Based on Article 61 of the Law on Administration ("Official Gazette of BiH", Nos. 32/02, 102/09, and 72/17) and Article 5 of the Rulebook on Detailed Conditions for Issuing Qualified Certificates ("Official Gazette of BiH", No. 14/17), the Director of the Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina hereby adopts the

CERTIFICATE POLICY
OF THE CERTIFICATION AUTHORITY OF THE AGENCY FOR IDENTIFICATION DOCUMENTS, REGISTERS AND DATA EXCHANGE OF BOSNIA AND HERZEGOVINA

INTRODUCTION

The Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina (hereinafter: IDDEEA) has established a Public Key Infrastructure (PKI) and, as a certifier (Certification Authority) within the meaning of the Law on Electronic Signature ("Official Gazette of BiH", No. 91/06), operates as a provider of services for issuing qualified electronic certificates and managing the lifecycle of electronic certificates under the name: **IDDEEA CA**.
IDDEEA CA issues qualified electronic certificates in accordance with the legal regulations, general acts, and instructions of IDDEEA CA governing this field. The legal framework for the activity of issuing qualified electronic certificates by IDDEEA CA consists of the following laws and bylaws:

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

The general operating rules of IDDEEA CA are contained in the following documents:

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

Qualified and non-qualified electronic certificates and qualified electronic time stamps issued by the IDDEEA CA are in compliance with the **eIDAS Regulation** of the European Union ("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 relating to the issuance of qualified electronic certificates.

The IDDEEA CA utilizes a hierarchy of multiple CA (Certification Authority) servers within its infrastructure for the issuance of qualified and non-qualified electronic certificates. The two-tier architecture of the IDDEEA CA Infrastructure consists of two CA servers:

- Root CA: **"IDDEEA-RootCA-2021"**;

Subordinate CAs for issuing certificates, signed by "IDDEEA-RootCA-2021":

- **"IDDEEA-IssuingCA"**.

Private cryptographic keys associated with qualified electronic certificates are used in the process of qualified electronic signing of electronic documents, which may be used in communication between authorities, communication between authorities and parties, in legal transactions and other legal actions, as well as in administrative, judicial, and other proceedings before state authorities and other institutions, provided that the law governing such proceedings prescribes the use of a qualified electronic signature.

Qualified electronic certificates confirm the link between the user's public cryptographic key and the identity of the user who performed the qualified signing of the electronic document.

Any other use of a qualified electronic certificate that is not defined by this document and is not in accordance with the provisions of the Law on Electronic Signature and other documents regulating this field is not permitted.

PUBLICATION AND REPOSITORY RESPONSIBILITIES

The IDDEEA CA publishes data and all documentation related to the issuance of electronic certificates on the website http://iddeea.gov.ba. The website is publicly accessible, as are all the data and documentation contained therein.

The IDDEEA CA publishes the following on its official website:

1. **Certification Policy (CP)** of the IDDEEA CA;
2. **Certification Practice Statement (CPS)** of the IDDEEA CA;
3. **Previous versions** of the IDDEEA CA Certification Policy and Certification Practice Statement;

4. **Service Agreement template** for the provision of certification services;
5. **Application form** for the issuance and use of electronic certificates;
6. **Request form** for changing the status of a certificate;
7. **Definitions of valid certificate profiles** of the IDDEEA CA, compliant with the EU eIDAS Regulation;
8. **User manuals** and instructions;
9. **Certificates of the IDDEEA CA** – RootCA-2021 and Subordinate CAs (IDDEEA IssuingCA) with associated hash values;
10. **Certificate Revocation Lists (CRL)** for the IDDEEA-RootCA-2021 and IDDEEA IssuingCA;
11. **Legal regulations** in the field of electronic signatures and trust services;
12. **Locations** of the Registration Authority (RA) offices;
13. **Notifications to users** regarding the provision of certification services;
14. **Other acts and notices.**

IDENTIFICATION AND AUTHENTICATION

The IDDEEA CA identifies the user based on the identification documents submitted by the user (a valid identity card or travel document). The user must submit all documentation in person.

