its obligations specified in clause 9.6.1 with no limitation to the liability mandated under applicable legislation, regulations or contractual agreements.
- Maintains insurance coverage in accordance with applicable requirements and ensures that relevant supplier agreements contain appropriate provisions for compensation of liabilities where applicable.

9.8 Limitation of liability

imID CJSC liability is limited to actual and legally provable damages established by the competent courts. imID shall not be liable where it demonstrates that it took all measures within its control to perform its obligations properly and the damage was caused independently of its intent or negligence and was not due to non-compliance with the

requirements of applicable legislation. imID CJSC shall not be liable in the absence of established gross negligence subject to the liability rules set under applicable law.

imID CJSC shall only be liable for damages arising from the use of its trust services in accordance with their intended purpose, the applicable policies regarding certificates. imID is not liable for, and shall not be liable for damages resulting from:

a. Subject private keys not being kept secret, including any compromise or misuse of private keys or credentials not caused by the imID CJSC;

b. Any errors in checking certificates on the part of Relying Parties;

c. Use of a certificate or trust service beyond its intended scope, validity period, or reliance limits;

d. Unauthorized, fraudulent, or negligent use of certificates, cryptographic keys, or credentials by subscribers, signatories, seal creators, or Relying Parties;

e. reliance on revoked, expired, or suspended certificates where up-to-date status information was available through status verification services;

f. non-performance of this Practice Statement, where such non-performance is due to Force Majeure, including for the loss of the evidentiary value of validity confirmation due to Force Majeure, alteration or corruption of data or communications not under the Company's control, as well as causes not attributable to imID, including failures arising from legislative or regulatory changes, or acts or omissions of third parties.

g. issuance of a certificate based on misrepresentation, error of fact, omission, or falsified information provided by the Subject, Subscriber, or any third party unless such reliance on falsified information was a result of imID CJSC's failure to apply required verification procedures;

h. the Subscriber's or Subject's failure to comply with the procedures and operating methods set out in this document;

j. interruption or delay of services caused by hardware, software, or network failures beyond its reasonable control;

k. data alteration, corruption, or loss arising outside its secure systems;

l. temporary unavailability of its services due to maintenance or disaster recovery procedures.

The Subscriber and Subject shall be liable to imID for any damages resulting from misuse of certificates, wilful misconduct, failure to meet regulatory obligations, or non-compliance with the provisions governing the use of the certificate.

To the fullest extent permitted by governing law, the Company shall not be liable for indirect, consequential, special, or incidental damages, including but not limited to loss of profits, loss of business opportunity, reputational damage, or loss of data, whether arising in contract, or otherwise.

In the event of any discrepancy, inconsistency, or conflict between the provisions of this Practice Statement and any contractual arrangement between imID and its counterparties, the terms and conditions of the relevant contract shall take precedence.

Nothing in this section shall exclude or limit any liability that cannot be excluded or limited under applicable law.

9.9 Indemnities

imID CJSC shall be liable for direct damages caused to any natural or legal person resulting from its failure to fulfil its obligations, subject to the limitations set out in Section 9.8 and applicable legislation.

No compensation shall be granted in respect of damages arising from causes entirely outside imID CJSC's operations and not attributable to act or omission of imID CJSC. The total compensation for all cases shall not exceed the maximum annual limits (including coverage limits, limits specified for each and every claim) defined in imID CJSC's Cyber liability and Errors and Omissions insurance policy after the damage established by the final and enforceable decision of the competent court.

9.10 Term and Termination

This Practice Statement enters into force on the date published in the revision history and remains in effect until superseded by a subsequent version. Certificates issued under this Practice Statement remain governed by the version in force at issuance for the duration of their validity. Upon cessation of trust services, imID CJSC fulfils its obligations as set out in section 5.8.

9.11 Individual Notices and Communications

Notices to imID CJSC required or permitted under this Practice Statement shall be directed to info@imid.am. imID CJSC communicates with Subscribers, Relying Parties, and Registration Points via the contact mechanisms specified in relevant Terms and Conditions. Publication of a new version of this Practice Statement in the repository (section 2.1) constitutes notice to all parties. An additional written notification may be sent to the countrpart ywhere such notification is required under the relevant bilateral agreement.

9.12 Amendments

9.12.1 Procedure for amendment

This Practice Statement or other publicly availably policies are reviewed at least annually and may be reviewed more frequently. All changes are reviewed and approved by imID CJSC before being made public. Changes to this Practice Statement are indicated by appropriate versioning.

imID CJSC will post a notice on its website of any major or significant changes to this Practice Statement.

The review process is coordinated by the designated document owner. The process includes: formal review of all content for accuracy and continuing adequacy; identification and documentation of proposed changes; management approval; version increment; and publication. Responsibility for maintaining the Practice Statement rests with the document owner, as specified in imID CJSC's Document Management Procedure.

9.12.2 Notification mechanism

imID CJSC may publish draft versions of publicly available policies and documents. The Subscriber and the Subject may provide reasoned comments within 30 days of publication of the draft version. The final version of Practice Statement and other publicly available policies and documents are published electronically on imID's website 30 days before their enactment if no specific terms for publication are set under specific documents.

