IDDEEA CA Certificate Policy (CP)

Electronic signature rules defined by IDDEEA as a Qualified Trusted Service Provider

Identification no.	
Version no.	1.0
Proposed by	Managing Director

Version	Date	Prepared by	Short description of the changes
1.0	2021-09-30	Security Officer	Initial version
•			

Contents

1. INTRODUCTION

1.1. Overview

- IDDEEA operates public key infrastructure to provide following Qualified Trust Services:

  1) issuance of qualified certificates for electronic signatures;

- The document herein is the public part of the rules defined by IDDEEA for Qualified Trust Services provided by the IDDEEA as a Qualified Trusted Services Provider. The purpose of this document is to clarify the technical, procedural and organizational activities, as well as the application of the public key infrastructure (PKI of IDDEEA) and the implemented certification procedures, which demonstrate the confidentiality of IDDEEA as a Qualified Trust Service Provider (TSP).

This document is harmonized with the requirements of Law on Electronic Documents, Electronic Identification and Trust Services in Bosnia and Herzegovina and the by-laws adopted on the basis of the said Law.
This document contains Certificate Policy (CP) for IDDEEA. The present document is structured in line with IETF RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" which contains the framework with a comprehensive list of topics that should to be covered in a certificate policy and/or a certification practice statement. Content is harmonized with:

- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1 Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5 Certificate Profiles; Part 5: QCStatements
- ETSI TS 119 495 Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

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

Table 1: List of qualified certificates

Certificate category	Description
Qualified DS for qualified e-signature	Qualified DS for qualified e-signature issued to a natural person where the private key and the related certificate reside on a QSCD

Table 2: List of normalized certificates

Certificate category	Description
Normalized DS – OCSP	Normalized OCSP

1.2. Document name and identification

- This document is IDDEEA Certificate Policy, hereinafter referred to as Policy or CP. The Policy is published on the following URL:

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

- The document IDDEEA PKI disclosure statement, drafted according to ETSI EN 319 411-1, Annex A.1, hereinafter referred to as PDS, is published on the following URLs:

    - https://www.iddeea.gov.ba/PKI/CP

- The following Object Identifiers (OIDs) are assigned to certificate categories issued under this Policy:

Certificate category	Certificate policy identification (OID)
Qualified DS for qualified e-signature	0.4.0.194112.1.2
Normalized DS - OCSP	0.4.0.194112.1.2

- may also issue different certificates, which must be clearly marked with a distinct policy or additional policy object identifier in the X.509 *certificatePolicies* extension. Object identifier shall be prefixed with the 1.3.6.1.4.1.*18560*. Identifier and should be unique for this prefix.

1.3. PKI participants

1.3.1. Certification Authorities

- IDDEEA CA operates as a public TSP, and for issuing public key certificates to natural and legal persons.

- IDDEEA CA operates Root TSP which issued self-signed certificate in the process of Root Key Generation ceremony and cross certificate to one subordinate (Issuing CA). IDDEEA is using one certification authority (Issuing CA) to issue all types of qualified and normalized certificates to end users.

- IDDEEA CA operates the following certification authorities:

- IDDEEA Root CA with validity from 20.09.2021 and validity to 20.09.2041 which has a self-signed certificate and is issued to IDDEEA certification authorities.

- IDDEEA Issuing CA with validity from 29.09.2021 and validity to 29.09.2031 which is signed by IDDEEA Root CA and is used for issuing end-entity certificates.

- The digital certificate “IDDEEA-RootCA-2021” content:

Serial Number	449FFCA0B7E0AFE2DC4C5D9754F945677B9028AC
Issuer	IDDEEA
Subject	CN=IDDEEA-RootCA-2021, O=IDDEEA, emailAddress=eid@iddeea.gov.ba, L=Banja Luka, street=Kralja Petra I Karadjordjevica 83A, 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
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 hash	A2:4E:6B:E6:78:98:AE:DD:5E:E9:5B:09:82:34:E5:80:48:37:E5:DD
SHA-256 hash	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 Issuing CA digital certificate “IDDEEA-IssuingCA with validity from 29.09.2021 and validity to 29.09.2031” contains:

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
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 hash	C2:A7:DF:30:66:40:D0:7E:D1:BF:E6:98:37:48:5E:32:E7:4A:60:5A
SHA-256 hash	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

- IDDEEA CA as a trusted service provider is obliged to implement measures and procedures that ensure the management of certificates, in accordance with the regulations in force in the Bosnia and Herzegovina and the internal rules of the certification service provider.
- IDDEEA CA employs people who are responsible for:
  - the overall operation of the TSP (IDDEEA PMA);
  - people who operate and maintain the TSP infrastructure, CA's private cryptographic keys, servers and software (Operations Authority – OA); and
  - people who are responsible for subscriber identification (Registration Authority – RA), and coordination with external RA.
- When necessary, these Policy rules distinguish the different users and roles accessing the TSP functions. When this distinction is not required, the term TSP is used to refer to the total TSP entity, including the software and its operations.

1.3.1.1. PMA

- The IDDEEA PMA is responsible for:
- development and maintaining of the IDDEEA CA Certificate Policy;
- development and maintaining the IDDEEA CA public documents (End User Agreement, etc.)
- submits IDDEEA CA Certificate Policy to the responsible management body for approval;
- registration and accreditation of the IDDEEA CA;
- appointing the IDDEEA CA Operational Authority and Registration Authority personnel;
- reviewing and compliance audit of the IDDEEA CA operations and activity to assure that the TSP is operated in accordance with the Policy and relevant legislation;
- reviewing and approving Certification Policy (CP), or Certification Practice Statement (CPS) of the external cross certified Certification Authorities;
- resolving disputes between the IDDEEA CA participants.

1.3.1.2. OA

- The IDDEEA CA OA is responsible for:
- TSP key pairs generation, the secure management of TSP private keys, and the distribution of TSP public keys;
- establishing an environment and procedure for certificate applicants to submit their certificate applications;
- the identification and authentication of individuals or entities applying for a certificate;
- the approval or rejection of certificate applications;

- signing and issuance of X.509 certificates binding subscribers with their public keys in response to approved certificate applications;
- disseminating X.509 certificates through Directories;
- the initiation of certificate revocations, either at the subscriber's request or upon the entity's own initiative;
- the revocation of certificates, including issuing and publishing Certificate Revocation Lists ("CRLs") and maintaining OCSP service;
- operating the TSPin accordance with Bosnia and Herzegovina laws and this Policy;
- approving and assigning individuals to fulfil PKI Officer positions;
- reviewing and auditing RA and LRA operations within its domain;
- requesting revocation of TSP Employee's and RAs' certificates.

1.3.2. IDDEEA CA Registration Authorities (RA)

- The Ministry of the Interior (MUP) is the competent body for issuing an identity card with an electronic memory element (e OI / e LK).
- The Ministry of the Interior is a registration body (hereinafter: registration service provider or RA) that verifies the identities and identification data of natural persons on the basis of which IDDEEA CA issues, renews, revokes and suspends certificates.
- The Ministry of the Interior independently manages its staff in police administrations and police stations (PU / PP) that act as local registration offices (LRA) and that perform the registration of persons in accordance with the Law on Identity Cards of BiH Citizens.
- PU / PP jobs are:
    - a) informing persons about the registration and issuance procedures (e OI / e LK).,
    - b) receiving requests for the issuance, revocation and suspension of certificates to (e OI / e LK).,
    - c) establishing the identity of persons and applicants,
    - d) enabling the conclusion of contracts with natural persons,
    - e) delivery of certificates and (e OI / e LK).

- MUP and IDDEEA have entered into an agreement committing the MoI to ensure the implementation of the security rules and procedures described in this document, in particular in Chapter 3 and points 5.3 and 5.5.

- RA uses two general RA categories. The first RA category (Local Registration Authority or LRA) includes RAs who are responsible for performing face-to-face identity proving and user information collection to support user enrolment and routine re-keys. The second RA category (Primary Registration Authority or PRA) includes appointed persons who review user information and approve registration requests.

1.3.3. Subscribers

- Persons are natural persons to whom an OI / eLK has been issued, who have received a certificate on the identity card and who have signed an Agreement with IDDEEA on the provision of certification services in accordance with the Law on the Identity Card of BiH Citizens. The person is directly responsible for acting in accordance with the Terms of Certification Services.

- A person is also an entity named in the certificate and a signatory who creates an electronic signature and uses the certificate in his personal name.

- Subscribers of are entities including natural persons (individuals) that use services.

- Subject is entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

- The subscriber bears ultimate responsibility for the use of the private key associated with the public key certificate, but the subject is the individual that is authenticated by the private key.

1.3.4. Relaying Parties

- Relying parties are entities including natural persons (individuals) that rely on a certificate and/or electronic signature verifiable with reference to a public key listed in a subject's certificate
- To verify the validity of a certificate they receive, relying parties must always refer to the IDDEEA CA CRL or OCSP prior to relying on information in a certificate.

1.3.5. Other participants

- Not applicable.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

- IDDEEA CA certificates may serve the following purposes:
- Applications requiring the use of qualified certificate in line with the Law on Electronic Documents, Electronic Identification and Trust Services of the Bosnia and Herzegovina.
  - Verification of electronically signed documents
  - Verification for electronically issued documents of legal entity
  - Certificate holder identification
  - Secure e-mail communication
  - Encrypt and decrypt documents in electronic form

    NOTE: does not keep copy of subscriber's private decryption keys for key recovery. It is subscriber's responsibility to maintain secure copy of private decryption keys.
- Other purposes at the request of the users and in line with the Law on Electronic Documents, Electronic Identification and Trust Services and other relevant laws in the Bosnia and Herzegovina.