Users cannot be anonymous and cannot use pseudonyms.

The IDDEEA CA guarantees the uniqueness of names within its domain. The IDDEEA CA assigns a unique name (Distinguished Name – DN) to each user, which is entered into the Subject field of the electronic certificate.

Names that would violate the intellectual property or copyrights of others are not permitted.

The IDDEEA CA is not obliged to verify whether the use of such names is lawful.

The user bears the responsibility for ensuring the lawful use of the chosen name.

A qualified electronic certificate for electronic signature may only be issued to a natural person, in accordance with the Law on Electronic Signature.

The user must be physically present during the registration process.

OPERATIONAL REQUIREMENTS IN THE CERTIFICATE ISSUANCE PROCESS

To be issued an electronic certificate, the user is required to:

1. **Complete and sign** the application form for the issuance and use of the electronic certificate and present an identification document for inspection;
2. **Fulfill** the identification requirements;
3. **Sign** the agreement on the issuance and use of the electronic certificate.

The application for the issuance and use of the electronic certificate contains data through which the IDDEEA CA can contact the certificate user.
The agreement contains the terms and conditions for the issuance and use of the certificate and enters into force upon signature by the contracting parties.
The use of a qualified electronic certificate is contracted for a period of five years starting from the date of issuance, or for the duration of the validity of the identity card or passport of an adult citizen of BiH, provided that the application for the issuance of the electronic certificate is submitted through an authorized Registration Authority of a diplomatic-consular mission of Bosnia and Herzegovina.
The IDDEEA CA will approve the application for the issuance of an electronic certificate if the following conditions are met:

1. The user has submitted the required documentation in person;
2. The submitted documentation has been verified;
3. All data entered into the application is considered appropriate and complete.

If the user fails to meet the conditions from the previous paragraph, or in any way violates the provisions of these Policies or Practice Statements, the IDDEEA CA shall reject the application for the issuance of the electronic certificate.
The issuance of the electronic certificate is performed as follows:

1. During the issuance process, the user identifies themselves in person at the Registration Office;
2. Following the direct identification process, the user, in cooperation with an authorized officer, completes/provides the data necessary for the Application for the issuance of a qualified digital certificate;
3. The requested data is entered into the Application, which the authorized IDDEEA CA officer electronically records in the IDDEEA RA application. After successfully completing the Application for the issuance of a qualified digital certificate, the authorized IDDEEA CA officer prints the Application form in hard copy and presents it to the applicant for review. The applicant is obliged to verify the accuracy of the entered data and confirm the same with their signature, whereby the Application is formally considered submitted;
4. The authorized officer at the Registration Office enters the user data, creates the request in the Registration Authority application, and forwards the verified request to the PKI IDDEEA operational body;

5. The user signs the agreement on the issuance and use of the electronic certificate;
6. The PKI IDDEEA operational body, based on the verified request, creates an order for the issuance of the electronic certificate.

The procedure and process for issuing an electronic certificate depend on the type of electronic certificate:

1. **Qualified digital electronic certificates on the identity card of a citizen of Bosnia and Herzegovina;**

The issuance process for electronic certificates and two pairs of keys consists of clearly separated parts (or functions), with their own distinct subsystems:
a) pre-presentation of the QSCD (generation of keys on the card, setting the password to secure the certificate),
b) obtaining the application form for the issuance of the electronic certificate,
c) review of the application form for the issuance of the electronic certificate,
d) preparation of the electronic certificate,
e) creation of the QSCD (issuance and storage of the electronic certificate, printing of subject data),
f) distribution of the electronic certificate, private password (PIN code), and notification to the subject.

The digital electronic certificate for QSCD and PIN is delivered to the RA and collected personally by the user or sent to the user via e-mail and/or SMS to the registered e-mail address and/or registered phone number.

2. **Qualified digital electronic certificate for remote electronic signing;**

The issuance process for electronic certificates and one pair of keys consists of clearly separated parts (or functions), with their own distinct subsystems:
a) review of the application form for the issuance of the electronic certificate,
b) preparation of the electronic certificate, registration, and activation code,
c) sending the registration and activation code and notifications to the user,
d) generation of keys on secure storage and issuance of the electronic certificate.

