Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina, Ivana Franje Jukića 2,
Banja Luka, Bosnia and Herzegovina

IDDEEA CA CERTIFICATION PRACTICE STATEMENT (CPS)

Version 2.3

Effective as of January 29, 2026

ID No	
Version	2.3
Propose	IDDEEA PMA

Version	Date	Developed by:	Description
1.0	2021-09-20	Security officer	First version
2.0[1]	2024-01-17	Security officer	Version 2.0
2.1	2025-07-15	Security officer	Version 2.1
2.2	2025-08-28	Security officer	Version 2.2
2.3	2026-01-29	Security officer	Version 2.3

[1] This document, originally titled 'Certification Policy of the Agency for Identification Documents, Registers and Data Exchange of BiH (IDDEEA), Rules on Electronic Signature established by IDDEEA as an authorized trust service provider', has been renamed and, as of version 2.0, is titled IDDEEA CA CERTIFICATION PRACTICE STATEMENT (CPS)

Contents

1. Introduction

The Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina (hereinafter: IDDEEA) has established a **Public Key Infrastructure (PKI)**. In its capacity as a **Trust Service Provider (TSP)**, pursuant to the Law on Electronic Signature ("Official Gazette of BiH", No. 91/06), it operates as a **Certification Authority (CA)** providing services for the issuance of qualified and non-qualified electronic certificates, certificate lifecycle management, and the issuance of qualified electronic **time stamps**, under the name: **IDDEEA CA**.
IDDEEA CA issues qualified electronic certificates in accordance with legal regulations, general acts, and IDDEEA CA instructions governing this field. The legal framework for the operation of IDDEEA CA's qualified electronic certificate issuance services consists of the following laws and bylaws:

- Law on Electronic Signature ("Official Gazette of BiH", No. 91/06),
- Law on Electronic Document ("Official Gazette of BiH", No. 58/14),
- Rulebook on Detailed Conditions for Issuing Qualified Certificates ("Official Gazette of BiH", No. 14/17).

The general operational rules of IDDEEA CA are contained within the following documents:

- **Certification Policy (CP)** of the Certification Authority of the Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina (hereinafter: Certification Policy),
- **Certification Practice Statement (CPS)** of the Certification Authority of the Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina.

The **Certification Practice Statement (CPS)** (hereinafter: Practice Statement) is a public document that defines the certification service delivery process and the methods for their use during the issuance and **lifecycle management** of electronic certificates and **electronic seals**. It details the operational procedures required to meet specified demands and the manner in which IDDEEA CA fulfills the technical, organizational, and procedural business requirements identified in the Certification Policy, as well as the use of electronic certificates by end-users.
The **trust services** provided by IDDEEA CA constitute the scope of this document. This document describes the complete lifecycle of qualified and non-qualified electronic certificates issued on **Secure Signature Creation Devices (SSCD/QSCD)** or as **software-based certificates** by IDDEEA CA. As public documents, the CP and CPS are published on the official IDDEEA CA website.
In addition to these documents, the following are available to users and all interested parties on the official IDDEEA CA website:

- Contract forms for the issuance and use of qualified electronic certificates,

- Application forms for the issuance and use of qualified electronic certificates,
- Request forms for status changes of qualified electronic certificates (revocation/suspension requests),
- User manuals,
- Other acts related to IDDEEA CA operations.

IDDEEA CA also establishes **Special Internal Operating Rules** and protection measures for the certification system (hereinafter: Special Rules). Special Rules are internal documents and constitute an IDDEEA trade secret.

Qualified and non-qualified electronic certificates and qualified electronic time stamps issued by IDDEEA CA are in compliance with the European Union eIDAS Regulation ("Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC") and relevant international standards and recommendations, as well as other standards, documents, and recommendations pertaining to the issuance of qualified electronic certificates

1.1 Overview

IDDEEA CA manages the Public Key Infrastructure for the provision of the following **qualified trust services**:

1. Issuance of **qualified certificates** for electronic signatures;
2. Issuance of qualified certificates for **remote electronic signatures**;

IDDEEA CA manages the Public Key Infrastructure for the provision of the following **trust services**:

1. Issuance of electronic certificates for **user authentication**, used for the reliable establishment of user identity across various sets of electronic services offered by IDDEEA, other public institutions, and the private sector.

These Rules are a public document and part of the regulatory framework defined by IDDEEA CA regarding the qualified trust services it provides as an authorized **Trust Service Provider (TSP)**. The purpose of this document is to clarify technical, procedural, and organizational activities, as well as the implementation of the Public Key Infrastructure (**PKI IDDEEA**) and the certification procedures performed, demonstrating the trustworthiness of IDDEEA as a **Qualified Trust Service Provider (QTSP)**.
This document contains the **Certification Policy (CP)** of IDDEEA. The document has been drafted in accordance with the **IETF RFC 3647** framework, "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework," which provides a comprehensive list of topics to be addressed in a CP and/or CPS.

The content is aligned with last versions of relevant ETSI standards (Attachment 1)

This document describes the public rules for the categories of qualified and **normalized certificates** listed in the tables below.

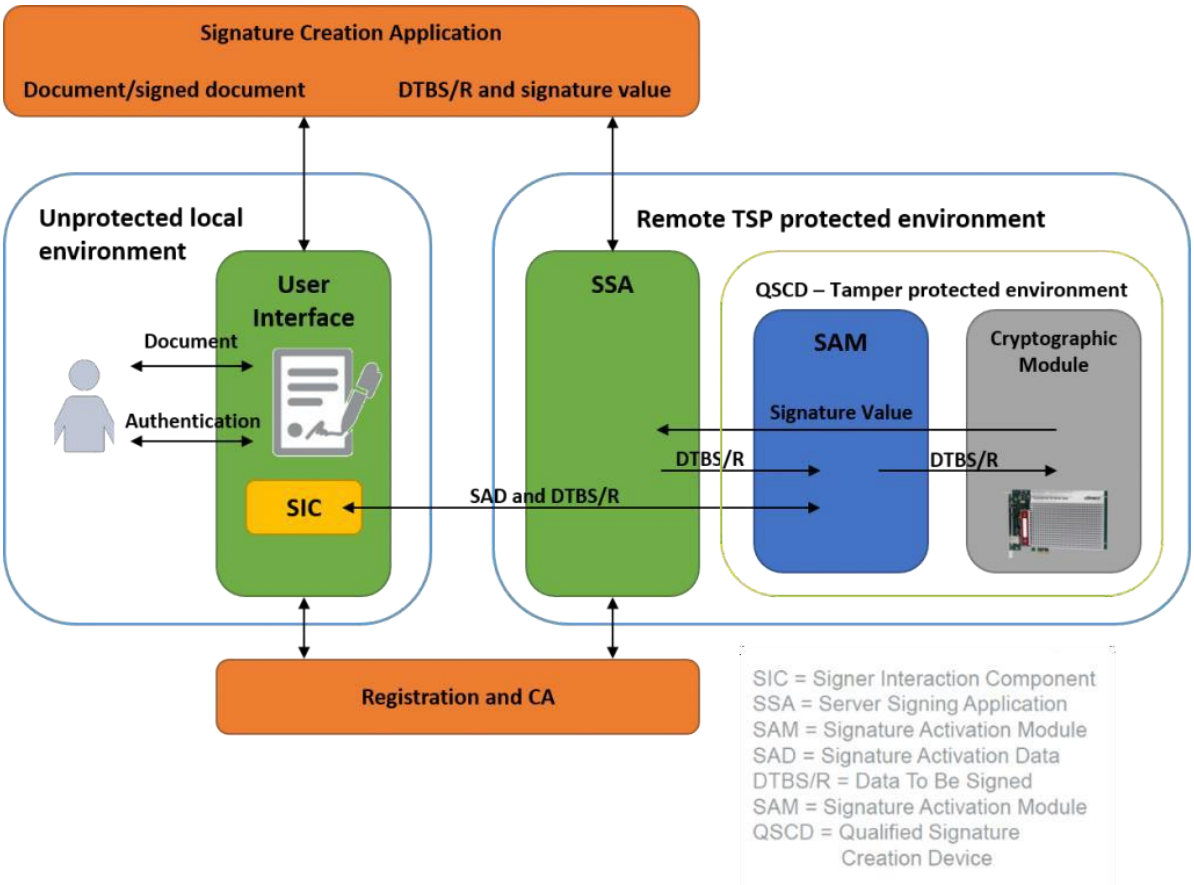
Table 1: List of Qualified Certificates

Certificate Category	Description
Electronic certificate for qualified e-signature	Electronic certificate for qualified electronic signature issued to a natural person, where the **private key** and the corresponding certificate are stored on a **QSCD** (Qualified Signature Creation Device).
Electronic certificate for qualified remote electronic signature	Electronic certificate for qualified electronic signature for **remote signing** issued to a natural person, where the **private key** and the corresponding certificate are stored on the **IDDEEA CA server-side infrastructure**.

Table 2: List of Normalized Certificates

Certificate Category	Description
Normalized electronic certificate – OCSP	**Normalized OCSP**

The following figure illustrates the system architecture for remote electronic document signing.



As illustrated by the presented remote electronic signing architecture, the system consists of several building blocks, primarily including:

- **Remote electronic document signing application** featuring a **User Interface (UI)** integrated with key user authentication processes, interaction with server-side electronic signing components, the registration process, and the issuance of **qualified electronic certificates**.
- **Server-side system for remote electronic document signing**, consisting of a **Server Signing Application (SSA)** and a **secure server-side repository** that stores user certificates and **private**

keys in encrypted form. These keys can only be decrypted using a **PIN code** held by the application user. The server-side remote signing system is also interfaced with the **Certification Authority (CA)** body responsible for issuing qualified electronic signature certificates.

- **User certificates for remote electronic signing**, which maintain the same structure, the same **Root Certification Authority (Root CA)**, the same **Issuing Certification Authority (Issuing CA)**, and all certificate fields as certificates for **qualified e-signatures**. This consistency is achieved through the described system architecture.

1.2 Document Name and Identification

This document represents the **Certification Policy** of IDDEEA (hereinafter: **Policy** or **CP**). The Policy is published at the following URL:

- https://www.iddeea.gov.ba/PKI/CP and is publicly accessible.

The document titled 'IDDEEA Public Key Infrastructure Disclosure Statement', prepared in accordance with the latest version of the 'Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements' standard, the current version of which is listed in Annex 1 of this document (hereinafter referred to as the PDS)

The following **Object Identifiers (OIDs)** are assigned to the certificate categories issued in accordance with this Policy:

Certificate Category	Certification Policy Identifier (OID)
Electronic certificate for qualified e-signature	0.4.0.194112.1.2
Electronic certificate for qualified remote electronic signature	0.4.0.194112.1.2
Normalized electronic certificate – OCSP	0.4.0.194112.1.2

IDDEEA CA may issue various certificates, which must be clearly marked with a specific policy or an additional policy object identifier within the X.509 certificatePolicies extension. The object identifier (OID) carries the prefix 1.3.6.1.4.1.18560 and should be unique within this prefix.

1.3 Public Key Infrastructure (PKI) Participants

1.3.1 Certification Authorities

IDDEEA CA acts as a public **Trust Service Provider (TSP)** and issues public key certificates to natural persons.
IDDEEA CA operates as a **Root Certification Authority (Root CA)**, issuing **self-signed certificates** during the **Root Key Generation Ceremony** and a **cross-certificate** to one hierarchically subordinate **Certification Authority (Sub-CA)**. IDDEEA CA utilizes a single

Certification Authority (an **Issuing CA**) for the issuance of all types of qualified and normalized certificates to end-entities.
IDDEEA CA manages the following Certification Authorities:

- **IDDEEA Root Certification Authority (Root CA)**: With a mandate from September 20, 2021, to September 20, 2041, which holds a self-signed certificate and issues certificates to IDDEEA's subordinate Certification Authorities.
- **IDDEEA Issuing Certification Authorities (Issuing CAs)**: Which issue **qualified end-entity certificates** with a mandate from September 29, 2021, to September 29, 2031, signed by the IDDEEA Root Certification Authority.