1.4.2. Prohibited certificate uses

- All certificates issued by the IDDEEA CA shall be used in accordance with the Bosnia and Herzegovina legislation.

1.5. Policy administration

1.5.1. administering the document

- IDDEEA CP is managed by IDDEEA.

1.5.2. Contact person

Address:	Agencija za identifikacione dokumente evidenciju I razmjenu podataka Bosne I Hercegovine- IDDEEA; Kralja Petra I Karađorđevića 83A; Banja Luka
E-mail:	eid@iddeea.gov.ba
Internet:	https://www.iddeea.gov.ba

1.5.3. Person determining CPS suitability for the policy

- Not applicable.

1.5.4. CPS approval procedures

- IDDEEA CA CP is developed and maintained by IDDEEA PMA and approved by the General Director.

1.6. Definitions and Abbreviations

Definitions:

Electronic signature is a collection of data in electronic form which is attached to or is logically linked to other data in electronic form and which the signatory uses for signing.

- **Signer/signatory** is a natural person who creates an electronic signature.
- **Information system** is the system used for compiling, sending, receiving, storing or other type of electronic data processing.
- **Signature-creation data** are the only data used during the creation of the electronic signature, such as codes or private cryptographic keys.
- **Signature-creation device** is a configured program or machine equipment used for forming the electronic signature.
- **Qualified-signature-creation device - QSCD** is: a device which provides unique, safe and confidential data on electronic signature, prevents the possibility of obtaining data on the electronic signature within a reasonable time and by means of reasonable devices from the data for verification of the electronic signature, ensure the protection from forgery of the electronic signature by using a currently available technology and provides for the signer to be able to safely guard the data on electronic signature against unauthorized access.

Signature-validation data are the only data used in the course of the electronic signature validation, such as codes or public cryptographic keys.

Signature-validation device for an electronic signature is a configured program or machine equipment which is utilized for validation of the electronic signature.

Certificate is a certification in an electronic form which certifies the relation between the data for validation of the electronic signature with a certain person, the certificate subject and the identity of that person.

Qualified certificate is a certificate containing the name or title and the country of the residence, i.e. the seat of the authority, the name or the title, i.e. the pseudonym of the subject or the title, i.e. the pseudonym of the information system bearing the designation of the subject, data for verification of the electronic signature which are related to the data for electronic signature, commencement and expiry of the certificate validity, certificate identification number, advanced electronic signature of the authority and possible limitations on the utilization of the certificate.

Normalized certificate is a certificate having the same technical properties and offering the same level of confidentiality as the qualified certificate, however without the legal constraints of its intended purpose.

Advanced electronic signatures are 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 his sole control; and

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 means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signature**.**

Certificate authority is any legal entity or natural person which issues certificates or provides other services relating to certificates, i.e., electronic signatures.

Subject is any entity identified in the certificate as lessee of a private key related with a public key included in the certificate.

Subscriber is a party requesting a certificate from a certificate authority on behalf of one or several subjects. The subscriber may also be a subject when issuing the certificate to an individual for personal use.

Relying party is an entity which has reasonable confidence in the certificate.

Computer user account - a computer user account denotes a set of attributes which enable access to the computer system for a certain person. Each user account is unique for each computer system, which is implemented by means of internal functions of the computer system. The basis for access to the user account is a pair of a username and a password. The username is a sequence of alpha-numeric characters which comprises an identification name of the user in a given computer system. Such identification name has to be unique on the level of the computer system. The password is also a sequence of alpha-numeric characters, which is known solely to the user account user. The user password for those computer systems which require a high level of security may be supplemented or replaced with a chip card.

Encryption key pair denotes a pair of symmetric keys comprised of a public encryption key and an auxiliary private decryption key. It is also known as a confidentiality key pair.

Private decryption key. See Encryption key pair.

Private signing key. See Encryption key pair.

Public encryption key. See Encryption key pair.

Public encryption key certificate is a certificate containing a public encryption key.

Public signature verification key. See Encryption key pair.

- **Public signature verification key certificate** is a certificate containing a public key for signature.
- **Signature key pair** is a pair of asymmetric keys comprised of a private signature key and an auxiliary public key for signature verification.
- **QSCD (Smart Card/token)** is a Qualified electronic Signature/Seal Creation Device in a form of a smart card / token on which private keys can be stored.
- **HSM (Hardware Security Module) –** physical device for safe storage of digital keys.
- **Trust Service Provider** means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.

Qualified Trust Service Provider means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.

Abbreviations:

A list of abbreviations, which are mentioned in this document and in the Policy, is given in the following table:

Abbreviation	**Explanation**
ARL	Authority Revocation List
TSP	Certificate Authority
CN	Common Name - Name X.500
CPS	Certification Practice Statement
CRL	Certificate Revocation List

DC	Digital Certificate
DN	Distinguished Name X.500
EAL	Evaluation Assurance Level
EKU	Extended Key Usage
RA	Registration Authority
LRA	Local Registration Authority
PRA	Primary Registration Authority
PMA	Primary Management Authority
OA	Operation Authority
FIPS 140-1	Federal Information Processing Standards http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf
PKCS #10	Public-Key Cryptography Standard #10
PKI	Public Key Infrastructure
PKIX	X.509 based PKI
PKIX-CMP	PKIX-Certificate Management Protocols, described in RFC 4510
X.509	Certificate standard described in RFC 5280
QSCD	Qualified Signature Creation Device a device for creating a qualified or advanced electronic signature and a qualified or advanced electronic seal in accordance with the requirements of the eIDAS
TSP	Trust Service Provider

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

- IDDEEA CA is publishing certification services related information in the repositories on the following addresses:

Public websites: https://www.iddeea.gov.ba/PKI/CPS

2.2. Publication of certification information

- IDDEEA CA is publishing:
- Certificate Revocation Lists (CRL)
- Certificate status over OCSP protocol
- CA's certificate
- Certificate Policy and PKI Disclosure Statement
- List of Registration Authorities
- User guides
- IDDEEA CA notices and announcements and other certification services related public information.

2.3. Time or frequency of publication

- Certificates are published immediately after they are issued as specified in Section 4.4. The CRL are published immediately after they are issued, and as specified in Section 4.9.7. All information is published promptly after it is changed or becomes available to the TSP.

2.4. Access controls on repositories

- All public information is accessible as read-only without restrictions. Repositories are additionally protected from unauthorized modifications.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

- The subject name attribute in the certificates issued by the IDDEEA CA contains the subscriber's authenticated name as defined in the table in section 3.1.4 Rules for interpreting various name forms. The certificate Subject attribute in the CA Certificate and in certificates issued to subscribers is in the form of X.501 Distinguished Name (DN) type. The DN is encoded as a Printable String or UTF8String and must be present in all issued certificates.

3.1.2. Need for names to be meaningful

- The set of certificates subject DN attributes uniquely identifies each certificate holder and has meaningful values. The serial number attribute is, when present, used to differentiate between names where the subject field would otherwise be identical.

3.1.3. Anonymity or pseudonymity of subscribers

- Not applicable.

3.1.4. Rules for interpreting various name forms

- The subject name field is defined as the X.501 type Name (x.500 Distinguished Name), in conformity with RFC 5280.
- IDDEEA CA "Subject" attribute and "Issuer" attribute in the CA certificates is as stated in the section 1.3.1.
- The X.500 Distinguished Name (Subject) in the certificates issued by the IDDEEA CA takes the following format:
- Natural person

Distinguished Name component	Value
Country (C =)	BA
(O =) For natural persons associated with	IDDEEA
organizationIdentifier For natural persons associated with organization	IDDEEA
Given name	Name
Surname	Surname
Common Name (CN=)	the certificate holder's given name and surname for natural persons
Serial Number (serialnumber=)	Unique serial number

3.1.5. Uniqueness of names

- IDDEEA CA assigns in the certificate subject a combination of Distinguished Name attributes, as defined in sections 3.1.2 and 3.1.4, to ensure un-ambiguity and uniqueness of names.

3.1.6. Recognition, authentication, and role of trademarks

- IDDEEA CA will strictly adhere to the rules for assigning names given under items Types of names and meaningful names. The subscribers are forbidden to request the name of the entities which would cause a breach of the intellectual and property rights of the other subscribers.
- IDDEEA CA makes reasonable efforts to resolve disputes that may arise over the allocation of names, e.g., the TSP may contact the applicant and agree that the Common Name (CN) attribute in the subject be modified, to distinguish the DN from an existing DN.
- may at its discretion, reject, change, re-issue or revoke certificates in relation to any DN.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

- Proof of possession of subscriber private keys is provided via a secure exchange between the TSP application and PKI client applications using Certificate Management Protocols in accordance with PKCS#10 Certification Request Syntax Standard.
- In the case when private key and certificate are generated by the TSP, then card with keys and pin are sent to the subject who requested the certificate, which ensures that the subscriber receives the private key.

3.2.2. Authentication of individual identity

- All individuals (natural persons), wishing to become IDDEEA CA subscriber, will be subjected to face-to-face verification. The natural person is identified by the person in charge of registration matters by viewing a valid national ID card or passport requesting the certificate or service.
- IDDEEA CA keeps a record of the means by which the identity of the individual has been verified.

3.2.3. Non-verified subscriber information

Not applicable.

3.2.4. Criteria for interoperation

- Procedures and practices of all cross-certified CAs shall be materially equivalent to the IDDEEA CA procedures and practices defined in this Certificate Policy. IDDEEA CA defines detailed requirements 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 rekeying takes place when the validity of the certificate or private key usage period expires.
- The subscribers requesting certificate renewal are authenticated as specified in sections 3.2.2 Authentication of identity and 3.2.3 Authentication of individual identity.