The registration code is sent to the user via two separate channels: one via e-mail and the other through another secure channel (a secure web portal accessible via a qualified electronic certificate, registered mail, or a special website where the holder is identified by a specific code received via SMS and other data known to them (e.g., Personal Identification Number (JMB), valid ID card or passport number, etc.)). Exceptionally, one of the above-mentioned codes may be handed to the user in person by an authorized person of the IDDEEA CA RA.

Procedures are designed in such a way that they cannot be carried out independently by a single person.

The IDDEEA CA may authorize trusted external contractors for certain tasks (e.g., printing owner data, printing PINs, delivery, etc.) based on a written contract, which it regularly monitors and for which it is responsible as if it were performing the tasks itself.

If it is subsequently determined that an electronic certificate contains incorrect data, the user is obliged to contact the IDDEEA CA for the issuance of a new certificate.

The IDDEEA CA does not perform renewals of electronic certificates. The entire process is executed by issuing a new electronic certificate.

Replacement of the public key in an electronic certificate is not performed. The entire process is executed by issuing a new electronic certificate.

The IDDEEA CA is obliged to revoke an electronic certificate for the following reasons:

1. In the event that any information contained in the certificate becomes inaccurate;
2. Changes to data in the certificate that require the issuance of a new certificate;
3. Subsequent determination that the data provided by the user during identification is incorrect;
4. Loss, damage, or misuse of technical means (hardware or software) or the private cryptographic key, i.e., compromise or suspicion of compromise of the private cryptographic key;
5. In the case of permanent unavailability of the private key;
6. In the case that the private key or activation data are no longer in the possession of the signatory or seal-maker;
7. In the case of termination of the relationship between the signatory and the business entity;
8. Non-fulfillment of the certificate user's obligations defined by these Policies, Practice Statements, and the contract;
9. If revocation of the electronic certificate is requested by the certificate user;
10. If the user of the electronic certificate ceases to exist;
11. In the event that the certificate no longer meets the formal requirements defined by the Policy and Practice Statement;
12. If circumstances change that significantly affect the validity of the certificate;
13. In the case of termination of the certification service agreement by the user;
14. For other reasons established by the Law on Electronic Signature and other regulations governing this field.

The revocation of an electronic certificate may be requested by:

1. The electronic certificate user – a natural person;
2. The IDDEEA CA;
3. A competent state authority based on law.

Following the revocation of an electronic certificate, the user may request the issuance of a new electronic certificate.

Certificate Revocation Lists (CRL) of the issuer are published every 24 hours.

Information regarding the revocation status of certificates issued by the IDDEEA CA is available via the IDDEEA CA **OCSP (Online Certificate Status Protocol)** service.

The availability of CRL and OCSP services is 24 hours a day, 7 days a week.

In the event that an electronic certificate is revoked or suspended before the scheduled publication, the IDDEEA CA shall immediately publish a new Certificate Revocation List, even before the expiration of the current list's validity.

Users and third parties are obliged to verify the status of an electronic certificate based on the publicly available IDDEEA CA Certificate Revocation List.

If a user knows or suspects that their private key has been compromised, they are obliged to immediately cease its use and submit a request for the revocation of the electronic certificate.

The IDDEEA CA may **suspend** electronic certificates and temporarily disable their use while verifying and clarifying circumstances related to a potential certificate revocation.

Upon the termination (lifting) of the suspension, the electronic certificate becomes active (valid) again, possessing all the functionalities it had prior to the suspension.

The user shall cease using the electronic certificate:

1. Upon the expiration of the electronic certificate's validity period;
2. Upon the revocation of the electronic certificate;
3. During the period of suspension of the electronic certificate.

The IDDEEA CA does not store the private keys of qualified electronic certificate users and is unable to disclose or recover them.