Content of the "IDDEEA-RootCA-2021" digital certificate:

Serial Number	449FFCA0B7E0AFE2DC4C5D9754F945677B9028AC
Issuer	IDDEEA
Subject	CN=IDDEEA-RootCA-2021, O=IDDEEA, emailAddress=eid@iddeea.gov.ba, L=Banja Luka, street=Ivana Franje Jukića 2, postalCode=78000, C=BA
Validity: Not Before	20.09.2021
Validity: Not After	20.09.2041
RSA Public Key	82:D0:61:16:28:EE:51:49:DF:40:C5:51:AA:DD:59:F8 66:B9:9D:1A:86:FB:7E:A8:37:33:54:B1:97:3C:72:26 C3:B8:B6:6C:0F:B0:35:CD:42:40:8A:87:22:DE:3A:90 5A:AA:29:52:AD:39:8E:C5:76:99:54:3B:3E:E1:00:12 DB:7E:0F:21:B1:31:EA:6B:87:5E:FC:B2:5B:AC:D7:FC F0:3C:BE:C3:BB:25:52:A5:C4:46:0B:94:8F:EF:C8:BE 25:4F:E2:F2:DC:69:60:F9:69:44:F7:2F:9A:01:2E:9E EE:88:A7:5D:7A:77:45:36:7F:70:ED:E9:A9:2C:2F:98 91:92:0B:FA:FB:B3:7F:62:C9:BA:EE:EE:60:60:26:65 66:FB:A6:7F:6A:F5:F7:2D:F6:39:50:68:68:EC:33:DD 4C:F8:35:42:92:57:0C:5E:8F:4A:DD:D4:83:2F:39:C3 D5:C7:68:CD:99:49:16:7F:1A:A8:F4:50:34:BF:5B:2C 10:C5:21:34:92:DF:35:AB:B6:4C:EF:32:12:EA:8B:AC CC:EE:71:06:1E:FF:46:53:DC:3B:32:F1:20:45:62:CC 50:39:DC:4F:14:7E:6D:2E:A1:D4:3A:82:45:61:4D:50 1B:91:06:35:C8:28:88:8B:26:FF:5C:40:DD:B5:42:08 C6:D8:AF:6D:02:B6:ED:EC:80:65:14:6F:AC:5D:E0:FB BC:B8:54:C3:F9:45:00:C4:F1:83:34:F8:2A:84:56:E8 DC:A3:37:FD:E2:1A:B9:9C:51:CC:37:20:BB:53:4D:64 37:BB:67:AD:85:D5:43:F7:80:60:C3:6E:F2:E5:51:5B B6:77:77:36:B0:03:45:33:06:2E:23:72:54:25:31:09 79:9C:05:4B:DF:D1:E2:E9:11:FE:2E:4D:93:B0:06:3D F0:84:02:56:D0:E7:FC:DE:11:6E:EE:F9:63:52:48:C6 68:6B:D4:76:E6:BB:A0:D5:96:A5:2B:DB:E7:58:99:16

	47:37:90:13:1F:FF:F7:EA:9B:75:9A:7B:40:B2:FC:46 C7:5E:BA:96:C9:09:E9:74:FC:88:7E:B9:3E:73:2A:3D 2A:33:06:95:28:4B:68:86:78:D1:FF:32:CB:57:26:BE D3:C9:17:47:B8:26:A1:1C:03:77:C7:EE:57:FA:CE:E4 59:2E:BC:FD:43:AB:C1:56:8B:66:7D:28:58:A5:00:E8 B4:45:08:AB:25:5E:51:94:81:07:C2:67:8A:27:55:36 0E:D0:45:94:F5:17:1F:D2:52:E0:DA:38:78:99:AA:9A 79:7B:E3:04:B2:DF:6B:92:09:C2:A5:95:85:70:4F:8B
Signature Algorithm	sha512WithRSAEncryption
Subject Key Identifier	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
Authority Key Identifier	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
SHA-1 Fingerprint	A2:4E:6B:E6:78:98:AE:DD:5E:E9:5B:09:82:34:E5:80:48:37:E5:DD
SHA-256 Fingerprint	57:75:50:3D:A6:29:84:27:01:5B:33:79:6B:13:44:C2 D6:8E:C4:39:72:99:7B:6D:BB:83:DD:41:67:E3:CF:E5

The digital certificate of the IDDEEA-IssuingCA (the Certification Authority for certificate issuance), with a validity period from September 29, 2021, to September 29, 2031, contains the following:

Serial Number	27AF82049AC3D91AE8664A4A6FFFB991AE89B66C
Issuer	IDDEEA
Subject	CN=IDDEEA-IssuingCA
Validity: Not Before	29.09.2021
Validity: Not After	29.09.2031
RSA Public Key	B0:DC:AF:AD:C5:1E:14:97:AC:A9:DA:77:C1:06:6A:61 D1:28:DA:45:78:93:B4:A6:70:8B:DE:82:37:EF:4B:61 7D:37:A8:C0:0E:A1:15:7E:D7:CB:9C:3D:43:7A:89:7C B6:FC:A5:93:12:CE:74:00:1B:5E:F7:C6:25:E8:C8:F0 DF:C9:D6:DF:EB:5C:B3:A2:A4:33:6C:54:D6:A4:EA:72 3D:D5:E2:38:F8:74:4C:B7:2F:4E:B4:92:13:3A:D5:07 50:34:57:BC:18:26:90:58:97:EA:BA:E1:17:DF:22:CA 3B:F3:2B:2C:5E:8D:77:93:BC:C8:75:3F:30:99:1C:87 D2:3A:36:80:6F:BC:D3:9D:D2:28:36:8E:84:51:DC:A1 80:FD:75:64:7E:D1:8E:E2:B0:9A:79:C6:36:9D:CB:3B 81:8D:90:E0:4C:D2:16:5F:F3:0A:4A:B9:39:04:B3:20 39:8B:DF:50:A5:22:64:54:27:C8:56:CC:C3:6E:5C:F0 D8:6D:2B:7B:09:13:FE:E9:6F:9A:16:29:3B:E4:A5:3B F2:74:68:39:88:4C:49:48:3A:35:A9:96:A6:D1:CC:22 B2:99:10:8F:05:C6:A3:A2:76:5A:DA:36:9E:7C:97:C2 4F:50:AA:A4:02:65:AA:34:53:56:0A:14:2A:A3:F4:BC 30:5E:E6:6A:71:71:1C:AF:E8:9B:2A:EB:5E:42:62:AD 39:2B:CA:C2:5F:02:7C:00:4F:D5:AE:F0:94:61:2D:B3 DF:D1:D1:50:96:3F:A9:63:2D:CC:B5:88:DD:FE:A3:AC 45:51:0E:76:D2:E7:E3:19:B0:EC:B3:06:DB:D9:FE:BD 2A:4C:5B:A9:77:AF:11:C1:1E:52:A8:3C:AD:BF:B5:86 9B:E5:B5:98:1D:94:CE:E2:7C:65:67:FF:D4:EF:51:0E

	49:96:82:6B:FF:35:C6:08:8F:0E:7F:83:39:EE:15:2C 6A:A0:EF:3C:F9:88:1D:13:5C:22:EA:1F:A6:73:4C:41 B9:04:F5:B6:76:1F:46:A3:75:75:A6:D4:D6:31:54:0B 3D:C6:8C:67:A3:4B:0E:93:4B:81:9B:5B:86:3E:DB:57 76:F1:0A:B8:ED:75:E9:1C:95:1C:E4:45:15:09:93:E4 12:CD:91:D7:44:4A:9C:1E:AE:A1:4D:13:DB:70:F3:15 59:BA:56:EF:76:C4:21:41:3B:C5:D5:16:58:1D:57:04 71:6D:CB:97:46:A8:7A:9A:4F:7B:1E:E3:9A:C7:3C:60 0A:5D:FB:A4:E9:83:15:49:11:23:21:B1:B4:34:2A:68 DF:9F:6F:C6:16:8B:F0:E9:0F:E6:24:5A:7C:5C:50:DF
Signature Algorithm	sha512WithRSAEncryption
Subject Key Identifier	55:4D:EF:8B:87:48:55:BA:DD:AA:0E:41:D6:B6:CB:7D:77:1A:11:DA
Authority Key Identifier	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
SHA-1 Fingerprint	C2:A7:DF:30:66:40:D0:7E:D1:BF:E6:98:37:48:5E:32:E7:4A:60:5A
SHA-256 Fingerprint	71:27:C8:24:E2:47:5C:B8:A9:25:E0:53:83:91:41:6C 2D:F0:0B:B9:C1:B6:85:95:1D:98:F3:A1:D0:AD:CE:EF

As a **Trust Service Provider (TSP)**, IDDEEA CA is obliged to implement measures and procedures ensuring certificate management in accordance with the applicable regulations in Bosnia and Herzegovina and the internal rules of the certification service provider. IDDEEA CA employs personnel responsible for:

- **Overall TSP operations**: The **IDDEEA Policy Management Authority (IDDEEA PMA)**;
- **Infrastructure management and maintenance**: Personnel who manage and maintain the TSP infrastructure, the **CA private cryptographic keys**, servers, and software (**Operational Authority – OA**); and
- **User identification and coordination**: Personnel responsible for user identification (**Registration Authority – RA**) and coordination with external RAs.

Where necessary, these rules distinguish between different users and the roles of those accessing TSP functions. When such distinction is not required, the term **TSP** is used to denote the overall TSP entity, including the software and its operations.

1.3.1.1 Policy Management Authority (PMA)

The **IDDEEA PMA** is responsible for:

- Drafting and maintaining the **IDDEEA CA Certification Policy**;
- Drafting and maintaining IDDEEA CA public documents (End-User Agreements, etc.);
- Developing the IDDEEA CA Certification Policy and submitting it for approval;
- The registration and **accreditation** of the IDDEEA CA;
- Appointing personnel to the **Operational Authority (OA)** and **Registration Authority (RA)**;

- Monitoring and auditing the compliance of IDDEEA CA operations and activities to ensure the TSP operates in accordance with the Policy and relevant legislation;
- Reviewing and approving the **Certification Policy (CP)** or **Certification Practice Statement (CPS)** of external cross-certified Certification Authorities;
- Resolving disputes between IDDEEA CA participants.

1.3.1.2 *Operational Authority (OA)*

The **IDDEEA CA Operational Authority** is responsible for:

- Generating **TSP key pairs**, secure management of **TSP private keys**, and distribution of **TSP public keys**;
- Establishing the environment and procedures for certificate applications;
- Identification and authentication of individuals or entities applying for a certificate;
- Approving and rejecting certificate issuance requests;
- Signing and issuing **X.509 certificates** that bind users to their public keys, as a response to approved certificate requests;
- Distributing X.509 certificates via **directories**;
- Initiating **certificate revocation**, either upon user request or at the IDDEEA CA's own initiative;
- Executing certificate revocation, including the issuance and publication of **Certificate Revocation Lists (CRLs)** and maintaining **Online Certificate Status Protocol (OCSP)** services;
- Managing the TSP in accordance with the laws of Bosnia and Herzegovina and this Policy;
- Approving and appointing individuals to **PKI officer** positions;
- Monitoring and auditing RA operations within its jurisdiction;
- Initiating the revocation of certificates held by TSP and RA employees.

1.3.2 IDDEEA CA Registration Authorities (RA)

The **Registration Authority** (hereinafter: **RA**) performs the following tasks for the IDDEEA CA:

- Verifying the identity of natural persons and other relevant data for certificate management;
- Receiving certificate application forms;
- Issuing necessary documentation to users or prospective users;
- Securely transmitting application forms, requests, and other information to the IDDEEA CA.

IDDEEA CA performs RA operations through its own RA, with the possibility of conducting tasks and duties on-site at other business or public sector institutions and organizations (**Mobile RA Office**).
The IDDEEA CA TSP may authorize other institutions and business or public sector organizations, in addition to its own RAs, to perform RA tasks or other activities as authorized by the IDDEEA CA TSP.
The IDDEEA CA contractually binds these institutions or organizations to fulfill strict security requirements in accordance with applicable legislation, EU regulations, and international, European, and domestic standards, recommendations, and rules, the CPS, and IDDEEA CA internal rules. This authorization may not include performing tasks and duties on-site at other business or public sector institutions or organizations (**Mobile RA Office**).
IDDEEA CA maintains geographically distributed RAs to facilitate easy registration for future subjects. Information regarding RA locations is available on the IDDEEA CA TSP website.

1.3.3 Subscribers

A **Subscriber** is a natural person to whom an **e-ID** (electronic identity card) is issued, who receives a certificate on the ID card or a certificate for remote signing, and who signs an Agreement with IDDEEA for the provision of certification services in accordance with relevant laws. The person is directly responsible for complying with the **Terms and Conditions of Certification Services**.
A Subscriber is also the person specified in the certificate and the **signer** who creates the electronic signature and uses the certificate on his/her behalf.
A **User** is a person, including natural persons (individuals), who utilizes the services.
A Subscriber is the person identified in the certificate as the holder of the **private key** associated with the **public key** provided in the certificate.
A Subscriber is the person bearing ultimate responsibility for the use of the private key associated with the public key certificate, while the **subject** is the individual whose authentication is performed using the private key.

1.3.4 Relying Parties (Third Parties)

Relying Parties are individuals or legal entities that rely on the issued certificates and other IDDEEA CA services.
Relying Parties must follow IDDEEA CA instructions and must always verify the certificate validity (**revocation status**), the purpose of certificate use, the validity period (expiry), etc. The obligations and responsibilities of relying parties are further detailed in Sections 4.5.2 and 9.6.4.
Relying Parties do not necessarily have to be subscribers of IDDEEA CA certificates or digital certificates from other trust service providers.

Before relying on the information provided in a certificate, Relying Parties must always consult the **IDDEEA CA CRL** or **OCSP** to confirm the validity of the certificates they have received.

1.3.5 Other Participants

Potential participants in the broader certification system include **TSP partners**, domestic or international **Trust Service Providers (TSPs)**, as well as the **Ministry of Communications and Transport** as the **regulatory body**.

1.4 Certificate Usage

IDDEEA CA manages (issues, validates, revokes, renews, stores, and publishes) **qualified certificates** for electronic signatures. These certificates are intended for natural persons.

1.4.1 Permitted Certificate Usage

Electronic signature certificates are intended for signing unilateral or mutual communications between certificate users and for use in various applications and for different market purposes. Among other uses, certificates may be used for:

- User identification;
- User identity disclosure/discovery;
- Signing documents in electronic form;
- **Encryption and decryption** of documents in electronic form.

Electronic signatures may be utilized in the following applications:

- Electronic or mobile banking (**e-banking / m-banking**);
- **e-Government** or **m-Government** applications;
- **e-Health** or **m-Health** applications;
- Electronic signatures or mobile forms;
- Secure communication with public sector bodies and organizations, as well as other natural and legal persons;
- Other applications or services where a certificate is required;
- **Access control**.

Other purposes are available upon user request and in accordance with the Law on Electronic Documents, the Law on Electronic Signature, and other relevant legislation in Bosnia and Herzegovina.
Note: The TSP does not maintain a copy of the users' **private decryption keys** for **key recovery** purposes. It is the sole responsibility of the user to maintain a secure backup of their private decryption keys.

1.4.2 Prohibited Certificate Usage

All certificates issued by IDDEEA CA must be used in accordance with the current legislation of Bosnia and Herzegovina.
The use of certificates issued under these rules in a manner contrary to the provisions of the rules, existing regulations, or outside the scope of permitted use specified in the previous section is strictly prohibited.
Certificates are not intended for **resale**.

1.5 Policy Administartion

1.5.1 Document Administration

The **Certification Policy (CP)** and the **Certification Practice Statement (CPS)** are managed by the **IDDEEA CA**, operating within the Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina.