3.3.2. Identification and authentication for re-key after revocation

- Subscribers requesting re-key after revocation are authenticated as specified in sections 3.2.2 Authentication of identity and 3.2.3 Authentication of individual identity.

3.4. Identification and authentication for revocation request

- Revocation requests can be made by the subscriber or certificate holders by calling TSP contact phone number and identifying with secret defined during registration process, in person

in the TSP registration authority office, or by digitally signed request, which shall be signed with the private signature key of the subject requesting revocation.

- TSP Authorized individuals requesting a revocation via a signed electronic communication are authenticated on the basis of their digital signature, even when the private signing key used is suspected of having been compromised.
- Otherwise, authorized individuals are authenticated based on information contained in the subscriber's file or as provisioned 3.2.2 Authentication of individual identity.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

- Certification application for public certificates can be submitted by:
- any individual (natural person) who fulfils the requirements specified in: Digital certificate application form, IDDEEA CA Certificate Policy and relevant agreement between TSP and the End-User.

4.1.2. Enrolment process and responsibilities

- IDDEEA CA issues certificates only after subscriber's identity validation and successful completion of the registration process. The main steps of the certificate enrolment process are:
  - Subscriber submits signed registration Digital certificate application form and provides valid identification documentation.
  - Subscriber accepts IDDEEA CA Certificate Policy and his obligations by signing the End-User Agreement.
  - Certification request is approved by IDDEEA CA Registration Authority.
  - The Registration Authority submits certification request Digital certificate form via appropriate registration application or directly to the IDDEEA OA.
  - IDDEEA OA creates a user with appropriate certificate profile and generates Activation Codes, which consist of a Reference Number and Authorization Code. If the request is sent via the registration application, the code generation is automatic or manual. Both Activation Codes are needed by the end user to request a certificate from a CA, or the TSP RA in a case when keys and certificates are prepared on a QSCD by the IDDEEA.

If keys and certificates are prepared on a QSCD by the TSP, the PIN and PUK are send by email and/or SMS to the subscriber; the QSCD is delivered in the sealed envelope by RA and picked by the subscriber in person or sent to the registered mail.

If activation Codes are sent to a certificate holder:

- Activation Codes for certificate enrolment are send to a certificate's holder:
  - Reference Number is e-mailed to the subscriber on the e-mail address provided on the Digital certificate application form.
  - Authorization Code is sent to subscriber using SMS
  - The subscriber uses Activation Codes to request his certificate from the TSP, by using client application provided by the IDDEEA CA, or internet browser. List of supported client applications and Internet browsers is published, together with user guides on IDDEEA CA website listed in section 2.1 Repositories.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

- IDDEEA CA performs identification and authentication forms as defined in sections 3.2.2 Authentication of individual identity.

4.2.2. Approval or rejection of certificate application

- Certification request for IDDEEA CA certificate will be approved if all of the following requirements are met:
  - The subscriber has submitted the Digital certificate form with successful identification and authentication in accordance with Article 3.2;

- The applicant has appropriate authorization, if acting on behalf of an (legal entity);
- Digital certificate form, provided identification documentation and authorizations has been verified successfully;
- The subscriber has signed relevant contract with IDDEEA CA.

- In the case that any of the criteria above is not met, or if a reasonable doubt exists that the requestor violates the provisions of this document, End-User Agreement or applicable legislation, IDDEEA CA Registration Authority will reject the certification request. IDDEEA CA reserves the right to reject certification request without giving any reasons.

4.2.3. Time necessary to process certificate applications

- Certification request application and identification documentation are verified and processed during requestor's presence in the IDDEEA CA Registration Authority office.
- Applications submitted will be processed within 30 days.

4.3. Certificate issuance

4.3.1. TSP actions during certificate issuance

- IDDEEA CA certificate issuance system will do the following upon receiving the certification request (PKCS#10):
- verify the validity of activation codes included in the received data;
- verify that the subscriber possesses private key associated with the public key sent for certification, as provisioned in section 3.2.1 Method to prove possession of private key;
- verify that the certificate requests for compliance with the PKCS#10 technical specification;
- issue the requested certificate if all of the above conditions are met.

4.3.2. Notification to the subscriber by the TSP of issuance of certificate

- IDDEEA CA application will present to the requestor issued certificate immediately, so there is no need for additional notification.
- For certificate types issued on the QSCD, the key and certificates are prepared on the QSCD by the TSP, subscriber is notified as part of the delivery process.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

- The certificate enrolment procedure depends on the certificate type.
- QSCD (smart card / Token) is delivered in the sealed envelope to the subscriber personally or by registered mail to the subscriber's address if it concerns a natural person, whereas for legal entities it is delivered to the address of the legal entity or personally collected;
- Certificates that are not issued on a QSCD (smart card / Token) are enrolled by the certificate holder by using Internet Browser application.
- For certificates that are not issued on a QSCD:
- The instructions for certificate enrolment can be found on IDDEEA CA website https://www.iddeea.gov.ba/PKI/CPS. The subscriber will also receive instructions by e-mail when he/she receives the reference number. The instructions themselves are subject to change in accordance with the current changes within the PKI and are not integral part of this Policy. For successful certificate enrolment, the last published instructions are relevant.

- The subscriber can enrol certificate only with valid activation data: reference number and authorization code. The lifetime of activation data is limited to 30 days. Upon the expiry of the activation data, the registration procedure needs to be repeated.
- In the case of unsuccessful enrolment process, certificate holder shall report the problem to the RA (see RA contact information in section 1.5.2 Contact person).
- The requestor will receive all certificates during on-line certificate enrollment process or on the QSCD. No additional confirmation of certificate acceptance is required.

4.4.2. Notification of certificate issuance by the TSP to other entities

- IDDEEA CA will not notify any other entities.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

- IDDEEA CA is issuing certificates that can support several key usages. This support is provided by the inclusion of the appropriate key usage extensions.
- Subscribers shall use certificates in accordance with keyUsage and extKeyUsage X.509 certificate extensions and for purposes defined in section 1.4.1 Appropriate certificate uses. Subscribers must keep their private key secure and take precautions to prevent key compromise and unauthorized usage.
- After the expiration of certificate validity or revocation of the certificate, the associated private key may no longer be used.

4.5.2. Relying party public key and certificate usage

- Relying party shall restrict reliance on public keys contained in certificates issued by the IDDEEA CA to appropriate use as detailed in section 1.4.1 Appropriate certificate uses. The relying party is also responsible to:
- Be aware of the limitations of the certificate and the TSP liability as specified in detail in this Policy.
- Ensure that the certificate has not been revoked by accessing on-line to any and all applicable Certificate Revocation Lists (CRLs) or OCSP.
- Immediately notify the TSP of any suspected or known misuse of any certificate issued by the TSP.

4.6. Certificate renewal (without generating a new key)

- Certificate renewal is a process in which a TSP issues new certificate for the same subject. Certificate renewal is not allowed or supported by the IDDEEA CA

4.6.1. Circumstances for certificate renewal

- Not supported as stated in section 4.6. Certificate renewal (without generating a new key).

4.6.2. Who may request renewal

- Not supported as stated in section 4.6. Certificate renewal (without generating a new key).

4.6.3. Processing certificate key renewal requests

- Not supported as stated in section 4.6. Certificate renewal (without generating a new key).

4.6.4. Notification of new certificate issuance to subscriber

- Not supported as stated in section 4.6. Certificate renewal (without generating a new key).

4.6.5. Conduct constituting acceptance of certificate with renewed key

- Not supported as stated in section 4.6. Certificate renewal (without generating a new key).

4.6.6. Publication of the renewed certificate by the TSP

- Not supported as stated in section 4.6. Certificate renewal (without generating a new key).

4.6.7. Notification of certificate issuance by the TSP to other entities

- Not supported as stated in section 4.6. Certificate renewal (without generating a new key).

4.7. Certificate re-key (renewal with generating a new key)

- Certificate re-key is a process in which a TSP issues new certificate to a subscriber. The new certificate contains the same subject information as the old certificate and new public keys.

4.7.1. Circumstances for certificate re-key

- Certificate re-key takes place:
- after certificate revocation;
- after the certificate has expired or near expiring.

4.7.2. Who may request certification with new public key

- Certificate re-key may be requested by subscriber, certificate holder or authorized representative who requested initial certificate issuance.

4.7.3. Processing certificate re-keying requests

- Certificate re-key is performed in the same manner as initial certificate request

4.7.4. Notification of new certificate issuance to subscriber

- As described in section 4.3.2 Notification to the subscriber by the TSP of issuance of certificate.

4.7.5. Conduct constituting acceptance of re-keyed certificate

- As described in section 4.4.1 Conduct constituting certificate acceptance.

4.7.6. Publication of the re-keyed certificate by the TSP

- As described in section 4.4.2 Publication of the certificate by the TSP.

4.7.7. Notification of certificate issuance by the TSP to other entities

- As described in section 4.4.3 Notification of certificate issuance by the TSP to other entities.

4.8. Certificate modification

- Certificate modification is procedure which facilitates subscribers to request a certificate with modified information. Certificate modification mandates certificate re-key and is processed as initial certification request.

4.8.1. Circumstances for certificate modification

- Subscriber may request certificate modification when the subject information, like name or e-mail, has changed.

4.8.2. Who may request certificate modification

- Certificate modification may be requested by subscriber, certificate holder or subject who requested initial certificate issuance.

4.8.3. Processing of certificate modification requests

- Certificate modification request is processed as initial certification request.

4.8.4. Notification of new certificate issuance to subscriber

- As described in section 4.3.2 Notification to the subscriber by the TSP of issuance of certificate.

4.8.5. Conduct constituting acceptance of modified certificate

- As described in section 4.4.1 Conduct constituting certificate acceptance. Publication of the modified certificate by the CA.