PHYSICAL, PROCEDURAL, AND PERSONNEL CONTROLS

The IDDEEA CA equipment is located in a secure room protected by a two-level electronic lock at the IDDEEA headquarters. Physical access control to the IDDEEA CA is implemented in accordance with the Law on Electronic Signature and relevant bylaws as follows:

1. Access to the premises and the secure zone is electronically recorded and entered into an electronic access log, which is subject to review;
2. Locks, electronic security systems, and fire protection systems comply with applicable standards;
3. The premises and the system are monitored 24/7 by authorized personnel of the IDDEEA CA;
4. Access can only be carried out in the presence of at least two authorized persons with access rights;
5. Access for system maintenance must be announced in advance, except in cases of system malfunctions where the PKI IDDEEA operational body determines that urgent intervention is required;
6. Every entry into the protected room is recorded within the electronic records.

The IDDEEA CA ensures that access to the certification system is restricted exclusively to authorized employees.

The premises housing the IDDEEA CA infrastructure at the IDDEEA headquarters are equipped with:

1. An Uninterruptible Power Supply (UPS) system and voltage stabilization for computer and communication equipment, connected to a power generator;
2. An independent air conditioning system that enables temperature and humidity control within the IDDEEA CA premises.

The IDDEEA CA equipment is located in a flood-secure area.

The IDDEEA CA equipment is protected by an automatic fire protection system in accordance with the prescribed and applicable legal regulations.

All computer media containing data on the operations of the IDDEEA CA, including backup media, are stored in fireproof safes/containers, one of which is located at the IDDEEA CA central location, and the other at a remote, secure location.

The IDDEEA CA guarantees that all tasks performed within the prescribed scope of activities are carried out by trusted persons with precisely defined duties and authorizations. The work of these persons is subject to constant checks. IDDEEA CA employees must be qualified to perform tasks defined in the Certification Practice Statement and are subject to professional competence verification.

In the event of actual or suspected unauthorized activities by an authorized person of the IDDEEA CA, their further access to the IDDEEA CA technical resources (hardware and software) will be disabled, and the IDDEEA CA will suspend or revoke all valid electronic certificates issued to that person.

Performed unauthorized activities shall be reported to the competent organizational units of IDDEEA, state authorities, and institutions, in accordance with applicable legal and internal regulations.

In the event of damage to technical resources (hardware and software) or data, where the CA application's private cryptographic key is not destroyed or damaged, the CA application services shall be restored as soon as possible.

In the event of a compromise of the CA application's private cryptographic key, the IDDEEA CA shall immediately:

1. Revoke the issued electronic certificates;
2. Revoke the CA application certificate;
3. Publish the Certificate Revocation List (CRL);
4. Notify the users of the issued electronic certificates.

Following the end of a disaster and the elimination of its cause, the IDDEEA CA shall, as soon as possible, return the system to production status and resume operations.

In the event of termination of operations, the IDDEEA CA is obliged to:

1. Notify all interested parties (the competent authority and its users) about the termination of operations;
2. Transfer its obligations to another CA, if such possibilities exist;
3. Revoke all issued electronic certificates that have not expired if it fails to transfer its obligations to another CA;
4. Destroy or completely disable the use of its private keys, which were used for creating certificates and the Certificate Revocation List, ensuring they cannot be reconstructed.

Users of issued electronic certificates shall be notified of the termination of operations via the official IDDEEA CA website or through other means, such as public information outlets or electronic mail.

TECHNICAL SECURITY CONTROLS

During the cryptographic key pair generation ceremony, protections applicable to the IDDEEA CA premises are utilized, along with protection provided by the **Hardware Security Module (HSM)**, the operating system, the CA application, and multi-factor authentication of authorized persons.

The user’s cryptographic key pair for signing and verifying a qualified electronic signature is generated on an **SSCD (Secure Signature Creation Device)** or systems intended for the

issuance of electronic certificates for remote electronic signatures, which serve as qualified electronic signature creation devices.

The lengths of the cryptographic keys for which the IDDEEA CA issues electronic certificates are:

1. **CA application cryptographic keys:** RSA keys with a minimum length of 4096 bits;
2. **User keys:** RSA keys with a minimum length of 2048 bits.