1.5.2 Contact Person

For inquiries related to the CPS and the Certification Policy, you may contact the authorized representatives of **IDDEEA CA** at the address provided below:

Adress:	Agency for identification documents, registers and data exchange - IDDEEA; Ivana Franje Jukića 2; Banja Luka, Bosna i Hercegovina
E-mail:	eid@iddeea.gov.ba
net:	https://www.iddeea.gov.ba

1.5.3 Person Determining CPS Suitability

Person Determining CPS Suitability with the Policy
In accordance with the assigned responsibilities, the authorized personnel of **IDDEEA CA** are responsible for ensuring the compliance of IDDEEA CA with the **CPS** and the **Certification Policy**.

1.5.4 CPS Approval Procedures

Approval Procedure for the Certification Practice Statement
The **IDDEEA CA Certification Policy** is drafted and maintained by the **IDDEEA PMA**, and is approved by the **Director of IDDEEA**.

1.6 Definitions and Abbreviations

Definitions:

- **Electronic Signature** – Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
- **Signatory (Signer)** – A natural person who creates an electronic signature.
- **Information System** – A system used for collecting, sending, receiving, storing, or otherwise processing electronic data.
- **Signature Creation Data** – Unique data used in the process of creating an electronic signature, such as codes or private cryptographic keys.
- **Signature Creation Device** – Configured software or technical equipment used to create an electronic signature.
- **Qualified Signature Creation Device (QSCD)** – A device that provides unique, secure, and confidential data related to an electronic signature; prevents the possibility of deriving electronic signature data within a reasonable timeframe and through justifiable means from the signature verification data; ensures protection against electronic signature forgery using currently available technology; and enables the signatory to securely protect the data in the electronic signature from unauthorized access.
- **Signature Verification Data** – Unique data used to verify an electronic signature, such as codes or public cryptographic keys.
- **Signature Verification Device** – Configured software or hardware used to confirm that an electronic signature is valid.

- **Certificate** – An electronic attestation which links signature verification data to a natural person, the certificate subject, and confirms the identity of that person.
- **Qualified Certificate** – A certificate containing the name and country of residence (or the seat of the body), the name or pseudonym of the user (or the pseudonym of the information system carrying the user's designation), electronic signature verification data corresponding to the electronic signature data, the beginning and end of the certificate's validity, the certificate identification number, the advanced electronic signature of the authority, and possible limitations on certificate usage.
- **Normalized Certificate** – A certificate with the same technical properties and providing the same level of confidentiality as a qualified certificate, but without legal limitations on its intended use.
- **Advanced Electronic Signature** – An electronic signature that meets the following requirements:
  a) it is uniquely linked to the signatory;
  b) it is capable of identifying the signatory;
  c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control;
  d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
- **Qualified Electronic Signature** – An advanced electronic signature that is created by a qualified electronic signature creation device (QSCD), and which is based on a qualified certificate for electronic signatures.
- **Certification Authority (CA)** – Any natural or legal person that issues Certificates or provides other services related to Certificates or electronic signatures.
- **Subscriber (User)** – Any natural or legal person identified in the certificate as the holder of the private key corresponding to the public key included in the certificate.
- **Applicant** – A person who submits a request for certificate issuance to a certification authority on behalf of one or more users. An applicant can also be the subscriber when the certificate is issued to an individual for personal use.
- **Relying Party (Third Party)** – A person who has a reasonable reliance on a certificate.
- **Computer User Account** – A user account denoting a set of characteristics that enable access to a computer system for a specific person. Each user account is unique to each computer system, implemented through internal system functions. Access is based on a username and password pair. A **Username** is a string of alphanumeric characters identifying the user in a given system. A **Password** is also a string of alphanumeric characters known exclusively to the account owner. For high-security systems, the password may be supplemented or replaced by a smart card.
- **Encryption Key Pair** – A pair of symmetric keys consisting of a public encryption key and a corresponding private decryption key. Also referred to as a confidential key pair.
- **Private Decryption Key** – *See Encryption Key Pair.*
- **Private Signing Key** – *See Encryption Key Pair.*
- **Public Encryption Key** – *See Encryption Key Pair.*
- **Public Key Encryption Certificate** – A certificate containing a public encryption key.
- **Public Signature Verification Key** – *See Signature Key Pair.*
- **Public Signature Verification Certificate** – A certificate containing a public signature key.

- **Signature Key Pair** – A pair of asymmetric keys consisting of a private signature key and a corresponding public signature verification key.
- **QSCD (Smart Card/Token)** – A device for creating a qualified electronic signature or seal in the form of a smart card or token where private keys can be stored.
- **HSM (Hardware Security Module)** – A physical device for the secure storage of digital keys.
- **Trust Service Provider (TSP)** – A natural or legal person who provides one or more trust services, either as a qualified or non-qualified trust service provider.

A Qualified Trust Service Provider (QTSP) is a trust service provider that provides one or more qualified trust services and is granted qualified status by the supervisory body.

Abbreviations:

The list of abbreviations used in this document and within the Policy is provided in the following table:

Abbreviation	Explanation
ARL	**Authority Revocation List**
CA	**Certification Authority**
CN	**Common Name**
CPS	**Certification Practice Statement**
CRL	**Certificate Revocation List**
DC	**Digital Certificate**
DN	**Distinguished Name**
EAL	**Evaluation Assurance Level**
EKU	**Extended Key Usage**
RA	**Registration Authority**
PMA	**Policy Management Authority**
OA	**Operational Authority**
FIPS 140-1	**Federal Information Processing Standard 140-1** –
PKCS #10	**Certification Request Syntax Standard**
PKI	**Public Key Infrastructure**
PKIX	**X.509-based PKI**
PKIX-CMP	**PKIX Certificate Management Protocol**, as described in **RFC 4210**
X.509	**Public Key Infrastructure Certificate and CRL Profile**, as described in **RFC 5280**
QSCD	**Qualified Signature Creation** A device for creating qualified or advanced electronic signatures and seals in accordance with **eIDAS** requirements (Smart card/Token)
TSP	**Trust Service Provider**

2. Publication and repository responsibilities

2.1 Respositories

IDDEEA CA publishes information related to certification services in repositories at the following address: https://www.iddeea.gov.ba/PKI/CPS.
IDDEEA CA shall make available all information relevant to its operations, notices to subjects and third parties, as well as other relevant documents.
The following documents are publicly available:

- **IDDEEA CA Certificate Policy (CP)**;
- **IDDEEA CA Certification Practice Statement (CPS)**;
- **Forms** for certificate applications, revocation requests, and other services subject to the agreement with the TSP;
- **User guides** for the secure use of digital certificates;
- **Information** on applicable regulations and standards related to the TSP's operations;
- **Other information** related to IDDEEA CA operations.

Documents that constitute the **confidential part** of IDDEEA CA internal rules are not available to the public.

2.2 Publication of Certification information

IDDEEA CA publishes:

- **Certificate Revocation List (CRL)**;
- **Certificate status** via the Online Certificate Status Protocol (OCSP);
- **Certification Authority (CA) certificates**;
- **Certificate Policy (CP)** and **Certification Practice Statement (CPS)**;
- **List of Registration Authorities (RAs)**;
- **User manuals**.

IDDEEA CA provides notices and information regarding other certification services relevant for public disclosure.

2.3 Publication Frequency Timelines

Certificates are published immediately upon issuance, as specified in Section 4.4. **Certificate Revocation Lists (CRLs)** are published immediately after issuance, as specified in Section 4.9.7. All information is published immediately upon modification or as soon as it becomes available to the **TSP**.

2.4 Repository Access Controls

All public information is available in a **read-only** format without restrictions. Repositories are additionally protected against **unauthorized modifications**.

3. Identification and Authentication

3.1.1 Types of names

The user name field in certificates issued by the **IDDEEA CA** contains the authenticated user name as defined in the table in Section 3.1.4 (Rules for Interpreting Various Name Forms). The subject name field in the CA certificate and in certificates issued to users is in the form of an **X.501 Distinguished Name (DN)**. The Distinguished Name is encoded as a **PrintableString** or **UTF8String** and must be specified in all issued certificates

3.1.2 Need for Meaningful Names

The set of DN attributes of the certificate user uniquely identifies each certificate holder and carries significant value. A **serial number** is included to distinguish names for which the subject field would otherwise be identical.

3.1.3 Anonymity or Pseudonymity of Users

The use of anonymous names or pseudonyms is **not permitted**.

3.1.4 Rules for Interpreting Various Name Forms

With the appropriate combination of letters, the **TSP** shall ensure the use of other unforeseen characters.
The user name field is defined as an **X.501 type Name** (X.500 Distinguished Name), in accordance with **RFC 5280**.
The "Subject" and "Issuer" fields in the **IDDEEA CA** certificates are as specified in Section 1.3.1.
The **X.500 Distinguished Name (Subject)** in certificates issued by the **IDDEEA CA** has the following format:

Natural Person:

Distinguished Name Component	Value
Country (C =)	BA
Organization (O =)	For natural persons: **IDDEEA**
OrganizationIdentifier	For natural persons: **IDDEEA**
Given Name	[First Name]
Surname	[Last Name]
Common Name (CN=)	ID card number or passport number of the certificate holder
Serial Number (serialNumber=)	Unique serial number

3.1.5 Uniqueness of Names

In the certificate subject, **IDDEEA CA** assigns a combination of **Distinguished Name** attributes, as defined in Section 3.1.2 and Section 3.1.4, to ensure the unambiguity and uniqueness of names.

3.1.6 Recognition, Authentication and Role of Trademarks

Users are required to use their real identities and may not apply under false names or pseudonyms. Furthermore, a user cannot be anonymous.
IDDEEA CA shall reject any request for anonymity or the use of a pseudonym.

3.2 Initial Identity Validation

The identity of a prospective user during the initial certificate issuance is verified at the **IDDEEA RA**. Prior to issuing a certificate, **IDDEEA CA** verifies the prospective user's data in the appropriate registers.

3.2.1 Method to Prove Possession of Private Key

The demonstration of the existence of a private key corresponding to the public key in the certificate is ensured through secure procedures before and during certificate acceptance, and in accordance with the **PKCS #10** standard.

3.2.2 Authentication of Individual Identity

A face-to-face identity check is performed for every individual (natural person) wishing to become a user of the **IDDEEA CA**. The officer responsible for registration duties identifies the natural person applying for a certificate or service by inspecting their valid ID card or passport in the presence of that person.
IDDEEA CA maintains records of the means used to confirm the person's identity.

3.2.3 Unverified User Information

IDDEEA CA does not verify the accuracy of the user's email address or phone number.

3.2.4 Criteria for Interoperation

IDDEEA CA is not North obligated to contract with or guarantee for other Trust Service Providers (TSPs), even if another TSP has the status of a Qualified TSP or a TSP of qualified digital certificates.
The procedures and practices of all cross-certified CAs must be equivalent to the procedures and practices of the **IDDEEA CA** as defined in this Certificate Policy. **IDDEEA CA** defines more detailed conditions on a case-by-case basis.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Routine re-keying is performed when the validity period of the certificate or the private key expires. The identity of the user for certificate re-issuance is verified:

- At the **IDDEEA CA RA**;
- Based on an already issued, valid digital certificate issued by the **TSP**, where **IDDEEA CA** verifies the natural person's data in the relevant registers.

3.3.2 Identification and Authentication for Re-key After Revocation

The authentication of users submitting a request for re-keying after revocation is performed as specified in Section 3.2.2 (Authentication of Individual Identity).

3.4 Identification and Authentication for Revocation Requests

The request for certificate **revocation** is submitted by the user:

- **In person** at the **RA**, where authorized personnel verify the identity of the applicant;
- **Electronically**, provided the revocation request is **digitally signed** with a qualified certificate, thereby proving the identity of the applicant.

If the certificate holder requests the revocation via telephone or email, the **IDDEEA CA** (Trust Service Provider) shall initiate the **suspension** of the certificate. The actual termination of the certificate is carried out only upon receipt of a **written request** for revocation.
Detailed revocation procedure: Section 4.9.3.

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A certification request for a public certificate may be submitted by any person (**natural person**) who meets the conditions specified in the Digital Certificate Registration Request, the **IDDEEA CA** Certificate Policy, and the accompanying agreements between the **TSP** and the end-user.
The prospective subjects of the certificates are natural persons.
To obtain a certificate, the following conditions must be met:

- A completed and personally submitted certificate application form and agreement at the **RA**;
- Identification requirements;
- A valid ID card of a citizen of BiH, or a valid passport of an adult citizen of Bosnia and Herzegovina if the application for a qualified electronic signature certificate for remote signing is submitted through an authorized Registration Office of a diplomatic-consular representation of Bosnia and Herzegovina, or the procedure for issuing/replacing a BiH citizen's ID card in the case of applying for a qualified electronic signature on the ID card.

Diplomatic passports, official passports, joint passports, and travel documents do not constitute a basis and cannot be used to obtain an electronic certificate for a qualified electronic signature for remote signing.
The application for the issuance and use of a certificate also contains information regarding the residence address, email address, and/or contact telephone number through which **IDDEEA CA** can contact the certificate user.

4.1.2 Certificate Application Processing and Responsibilities

A certificate is issued based on a validly completed and signed certificate application form by the prospective certificate user (natural person). The natural person submits the certificate application form to the **IDDEEA CA RA**. The certificate application form can be obtained at the **IDDEEA CA RA** and on the **IDDEEA CA** website.
The prospective certificate user submits the certificate application form in writing.
Before issuing the certificate application form, **IDDEEA CA** informs the prospective user about the rules, the **CPS**, and the operations of **IDDEEA CA**.
IDDEEA CA issues certificates only after verifying the user's identity and successfully completing the registration process. The main steps of the certificate enrollment process are:

- The user submits a signed digital certificate registration request and provides a valid identification document.
- The user agrees to the **IDDEEA CA** Certificate Policy and their obligations upon signing the End-User Agreement.