4.8.6. Publication of the modified certificate by the TSP

- As described in section 4.4.2 Publication of the certificate by the TSP.

4.8.7. Notification of certificate issuance by the TSP to other entities

- As described in section 4.4.3 Notification of certificate issuance by the TSP to other entities.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

- Certification revocation shall be requested:
  - If it is required by the subscriber or the certificate holder;
  - If the TSP confirms that a certificate holder has passed away or has lost his business abilities or the legal entity ceased to exist or if circumstances which have significant effect on the complete validity of the certificate have changed;
  - When any of the information contained in the certificate is known or suspected to be inaccurate;
  - When the private key associated with the certificate is compromised or suspected to have been compromised;
  - When any activation data, such as a password or PIN, used to protect the private key are compromised or suspected to have been compromised;
  - If the TSP determinates that the certificate was not properly issued in accordance with IDDEEA CA Certificate Policy;
  - Subscriber or certificate holder violates the provisions of IDDEEA CA Certificate Policy or the applicable law (non-fulfilment of the subscriber's obligations);
  - All remaining reasons stated in the Law on Electronic Documents, Electronic Identification and Trusted Services.
- IDDEEA CA Policy Management Authority may revoke IDDEEA CA certificate when it deems the revocation necessary.

4.9.2. Who may request revocation

- Certificate revocation may be requested by:
  - Subscriber (i.e., the legal entity) or subject (certificate holder);
  - Authorized representative who requested certificate issuance;
  - IDDEEA CA;
  - Competent court.

4.9.3. Procedure for revocation request

- ~~Subscriber or~~ certificate holder may request certificate revocation in the following ways:
  - By electronically signed revocation request sent by mail;
  - In person via contact with IDDEEA CA registration authority office; or
  - Via telephone call, whereas the person must know the secret word/password entered in the Digital certificate application form;
  - Certificate revocation request is identified as defined in section 3.4 Identification and authentication for revocation request.

Revocation due to data modification in the certificate itself

1. Revocation request:
   - The subscriber sends the request to IDDEEA CA Registration Authority via e-mail or personally. The valid request is considered to be the one signed with the key issued by IDDEEA CA.
   - The subscriber should be identified (in person) and to hand over the request (form) for the certificate revocation.
   - IDDEEA CA Registration Authority checks and approves the revocation.
2. IDDEEA CA.Registration Authority triggers the revocation of the certificate via application, by stating the reasons of revocation or sends the request for revocation to IDDEEA CA. Operation Authority to perform the revocation stating the reasons thereof.
3. For the issuance of new keys, the subscribers are authenticated as specified in sections 3.2.2 Authentication of identity and 3.2.3 Authentication of individual identity.

Revocation due to private key compromising

1. Revocation request:
   - The subscriber sends the request to IDDEEA CA Registration Authority via e-mail or in person.
   - Via telephone call, whereby the subscriber must know the secret word/password entered in the initial registration request.
   - The subscriber should be identified (in person) and to hand over the request (form) for the certificate revocation.
   - IDDEEA CA. Primary Registration Authority checks and approves the revocation.
2. IDDEEA CA Primary Registration Authority triggered the revocation of the certificate via application, by stating the reason as “compromised” or sends the request for revocation to IDDEEA CA Operation Authority to perform the revocation stating the reason “compromised”.
3. In case of request for the issuance of new keys, the subscribers are authenticated as specified in sections 3.2.2 Authentication of individual identity.

Certificate revocation due to non-compliance with the obligations by the subscriber

Should the subscriber fail to fulfil his/her obligations and duties towards and in accordance with this policy and the contract concluded with IDDEEA CA his/her certificate may be revoked, whereas:

1. RA checks status of the subscriber's digital signature in the TSP
2. IDDEEA CA Operation Authority personnel revoke the certificate by stating the reasons thereof

4.9.4. Revocation request grace period

- The subject who became aware of circumstances that require certificate revocation shall request revocation as soon as possible, and without unnecessary delay.
- IDDEEA CA may execute the certificate revocation due to non-compliance with the obligations by the subscriber right after the expiration of the time period within which the subscriber should have fulfilled his/her obligations.

4.9.5. Time within which CA must process the revocation request

- In other certificate revocation cases, the time period between the acceptance of the request and the certificate revocation should be no longer than 24 hrs.

4.9.6. Revocation checking requirement for relying parties

- A relying party shall check the IDDEEA CA CRL or OCSP before using any certificate issued by IDDEEA CA. If no valid revocation checking can be performed, due to system failure or loss of service, no IDDEEA CA certificate should be accepted.
- A relying party shall verify the CRL or OCSP response by checking by checking its digital signature with the associated TSP certificate, and whether it has expired.

4.9.7. CRL issuance frequency (if applicable)

- IDDEEA CA regularly publishes new CRL every 24 hours. CRL validity period is up to 48 hours. The IDDEEA CA updates the CRL immediately or as soon as possible after a valid revocation request is processed. The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties is at most 60 minutes.

4.9.8. Maximum latency for CRLs (if applicable)

- Not determined. (See section 4.9.7)

4.9.9. On-line revocation/status checking availability

- OCSP service is provided by the TSP. Service location is indicated by the extension authorityInfoAccess included in every issued certificate.

4.9.10. On-line revocation checking requirements

- See 4.9.6.

4.9.11. Other forms of revocation advertisements available

- Not applicable.

4.9.12. Special requirements regarding key compromise

- No special requirements are required in the case of Certificate Holder key compromise.

4.9.13. Circumstances for suspension

- Certificate suspension may be requested when the certificate holder leaves for an extended period of time, for example, on maternity leave. IDDEEA CA may also suspend subscriber's certificates while certificate revocation request is being verified.
- Suspended certificates are published on the Certificate Revocation List (CRL) for the period of suspension.

4.9.14. Who can request suspension

- Certificate suspension and un-suspension may be requested by:

- Subscriber or subject (certificate holder)
- Authorized representative who requested certificate issuance
- IDDEEA CA Registration Authority (RA)
- IDDEEA CA members.

4.9.15. Procedure for suspension request

- As described in section 4.9.3 Procedure for revocation request.

4.9.16. Limits on suspension period

- Suspension period is not limited.

4.10. Certificate status services

4.10.1. Operational characteristics

- Certificate status is published using X.509 Certificate Revocation List (CRL) via the OCSP protocol.
- CRL is published through the LDAP directory and website. Exact locations (LDAP and http URLs) are published by using X.509 CRL Distribution Points extension.
- The availability of OCSP service is indicated as a URL in the certificates.
- The CRL profile and OCSP service protocol are described in sections 7.2 and 7.3.

4.10.2. Service availability

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

4.10.3. Optional features

- Not applicable.

4.11. End of subscription

- Subscription ends after the expiry or revocation of the certificate. IDDEEA CA keeps the documentation and certificate data for at least 10 years after the certificate expiry or is revoked.

4.12. Key escrow and recovery

- IDDEEA CA does not support key escrow.

4.12.1. Key escrow and recovery policy and practices

- Not Applicable

4.12.2. Session key encapsulation and recovery policy and practices

- Not applicable.

5. CAPACITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

5.1.1. Site location and construction

- The technical assets of IDDEEA CA (network computer systems, carrier terminals and IT resources) are located in dedicated, continuously monitored premises (sites) in the secure building (facility).
- The system components and operation of IDDEEA CA are located within a physically protected environment to prevent and unauthorized use of, access to, or disclosure of sensitive information. Physical security controls have been implemented consistent with applicable physical security best practices. Safeguards include:
- Access is restricted to IDDEEA CA employees
- All other accesses are under escort and each access is logged
- Maintenance and service employees are video monitored during their visits
- Secure electronic locks and access system
- Monitored 24 hours/7 days a week guarded by on-site guards, and video surveillance from the building's monitoring centre

5.1.2. Physical access

- Only authorized IDDEEA CA employees, in accordance with their function, have access to particular parts of IDDEEA CA infrastructure. Every access to IDDEEA CA sites is recorded electronically and entered into the electronic journal on site access.

5.1.3. Power supply and air conditioning

- IDDEEA CA IT Centre is equipped with an air conditioner to control the heat and humidity, and all critical components are connected to uninterrupted power supply (UPS) units, which also condition the power supply.

5.1.4. Water exposure

- In the premises of IDDEEA CA there are no plumbing installations. All technical measures have been taken for the protection from plumbing installations in the environment.

5.1.5. Fire prevention and protection

- IDDEEA CA premises are protected with a system for early fire discovery, automatic fire alarm and extinguishing system.

5.1.6. Media storage

- All computer media containing IDDEEA CA data, including the media with data back-up, are stored in fireproof containers, one of which is located within IDDEEA CA, and the other one at a remote safe location.

5.1.7. Waste disposal

- Paper documents and magnetic media are destroyed before disposal in a way ensuring that the information cannot be reproduced. TSP retains all unserviceable hardware components for their secure disposal.

5.1.8. Off-site backup

- IDDEEA CA uses a secure remote location for data media storage. The media are stored in a remote secure location protected from external influences and with a controlled access, which has a high level of protection, i.e., a bank safe principle. The access to the safe is limited down to two authorized persons.

5.2. Procedural controls

5.2.1. Trusted roles

- Depending on their role, IDDEEA CA employees may have an account on the TSP host computer, the TSP application, or on both the TSP host computer and the TSP application. TSP application used by the IDDEEA CA implements a number of trusted roles that are assigned to TSP employees according to their responsibilities. Operating system account rights on the TSP host computer limit the access of IDDEEA CA employees to what they require in order to perform their duties.