The generation of the CA application's public cryptographic key parameters is performed within the IDDEEA CA hardware security modules, while the user's public cryptographic key parameters are generated in cryptographic SSCD devices and IDDEEA CA software, depending on the certificate profile under which the certificate is issued.

The purpose of the public cryptographic key of a qualified electronic certificate or user seal is the verification of a qualified electronic signature or seal and ensuring non-repudiation.

The IDDEEA CA has implemented multi-party authorization for access to the private cryptographic keys of the IDDEEA CA applications – **IDDEEA-RootCA-2021** and **IDDEEA-IssuingCA**.

The IDDEEA CA does not offer the possibility of private cryptographic key recovery.
The creation of copies (backups) of private cryptographic keys associated with users' qualified electronic certificates is not performed.

The validity periods for IDDEEA CA certificates are as follows:

The validity period for public and private cryptographic keys in certificates issued by the IDDEEA CA is:

1. **TSP Root public verification key and electronic certificate:** 20 years.
2. **TSP Root private signing key:** 20 years.
3. **TSP Issuing CA public verification key and electronic certificate:** 10 years.
4. **TSP Issuing CA private key:** 10 years.
5. **User public verification key and electronic certificate:** up to 10 years.
6. **User private key:** up to 10 years.
7. **OCSP public verification key and electronic certificate:** up to 3 years.
8. **OCSP private signing key:** up to 3 years.
9. The IDDEEA CA may adjust the validity period of certain user cryptographic keys based on specific requirements and public procurement requests in accordance with regulations and the type of electronic certificate.

Each user of a qualified electronic certificate is responsible for safeguarding the password of their SSCD device, as well as the access codes and passwords for accessing remote electronic signature services.

The following technical-security controls and mechanisms are implemented on the IDDEEA CA system:

1. **Access control** to the IDDEEA CA application system services;
2. **Access control** to the IDDEEA CA application functions;
3. **Strict separation of roles** between authorized IDDEEA CA personnel;
4. **Use of cryptographic modules** for storing the cryptographic keys of authorized IDDEEA CA personnel;
5. **Secure archiving** of IDDEEA CA application data and electronic logs;
6. **Protection of electronic logs** and the data contained therein regarding all security-related events;
7. **Establishment of recovery mechanisms** for the system, cryptographic keys, and the IDDEEA CA application database.

The IDDEEA CA possesses mechanisms and procedures applied in the control and supervision of all technical systems. In the event of a breach of the IDDEEA CA system security or a loss of integrity, the IDDEEA CA shall notify the competent authority within 24 hours.

The IDDEEA CA computer network consists of interconnected network segments housing servers and workstations. These segments are interconnected via network devices and firewalls. Security rules on the firewalls and network devices allow traffic only between servers and workstations using the protocols necessary for the performance of IDDEEA CA activities and for access to IDDEEA CA services.

Electronic certificates and Certificate Revocation Lists (CRLs) contain a time reference for the date and time of issuance, the date and time of certificate expiration, and the date and time of the issuance of the next CRL. This time reference is not a cryptographic timestamp. The accurate time system is synchronized via the **NTP (Network Time Protocol)** with an external **UTC (Coordinated Universal Time)** source, which, in accordance with legal regulations, is provided by the Institute of Metrology of Bosnia and Herzegovina.

CERTIFICATE CONTENT, CERTIFICATE REVOCATION LIST (CRL), AND OCSP PROFILES

The IDDEEA CA issues certificates compliant with the **X.509 version 3** specification.

The document describing the IDDEEA CA certificate profiles is available on the IDDEEA CA website under the title **'IDDEEA Certificate Profiles'**.

The IDDEEA CA signs qualified electronic certificates and Certificate Revocation Lists using the **SHA512RSA** algorithm in accordance with the documents **RFC 5280** – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, **RFC 4055** – Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public

Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, and **RFC 6931** – Additional XML Security Uniform Resource Identifiers (URIs).