The digital certificate registration request is approved by the **IDDEEA CA** Registration Authority.
The Registration Authority submits the digital certificate registration request via the appropriate registration application or directly to the **IDDEEA CA** Operating Body.
The **IDDEEA CA** Operating Body creates a user with the corresponding certificate profile and generates activation codes consisting of a registration number and an authorization code. If the request is sent via the application, code generation is either automatic or manual.
Both activation codes are delivered to the end-user when the certificates are prepared by **IDDEEA CA** on a smart card/token.
If the keys and certificates are prepared by the **TSP** on a smart card/token, the **PIN** may be delivered in the following ways:

- Via email and/or SMS;
- Picked up in person by the user at the **RA**;
- Or sent to the registered address via mail.

Activation and registration codes for qualified certificates are delivered to the certificate holder in one of the following ways:

- In person at the **RA**;
- The registration number is sent to the user via the email address provided in the digital certificate registration request;
- The registration number is sent via SMS to the telephone number provided in the digital certificate registration request.

The user utilizes the activation code through a **user application** (web or client application) provided by **IDDEEA CA**. The list of supported applications is published along with the user manual on the **IDDEEA CA** website, as specified in Section 2.1 (Repositories).

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

An authorized officer from the **RA** confirms the identity of the user, who must present a valid photo identification document (ID card or passport) during the visit to the **RA**.
Authorized officers must verify the identity of the prospective user and all data provided in the

certificate application form that is available in official records or other valid official documents. The **RA** checks the completed certificate application forms and collects the original documentation, which is then securely transferred to the **IDDEEA CA** Operating Body. **IDDEEA CA** performs identification and authentication functions as defined in Section 3.2.2 (Authentication of Individual Identity).

4.2.2 Approval or Rejection of Certificate Applications

A request for registration or obtaining a certificate from **IDDEEA CA** will be approved only if all the following conditions are met:

- Registration for digital certificate issuance is successfully completed, including successful identification and authentication in accordance with Section 3.2;
- The submitted identification documentation has been successfully verified;
- The user has signed the corresponding agreement with **IDDEEA CA**.

If any of the above criteria are not met, or if there is a reasonable suspicion that the applicant is violating the provisions of this document, the End-User Agreement, or applicable legislation, the **IDDEEA CA** registration officer shall reject the certification request. **IDDEEA** reserves the right to reject any certification request without providing reasons for the rejection.

4.2.3 Time to Process Certificate Applications

The certificate application form and identification document are verified and processed in the presence of the applicant at the **IDDEEA CA** Registration Authority premises.
The submitted request is further processed within **30 days** in the case of issuing a digital certificate on the ID card of a citizen of Bosnia and Herzegovina, and within a maximum of **10 days** in the case of issuing digital certificates for remote electronic signatures.

4.3 Certificate Issuance

4.3.1 TSP Actions during Certificate Issuance

Upon receiving a certificate issuance request, the **IDDEEA CA** certificate issuance system:

- Verifies the validity of the data entered during the registration process;
- The data validity check is performed either automatically or manually;
- Issues the requested certificate, provided all the aforementioned conditions are met.

The procedure and process for certificate issuance depend on the type of certificate:

4.3.1.1 Qualified Digital Certificates on the BiH Citizen ID Card

The issuance process for certificates and two key pairs consists of clearly separated parts (or functions), with their own distinct subsystems:

- Pre-personalization of the **QSCD** (key generation on the card, setting the password to secure the certificate);
- Obtaining the certificate issuance application form;
- Reviewing the certificate issuance application form;
- Certificate preparation;
- Creation of the **QSCD** (issuance and storage of the certificate, printing of subject data);
- Distribution of the certificate, private password (**PIN code**), and notice to the subject.

The digital certificate for the **QSCD** and the **PIN** are delivered to the **RA** and picked up in person by the user, or sent to the user via email and/or SMS to the registered email address and/or registered telephone number.

4.3.1.2 Qualified Digital Certificates for Remote Electronic Signing

The issuance process for certificates and one key pair consists of clearly separated parts (or functions), with their own distinct subsystems:

- Reviewing the certificate issuance application form;
- Preparation of the certificate, registration, and activation code;
- Sending the registration and activation code and notice to the user;
- Key generation in secure storage and certificate issuance.

The registration code is sent to the user via two separate channels: one via email, and the other via another secure channel (a secure web portal accessible via a qualified certificate, registered mail, or a special website where the holder identifies themselves using a unique code received via SMS and other known data (e.g., Personal Identification Number – **JMBG**, valid ID card number, or similar)). Exceptionally, one of the aforementioned codes may be delivered to the user in person by an authorized **IDDEEA CA RA** officer.
Procedures are designed so that they cannot be carried out by a single person independently.
IDDEEA CA may authorize vetted external contractors for certain tasks (e.g., printing holder data, PIN printing, delivery, etc.) based on a written agreement, which it regularly monitors and for which it remains responsible as if performing the tasks itself.

4.3.2 Notification to User by the CA of Issuance of Certificate

The **IDDEEA CA** application will immediately deliver the certificate to the applicant; therefore, no additional notification is required.
For certificates issued via smart card/token, where the key and certificates are prepared by the **TSP** on the smart card/token, the user is notified during the delivery process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The certificate acceptance procedure depends on the type of certificate:
In the case of a **qualified digital certificate on the BiH citizen ID card**, certificate acceptance does not apply because the prospective user receives the certificate via the **QSCD**, and the **PIN** is delivered to the **RA** and picked up in person by the user, or sent to the user via email and/or SMS to the registered email address and/or registered telephone number. See Section 4.3.1.
For certificates not issued on a smart card/token, the certificate holder gains access to the remote electronic signing platform through the corresponding **CA web application**. After successfully completing the online registration process (using the registration number obtained by submitting a request at the **RA**), they activate their own certificate for remote electronic signing.
In the case of **qualified digital certificates for remote electronic signing**, it is not mandatory for the certificate to be accepted, but only activated, since the **IDDEEA CA** custodian securely stores it according to the user's authorization. Only the codes for accessing the secure certificate are delivered to the user; see Section 4.3.1.
Instructions for certificate renewal can be found on the **IDDEEA CA** website: https://www.iddeea.gov.ba.

Instructions for using the qualified certificate for remote electronic signing will be delivered to the user via email during the registration process. The instructions themselves are subject to change in accordance with current changes within the **PKI** and are not an integral part of this Policy.
The certificate user must verify the data in the certificate immediately upon receipt and promptly notify **IDDEEA CA** in case of potential errors or issues.

4.4.2 Publication of the Certificate by the CA

IDDEEA CA does not notify third parties about the issuance of individual certificates. The **RA** may come into possession of information regarding issued certificates for which the certificate issuance application form has been accepted.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The user or prospective certificate user is obligated to:

- **Familiarize** themselves with and act in accordance with the rules prior to certificate issuance;
- **Comply** with the rules and other applicable provisions;
- **Verify** the information on the certificate upon receipt or activation and, in case of potential errors or issues, immediately notify **IDDEEA CA** or request certificate revocation;
- **Monitor** and adhere to all notices issued by **IDDEEA CA**;
- **Update** the necessary software in accordance with notices to ensure secure operation with certificates;
- **Immediately notify IDDEEA CA** of any changes related to the certificates;
- **Request certificate revocation** in the event of a compromised private key that may affect usage reliability, or in case of a risk of misuse;
- **Request certificate revocation** in the event of loss or theft of a mobile device, credentials, or in case of a risk of misuse.

Use the certificate only for the **purposes specified** in the certificate (see Section 7.1) and in the manner determined by the **IDDEEA CA** rules.
The user or prospective certificate user also has the following obligations regarding **private key protection**:

- Carefully protect the enrollment or activation data from unauthorized persons;
- Store the private key and certificate on **secure storage devices** in accordance with **IDDEEA CA** notices and recommendations;
- Keep the private key and all other confidential information under appropriate passwords according to **IDDEEA CA** recommendations, or ensure protection that grants access only to the user;
- Carefully safeguard the passwords used for the protection of or access to the private key;
- Take steps in accordance with **IDDEEA CA** notices following the expiration or revocation of the certificate.

IDDEEA CA issues certificates that support several key usages. This support is provided by including the appropriate **key usage extensions**.
Users shall use certificates in accordance with the **X.509 keyUsage** and **extKeyUsage** extensions and for the purposes defined in Section 1.4.1 (Appropriate Certificate Usage). Upon certificate expiration or revocation, the corresponding private key may no longer be used.

4.5.2 Relying Party Public Key and Certificate Usage

A **relying party** shall limit the use of public keys contained in certificates issued by **IDDEEA CA** to the appropriate usage as specified in Section 1.4.1 (Appropriate Certificate Usage). The relying party is also responsible for:

- Ensuring that the certificate has not been revoked by electronically accessing any and all valid **Certificate Revocation Lists (CRLs)** or the **OCSP** protocol;
- Immediately notifying the **TSP** of any suspected or known misuse of any certificate issued by the **TSP**;
- Being aware of the certificate limitations and **TSP** liabilities as detailed in this Policy.

A relying party that relies on a certificate must:

- Handle and use certificates in accordance with the rules and other applicable provisions;
- Carefully examine all risks and liabilities related to certificate use and establish rules for such use;
- Inform **IDDEEA CA** if they discover that a user's private keys have been compromised in a way that may affect usage reliability or in case of a risk of misuse, or if the data stated in the certificate has changed;
- Use the certificate only for the purposes specified in the certificate (see Section 6.1.1) and in the manner established by the rules;
- During the certificate's use, ensure it is not listed in the **revocation registry**;
- Verify that the digital signature was created during the **validity period** and in accordance with the appropriate purpose of the certificate;
- Verify the signature of the **IDDEEA CA**, as published in this **CPS** document and on the **IDDEEA CA** website;

- Comply with other regulations in the event of signing additional agreements regarding certificate use with **IDDEEA CA**.

For the verification of signature/seal validity or other cryptographic operations, the **relying party** must use software and hardware capable of securely verifying the aforementioned requirements for the secure use of certificates.

4.6 Certificate Renewal (Without Re-keying)

Certificate renewal is the process in which the **TSP** issues a new certificate for the same user. **IDDEEA CA** does not permit or provide for certificate renewal.

4.6.1 Circumstance for Certificate Renewal

Not applicable, as specified in Section 4.6 (Certificate Renewal (Without Re-keying)).

4.6.2 Who May Request Renewal

Not applicable, as specified in Section 4.6 (Certificate Renewal (Without Re-keying)).

4.6.3 Processing Certificate Renewal Request

Not applicable, as specified in Section 4.6 (Certificate Renewal (Without Re-keying)).

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable, as specified in Section 4.6 (Certificate Renewal (Without Re-keying)).

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable, as specified in Section 4.6 (Certificate Renewal (Without Re-keying)).

4.6.6 Publication of Renewal Certificate by the CA

Not applicable, as specified in Section 4.6 (Certificate Renewal (Without Re-keying)).

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable, as specified in Section 4.6 (Certificate Renewal (Without Re-keying)).

4.7 Certificate Re-keying

Certificate re-keying is the process in which the **TSP** issues a new certificate to the user. The new certificate contains the same user information as the old certificate but includes new public keys.

4.7.1 Circumstance for Certificate Re-keying

Certificate re-keying is performed:

- Upon **revocation** of the certificate;
- Upon **expiration** of the validity period or shortly before the expiration.

4.7.2 Who May Request Certification of a New Public Key

The **user** (certificate holder) who requested the original issuance of the certificate may request certificate re-keying

4.7.3 Processing Certificate Re-keying Requests

Certificate re-keying is performed:

- In the same manner as the **initial certificate issuance**;

- In the event that the user's ID card or passport remains valid after the certificate expires, **IDDEEA CA** may, shortly before expiration, allow the user to re-key the certificate by electronically signing a new request using a client or web application.

4.7.4 Notification of New Certificate Issuance to Subscriber

As specified in Section 4.3.2 (Notification to User by the CA of Issuance of Certificate).

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As specified in Section 4.4.1 (Conduct Constituting Certificate Acceptance).

4.7.6 Publication of the Re-keyed Certificate by the CA

As specified in Section 4.4.2 (Publication of the Certificate by the CA).

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3 (Notification of Certificate Issuance by the CA to Other Entities).

4.8 Certificate Modification

Certificate modification is a procedure that facilitates the submission of requests for certificates with modified data. Certificate modification implies **certificate re-keying** and is processed in the same way as the initial request.

4.8.1 Circumstance for Certificate Modification

A user may request certificate modifications if the user's information, such as name or email address, changes.

4.8.2 Who May Request Certificate Modification

The user who requested the original issuance of the certificate may request a certificate modification.

4.8.3 Processing Certificate Modification Requests

Requests for certificate modification are processed in the same manner as the initial certificate issuance requests.

4.8.4 Notification of New Certificate Issuance to Subscriber

As specified in Section 4.3.2 (Notification to User by the CA of Issuance of Certificate).

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As specified in Section 4.4.1 (Conduct Constituting Certificate Acceptance). The publication of the modified certificate is performed by **IDDEEA CA**.

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 4.4.2 (Publication of the Certificate by the CA).

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3 (Notification of Certificate Issuance by the CA to Other Entities).

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate revocation may be requested:

- At the request of the **user** or the certificate holder;
- If the **TSP** confirms that the certificate holder has deceased, lost business capacity, or if circumstances significantly affecting the validity of the certificate have changed;
- If it is known or suspected that any information contained in the certificate is inaccurate;
- If the **private key** associated with the certificate is compromised or suspected to be compromised;
- When any **activation data**, such as a password or PIN used to protect the private key, is compromised or suspected to be compromised;
- If the **TSP** determines that the certificate was not properly issued in accordance with the **IDDEEA CA Certificate Policy**;
- When the user or certificate holder violates the provisions of the **IDDEEA CA Certificate Policy** or applicable law (non-compliance with user obligations);
- For any other reason specified in the **Law on Electronic Signature**;
- If the **IDDEEA CA Policy Management Authority** deems it necessary.

4.9.2 Who can Request Revocation

A certificate revocation may be requested by:

- An authorized officer of the **IDDEEA CA**;
- The **user**;
- A competent court, misdemeanor authority, or administrative unit.