The schedule of the TSP roles is given in the table below:

responsible employees	Operational system level access	TSP Application-level access
CA Master User	Yes	Yes
CA Security Officer	No	Yes
CA Administrator	No	Yes
Directory Administrator	No	No
Primary Registration Authority employees	No	Yes
Local Registration Authority employees	No	No
Legal advisor	No	No

- Different levels of physical and systems access control based on TSP application roles and system account rights are used to ensure a segregation of duties.

- Trusted roles are:

role	Responsibilities
CA Master User	• Authorizes the initial TSP application and Hardware Security Module (HSM) configuration and its ongoing maintenance • Start and stop TSP application services • Create initial PKI Security Officers • Recover PKI Security Officers when they forget their password • Recover the TSP administration service in the event its profile becomes damaged • Initialize HSM replacement • Recover HSM operator's smart cards • Restore and re-encrypt the TSP database
CA Security Officer	• Manage user accounts of other PKI Security Officers and PKI Administrators • Manage subscriber accounts • Manage key recovery for subscribers • Process audit logs • Set and alter the TSP application security policy • Manage TSP application certificate profiles • Cross-certify with external CAs • Create reports
CA Administrator	• Manage subscriber accounts • Manage certificates • Create reports

Directory Administrator	• Add and delete users to/from the directory • Configure the directory
Primary Registration Authority employees	See section 1.3.2
Local Registration Authority employees	See section 1.3.2

5.2.2. Number of persons required per task

- 2 (two) persons with appropriate trusted role are required to perform the following tasks:
  - TSP key revocation
  - Setting key and certificate policies
  - Creation of user accounts with the role of CA security officer or CA administrator
  - IDDEEA CA private key updates
  - Password reset to CA Master Users accounts
  - Cross-certifying with the external CA
- A single person may perform all other tasks. All activities performed by trusted TSP role holders are logged and audited.

5.2.3. Identification and authentication for each role

- PKI employees with trusted TSP role are subjected to the security screening before they are appointed to work as members of IDDEEA CA Operation Authority.
- IDDEEA CA Operation Authority will be checked in accordance with the rules defined in this policy, before they are assigned any of the following privileges:
  - Adding entry to the appropriate access list for entrance in the protected premises of IDDEEA CA (security and operational zone)
  - Obtaining certificate necessary for performing the assigned trusted role
  - Obtaining operating system user account
  - Obtaining smart card / token
  - The operating system and application user accounts and the certificates are created for each responsible person separately.
- The common use of orders or certificates among IDDEEA CA employees is forbidden. The employees are limited to activities authorized for the given role through the control set by the application, the operational system and the procedures of IDDEEA CA.
- IDDEEA CA employees use only smart cards/tokens in order to fulfil the responsibilities they have been assigned within their roles.

5.2.4. Roles requiring separation of duties

- The operating system administrator has the necessary rights to install, configure and maintain TSP host computer hardware and software.
- 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 principal of segregation of duties is strictly respected, so that one person cannot use

cryptographic materials to execute secure sensitive operations, but it is always necessary to ensure the presence of at least two persons.

5.3. Employee control

- IDDEEA CA responsible persons are employed for an indefinite or definite time period, engaged on the basis of a contract which determines their working responsibilities. They should be adequately qualified to execute their working responsibilities.
- Registration Authority employees are employed for an indefinite or definite time period. They should be adequately qualified to execute their working responsibilities.
- IDDEEA CA employees and Registration Authority employees are obliged with a contract not to announce or disclose confidential information related to IDDEEA CA security or information on the subscribers.
- Pursuant to the contract, the subscribers are introduced with the security regulations which they need to apply in order to protect their computers and the encryption devices, as well as this policy according to which their certificates have been issued.

5.3.1. Qualifications, experience, and clearance requirements

- The employment practices for IDDEEA CA take into consideration the qualification requirements of each position, previous assignments of potential candidates, and the number of years of experience in similar positions.

5.3.2. Background check procedures

- TSP follows the personnel screening and policy outlined in section 6.1.2 Personnel screening and ISO/IEC 27001 requirements.

5.3.3. Training requirements

- IDDEEA CA provides training for its employees.
- For IDDEEA CA responsible persons, the training involves procedures for system and data protection, training specific for their roles and responsibilities, training for the usage of the IDDEEA CA application and training for taking over procedures for Disaster Recovery and Business Continuity Procedure.
- For the Registration Authority employees, the training involves procedures on system and data protection and training specific to their roles and responsibilities.

5.3.4. Retraining frequency and requirements

- IDDEEA CA employee trainings are organized according to the actual needs and technology changes.

5.3.5. Job rotation frequency and sequence

- Job rotation is not implemented.

5.3.6. Sanctions for unauthorized actions

- In a case there is a suspicion that an unauthorized activity was performed or an unauthorized activity was really performed by a person performing tasks related to the work of IDDEEA CA or the Registration Authority, IDDEEA CA will disable his/her further access to the technical assets (hardware and software), IDDEEA CA will suspend or revoke all the certificates issued to that person.
- The executed unauthorized activities are reported to the competent state authorities and institutions, in accordance with the prevailing laws, bylaws and internal regulations.

5.3.7. Independent contractor requirements

- IDDEEA CA normally doesn't employ contracted staff on any sensitive operation. Where such employees are engaged, appropriate checks are conducted. All contractors are required to sign a non-disclosure agreement in accordance with the internal regulations of IDDEEA CA.

5.3.8. Documentation supplied to the employees

- IDDEEA CA responsible persons have access to TSP documentation, including hardware, software, and TSP application manuals, operational procedures, safety and fire protection procedures, access control procedures and this Policy.

5.4. Audit logging procedures

5.4.1. Types of events recorded

- The following types of events are recorded automatically or manually by IDDEEA CA for audit purposes:
  - Events related to subscriber keys and certificates: registration, issuance, revocation, suspension
  - Events related to TSP keys
  - Events related to administration, data repository and public directory
  - Events of operational systems and hardware equipment
  - Events related to physical access to TSP
- Most of the electronic logs contain the date and time of each event and the identity of the entity that generated it. All entries to physical audit logs are identified by date and time.
- Logs are collected and consolidated in IDDEEA CA Operation Authority.

5.4.2. Log processing frequency

- The logs will be checked on a daily basis.
- The check includes:
  - Collecting all logs from the last log processing
  - Review audit log entries.
  - Review of the collected logs

Analysis and notification related to all relevant events in order to resolve or limit problem escalation.
Move, purge or destroy expired logs

5.4.3. Retention period for audit log

- At least 10 years, in accordance with the relevant laws.

5.4.4. Audit log protection

- Access to the host computer system containing audit log files is allowed only to authorized persons, with combination of physical controls and computer security controls. The computer system, audit log backup cartridges and physical audit logs are kept at IDDEEA CA Operation Authority high security zone, 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-marked. The operating system protects the integrity of its audit log files by using operating system functionality.

- Audit log entries generated by the TSP application are individually time-marked. TSP application protects the integrity of its audit log files by using public key encryption and verification of each entry on retrieval.

5.4.5. Audit log backup procedures

- Audit log files are backed-up daily as part of the regular IDDEEA CA host system backup.
- Backup are stored in a fire-resistant container in the IDDEEA CA Operation Authority.
- The backups, which contain a consolidated copy of the audit log files, are sent to a secure off-site storage facility for off-site storage and archiving purposes.

5.4.6. Audit collection system (internal vs. external)

- IDDEEA CA audit collection system is a combination of automated and manual processes performed by the TSP host operating system, the TSP application, and by IDDEEA CA employees, as stated in the table below:

Events Recorded	Collection System	Recording Entity
TSP application start up and shutdown	Automatic	TSP host operating system
TSP host operating system start up and shutdown	Automatic	TSP host operating system
Successful and failed attempts to create, modify, remove, disable, enable, and recover subscribers	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 log-in and log-off attempts to the TSP application	Automatic	TSP application
Successful and failed log-in and log-off attempts to the host computer	Automatic	TSP host operating system
Unauthorized attempts to access system files	Automatic	TSP host operating system
Unauthorized attempts to access 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 creation policies (e.g., validity period)	Automatic	TSP application
Successful and failed attempts by the TSP to connect, read, and write to the directory	Automatic	TSP application
Distinguished name changes	Automatic	TSP application
TSP database backup and restore	Automatic	TSP application and TSP host operating system
Audit log backup, restore, and purge	Automatic	TSP host operating system and TSP employees
Physical access to TSP sites	Manual	TSP employees
System configuration changes	Manual	TSP employees
Software and hardware update	Manual	TSP employees
Scheduled and unscheduled maintenance on the system and site	Manual	TSP employees
Discrepancies and compromises	Manual	TSP employees
Employee changes	Manual	TSP employees
Destruction of designated information	Manual	TSP employees

5.4.7. Notification to event-causing subject

- The subject that caused the audit event is not notified.

5.4.8. Vulnerability assessment

- IDDEEA CA conducts vulnerability assessments as part of the audit logs processing procedures.

5.5. Records archiving

5.5.1. Types of records archived

- The following records are retained by IDDEEA CA
- Audit information specified in section 5.4 Audit logging procedures
- Subscriber's agreements and all forms belonging to the request
- Certificates, certificate revocation status
- Discrepancy and compromise reports and correspondence

5.5.2. Retention period for archive

- At least 10 years, in accordance with the relevant laws.

5.5.3. Archive protection

- Access to IDDEEA CA archive information is granted to TSP employees according to the need -to-know basis.

5.5.4. Archive backup procedures

- The archived data are kept on dedicated archive media or as a paper copy. At least once a month these archives are relocated at a secure place at a distant location intended for their storage.
- Archive material is stored off-site in a secure facility where physical and security controls are comparable to those implemented for the TSP primary site

5.5.5. Requirements for time-stamping of records

- Archive records are time marked at the time of their creation, using the system time of the system on which the event is recorded.
- Archive records are time marked at the time of their creation, using the system time of the system on which the event is recorded. All systems are synchronized with time source traceable to UTC.