The IDDEEA CA issues **X.509 version 2** Certificate Revocation Lists (CRL). The Certificate Revocation List profile is compliant with the **RFC 5280** document – Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

COMPLIANCE AUDITS OF IDDEEA CA OPERATIONS AND OTHER ASSESSMENTS

The IDDEEA CA performs risk analysis by conducting system vulnerability tests to identify critical services requiring the use of secure systems and high security levels:

1. Prior to the commencement of certification services;
2. During operational activities as needed, and at least every 6 months.

The IDDEEA CA performs regular internal operational audits by conducting system vulnerability tests twice a year.

It is possible to perform more than two audits per year if requested by the competent authority or as a result of unsatisfactory findings from a previous audit.
The Head of the IDDEEA Technical Sector, or another person specifically authorized by the Director, is responsible for conducting internal audits and designating the persons to perform them.

The internal audit is conducted by engaging an expert from within or outside the IDDEEA CA who must have experience in the following areas:

1. Public Key Infrastructure (PKI) technology;
2. Certification Authority operations;
3. Auditing of certification authorities or other information and communication systems.

In the event of identified deficiencies, activities to rectify them are carried out as soon as possible.

The audit report is an internal document of the IDDEEA CA and is not publicly disclosed. It is intended exclusively for authorized persons of the IDDEEA CA for the purpose of rectifying any discovered deficiencies.

eIDAS 2.0 COMPLIANCE

As part of the preparations for the upcoming eIDAS 2.0 regulatory framework, IDDEEA applies the latest versions of the technical standards listed in Annex 1 of this document, in order to facilitate accreditation and comparison with EU standards. To ensure long-term regulatory relevance, the integration of the IDDEEA infrastructure with European digital identity systems is planned, including the **EU Digital Identity Wallet (EUDI)**.

This compliance will enable the interoperability of qualified electronic certificates at the EU level and ensure timely adaptation to the requirements of the eIDAS 2.0 regulation

OTHER BUSINESS AND LEGAL MATTERS

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

The IDDEEA CA bears financial responsibility for performing its activities in accordance with the applicable legal regulations.

The 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:

1. The insured sum for which insurance must be contracted per single damaging event cannot be less than **50,000.00 KM**, whereby a damaging event is understood as individual damage resulting from the use of one qualified electronic certificate in a single act of legal transactions;
2. The total insured sum for which the CA's liability insurance must be contracted cumulatively on an annual basis, for all damaging events, cannot be less than **1,500,000.00 KM**.

Authorized persons of the IDDEEA CA and users undertake:

1. To maintain the confidentiality of data by applying measures used for the protection of their own secret data and to use them only for the purposes for which they were collected or formed in relation to the provisions of the Certification Practice Statement;
2. Not to disclose secret data without authorization and without prior written approval provided by the user or the competent authority.

The IDDEEA CA is obliged to comply with the provisions of the **Law on the Protection of Personal Data** in its operations.

All intellectual property rights of the IDDEEA CA, including trademarks and copyrights, remain the exclusive property of the IDDEEA CA.

The IDDEEA CA guarantees the provision of certification services in accordance with the law, other regulations, the Certification Practice Statement, and other acts of the Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina that are harmonized with the applicable regulations of Bosnia and Herzegovina.
The IDDEEA CA is obliged to:

1. Verify the identity of the user during the process of issuance or change of the electronic certificate status, as well as the accuracy of the data in the application for issuance and use, or the request for changing the status of the electronic certificate;
2. Issue a qualified electronic certificate in accordance with the law;
3. Ensure that the qualified electronic certificate contains all necessary data in accordance with the law;
4. Enter into the qualified electronic certificate basic data regarding its own identity and the identity of the user, as well as the user's public cryptographic key which is paired with their private cryptographic key;
5. Ensure visible information in the electronic certificate regarding the exact date and time (hour and minute) of the certificate's issuance;
6. Approve or reject the execution of a request to change the status of a qualified electronic certificate in accordance with the law;
7. Maintain an up-to-date, accurate, and securely protected Certificate Revocation List (CRL) and ensure it is publicly accessible;
8. Ensure visible information in the CRL regarding the exact date and time (hour and minute) of the electronic certificate's revocation;
9. Supervise the operations of the organizational units within the IDDEEA CA.