4.9.3 Produce for Revocation Request

The certificate holder may request a certificate revocation in the following manner:

- **In person** during **RA** business hours;

- **Electronically**, twenty-four (24) hours a day, every day of the year, in cases of potential misuse or certificate unreliability; otherwise, during the official business hours of government authorities.

If the revocation request is submitted:

- **In person**: It is necessary to complete the appropriate certificate revocation request and submit it to the **RA**;
- **Electronically**: The user must send an electronic message to **IDDEEA CA** with a revocation request, which must be **digitally signed** with a trusted certificate for validation purposes;
- If the user requests revocation via **telephone, email, or fax**, **IDDEEA CA** will **suspend** the certificate. The actual revocation will be carried out only upon receipt of a **written request** for revocation.

The user must always be notified of the date, time, and reasons for the revocation.
Courts, misdemeanor authorities, and administrative units requesting revocation shall do so in accordance with the law and official procedures (criminal proceedings, civil proceedings, general administrative proceedings, etc.).
The provisions relating to revocation apply reasonably to procedures concerning the regeneration of access codes for qualified certificates and registration and activation codes for secure remote signature electronic certificates.
The request for certificate revocation is specified in Section 3.4 (Identification and Authentication for Revocation Requests).

Revocation Due to Changes in Certificate Data

1. **Revocation Request:**
   The user submits a request to the **IDDEEA RA** in person or via email. A request signed with a key issued by **IDDEEA CA** is considered a valid request.
   The user identifies themselves (in person) and submits a request (form) for certificate revocation. The **IDDEEA RA** verifies and approves the revocation.
2. The **IDDEEA RA** initiates the certificate revocation through the application, stating the reasons for revocation, or sends a revocation request to the **IDDEEA CA** Operating Body to perform the revocation, also specifying the reasons.
3. For the issuance of new keys, users are authenticated as specified in Section 3.2.2 (Authentication of Individual Identity).

Revocation Due to Compromised Private Key

1. **Revocation Request:**
   The user submits a request to the **IDDEEA RA** via email or in person.
   By telephone call, provided the person knows the secret word/password/PIN entered in the digital certificate registration request form.
   The user identifies themselves (in person) and submits a request (form) for certificate revocation. The **IDDEEA RA** verifies and approves the revocation.

2. The **IDDEEA RA** initiates the certificate revocation through the application by identifying the compromised status, or sends a revocation request to the **IDDEEA CA** Operating Body to perform the revocation upon identifying the compromised status.
3. In the event of a request for the issuance of new keys, user authentication is performed as specified in Section 3.2.2 (Authentication of Individual Identity).

Certificate Revocation Due to Non-compliance with User Obligations
If a user fails to fulfill their obligations and duties in accordance with this Policy and the agreement concluded with **IDDEEA**, their certificate shall be revoked, whereby:

- The **RA** verifies the status of the user's digital signature with the **TSP**;
- Employees of the **IDDEEA CA** Operating Body perform the certificate revocation, stating the reasons for it.

4.9.4 Revocation Request Grace Period

A user who becomes aware of circumstances requiring certificate revocation is obliged to request the revocation as soon as possible, without undue delay.
IDDEEA CA may perform certificate revocation due to the user's non-compliance with obligations immediately upon the expiration of the deadline by which the user was supposed to fulfill said obligations.

4.9.5 Time within Which CA Must Process the Revocation Request

Upon acceptance of a valid revocation request, **IDDEEA CA**:

- **Revokes the certificate** no later than within four (4) hours if the revocation was submitted due to a risk of misuse, unreliability, etc.;
- Otherwise, revokes it on the first working day following the receipt of the revocation request.

Upon revocation, such a certificate is immediately (within a maximum of 5 seconds) added to the **revocation registry**.
In other cases of certificate revocation, the processing period should not exceed 24 hours from the receipt of the request.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties shall check the **IDDEEA CA CRL** or the **OCSP** protocol before using any certificate issued by the **IDDEEA CA**. If a valid revocation check cannot be performed due to system failure or loss of service, no **IDDEEA CA** certificate should be accepted.

A relying party verifies the response from the **CRL** or **OCSP** by checking its electronic signature with the associated **TSP** certificate and ensuring it has not expired.

4.9.7 CRL Issuance Frequency

IDDEEA CA regularly publishes a new **Certificate Revocation List (CRL)** every 24 hours. The validity period of the **CRL** is up to 48 hours. **IDDEEA CA** updates the **CRLs** immediately or as soon as possible after a valid certificate revocation request is processed. The maximum time between the final confirmation of a certificate revocation (or suspension) and the actual change in the certificate status information available to relying parties is 60 minutes.

4.9.8 Maximum Latency for CRLs

Not specified. (See Section 4.9.7)

4.9.9 On-line Revocation/Status Checking Availability

The **TSP** provides an **OCSP** service. The service location is indicated by the `authorityInfoAccess` extension present in each certificate.

4.9.10 On-line Revocation Checking Requirements

Users and relying parties are obliged to check the status of electronic certificates based on the available **IDDEEA CA** revocation registry.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Ree-key Compromise

No special requirements are requested in the event of a compromise of the certificate holder's key.

4.9.13 Certificate Suspension

If a certificate user requests revocation via telephone or electronically, the certificate is **temporarily suspended** until the original written request is received.
If the certificate user, a relying party, or another person, court, misdemeanor authority, administrative unit, related authorities, or the **TSP** itself expresses suspicion that the certificate contravenes the policy or applicable regulations, the certificate shall be temporarily suspended until a final decision is made.

Certificate suspension may be requested in the event that the certificate holder is absent for an extended period, e.g., maternity leave. **IDDEEA CA** may suspend the holder's certificate during the processing of a certificate revocation request.
Suspended certificates are published in the **Certificate Revocation List (CRL)** for the duration of the suspension.

4.9.14 Who Can Request Suspension

See Section 4.9.13.

4.9.15 Procedure for Suspension Request

As described in Section 4.9.3 (Procedures for Revocation Request).

4.9.16 Limits on Suspension Period

The suspension period is **not limited**.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status is published using the **X.509 Certificate Revocation List (CRL)** via the **OCSP protocol**.
The **CRL** is published through an **LDAP directory** and a website. The exact locations (**LDAP and HTTP URLs**) are published using the **X.509 CRL Distribution Points** extension.
The availability of the **OCSP service** is indicated as a **URL** within the certificate.
The **CRL profile** and the **OCSP service protocol** are described in Sections 7.2 and 7.3.
4.10.2 Service Availability

The **IDDEEA CA** certificate status service is available 24 hours a day, 7 days a week, with a maximum annual unplanned downtime of seven (7) days per year.

4.10.2 Service Availability

The status of the IDDEEA Certificate Authority (CA) certificates is available 24 hours a day, 7 days a week, with a maximum unscheduled downtime of 7 days per year.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

A certificate **ceases to be valid** upon the expiration of its validity period or following its **revocation**. **IDDEEA CA** shall retain documentation and certificate data for at least **ten (10) years** after the expiration or revocation of the certificate.

4.12 Key Escrow and Recovery

IDDEEA CA does not support **key escrow** and recovery.

4.12.1 Key Escrow and Recovery Policy Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The technical assets of **IDDEEA CA** (network computer systems, subscriber terminals, and IT resources) are located in dedicated, constantly monitored rooms within a secure building. System components and the operations of the **IDDEEA CA** Operating Body are situated within a physically protected environment to prevent unauthorized use, access, or disclosure of sensitive information. Physical security controls are implemented in accordance with current best practices for physical security.
Protective measures include:

- Access is restricted solely to **IDDEEA CA** employees;
- All other access is escorted, and every entry is recorded;
- Maintenance and service personnel are under video surveillance during their visits;
- Secure electronic locks and access control systems;
- 24/7 monitoring and video surveillance from the building's security center.

5.1.2 Physical Access

Only authorized **IDDEEA CA** employees, in accordance with their duties, have access to specific parts of the **IDDEEA CA** infrastructure. Every entry into the **IDDEEA CA** premises is electronically logged and entered into an electronic access journal.

5.1.3 Power and Air Conditioning

The **IDDEEA CA** IT center is equipped with air conditioning that regulates heat and humidity, and all critical components are connected to an Uninterruptible Power Supply (**UPS**).

5.1.4 Water Exposures

There are no water installations within the **IDDEEA CA** premises. All technical measures have been taken to protect against water installations in the surrounding environment.

5.1.5 Fire Prevention and Protection

The **IDDEEA CA** premises are protected by an early fire detection system, an automatic fire alarm, and a fire suppression system.

5.1.6 Media Storage

All computer media containing **IDDEEA CA** data, including backup media, are stored in fireproof cabinets, one located within **IDDEEA CA** and the other at a remote secure location.

5.1.7 Waste Disposal

Paper documents and electronic media are destroyed prior to disposal in a manner that ensures information cannot be reproduced. The **TSP** retains all non-serviceable hardware components for secure disposal.

5.1.8 Off-site Backup

IDDEEA CA stores data media at a remote secure location. The media are kept in a remote secure site protected from external influences with controlled access, featuring a high level of protection equivalent to a bank vault. Access to the vault is restricted to two authorized persons

5.2 Procedural Controls

5.2.1 Trusted Roles

Depending on their roles, **IDDEEA CA** employees may have accounts on the **TSP** host computer, the **TSP** application, or both. The **TSP** application used by the **IDDEEA CA** implements a specific number of **trusted roles** assigned to **TSP** employees in accordance with their responsibilities. User rights for operating system accounts on the **TSP** host computer restrict **IDDEEA CA** employees' access to only those resources necessary to perform their tasks.

- **The distribution of TSP roles is:**

Responsible Employees	OS Access Level	TSP Application Access Level
CA Master User	Yes	Yes
CA Security Officer	No	Yes
CA Administrator	No	Yes
Directory Administrator	No	No
Registration Officers	No	Yes
Registration Authority Officers	No	No
Legal Counsel	No	No

Different levels of physical protection and access control based on roles within the **TSP application** and system user rights are used to ensure **separation of duties**.
The trusted roles are:

Role	Duties
CA Master User	• Approves initial **TSP** application and **Hardware Security Module (HSM)** configuration and maintenance • Starts and stops **TSP** application services • Appoints the first **PKI Security Officers** • Resets accounts for **PKI Security Officers** in case of forgotten passwords • Restores **TSP** administrative services in case of profile corruption • Initiates the **HSM** replacement process • Renews **HSM** operator smart cards • Restores and re-encrypts the **TSP** database
CA Security Officer	• Manages user accounts of other **PKI Security Officers** and **PKI Administrators** • Manages user accounts • Manages key recovery for users • Processes audit logs • Sets and modifies the **TSP** application security

	policy • Manages **TSP** application certificate profiles • Performs cross-certification with external certification authorities • Prepares reports
CA Administrator	• Manages user accounts • Manages certificates • Prepares reports
Directory Administrator	• Adds and deletes users in the directory • Configures the directory
Registration Officers	• See Section 1.3.2
Registration Authority Officers	• See Section 1.3.2

5.2.2 Number of Person Required per Task

Two (2) persons with the appropriate trusted roles are required to perform the following tasks:

- Revocation of the **TSP key**;
- Preparation of key and certification policies;
- Creation of user accounts with the role of **CA Security Officer** or **CA Administrator**;
- Updating the **IDDEEA CA private key**;
- Password resets for **CA Master User** accounts;
- Cross-certification with an external **CA**.

A single person may perform all other tasks. All activities performed by holders of trusted **TSP** roles are logged and reviewed.

5.2.3 Identification and Authentication for Each Role

- **PKI employees** with a trusted **TSP** role are subject to a security background check before being appointed to work as members of the **IDDEEA CA Operating Body**.
- The **IDDEEA CA Operating Body** shall be verified in accordance with the rules specified in this Policy before being granted any of the following privileges:
    - Adding entries to the corresponding access list for entry into the **IDDEEA CA** protected premises (security and operational zones);
    - Obtaining the necessary certificate to perform the assigned trusted role;
    - Obtaining a user account in the operating system;
    - Obtaining a smart card/token.
- Operating system and application user accounts, as well as certificates, are created individually for each responsible person.

The daily sharing or joint use of accounts or certificates among **IDDEEA CA** employees is prohibited. Employees are restricted to activities authorized for their specific role through controls implemented by the application, the operating system, and **IDDEEA CA** procedures. **IDDEEA CA** employees use only smart cards/tokens to fulfill the duties assigned to them within their roles.

5.2.4 Roles Requiring Separation of Duties

The **Operating System Administrator** has the necessary rights to install, configure, and maintain the **TSP** host computer hardware and software.
When assigning user roles and physical access rights, the principle of **separation of duties** is strictly observed, ensuring that one person cannot use cryptographic materials to perform security-sensitive operations; instead, the presence of at least two persons is always required.

5.3 Personnel Controls

Responsible persons within **IDDEEA CA** are employed for an indefinite period, engaged under contracts that define their work obligations. They must be adequately qualified to perform their duties.
Employees in the **Registration Authority (RA)** are employed for an indefinite period. They must be adequately qualified to perform their duties.
IDDEEA CA and **RA** employees are contractually bound not to publish or disclose confidential information related to **IDDEEA CA** security or user information.
In accordance with the agreement, users are informed of the security provisions they must apply to protect their computers and encryption devices, as well as this Policy under which their certificates were issued.

5.3.1 Qualification, Experience and Clearance Requirements

IDDEEA CA hiring practices involve considering qualification requirements for each position, the previous duties of potential candidates, and the number of years of experience in similar positions.

5.3.2 Background Check Procedures

The **TSP** adheres to employee screening and the policy specified in Section 6.1.2 (Employee Screening and ISO/IEC 27001 requirements).

5.3.3 Training Requirements

IDDEEA CA provides training for its employees.
For responsible persons within **IDDEEA CA**, training includes system and data protection procedures, role-specific training for their duties, training on the use of the **IDDEEA CA** application, and training on disaster recovery and business continuity procedures.
For registration authority employees, training includes system and data protection procedures and specific training for their roles and duties.