5.5.6. Archive collection system (internal or external)

- IDDEEA CA is using IDDEEA CA internal backup and archiving system.

5.5.7. Procedures to obtain and verify archive information

- Access to retained data is allowed to representative of IDDEEA CA on the need-to-know bases, or in accordance with applicable law.

5.6. Key changeover

- Key changeover of the TSP private key will be performed in due time before TSP certificate expires. On key changeover of the TSP private key, a new TSP public key will be made available to certificate holders via the TSP public repository.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

- IDDEEA CA implements ISO/IEC 27001 compliant procedure for responding to security incidents and malfunctions.

5.7.2. Computing resources, software and/or data are corrupted

- IDDEEA CA has implemented a contingency and disaster recovery plan, which addresses the recovery of its operations following the corruption of computing resources, software, and data.

5.7.3. Entity private key compromise procedures

- In the event when TSP private signature key is being compromised, the TSP will revoke and re-issue all IDDEEA CA certificates which are currently used.

5.7.4. Business continuity capacity after a disaster

- After a natural or other type of disaster the operation of the TSP operations and IT centre will be re-established on an independent disaster recovery site, using the backup data. IDDEEA CA will take all reasonable measures to re-establish the services in the shortest possible period, but not longer than five (**5**) working days.

5.8. TSP or RA termination

- In the event of the IDDEEA voluntary termination of operations, the TSP will:
- Notify the National Supervisory Body and all current subscribers at least ninety (90) days before of its intent to cease operations.
- In agreement with the National Supervisory Body transfer operations to another trust service provider or revoke all valid certificates on or after the expiration of the notice period.
- In the case that transfer to another service provider will not be possible, IDDEEA CA will submit to the Ministry of Transport and Communications BiH all the documentation, data and equipment in accordance with the Law on Electronic signatures
- Ensure that all documentations and archives will be transferred to another Trust Service Provider or to Ministry of Transport and Communications BiH or ensure to be retained for a minimum of ten (10) years from the last day of operation.
- Ensure availability and access to relevant CRLs and OSCP for a period of 6 months following revocation of all certificates.
- Before service termination, IDDEEA will destroy CA's private keys, including backup copies, or withdrawn from use, in a manner such that the private keys cannot be retrieved.
- Publish service termination information on IDDEEA public websites.

6. TSP TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

- IDDEEA CA's signature key pair is created on a Hardware Security Module (HSM) during the initial TSP key generation procedure and is protected by a master key. In the course of the generation of the CA's cryptographic keys pair, multiple authentications of authorized persons and protection which applies for the premises of IDDEEA CA is used.
- TSP Certificate holder's signature key pair is always generated by the PKI client application or on a QSCD (smart card / token).
- Private key used for qualified electronic signature or qualified electronic seal are generated in hardware token compliant with QSCD specification. Private key used for other certificate types are generated in the software crypto token on the user side or any hardware token (signature creation device).

6.1.2. Private Key delivery to subscriber

- Private keys generated on a QSCD are generated by the TSP and delivered to the user.
- Private keys for other certificates (not issued in a QSCD) are generated by the user with his PKI client application, so they do not need to be delivered to the certificate holder.

6.1.3. Public key delivery to certificate issuer

- TSP Public keys are delivered to the TSP application by using PKCS#10 format. PKCS#10 request must be signed by the private key corresponding to a public key contained in a PKCS#10 request.

6.1.4. TSP public key delivery to relying parties

- IDDEEA CA's public signature verification key is delivered by TSP to the subscribers in a X.509 certificate format, as part of the enrolment procedure.
- The public key of IDDEEA CA is available in form of a certificate on the following locations:
- In the public LDAP directory:
- On the website:
- TSP's certificate can be also obtained by contacting IDDEEA CA (see 1.5.2 Contact person).
- In all cases, the entity using IDDEEA CA certificates must verify the authenticity and integrity of the TSP certificate.

6.1.5. Key sizes

- TSP generates its asymmetric private signature keys with minimum 3072-bit RSA.
- The certificate holder shall generate its asymmetric private signature key with minimum 2048-bit RSA.

6.1.6. Public key parameters generation and quality checking

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

6.1.7. Key usage purposes (defined in X.509 v3 key usage field)

- IDDEEA CA uses the keyUsage field in the certificates for marking the purpose of the public keys in the certificates, as defined in RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile":

- Besides keyUsage, IDDEEA CA also uses Extended Key Usage (extKeyUsage) for additionally marking or limiting the usage of the public keys in the certificates as defined in RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”:
    - serverAuth: TLS WWW server authentication
    - clientAuth: TLS WWW client authentication
    - codesigning: Signing of downloadable executable code
    - email Protection: E-mail protection
    - timestamping: Binding the hash of an object to a time
    - EKU Ossining: Signing OCSP responses

- TSP For signing certificates and Certificate Revocation Lists only private CAs cryptographic keys is used.

- The cryptographic keys and certificates of the responsible persons for IDDEEA CA are used only for operating with technical assets owned by IDDEEA CA (hardware and software).

- The remaining certificates of IDDEEA CA can be used for the purpose shown in the Key Usage field, as shown in the table below.

- The key usage is indicated in the certificates issued by IDDEEA CA in the keyUsage and extKeyUsage field, depending on the type of the certificate and the type of the public key in the certificate, as shown in the table below.

Certificate type	**Usage in the keyUsage field**
CAs (Root CA, ORGANIZATION)	keyCertSign, cRLSign
Qualified DS for qualified e-signature	digitalSignature, nonrepudiation, keyEncipherment
Normalized DS – OCSP	digitalSignature extKeyUsage: OCSPSigning

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

- All TSP digital signature key generation and certificate signing operations are performed in a hardware cryptographic module meeting the standard FIPS 140-2 Level 3. All other TSP cryptographic operations are performed in a cryptographic module meeting the standard FIPS 140-2 Level 3.

- Private keys used for qualified electronic signature and qualified electronic seal are generated and used in a hardware cryptographic module certified according to QSCD specifications.

- The certificate holder’s private key relies upon the physical and logical controls which protect the certificate holder computer system. It is the certificate holder’ responsibility to ensure the private key is kept in an environment with sufficient levels of physical protection. However, it is recommended that certificate holder QSCD rated which at least meets the standard FIPS 140-2 level 2 or other standard verified to an equivalent level of assurance.

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 key escrow.

6.2.4. Private key backup

- The TSP maintains a copy of the CA's private signing key.
- TSP Subscriber's private keys are not backed up by the IDDEEA CA

6.2.5. Private key archiving

- Private keys are not archived.

6.2.6. Private key transfer into or from a cryptographic module

- IDDEEA CA s private signing key is generated within a hardware security module (HSM). Transfers of private TSP keys to or from the HSM are limited to backup and restoring purposes. Private TSP keys exported to/imported from another HSM are protected by encryption, so TSP's private signing key never appears in a clear form outside HSM.
- Keys which are stored on QSCD (smart cards / tokens) cannot be transferred.

6.2.7. Private key storage on cryptographic module

- IDDEEA CA's private signing key is used only on the hardware security module (HSM). CA's private signing key is stored on a cloned Hardware Security Module token for backup and recovery purposes.

6.2.8. Method of activating private key

- The private cryptographic key for signing of IDDEEA CA is activated after the start of the application of the certification body. A smart card / token for access to the hardware cryptographic module as well as the subscriber's password with CA Master User role are required for activation.
- The user's private cryptographic keys generated on a QSCD are activated after the successful authentication with a PIN.

6.2.9. Method of deactivating private key

- The cryptographic key for signing of IDDEEA CA is deactivated by stopping the TSP application.
- The client applications have to deactivate the private cryptographic key when the subscriber will log off the system, i.e., the application.

6.2.10. Method of destroying private key

- The private TSP keys are deleted when TSP certificate expires. This is accomplished by deleting the private key on the HSM and deleting backups on backup HSM.
- Service keys stored on smart cards are deleted by destroying the card.
- The client applications have to clear the private cryptographic keys from the operational memory before they reassign it. They also have to delete the entire space on the disk which is used for the private cryptographic keys before that space is assigned to the operational 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 archiving

- IDDEEA CA archives the CA's public keys and the subscribers' public keys as defined in section 5.5.4 Archive backup procedures.

6.3.2. Certificate operational periods and key pair usage periods

- The usage period of the public and private cryptographic keys in the certificates issued by IDDEEA CA is:

- TSP's Root public verification key and certificate: 20 years.
- TSP's Root private signing key: 20 years.
- TSP's Issuer public verification key and certificate: 10 years.
- TSP's Issuer private signing key: 10 years.
- Subscriber’s public verification key and certificate: up to 10 years.
- Subscriber’s private signing 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 can adapt the validity period to certain subscriber’s cryptographic keys based on specific user requirements and public procurement requirements in accordance with the 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 kept encrypted in the TSP’s database until delivery to the subscribers. Numbers and codes are unique and are generated in an unpredictable way.

- For the key generated on the QSCD the PIN is generated by the TSP and sent or handed over to the subscriber as part of the delivery process as defined in section 4.1.2 Enrolment process and responsibilities.

6.4.2. Activation data protection

- Activation codes are generated securely by the TSP application and are kept in the TSP's database in encrypted form.