The IDDEEA CA provides services in accordance with applicable regulations and internal acts.

The user is obliged to:

1. Protect the means and data for creating a qualified electronic signature from unauthorized access and use;
2. Submit all necessary data and information regarding their identity and any changes that affect or may affect the accuracy of their identity determination immediately, and no later than within 24 (twenty-four) hours from the moment the change occurs;
3. Immediately request the revocation of their qualified electronic certificate in all cases of loss or damage to the means or data used for creating a qualified electronic signature;
4. Use the qualified electronic certificate for its intended purpose;
5. Fulfill other obligations in accordance with the law and the concluded agreement made in accordance with applicable regulations.

Each participant is guaranteed that the IDDEEA CA provides certification services in accordance with the law, the Certification Practice Statement, and other applicable regulations of the IDDEEA CA.

The IDDEEA CA is not liable for damages resulting from failure to comply with the rights and obligations prescribed by law, applicable bylaws, and the Certification Practice Statement.

The IDDEEA CA is obliged to issue qualified electronic certificates in the prescribed manner and is liable for damages caused to a person who relied on that certificate, in accordance with the law, the CA's acts, and the agreement concluded between the IDDEEA CA and the user.
In the event of termination of operations, the IDDEEA CA shall:

1. Notify the Office for Supervision and Accreditation of CAs and all current users at least ninety (90) days prior to the intended termination;
2. In agreement with the Office for Supervision and Accreditation of CAs, transfer its activities to another trust service provider or revoke all valid certificates on or after the expiration of the notice period;
3. In the event that transferring services to another provider is not possible, the IDDEEA CA shall submit all documentation, data, and equipment to the Ministry of Transport and Communications of Bosnia and Herzegovina in accordance with the Law on Electronic Signature;
4. Ensure that all documentation and archives are transferred to another trust service provider or to the Ministry of Transport and Communications of Bosnia and Herzegovina, or stored for at least ten (10) years from the final day of operations;
5. Ensure the availability and access to relevant Certificate Revocation Lists (CRLs) and OCSP for a period of 6 months after the revocation of all certificates.

Prior to the termination of service provision, the 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 retrieved.

A notice regarding the termination of service provision shall be published on the IDDEEA website.

The user is liable for damages caused by their own fault.

The user is responsible if they intentionally or negligently delete the certificate and/or the associated private key from the identity card. A deleted certificate and/or associated private key are not subject to complaint or warranty. The user is responsible for safeguarding the access codes and passwords necessary for the use of the electronic signature for remote signing.

The user is not liable for damages if they prove that they acted in accordance with the law, bylaws, and the concluded agreement.

Should a dispute arise between IDDEEA and the user of a qualified electronic certificate, or third parties, regarding mutual rights and obligations or the interpretation of the agreement and the

Certification Practice Statement, IDDEEA shall endeavor to resolve the dispute amicably, by mutual agreement. If an agreement is not reached, the dispute shall be resolved by the competent court in Banja Luka.

The IDDEEA CA is exempt from liability for any damage caused to a user, another participant, or a third party during the provision of certification services if the damage occurred due to reasons beyond the control of the IDDEEA CA, i.e., due to force majeure.

This Certification Policy of the Identification Documents, Registers, and Data Exchange Agency Certification Authority supersedes Certification Policy No: 15-02-07-5-807/2023, dated January 17, 2024.

This Certification Policy shall enter into force on the date of its adoption.

X

DIREKTOR

Prof. dr. Almir Badnjević

Signed by: Almir Badnjević

дигитално потписано / digitalno potpisano / digitally signed

Date: January 29, 2026

ANNEX 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	2025-09
ETSI EN 319 412-1	V1.4.1	2025-11
ETSI EN 319 412-2	V1.4.1	2025-11
ETSI EN 319 412-3	V1.4.1	2025-11
ETSI EN 319 412-5	V2.4.1	2025-11
ETSI EN 319 421	V1.3.1	2025-07