5.3.4 Retraining Frequency and Requirements

Training for **IDDEEA CA** employees is organized according to actual needs and technological changes.

5.3.5 Job Rotation Frequency and Sequence

Job rotation is not applied.

5.3.6 Sanctions for Unauthorized Actions

In the event of suspicion that an unauthorized activity has been performed, or if an unauthorized activity was indeed performed by a person engaged in tasks related to the operation of the **IDDEEA CA** or the **Registration Authority**, **IDDEEA CA** will terminate their further access to technical equipment (hardware and software).
IDDEEA CA will seize or revoke all certificates issued to that person.
Unauthorized activities are reported to the competent state authorities and institutions, in accordance with applicable laws, bylaws, and internal acts.

5.3.7 Independent Contractor Requirements

IDDEEA CA does not have a practice of hiring external contractors for sensitive tasks. However, if such contractors are engaged, appropriate background checks are conducted. All contractors must sign a non-disclosure agreement (**NDA**) in accordance with internal **IDDEEA CA** procedures.

5.3.8 Documentation Supplied to Personnel

Responsible persons within **IDDEEA CA** have access to **TSP** documentation, including hardware and software manuals, **TSP** application manuals, operating procedures, security and fire safety procedures, access control procedures, and this Policy.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

IDDEEA CA regularly monitors and records everything that significantly affects:

- The security of the infrastructure;
- The operation of all security systems;
- Whether there has been an intrusion or an attempted intrusion by unauthorized persons into equipment or data.

Detailed information regarding the above is established in accordance with the Regulation on Internal Rules of **IDDEEA CA**.

5.4.2 Frequency of Processing Log

IDDEEA CA conducts security checks of its infrastructure and records on a daily basis.

5.4.3 Retention Period for Audit Log

In accordance with applicable regulations, audit logs are retained for at least **ten (10) years**.

5.4.4 Protection of Audit Log

Access to the host computer system containing audit log files is permitted only to authorized persons, through a combination of physical and computer security controls. The computer system, backup of audit logs, and physical audit records are stored in a high-security zone at the **IDDEEA CA Operating Body**, which is equipped with physical and environmental controls as defined in Section 5.1 (Physical Controls).

Audit log entries generated by the **TSP** host operating system are individually time-stamped. The operating system protects the integrity of its audit log files using operating system functionality. Audit log entries generated by the **TSP** application are individually time-stamped. The **TSP** application protects the integrity of its audit log files using public key encryption and verification of each entry upon retrieval.

5.4.5 Audit Log Backup Procedures

Backup of audit log files is performed daily as part of the regular backup of the **IDDEEA CA** host system.
Details are established in the internal rules of **IDDEEA CA**.

5.4.6 Audit Collection System (Internal or External)

The **IDDEEA CA** audit collection system is a combination of automatic and manual processes performed by the **TSP** host operating system, the **TSP** application, and **IDDEEA CA** employees, as shown in the following table:

Recorded Events	Collection System	Recording Entity
Start-up and shutdown of the TSP application	Automatic	TSP host operating system
Start-up and shutdown of the TSP host operating system	Automatic	TSP host operating system
Recorded Events	**Collection System**	**Recording Entity**
Successful and failed attempts to create, modify, remove, disable, enable, and recover users	Automatic	TSP application
Successful and failed attempts to create, modify, remove, disable, enable, and recover TSP host operating system accounts	Automatic	TSP host operating system
Successful and failed attempts to create, modify, remove, disable, enable, and recover TSP application accounts	Automatic	TSP application
Successful and failed attempts to log in to the TSP application	Automatic	TSP application
Successful and failed attempts to log in to the host computer	Automatic	TSP host operating system
Unauthorized attempts to access system files	Automatic	TSP host operating system

Unauthorized attempts to access the PKI network	Automatic	Routers and TSP host operating system
Successful and failed attempts to generate, update, and recover keys	Automatic	TSP application
Successful and failed attempts to create, update, suspend, revoke, and recover certificates	Automatic	TSP application
Changes to certificate issuance policies (e.g., validity period)	Automatic	TSP application
Successful and failed TSP attempts to connect, read, and write to the directory	Automatic	TSP application
Significant name changes	Automatic	TSP application
TSP database backup and recovery	Automatic	TSP application and TSP host operating system
Backup, recovery, and deletion of audit logs	Automatic	TSP host operating system and TSP employees
Physical access to TSP premises	Manual	TSP employees
System configuration changes	Manual	TSP employees
Software and hardware updates	Manual	TSP employees
Planned and unplanned system and site maintenance	Manual	TSP employees
Discrepancies and adjustments	Manual	TSP employees
Personnel changes	Manual	TSP employees
Destruction of specific information	Manual	TSP employees

5.4.7 Notification to Event-Causing Subject

It is not necessary to notify the subject that caused the event.

5.4.8 Vulnerability Assessments

IDDEEA CA performs system vulnerability assessments as part of the audit log processing procedure.

5.5 Records Archival

5.5.1 Types of Records Archived

IDDEEA CA maintains the following records:

- Audit information specified in Section 5.4 (Audit Logging Procedures);
- Logs;
- Records;
- All evidence of performed user identification;
- All application forms;
- Certificates and Certificate Revocation Lists (CRLs);
- Policies;
- **CPS**;
- **IDDEEA CA** publications and notices, and other documents in accordance with applicable regulations.

5.5.2 Retention Period for Archive

In accordance with relevant laws, the archive is retained for at least **ten (10) years**.

5.5.3 Protection of Archive

Access to **IDDEEA CA** archive data is permitted only to **TSP** employees on a **need-to-know** basis.

5.5.3.1 Archive Backup Procedures

Archived data is kept on dedicated archival media or as a hard copy. Archived data is stored securely.
Archival material is handled in accordance with applicable regulations, standards, and recommendations specified in the **IDDEEA CA** internal rules.

5.5.4 Requirements for Time-Stamping of Records

Archival records are time-stamped at the time of their creation, using the system time of the device where the event was recorded.
All systems are synchronized with time traceable to **UTC**.

5.5.5 Archive Collections System (Internal or External)

IDDEEA CA uses an internal backup and archival system within **IDDEEA**.

5.5.6 Procedures to Obtain and Verify Archive Information

Access to stored data is permitted only to **IDDEEA CA** representatives with authorized access to information or in accordance with applicable law.

5.6 Key Changeover

The **TSP private key changeover** will be performed in a timely manner before the expiration of the **TSP certificate**. Upon the changeover of the **TSP private key**, the new **TSP public key** will be made available to certificate holders through the **TSP public repository**.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

IDDEEA CA implements an **ISO/IEC 27001** compliant procedure for handling security incidents and failures.

5.7.2 Computing Resources, Software and/or Data Corruption

IDDEEA CA has adopted a contingency and **disaster recovery plan** related to the restoration of operations following the corruption of computing resources, software, and data.

5.7.3 Procedures in the Event of User Private Key Compromise

In the event of a compromise of the **TSP signing private key**, the **TSP** shall revoke and re-issue all **IDDEEA CA** certificates currently in use.

5.7.4 Business Continuity Capabilities after a Disaster

Following a natural or other type of disaster, **TSP** operations and the IT center will be restored at an independent **disaster recovery site** using backup data. **IDDEEA CA** shall take all reasonable measures to restore services as soon as possible, but no later than **five (5) working days**.

5.8 CA or RA Termination

In the event that **IDDEEA CA** voluntarily terminates its activities, the **TSP** shall:

- **Notify** the Supervisory and Accreditation Body and all current users at least **ninety (90) days** prior to the intended termination of operations;
- In agreement with the Supervisory and Accreditation Body, **transfer** its activities to another Trust Service Provider or revoke all valid certificates on or after the expiration of the notice period;
- In the event that a transfer of services to another provider is not possible, **IDDEEA CA** shall deliver all documentation, data, and equipment to the **Ministry of Communications and Transport of Bosnia and Herzegovina** in accordance with the Law on Electronic Signature;
- Ensure that all documentation and archives are transferred to another Trust Service Provider or to the **Ministry of Communications and Transport of Bosnia and Herzegovina**, or are retained for at least **ten (10) years** from the last day of operation;
- Ensure the availability of and access to relevant **Certificate Revocation Lists (CRLs)** and **OCSP** for a period of **six (6) months** after the revocation of all certificates.

Before the termination of services, **IDDEEA CA** shall destroy the **CA private keys**, including backups, or withdraw them from use in a manner that ensures the private keys cannot be recovered.
A notice regarding the termination of services shall be published on the **IDDEEA** website.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The **IDDEEA CA** signing key pair is created on a **Hardware Security Module (HSM)** during the initial **TSP** key generation procedure and is protected by a master key. During the generation of the **CA** cryptographic key pair, multi-factor authentication of authorized persons and the physical protection of the **IDDEEA CA** premises are employed.
The **TSP** subscriber signing key pair is always generated via a **PKI user application** or on a **QSCD device** (smart card/token).
Private keys used for a **qualified electronic signature** or a **qualified electronic seal** are generated within a hardware token that complies with the **QSCD specification**. Private keys used for other types of certificates are generated in a software crypto-token on the user's side or on a hardware token (signature creation device).
User keys are generated depending on the type of certificate in accordance with the table below:

6 TECHNICAL SECURITY CONTROLS	6 TECHNICAL SECURITY CONTROLS	6 TECHNICAL SECURITY CONTROLS
6.1 Key Pair Generation and Inst**allation**	**6.1 Key Pair Generation and Installation**	**6.1 Key Pair Generation and Installation**
6.1.1 Key Pair Generation The **IDDEEA CA** signing key pair is created on a **Hardware Security Module (HSM)** during the initial **TSP** key generation procedure and is protected by a master key. During the generation of the **CA** cryptographic key pair, multi-factor authentication of authorized persons and the physical protection of the IDDEEA CA premises are employed.	**6.1.1 Key Pair Generation** The **IDDEEA CA** signing key pair is created on a **Hardware Security Module (HSM)** during the initial **TSP** key generation procedure and is protected by a master key. During the generation of the **CA** cryptographic key pair, multi-factor authentication of authorized persons and the	**6.1.1 Key Pair Generation** The **IDDEEA CA** signing key pair is created on a **Hardware Security Module (HSM)** during the initial **TSP** key generation procedure and is protected by a master key. During the generation of the **CA** cryptographic key pair, multi-factor authentication of authorized persons and the physical protection of the **IDDEEA CA** premises are employed.

	physical protection of the **IDDEEA CA** premises are employed.	
The TSP subscriber signing key pair is always generated via a PKI user application or on a QSCD device (smart card/token).	The TSP subscriber signing key pair is always generated via a PKI user application or on a QSCD device (smart card/token).	The **TSP** subscriber signing key pair is always generated via a **PKI user application** or on a **QSCD device** (smart card/token).

6.1.2 Private Key Delivery to Subscriber

The **TSP** generates private keys on a **QSCD** device and delivers them to the user.
Private keys for other certificates (those not issued on a **QSCD** device) are generated by the users themselves via their **PKI application**, and as such, are not delivered to the certificate holder.

6.1.3 Public Key Delivery to Certificate Issuer

TSP public keys are delivered to the **TSP application** in **PKCS#10** format. The **PKCS#10** request must be signed with the private key corresponding to the public key contained within the request.

6.1.4 TSP Public Key Delivery to Relying Parties

The **TSP** delivers public keys for the verification of the **IDDEEA CA** signature to users in the form of **X.509** certificates as part of the enrollment procedure.
The **IDDEEA CA** public key is available in certificate form at the following locations:

- In the public **LDAP** directory;
- On the website.

The **TSP** certificate can also be obtained by contacting **IDDEEA CA** (see Section 1.5.2, Contact Person).
In any case, the entity using **IDDEEA CA** certificates must verify the authenticity and integrity of the **TSP** certificate.

6.1.5 Key Sizes

The **TSP** generates its asymmetric signing keys with a length of at least **3072-bit RSA**.
The certificate holder generates their asymmetric private signing keys with a length of at least **2048-bit RSA**.

6.1.6 Public Key Parameters Generation and Quality Checking

IDDEEA CA currently does not issue **DSA** (Digital Signature Algorithm) keys.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

- **IDDEEA CA** uses the **keyUsage** extension fields in certificates to indicate the intended purpose of the public keys, as defined in **RFC 5280** "Internet X.509 Public Key Infrastructure Certificate and CRL Profile."
- In addition to this extension, **IDDEEA CA** also uses the extended key usage (**extKeyUsage**) to further specify the purpose or limit the use of public keys in certificates, as defined in **RFC 5280**:
    - **serverAuth**: TLS WWW server authentication;
    - **clientAuth**: TLS WWW client authentication;
    - **codeSigning**: Signing of downloadable executable code;
    - **emailProtection**: Email protection;
    - **timeStamping**: Binding the hash of an object to a time;
    - **OCSPSigning**: Signing OCSP responses.

Only **CA private cryptographic keys** are used for signing certificates and Certificate Revocation Lists (CRLs).
Cryptographic keys and certificates of responsible persons within **IDDEEA CA** are used exclusively for operating technical assets owned by **IDDEEA CA** (hardware and software).
Other **IDDEEA CA** certificates may be used for the purposes specified in the **keyUsage** field, as shown in the table below.
Key usage is specified in certificates issued by **IDDEEA CA** in the **keyUsage** and **extKeyUsage** extension fields, depending on the type of certificate and the type of public key in the certificate, as shown in the table below:

Certificate Type	Usage in "keyUsage" Field
CAs (Root CA, ORGANIZATION)	keyCertSign, cRLSign
Electronic Certificate for Qualified Electronic Signature	digitalSignature, nonRepudiation, keyEncipherment
Normalized DS – OCSP	digitalSignature

	extKeyUsage: OCSPSigning

6.2 Private Key Protection and Cryptographic Module Controls

6.2.1 Cryptographic Module Standards and Controls

The generation of all **TSP** digital signing keys and activities related to certificate signing are performed within a **Hardware Security Module (HSM)** that meets the **FIPS 140-2 Level 3** standard. All other cryptographic activities are performed in a cryptographic module that complies with the **FIPS 140-2 Level 3** standard.
Private keys used for **qualified electronic signatures** and **qualified electronic seals** are generated and used within a **Hardware Security Module (HSM)** certified in accordance with **QSCD** specifications.
The private keys of the certificate holder rely on the physical and logical controls protecting the holder's computer system. It is the responsibility of the certificate holder to ensure the private key is kept in an environment with a sufficient level of physical protection. However, it is recommended that the certificate holder uses a **QSCD** rating that satisfies at least the **FIPS 140-2 Level 2** standard or another standard verified to an equivalent security level.