6.4.3. Other aspects of activation data

- No stipulations.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

- IDDEEA CA has implemented a number of technical computer security controls, which are enforced by the TSP’s host operating system and the TSP application, including:

- Access control to TSP services
- Strict separation of duties and roles of TSP's operational persons
- Use of smart cards to store the profile of CA security officers and certificate administrators
- Encrypted sessions between the TSP application and subscribers’ PKI client applications
- Encryption of sensitive data in a TSP's database
- Archive of TSP's and subscriber's certificate history and audit data
- Audit of security related events
- Recovery mechanisms for keys and the TSP application

6.5.2. Computer security rating

- TSP Host operating systems are commercial off-the-shelf products.

6.6. Life cycle technical controls

6.6.1. Development controls

- All applications and products used by the IDDEEA CA are commercial off-the-shelf products.

6.6.2. Security management controls

- IDDEEA CA has implemented problem, change, and configuration management procedures for all PKI software and hardware components consistent with ISO/IEC 27001 requirements.

6.6.3. Life cycle security controls

- TSP tests all software and procedures in a controlled environment.

6.7. Network security controls

- The computer network of IDDEEA CA is composed of connected network segments, where the servers and the operation stations are placed. The segments are interconnected by firewalls. The computer network of IDDEEA CA is connected to Internet through several levels of firewalls. The security regulations of the firewalls allow the traffic only for the protocols which are necessary for an access to the services of IDDEEA CA.

6.8. Timestamping

- Date and time are added to all system and application-level log records. System time is synchronized to multiple external references traceable to UTC. For synchronization NTP protocol is used.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

7.1.1. Certificate version number

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

X.509 extension	Description
Signature	TSP signature to authenticate certificate
issuer	TSP name
Validity	Activation and expiry date of certificate validity
subject	Subscriber's distinguished name
subjectPublicKeyInformation	Algorithm ID, key
version	Version of X.509 certificate, version 3 (2)
serialNumber	Unique serial number of certificates

7.1.2. Certificate extensions

- The following basic X.509 fields are used in all certificates:

X.509 extension	Description
Signature	TSP signature to authenticate certificate
issuer	TSP name
Validity	Activation and expiry date of certificate validity
subject	Subscriber's distinguished name
subjectPublicKeyInformation	Algorithm ID, key
version	Version of X.509 certificate, version 3 (2)
serialNumber	Unique serial number of certificates

- TSP certificates contain the following mandatory critical extensions:

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

- Subsriber's and service certificates can contain following extensions:

X.509 extension		Description
authorityKeyIdentifier		Hash of the issuer key
subjectKeyIdentifier		Hash of the holder's key
keyUsage		As specified in section 6.1.7 Key usage purposes Extension is always mareked as critical.
extendedKeyUsage		As specified in section 6.1.7 Key usage purposes
privateKeyUsagePeriod		As specified in section 6.3.2 Certificate operational periods and key pair usage periods
certificatePolicies:		Certificate policy OID = OID as specified in section 1.2 Document name and identification
	CertPolicyID	
	CPS URI	
CRLDistributionPoints		CRL locations
subjectAlternativeName		Alternative holder's name
basicConstraints		CA=false

Authority Information Access	accessMethod=caIssuers; and accessMethod=OCSP
qcStatement	According to ETSI EN 319 412-5

7.1.2.1. Private certificate extensions

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

7.1.3. Algorithm object identifiers

Algorithm	Identification number
RSA	1.2.840.113549.1.1.1
SHA512 with RSA	1.2.840.113549.1.1.13

7.1.4. Name forms

- Certificates issued by IDDEEA CA contain the full distinguished name of the certificate authority and certificate subject in the issuer name and subject name fields. Distinguished names encoding is in UTF8 string or PrintableString format.

7.1.5. Name constraints

- Not used.

7.1.6. Certificate policy object identifier

- All certificates issued by the TSP contain OID of the Certificate Policy under which the certificate was issued. The OID for each certificate policy is defined in section 1.2 Document name and identification.

7.1.7. Usage of Policy Constraints extensions

- Not used.

7.1.8. Policy qualifiers syntax and semantics

- Policy qualifies are used in accordance with RFC5280.

7.1.9. Processing information for critical Certificate Policy extensions

- PKI client applications must process certificate extension marked as critical in accordance with RFC 5280.

7.2. CRL profile

7.2.1. Certificate version number(s):

- The TSP issues X.509 v2 format CRLs by using multiple distribution points within its LDAP directory and http web server.

- The following basic X.509 fields are used:

X.509 extension	Description
version	Set to v2
signature	Identifier of the algorithm used to sign the CRL

issuer	CA's distinguished name
thisUpdate	Time of CRL issue
nextUpdate	Time of the next CRL issue
revokedCertificate	Serial numbers of revoked certificates

7.2.2. CRL and CRL entry extensions

X.509 extension	Description
CRLNumber	Number of the certificate revocation list
authorityKeyIdentifier	Hash of the issuer key
reasonCode	TSP May contain values in accordance with RFC5280
invalidityDate	Populated by the TSP application as specified by operator.
expiredCertsOnCRL	CRL containing this extension includes revocation status information for certificates that have been already expired.

7.3. OCSP profile

- OCSP profile as defined in RFC 6960 is used.

7.3.1. Certificate version number

- OSCP v1 according RFC 6960 is used.

7.3.2. OCSP extensions

- The OCSP request extensions:

Extension	Description
nonce	The nonce value binds a request and a response to prevent replay attacks. Value shall be in accordance with RFC6280.

- The OCSP response extensions:

Extension	Description
nonce	The same value as in a request if contained in a request.
ArchiveCutoff	Amount of time for which the OCSP keeps revocation information beyond a certificate's expiration.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or circumstances of assessment

- The compliance audit of IDDEEA CA with the relevant laws is carried out in line with the Law on Electronic Signature and other valid legal provisions of the Bosnia and Herzegovina.
- IDDEEA CA carries out obligatory internal audits at least once a year.

8.2. Identity/qualifications of the assessor (internal audit)

- The internal auditor is employed in IDDEEA CA, with appropriate IT knowledge and auditing experience.
- The independent external auditor shall be employed by a competent independent professional company that complies with appropriate national and international standards and codes of practice.
- The internal or external auditor shall meet the following criteria:
  - Significant experience in the application of PKI and cryptographic technology
  - Experience in using and work with the TSP application
  - Experience in conducting certification activities or audits of information technology systems

8.3. Assessor's relationship to assessed entity (internal audit)

- The internal or external auditor shall be conflict-of-interests-free and independent from the TSP.

8.4. Assessment related questions

- The internal audit establishes whether:
  - The policy meets the technical, procedural and organizational TSP activities in sufficient details, in line with the requirements of the Law on Electronic Signature, and other valid legal provisions of the Bosnia and Herzegovina.
  - TSP system includes and is in line with the technical, procedural and organizational practices and policies.

8.5. Actions taken as a result of deficiency

- IDDEEA CA shall undertake appropriate actions to resolve any deficiencies or non-conformities identified as a result of an audit within an agreed timeframe dependent upon the severity of the risk involved.

8.6. Communication of results

- The audit information pertaining to IDDEEA CA 's compliance with the relevant laws are considered extremely sensitive and are not to be disclosed to anyone or for any reasons, except for auditing needs or in cases imposed by law.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate issuance or renewal fees

- IDDEEA CA charges for its PKI certification services. The pricelist is published on the TSP's public websites.

9.1.2. Certificate access fees

- See section 9.1.1 Certificate issuance or renewal fees.

9.1.3. Revocation or status information access fees

- 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 requestors may cancel a certificate request prior to issuance of activation codes at no cost. No fees will be refunded once the activation codes have been delivered, certificate has been issued, or software has been delivered or installed.

9.2. Financial responsibility

9.2.1. Insurance coverage

- IDDEEA CA has insurance coverage under the General Liability and Product Liability Insurance, including Pure Financial Loss coverage, which is customary to the core business. The coverage limits are in accordance with the legislation of the Bosnia and Herzegovina.

9.2.2. Other assets

- Not applicable.

9.2.3. Insurance or warranty coverage for end-users

- Subscribers and relaying parties are solely responsible to ensure adequate insurance or warranty coverage respective to their certificate usage or service.

9.3. Personal data protection

- Any personal data provided to IDDEEA CA or its authorized agents will be held in accordance with the requirements laid down in the Law on Personal Data Protection of the Bosnia and Herzegovina. Release of said information should only be in accordance with the Law on Personal Data Protection, IDDEEA CA - Personal Data Protection Policy or as required by any other applicable legislation.

9.3.1. Scope of confidential information

- All information collected, generated, transmitted or kept by IDDEEA CA is considered confidential, except the information set out in section 9.3.2, which is considered as non-confidential.

9.3.2. Information not within the scope of confidential information

- Information, which is published as part of an IDDEEA CA certificate, CRL, Certificate Policy or other information published in the CA's public repository, shall not be considered confidential.

9.3.3. Responsibility to protect confidential information

- IDDEEA CA is responsible to protect confidential data in accordance with IDDEEA CA Personal Data Protection Policy and Law on Personal Data Protection of Bosnia and Herzegovina and other relevant legislation.

9.4. Privacy of personal information

9.4.1. Privacy plan

- As stipulated in sections 9.3 and 9.4.

9.4.2. Information treated as private

- Any information about certificate holder or subscriber, not already published in a certificate issued by IDDEEA CA, CRL or public LDAP directory is considered private.

9.4.3. Information not deemed private

- Any information contained in a certificate issued by IDDEEA CA, CRL, Certificate Policy or other information published in the CA's public repository is not considered private.

9.4.4. Responsibility to protect confidential information

- As stipulated in section 9.3.3.

9.4.5. Notice and consent for private information use

- IDDEEA CA will use private information solely for the purposes the subscriber has given consent in the registration process.

9.4.6. Disclosure pursuant to judicial or administrative process

- IDDEEA CA will disclose confidential information only to representatives of institutions responsible for implementation of the laws in accordance with the applicable legislation.