The only modifications that do not require prior notification are editorial updates, changes to the contact details of the document management representative, and adjustments that do not significantly affect a substantial number of individuals.

9.12.3 Circumstances under which OID must be changed

No stipulation

9.13 Dispute resolution procedures

All disputes arising between the Parties shall be resolved through good-faith negotiations. If the Parties fail to reach an agreement, the dispute shall be submitted to the competent court having jurisdiction at the location of imID CJSC, unless otherwise stipulated in a specific agreement.

The Subscriber or other party can submit their claim or complaint to the following email: info@imiD.am

9.14 Governing law

This Practice Statement is governed by the laws of the Republic of Armenia.

9.15 Compliance with applicable law

imID CJSC ensures the compliance with the set of legal acts and technical standards presented in Section 1.1.

9.16 Miscellaneous provisions

9.16.1 Entire contract

imID CJSC ensures that all RA are bound by the relevant and applicable provisions of this Practice Statement through contractual obligations.

imID CJSC requires every party using its products and services to enter into an agreement that delineates the associated terms and conditions of the relationship. If an agreement has provisions that differ from this Practice Statement, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

No entity operating under this Practice Statement may assign its rights, in whole or in part, without the proper written consent of imID CJSC. Unless specified in a contract with a party, imID CJSC does not provide notice of assignment of its rights.

9.16.3 Severability

If any provision of this document is held invalid or unenforceable by a competent court or tribunal, the remainder of the document remains valid and enforceable. Each provision that limits liability, disclaims warranties, or excludes damages is severable and independent from any other provision.

9.16.4 Enforcement

Any waiver or lack of immediate implementation of any right under this Practice Statement does not create a continuing waiver of such right or authorize an expectation of withdrawal from its implementation.

9.16.5 Force Majeure

imID CJSC cannot be held responsible for any consequences caused by circumstances beyond reasonable control, including but without limitation to:

- war;
- import or export 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.

Communication and performance in the case of Force Majeure are regulated between the parties with the contracts.

Failure to fulfil obligations under the imID CJSC Practice Statement or any related Policies shall not be deemed a breach if such failure results from a Force Majeure event. In such cases, none of the parties may seek damages or any other form of compensation from one another for delays or non-performance arising due to Force Majeure.

9.16.6 Accessibility Clause

In accordance with the relevant legislation, imID CJSC does its best to guarantee that all potential service users, especially people with disabilities, can access services provided by imID CJSC on an equal basis. imID CJSC accepts that its services imply at least some sort of qualitative capabilities and legal capacity, but nonetheless truly aspires to provide trust services and related technical solutions in a non-discriminating way.

9.17 Other Provisions

No stipulation

10. Appendix

10.1 Definitions and Acronyms

10.1.1 Terminology

Term	Description
auditor	person who assesses conformity to requirements as specified in given requirements documents
authentication	provision of assurance that a claimed characteristic of an entity is correct [SOURCE: ISO 27002:2022]
Certificate Revocation List (CRL)	signed list indicating a set of certificates that have been revoked by the certificate issuer
certificate	public key of a Subject, together with some other information, rendered unforgeable by encipherment with the private key of the Certification Authority which issued it

Certification Authority (CA)	authority trusted by one or more users to create and assign certificates
eIDAS Regulation	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, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
high security zone	specific physical location of the security zone (see ETSI EN 319 401 clause 7.8) where the Root CA key is held
secure zone	area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the TSP
incident	any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems
information security breach	compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to protected information transmitted, stored or otherwise processed [SOURCE: ISO 27002:2022]
Practice Statement	the current version of Practice Statement document outlining practices, procedures, and guidelines related to providing trust services. It serves as a reference for customers and stakeholders to understand how the trust service provider operates and what standards they adhere to. (present document)
revocation	permanent termination of the certificate's validity before the expiry date indicated in the certificate or in t
risk	potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident
Root CA	Certification Authority which is at the highest level within TSP's domain, and which is used to sign subordinate CA(s)
Registration Authority	Entity that is responsible for identification and authentication of subjects of certificates. Additionally, an RA accepts certificate applications, initiates and authorises certificate issuance/revocation following successful verification.
Registration Points	Service points where Registration Authority services are delivered.
Subject	entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
Subscriber	The person bound by agreement with a trust service provider to any Subscriber obligations
subordinate CA	Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA
Supervisory Body	The Ministry of High-tech Industry of Republic of Armenia

Trust Service Policy (Policy)	Set of rules that indicates the applicability of a trust service to a particular community and/or class of application, delivered through specific means and conditions with common security requirements
Trust Service Provider (TSP)	entity which provides one or more trust services
vulnerability	weakness of an asset or control that can be exploited by one or more threats [SOURCE: ISO 27002:2022]

10.1.2 Acronyms

Acronym	Full Form
CA	Certification Authority
CAB	Conformity Assessment Body
CRL	Certificate Revocation List
CJSC	Closed Joint-Stock Company
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
OID	Object Identifier
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RQSCD	Remote Qualified Signature Creation Device
TSP	Trust Service Provider
TSA	Time Stamp Authority
TSU	Time Stamping Unit

End of Document