6.2.2 Private Key (n out of m) Multi-person Control

As defined in Section 5.2.2 (Number of Persons Required per Task).

6.2.3 Private Key Escrow

IDDEEA CA does not support **private key escrow** with third parties.

6.2.4 Private Key Backup

In accordance with applicable regulations and the **CPS**, the backup of the **IDDEEA CA** private key is specified in the internal rules of **IDDEEA CA**.

6.2.5 Private Key Archival

Private keys are **not archived**.

6.2.6 Private Key Transfer into or form a Cryptographic Module

The **IDDEEA CA** signing private keys are generated within a **Hardware Security Module (HSM)**. The transfer of **TSP** private keys to or from the **HSM** is restricted solely to backup or recovery purposes. **TSP** private keys are protected by encryption when transferred from one **HSM** to another, ensuring the **TSP** signing private key is never unprotected while outside the **HSM**.
Keys stored on a **QSCD device** (smart cards/tokens) are not transferred.

6.2.7 Private Key Storage on Cryptographic Module

The **IDDEEA CA** signing private key is used only within a **Hardware Security Module**. The **CA** signing private key is stored on a replicated **HSM** token for backup and recovery purposes.

6.2.8 Method of Activating Private Key

The **IDDEEA CA** private cryptographic signing key is activated upon starting the certification authority application. Activation requires a smart card or token for accessing the **HSM**, as well as a user password with the **CA Master User** role.
User private cryptographic keys generated on a **QSCD device** are activated after successful **PIN** authentication.

6.2.9 Method of Deactivating Private Key

The **IDDEEA CA** cryptographic signing key is deactivated by terminating the **TSP** application. User applications deactivate the private cryptographic key when the user logs out of the system or application.

6.2.10 Method of Destroying Private Key

TSP private keys are deleted when the **TSP** certificate ceases to be valid, by erasing the private key on the **HSM** and by deleting backups on the redundant **HSM**.
Service keys stored on a smart card are deleted by **destroying the card**.
User applications must erase private cryptographic keys from the **operational memory** before reallocating it. They must also erase the entire disk space used for private cryptographic keys before that space is reallocated to the **operating system**.

6.2.11 Cryptographic Module Rating

See Section 6.2.1 (Cryptographic Module Standards and Controls).

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

IDDEEA CA archives **CA** public keys and user public keys as defined in Section 5.5.4 (Archive Backup Procedures).

6.3.2 Certificate Key Pair Validity Periods

The validity period of public and private cryptographic keys in certificates issued by **IDDEEA CA** is as follows:

- **TSP Root public verification key and certificate**: 20 years;
- **TSP Root private signing key**: 20 years;
- **TSP Issuer public verification key and certificate**: 10 years;
- **TSP Issuer private key**: 10 years;
- **User public verification key and certificate**: up to 10 years;
- **User private key**: up to 10 years;
- **OCSP public verification key and certificate**: up to 3 years;
- **OCSP private signing key**: up to 3 years.

IDDEEA CA may adjust the validity period of certain user cryptographic keys based on specific requirements and public procurement demands, in accordance with regulations and the type of certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Reference numbers and authorization codes are generated by the **TSP application** and are stored encrypted in the **TSP database** until delivery to users. The numbers and codes are unique and generated in an unpredictable manner.
The **TSP** generates a **PIN code** for the key generated on the **QSCD** device, which is sent or delivered to the user as part of the procedure defined in Section 4.1.2 (Certificate Application Processing and Responsibilities).
The **registration and activation codes** for a qualified electronic certificate for remote signing are securely created by **IDDEEA CA**. These codes are transmitted to the user via two separate channels: one via email, and the other via another secure channel (a secure web portal accessible by a qualified certificate, via SMS, or another similar secure channel). Exceptionally, an authorized **IDDEEA CA RA** officer may deliver one of the aforementioned codes to the user in person. The codes are intended solely for activating access to the **cloud certificate**, during which the user sets their own personal code (**PIN code**).

6.4.2 Activation Data Protection

Activation codes are generated securely within the **TSP application** and are stored encrypted in the **TSP database**.

6.4.3 Other Aspects of Activation Data

Not specified.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

IDDEEA CA performs a series of computer security technical controls, implemented by the **TSP host operating system** and the **TSP application**, including:

- Access control to **TSP services**;
- Strict **separation of duties** and roles for **TSP** operational personnel;

- Use of **smart cards** for storing profiles of **CA Security Officers** and **Certificate Administrators**;
- **Encrypted sessions** between the **TSP application** and user applications;
- **Encryption** of sensitive data within the **TSP database**;
- **Archiving** of certificate history and audit data for both the **TSP** and users;
- **Auditing** of security-related events;
- **Recovery mechanisms** for keys and the **TSP application**.

6.5.2 Computer Security Rating

The **TSP host operating systems** are commercial off-the-shelf (**COTS**) products.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

All applications and products used by **IDDEEA CA** are products that comply with the relevant standards in this field.

6.6.2 Security Management Controls

IDDEEA CA implements problem, change, and configuration management procedures for all **PKI** software and hardware components in accordance with **ISO/IEC 27001** requirements.

6.6.3 Life Cycle Security Controls

The **TSP** tests all software and procedures in a controlled environment.

6.7 Network Security Controls

The **IDDEEA CA** computer network consists of interconnected network segments where servers and operational stations are located. These segments are interconnected via **firewalls**. The **IDDEEA CA** computer network is connected to the Internet through several levels of protection (firewalls). The security rules of these firewalls permit traffic only for protocols that are essential for accessing **IDDEEA CA** services.

6.8 Time-Stamping

The date and time are added to all audit logs at both the system and application levels. System time is synchronized with multiple external references traceable to **UTC**. The **NTP** protocol is used for synchronization.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profiles

7.1.1 Version Number(s)

IDDEEA CA issues certificates in the **X.509v3** format and in accordance with **RFC 5280**, **EN 319 412-2**, **EN 319 412-3**, and **EN 319 412-5**. The following basic **X.509** fields are used:

X.509 Extension/Field	Description
Signature	**TSP** signature for certificate authentication
Issuer	**TSP** name
Validity Period	Activation and expiration dates of the certificate
Subject	**Distinguished Name (DN)** of the user
Subject Public Key Info	Algorithm ID, public key
Version	**X.509** certificate version, version 3 (2)
Serial Number	Unique serial number of the certificate

7.1.2 Certificate Extensions

The following basic **X.509 extension** fields are used:

X.509 Extension/Field	Description
Signature	**TSP** signature for certificate authentication
Issuer	**TSP** name
Validity Period	Activation and expiration dates of the certificate
Subject	**Distinguished Name (DN)** of the user
Subject Public Key Info	Algorithm ID, public key

Version	**X.509** certificate version, version 3 (2)
Serial Number	Unique serial number of the certificate

TSP certificates contain the following critical extensions:

X.509 Extension	Description
keyUsage	keyCertSign, cRLSign
basicConstraints	CA=TRUE, pathLenConstraint

User and service certificates may contain the following extensions:

X.509 Extension	Description
authorityKeyIdentifier	**Hash** of the issuer's key
subjectKeyIdentifier	**Hash** of the holder's key
keyUsage	As defined in Section 6.1.7 (Key Usage Purposes). Extensions are always marked as **critical**.
extendedKeyUsage	As defined in Section 6.1.7 (Key Usage Purposes).
privateKeyUsagePeriod	As defined in Section 6.3.2 (Certificate and Key Pair Validity Periods).
certificatePolicies CertPolicyID CPS URI	**Certificate Policy OID** = OID as defined in Section 1.2 (Document Name and Identification).
cRLDistributionPoints	**CRL** locations
subjectAlternativeName	Alternative name of the user
basicConstraints	**cA=false**
authorityInfoAccess	**accessMethod=calssuers**; and **accessMethod=OCSP**
qcStatement	According to **ETSI EN 319 412-5 V2.5.1**

7.1.3 Private Certificate Extensions

X.509 Extension	OID
Key Usage: digitalSignature, nonRepudiation, keyEncipherment	2.5.29.15
Extended Key Usage: Document Signing	1.3.6.1.4.1.311.10.3.12
Extended Key Usage: PDF Signing	1.2.840.113583.1.1.5

7.1.4 Algorithm Object Identifiers (OIDs)

Algorithm	Object Identifier (OID)

RSA	1.2.840.113549.1.1.1
SHA512 with RSA	1.2.840.113549.1.1.13

7.1.5 Name Forms

In all certificates issued by **IDDEEA CA**, the full **Distinguished Name** of the certification authority and the certificate subject is entered into the **Issuer** and **Subject** fields, respectively. The encoding of these names is performed in **UTF8String** or **PrintableString** format.

7.1.6 Name Constraints

Not applicable.

7.1.7 Certificate Policy Object Identifier

All certificates issued by the **TSP** contain the **Certificate Policy OID** under which the certificate is issued. The **OID** for each certificate is defined in Section 1.2 (Document Name and Identification).

7.1.8 Policy Constraints Extensions

Not applicable.

7.1.9 Policy Qualifiers Syntax and Semantics

Policy qualifiers are used in accordance with **RFC 5280**.

7.1.10 Processing Semantics for the Critical Certificate Policies Extensions

PKI user applications must process the certificate policy extension as **critical**, in accordance with **RFC 5280**.

7.2 CRL Profile

7.2.1 Version Number(s)

The **TSP** issues **Certificate Revocation Lists (CRLs)** in the **X.509 v2** format, using a set of distribution points within the **LDAP directory** and **HTTP web servers**.
The following basic **X.509 extension** fields are used:

X.509 Extension/Field	Description
Version	Set to **v2**
Signature	Algorithm identifier used for signing the **Certificate Revocation List**
Issuer	**Distinguished Name (DN)** of the **CA**
thisUpdate	Date of issuance of the **Certificate Revocation List**
nextUpdate	Date of the next scheduled issuance of the **Certificate Revocation List**
revokedCertificates	Serial numbers of the revoked certificates

7.2.2 CRL and CRL Entry Extensions

X.509 Extension	Description
CRLNumber	Serial number of the Certificate Revocation List
authorityKeyIdentifier	**Hash** of the issuer's key
reasonCode	The **TSP** may include values in accordance with **RFC 5280**
invalidityDate	Populated by the **TSP application** as determined by the operator
expiredCertsOnCRL	A Certificate Revocation List containing this extension includes revocation status information for certificates that have already expired

7.3 OCSP Profile

The **OCSP profile** used is defined in **RFC 6960**.

7.3.1 Version Number(s)

OCSP version v1, in accordance with **RFC 6960**, is used.

7.3.2 OCSP Extensions

The **OCSP request** extensions are:

Extension	Description
nonce	The **nonce** value binds the request and response to prevent replay attacks. The value shall be in accordance with **RFC 6280**.

OCSP response extensions are:

Extension	Description
nonce	The same value as in the request, if so requested in the request.
archiveCutoff	The time period for which **OCSP** retains revocation information after the certificate has expired.

8. Compliance audit and other assessments

8.1 Frequency or Circumstances of Assessment

The compliance audit of **IDDEEA CA** is conducted in accordance with the Law on Electronic Signature and other applicable legal regulations of Bosnia and Herzegovina.
IDDEEA CA performs mandatory internal audits at least once a year.

8.2 Identity/Qualifications of Assessor

The internal audit officer possesses the appropriate technological and legal expertise. The external auditor must also possess the appropriate technological and legal expertise.

8.3 Assessor's Relationship to Assessed Entity

The internal or external auditor does not perform tasks related to or connected with certificate management.

8.4 Topics Covered by Assessment

The internal audit determines whether:

- The Policy sufficiently fulfills the technical, procedural, and organizational activities of the **TSP**, in accordance with the requirements of the Law on Electronic Signature and other applicable regulations of Bosnia and Herzegovina.
- The **TSP** system is compliant with technical, procedural, and organizational practices and policies.

8.5 Actions Taken as a Result of Deficiency

IDDEEA CA shall take appropriate actions to resolve any deficiencies or non-compliances identified as a result of the audit within an agreed timeframe, which depends on the severity of the associated risk.

8.6 Communication of Results

Audit information regarding **IDDEEA CA**'s compliance with relevant laws is considered highly sensitive and shall not be disclosed to anyone or for any reason, except for audit purposes or in cases mandated by law.

9. Other Business and legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

IDDEEA CA may charge for the issuance of electronic certificates based on specific decisions of the **Council of Ministers of Bosnia and Herzegovina**, which, if adopted, will be published on the **IDDEEA CA** website.

9.1.2 Certificate Access Fees

See Section 9.1.1 (Certificate Issuance or Renewal Fees).

9.1.3 Revocation or Status Information Access Feess

See Section 9.1.1 (Certificate Issuance or Renewal Fees).

9.1.4 Fees for Other Services

See Section 9.1.1 (Certificate Issuance or Renewal Fees).

9.1.5 Refund Policy

Certificate applicants may cancel their certificate request free of charge prior to the issuance of activation codes.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

IDDEEA CA is obliged to ensure the minimum amount of liability insurance for potential damage resulting from the provision of qualified electronic certificate issuance services in accordance with applicable regulations, such that:

- The insured sum for which insurance must be contracted per single harmful event may not be less than **50,000.00 KM**, defining a harmful event as individual damage resulting from the use of one qualified electronic certificate in a single act of legal transactions;
- The total cumulative annual insured sum for which the **CA's** liability insurance must be contracted for all harmful events may not be less than **1,500,000.00 KM**.