9.4.7. Other information disclosure circumstances

- IDDEEA CA will disclose private information only in circumstances laid down in IDDEEA CA Personal Data Protection Policy, Law on Personal Data Protection of Bosnia and Herzegovina and other relevant legislation, on a courts or other legitimate authority request, provided that the request is issued on legal basis.

9.5. Intellectual property rights

- Not applicable.

9.6. Representations and warranties

9.6.1. TSP representations and warranties

- IDDEEA CA should issue certificates, perform other certificate management procedures and manage CA's infrastructure in accordance with this Certificate Policy and applicable laws. TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP functionality is undertaken by RA or sub-contractors.

- In summary, non-exclusive list of IDDEEA CA obligations is:
  - publicly publish Certificate Policy;
  - provide a procedure(s) for the user of the Certificate for the submission of request for obtaining certificate;

- issue keys and certificates in accordance with the activities explained in this Policy, perform secure management of the private key of IDDEEA CA CAs and distribution of the public key of IDDEEA CA CAs;
- approving or denying the requests of the subscribers of the certificates;
- signing and issuing X.509 certificates with the holder's public keys as an answer to approved certificate requests;
- publishing X.509 certificates in directories;
- revocation of certificates, including publishing of the Certificate Revocation List;
- determining the identity of the application users who file for a certificate, for renewing a certificate or requests for a new certificate in the event of revocation of the certificate;
- ensure that the persons in charge of registration are suitably trained and act in accordance with the rules applying thereto in this policy;
- ensure that the end users are aware and agree to accept the terms and conditions for obtaining the keys and certificates;
- confirm the operation in accordance with the activities described in this Policy by means of periodic audits of the operation (at least every 24 months);
- hire persons who, in addition to meeting the general employment conditions, meet the special conditions stipulated in the Law on Electronic Documents, Electronic Identification and Trusted Services;
- ensure that the information about the subscriber and the TSP contained in the certificates is accurate;
- prove applicants' identity before issuing a certificate;
- ensure accuracy and integrity of information published in the LDAP directory or other repository;
- provide access to on-line public directory;
- issue certificates to approved requestors in accordance with this Certificate Policy;
- provide access to on-line public directory;
- revoke certificates issued by the CA, upon receipt of a valid request to do so, or in accordance with this Certificate Policy;
- issue and publish Certificate Revocation Lists (CRLs);
- maintain OCSP service;
- ensure that its RAs are aware of the stipulations concerning them in this Certificate Policy.

9.6.2. RA representations and warranties

- RA is responsible for accuracy and completeness of subscribers' information on the approved application forms. The detailed obligations of the RA are set out in relevant sections of this Certificate Policy.

9.6.3. Subscriber representations and warranties

- The subscriber takes full responsibility for the use of the private key related with the public key in the certificate whereby the holder is an individual identified by the private key.
- When the certificates are issued to an individual for their personal use, the subscriber and the holder shall form one and the same entity.
- Before keys and certificates are issued, the subscribers conclude a contract with IDDEEA CA, taking into consideration the rules and terms of use.
- The subscribers are responsible for:
  - being fully aware of their duties and responsibilities as stipulated in the relevant documentation as stated above and the rules under which the certificates have been issued;
  - initiation within five working days from the moment of receiving the Initiation code sent by IDDEEA CA - use of private keys for the intended purpose;

- controlling the access to a computer, device or special hardware device which contains private key for which they are responsible;
- protection of passwords used for access to private keys;
- urgently notifying IDDEEA CA of any doubt about compromising their private key.

- By accepting a certificate issued by IDDEEA CA the subscriber should:
  - keep their private signature key secret;
  - keep their password secret;
  - immediately notify the CA, of any inaccuracies or changes to the information contained in the certificate;
  - exclusively use their certificate for lawful purposes and the authorized purpose described in detail in section 1.4 Certificate usage;
  - immediately notify the CA, of a suspected or detection of private key compromise;
  - 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

- For checking the validity of the certificate, they obtain, the relying parties must always refer initially to IDDEEA CA list of revoked certificates.

- The relying party, which is entrusted with the certificate issued by IDDEEA CA is obliged to:
  - limit the validity of the certificate only for the purpose defined in this document
  - check the validity of the certificate
  - read this document and learn the duties, responsibilities and limitations of the TSP
  - request revocation of the certificate if:
    - acquires knowledge that the private key has been compromised in a manner which influences the proper use, or
    - there is a danger of misuse, or
    - there are changes in the data stated in the certificate.

- Before acquiring IDDEEA CA certificate, it is the responsibility of the relying party to:
  - be aware of the limitations of the certificate and the TSP's liability as detailed in this Policy;
  - restrict reliance on certificates issued by the TSP to appropriate uses as detailed in section 1.4 Certificate usage;
  - ensure that the certificate has not been revoked by accessing valid, any and all, applicable Certificate Revocation Lists (CRLs) or OCSP;
  - immediately notify IDDEEA CA of any suspected or known misuse of any certificate issued by the TSP.

9.6.5. Representations and warranties of other participants

- Any other participants are obliged to use certificates and act in accordance to this Policy and the applicable laws.

9.7. Disclaimers of warranties

- Except for the warranties stated in this Certificate Policy and related agreements, and to the fullest extent permissible by law, IDDEEA CA excludes any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use. In particular the TSP excludes:

- any liability for possible damage which may occur from the moment the TSP receives valid revocation request, to the moment of publishing revocation information on the CRL in accordance with section 4.9.6;
- any warranty as to accuracy or reliability of any information contained in the certificates which is not supplied by IDDEEA CA;
- liability for representations of information contained in the certificate;
- any warranty as to the authority or status of any person using IDDEEA CA certificate;
- any liability as to matters outside its own control including the availability or working of the Internet, or telecommunication or other infrastructure or the RA's systems, including hardware and software;
- any liability for damages as a result of force majeure events as described in detail in section 9.16.5 Force Majeure.

9.8. Limitations of responsibility

IDDEEA CA disclaims any liability of any kind whatsoever for any award, damages, or other claim or obligation of any kind arising from tort, contract, or any other reason with respect to any service associated with the issuance, use of, or reliance upon, a certificate issued by IDDEEA CA of use by a subscriber or relying parties.

9.9. Indemnification

- Each party bears sole responsibility for indemnifying IDDEEA CA or other parties for losses or damage which are result of fraudulent usage of certificates or not acting in accordance with this Certificate Policy and the applicable laws.

9.10. Term and termination

9.10.1. Term

- IDDEEA CA Certificate Policy and other documents became effective as they are approved by ORGANIZATION, and published on the IDDEEA CA website defined in section 2.1 Repositories.

9.10.2. Termination

- IDDEEA CA Certificate Policy validity is not time limited. Current version is effective until the publishing of a new version.

9.10.3. Effect of termination and survival

- After the Certificate Policy expiry, which is a result of publishing a new version, the certificate shall be used in accordance with the Certificate Policy version effective on the date the certificate was issued. In the case the circumstances change to the extent that is not possible, IDDEEA CA will notify the subscribers as defined in section 9.12.2 Notification mechanism and period and the relying parties via the public website 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 defined in section 2.1 Repositories.
- See also section 9.12.2 Notification mechanism and period.

9.12. Modifications

9.12.1. Procedure for amendments

- IDDEEA CA's employees and other subjects may send their comments directly to the Policy Management Authority in written form or via e-mail, on the addresses indicated in section 1.5.2 Contact person.

9.12.2. Notification mechanism and period

- IDDEEA CA may decide not to notify subscribers and relying parties in the case of changes with a little or no impact. IDDEEA CA decides if changes have any impact on the subscribers or relying parties, at its sole discretion.
- All Certificate Policy changes will be published as described in section 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES. IDDEEA CA will notify subscribers about the changes that have impact on the subscribers or relying parties, via e-mail.

9.12.3. Circumstances under which OID must be changed

- Certificate Policy OID will be changed in the case when the changes affect the subscribers or relying parties.

9.13. Dispute resolution provisions

- All disputes related to corporate certificates shall be referred in writing to IDDEEA CA at the address defined in section 1.5.2 Contact person. The dispute should be resolved by means of agreement if possible. The dispute not settled by negotiations should be settled by the competent court.

9.14. Governing law

- This Certificate Policy and the relationships between the TSP, the RA, the subscribers, subjects (certificate holders) and any relying parties are subject to and will be interpreted in accordance with the laws of Bosnia and Herzegovina.

9.15. Compliance with applicable law

- Law on Personal Data Protection
- Law on Electronic Documents, Electronic Identification and Trusted Services and the by-laws adopted on the basis of the said Law
- other relevant legislation.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

- This IDDEEA CA Certificate Policy and IDDEEA CA end-user agreement state all relevant provisions of the relation between IDDEEA CA and the certificate holders of IDDEEA CA public certificates.

9.16.2. Assignment

- The subscribers or certificate holders are not allowed to assign the rights and obligations arising from this agreement, in whole or in part to a third party on any basis.

9.16.3. Events of inapplicability of provisions (severability)

- Invalidity of one or more parts of this document, shall not affect the validity of other provisions, providing that material provisions are not affected (certificate trust and certificate usage).

9.16.4. Enforcement (attorneys' fees and waiver of rights)

- None.

9.16.5. Force Majeure

- Force Majeure denotes emergency and unpredictable situations like natural disasters, terrorism, power or telecommunications outage, fire, unpredictable incidents like viruses or service blockage due to hacker attacks, governmental measures, impairment of cryptographic algorithms strength.
- IDDEEA CA or other parties shall not be made responsible and/or liable for any damages caused by Force Majeure events.

9.17. Other provisions

None.