9.2.2 Other Assets

No provisions.

9.2.3 Insurance or Warranty Coverage for End-Entities

Users and relying parties are solely responsible for ensuring adequate insurance or warranty coverage regarding the use or service of their certificate.

9.3 Confidentiality of Business Information

All personal data submitted to **IDDEEA CA** or its authorized representatives are stored in accordance with the requirements prescribed by the **Law on Personal Data Protection of**

Bosnia and Herzegovina. The disclosure of said information shall only be in accordance with the Law on Personal Data Protection, the **IDDEEA CA** Personal Data Protection Policy, or other applicable regulations.

9.3.1 Scope of Confidential Information

All information collected, generated, transmitted, or stored by **IDDEEA CA** is considered confidential, except for the information specified in Section 9.3.2, which is considered non-confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Information published as part of the **IDDEEA CA** certificates, **Certificate Revocation Lists (CRLs)**, Certificate Policy, and other information published in the **CA public repository** is not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

IDDEEA CA is responsible for the protection of confidential information in accordance with the **IDDEEA CA Personal Data Protection Policy**, the Law on Personal Data Protection, and other applicable regulations.

9.4 Privacy of Person Information

9.4.1 Privacy Plan

As specified in Sections 9.3 and 9.4.

9.4.2 Scope of Private Information

All information related to the certificate holder or user that is not published in the certificate issued by **IDDEEA CA**, the **CRL**, or the public **LDAP directory** is considered confidential.

9.4.3 Information Not Deemed Private

All information contained within the certificate issued by **IDDEEA CA**, the **CRL**, or the public **LDAP directory** is not considered confidential.

9.4.4 Responsibility to Protect Private Information

As specified in Section 9.3.3.

9.4.5 Notice and Consent to Use Private Information

IDDEEA CA shall use private information only for the purposes for which the user provided consent during the registration process.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

IDDEEA CA shall disclose confidential information only to representatives of institutions competent for law enforcement in accordance with applicable regulations.

9.4.7 Other Information Disclosure Circumstances

IDDEEA CA shall disclose private information only under the circumstances established by the **IDDEEA CA Personal Data Protection Policy**, the Law on Personal Data Protection of Bosnia and Herzegovina, and other relevant laws, upon the request of a court or other competent authority, provided the request has a legal basis.

9.5 Intellectual Property Rights

Not applicable.

9.6 Representations and Warranties

9.6.1 TSP Representations and Warranties

IDDEEA CA shall issue certificates, perform other certificate management procedures, and manage the **CA infrastructure** in accordance with the Certificate Policy and applicable laws. The **TSP** is responsible for compliance with the procedures specified in this Policy, even when **TSP** functionality is undertaken by the **RA** or other authorized bodies.

IDDEEA CA is obligated to:

IDDEEA CA is obligated to:

- **Act** in accordance with its internal rules and other applicable regulations;
- **Act** in accordance with international recommendations;
- **Publish** all relevant documents defining its operations (policies, certificate application forms, revocation requests, price lists, instructions for the secure use of qualified digital certificates, etc.);
- **Publish** on its website all information regarding changes in **TSP** activities that in any way affect certificate subjects and third parties;
- **Ensure** the operation of notification services in accordance with **IDDEEA CA** provisions and other applicable regulations;
- **Adhere** to provisions relating to the secure processing of personal and confidential information concerning the **TSP**, certificate subjects, or third parties;
- **Revoke** certificates and publish them on the **CRL** upon discovering reasons specified in this **CPS** or other applicable regulations;
- **Issue** qualified digital certificates in accordance with this **CPS** and other regulations and recommendations;
- **Issue** the Certificate Policy;
- **Ensure** the accuracy of data regarding issued certificates;
- **Ensure** the correct publication of the **CRL**;
- **Ensure** the uniqueness of **Distinguished Names (DN)**;
- **Ensure** appropriate physical security of the premises and access to the **TSP** premises;
- **Professionally ensure** continuous operation and maximum availability of the service;
- **Professionally manage** the continuous operation of all other supporting services;

- **Resolve** any issues in the best possible manner and within the shortest possible timeframe;
- **Manage** the optimization of the hardware and software used;
- **Inform** users about important matters; and
- **Fulfill** all other requirements in accordance with this Policy.

IDDEEA CA ensures maximum availability of its services every day of the year, except in the following cases:

- Planned and pre-announced technical or service interventions on the infrastructure;
- Unplanned technical or service interventions on the infrastructure resulting from unforeseen failures;
- Technical or service interventions due to infrastructure failure outside the jurisdiction of **IDDEEA CA**, and unavailability resulting from **force majeure** or extraordinary events.

IDDEEA CA shall announce infrastructure maintenance or modernization at least **three (3) days** prior to the start of the activity.
IDDEEA CA is solely responsible for all information in this document and for the implementation of all provisions in this **CPS**.
Other obligations of the **IDDEEA CA TSP** may be determined by potential mutual agreement with a third party.

9.6.2 Registration Authority (RA) Representations and Warranties

The **RA** is obligated to:

- **Verify** the identity of users or prospective users;
- **Receive** certificate application forms for **IDDEEA CA** services;
- **Verify** the certificate application forms;
- **Issue** the necessary documentation to users or prospective users;
- **Securely transmit** forms and other information to **IDDEEA CA**.

The **RA** bears responsibility for the implementation of all provisions, rules, and other **CPS** conditions agreed upon with **IDDEEA CA**.

9.6.3 Subscriber Representations and Warranties

The user assumes full responsibility for the use of the private key associated with the public key in the certificate, whereby the holder is a natural person identified by the private key.
Prior to the issuance of keys and certificates, or upon submitting a certificate request, users conclude an agreement with **IDDEEA CA**, taking into account the terms and conditions of use.
Users are responsible for:

- **Accurately stating** their identity and all other elements in the Request for Issuance of Qualified Certificates;
- **Protecting** data and signature creation devices from unauthorized use;
- **Immediately notifying IDDEEA CA** of the loss of devices, disclosure of data, or unauthorized use of data and qualified electronic signature creation devices;
- **Notifying IDDEEA CA** of any changes to the information based on which the qualified certificate was issued;
- **Using** certificates in accordance with these Rules.

By accepting a certificate issued by IDDEEA CA, the user shall:

- **Keep** their private signing key secret;
- **Keep** their password secret;
- **Immediately notify** the **CA** of any inaccuracies or changes in the information contained in the certificate;
- **Exclusively use** their certificate for lawful and authorized purposes as detailed in Section 1.4 (Certificate Usage);
- **Immediately notify** the **CA** of any suspected or discovered compromise of the private key;
- **Immediately notify IDDEEA CA** of any suspected or known misuse of any certificate issued by the **CA**.

9.6.4 Relying Party Representations and Warranties

To verify the validity of the certificates they receive, relying parties must always first refer to the **IDDEEA CA Certificate Revocation List (CRL)**.
A relying party entrusted with a certificate issued by **IDDEEA CA** is obligated to:

- **Limit** the validity of the certificate solely to the purposes defined in this document;
- **Verify** the validity of the certificate;
- **Read** this document and become familiar with the duties, responsibilities, and limitations of the **TSP**.

- **Request certificate revocation if:**
    - They have knowledge that the private key is compromised in a way that affects proper use;
    - There is a risk of misuse;
    - There are changes in the data stated in the certificate.

Before relying on a certificate, the responsibilities of relying parties are to:

- **Be aware** of certificate limitations and **TSP** liabilities as detailed in this Policy;
- **Limit reliance** on certificates issued by the **TSP** to the appropriate use as detailed in Section 1.4 (Certificate Usage);

- **Ensure** that the certificate has not been revoked by accessing any and all applicable and valid **Certificate Revocation Lists (CRL)** or **OCSP**;
- **Immediately notify IDDEEA CA** of any suspected or known misuse of any certificate issued by the **TSP**.

9.6.5 Other Participants Representations and Warranties

All other participants are obliged to use certificates and act in accordance with this Policy and applicable regulations.

9.7 Disclaimers of Warranties

Except for the warranties specified in this Certificate Policy and related agreements, and to the maximum extent permitted by law, **IDDEEA CA** excludes any other possible warranties, conditions, or representations (express, implied, oral, or written), including any warranty of merchantability or fitness for a particular purpose. The **TSP** specifically excludes:

- Any liability for potential damage that may arise from the moment the **TSP** receives a valid revocation request until the moment the revocation information is published on the **CRL** in accordance with Section 4.9.6;
- Any warranty regarding the accuracy or reliability of any information contained in certificates not provided by **IDDEEA CA**;
- Liability for the representation of information contained in the certificate;
- Any warranty regarding the authorization or status of any person using an **IDDEEA CA** certificate;
- Any liability related to matters beyond its own control, including the availability or operation of the Internet, or the telecommunications or other infrastructure or systems of the **RA**, including hardware and software;
- Any liability for damage resulting from **force majeure** as detailed in Section 9.16.5 (Force Majeure).

9.8 Limitations of Liability

IDDEEA CA disclaims liability of any kind for any type of compensation, damages, or other claims or obligations of any kind based on tort, contract, or any other reason in connection with any service related to the issuance, use of, or reliance on a certificate issued by **IDDEEA CA**.

9.9 Indemnities

Each party bears sole responsibility for indemnifying **IDDEEA CA** or other parties for losses or damages resulting from the fraudulent use of certificates or failure to act in accordance with this Certificate Policy and applicable laws.

9.10 Term and Termination

9.10.1 Term

The **IDDEEA CA** Certificate Policy and other documents become effective upon approval by the competent authorities within **IDDEEA CA** and publication on the **IDDEEA CA** website, as defined in Section 2.1 (Repositories).

9.10.2 Termination

The validity of the **IDDEEA CA** Certificate Policy is not time-limited. The current version ceases to be valid when a new version is published.

9.10.3 Effect of Termination and Survival

Upon the termination of this Certificate Policy as a result of the publication of a new version, certificates shall be used in accordance with the version of the Certificate Policy that was valid on the date of certificate issuance. In the event that circumstances change to an extent where this is not possible, **IDDEEA CA** shall notify users as defined in Section 9.12.2 (Notification Mechanism and Period) and third parties via the website as defined in Section 2.1 (Repositories).

9.11 Individual Notices and Communications with Participants

IDDEEA CA distributes the current version of this Certificate Policy and the current version of all other public documents via its website, as defined in Section 2.1 (Repositories).
See also Section 9.12.2 (Notification Mechanism and Period).

9.12 Amendments

9.12.1 Procedure for Amendments

IDDEEA CA employees and other entities may submit their comments directly to the **Policy Management Authority** in writing, via email, or to the addresses specified in Section 1.5.2 (Contact Person).

9.12.2 Notification Mechanism and Period

IDDEEA CA may decide whether to notify users and third parties in the case of amendments with little or no impact. **IDDEEA CA** determines, at its own discretion, whether amendments impact users and third parties.
All changes to the Certificate Policy will be published as described in Section 2 (PUBLICATION AND REPOSITORY RESPONSIBILITIES). **IDDEEA CA** will notify users of changes affecting users or third parties via email.

9.12.3 Circumstances under which OID Must Be Changed

The Certificate Policy **OID** shall be changed in cases where amendments affect users or third parties.

9.13 Dispute Resolution Provisions

All disputes related to certificate operations shall be submitted in writing to **IDDEEA CA** at the address defined in Section 1.5.2 (Contact Person). If possible, the dispute should be resolved by mutual agreement. Any dispute not resolved through negotiations shall be settled by the **competent court**.

9.14 Governing Low

This Certificate Policy and the relationship between the **TSP**, **RA**, users, subjects (certificate holders), and other third parties are governed by and construed in accordance with the **laws of Bosnia and Herzegovina**.

9.15 Compliance with Applicable Low

The documents and operations of **IDDEEA CA** are compliant with the applicable legislation in Bosnia and Herzegovina, which primarily includes:

- The **Law on Personal Data Protection** of Bosnia and Herzegovina;
- The **Law on Electronic Documents** and the **Law on Electronic Signature** of Bosnia and Herzegovina, along with bylaws adopted based on said Laws;
- Other relevant regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The **IDDEEA CA** Certificate Policy and the **IDDEEA CA End-User Agreement** set forth all relevant provisions governing the relationship between **IDDEEA CA** and the holders of **IDDEEA CA** public certificates

9.16.2 Assignment

Users and certificate holders are not permitted to assign the rights and obligations arising from this agreement, either in whole or in part, to a third party on any grounds.

9.16.3 Severability

The unenforceability of one or more parts of this document shall not affect the applicability of the remaining provisions, provided that it does not affect the material provisions (certificate reliability and certificate usage).

9.16.4 Enforcement (Attorneys' Fees and Wavier of Rights)

Not applicable.

9.16.5 Force Majeure

Force Majeure denotes urgent and unpredictable situations such as natural disasters, terrorism, power or telecommunications outages, fires, unpredictable incidents such as viruses or denial-of-service (DoS) attacks due to hacking, government measures, and the compromise of cryptographic algorithm strength.
IDDEEA CA or other parties shall not be held liable for any damage caused by **force majeure** events.

9.17 Other Provisions

Not applicable

X

DIREKTOR

Prof. dr. Almir Badnjević

Signed by: Almir Badnjević

дигитално потписано / digitalno potpisano / digitally signed

Date: January 29, 2026.

Attachment 1

- **ETSI EN 319 401 V3.2.1** (2026-01)
- **ETSI EN 319 411-1 V1.5.1** (2025-04)
- **ETSI EN 319 411-2 V2.6.1** (2025-06)
- **ETSI EN 319 412-1 V1.6.1** (2025-06)
- **ETSI EN 319 412-2 V2.4.1** (2025-06)
- **ETSI EN 319 412-3 V1.4.1** (2025-06)
- **ETSI EN 319 412-5 V2.5.1** (2025-06)
- **ETSI TS 119 495 V1.7.1** (2025-05)

- **ISO 27001:2022** (2022-10)