Approved with Decision No. 2379 of 19.12.2005 of the Communications Regulation Commission
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>3</td>
</tr>
<tr>
<td>DOCUMENT HISTORY</td>
<td>7</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>8</td>
</tr>
<tr>
<td>I. User Manual</td>
<td>9</td>
</tr>
<tr>
<td>II. CERTIFICATION PRACTICE STATEMENT</td>
<td>12</td>
</tr>
<tr>
<td>1. INTRODUCTION</td>
<td>12</td>
</tr>
<tr>
<td>1.1. GENERAL TERMS AND CONDITION</td>
<td>13</td>
</tr>
<tr>
<td>1.2. Document Name and Identification</td>
<td>15</td>
</tr>
<tr>
<td>1.3. PKI Participants</td>
<td>15</td>
</tr>
<tr>
<td>1.4. Certificate usage</td>
<td>20</td>
</tr>
<tr>
<td>1.5. Policy Administration</td>
<td>28</td>
</tr>
<tr>
<td>1.6. Acronyms</td>
<td>29</td>
</tr>
<tr>
<td>2. Publication and Repository Responsibilities</td>
<td>32</td>
</tr>
<tr>
<td>2.1. Repositories</td>
<td>32</td>
</tr>
<tr>
<td>2.2. Publishing information for the certificates</td>
<td>33</td>
</tr>
<tr>
<td>2.3. Frequency of publications</td>
<td>33</td>
</tr>
<tr>
<td>2.4. Access to the directory of certificates</td>
<td>34</td>
</tr>
<tr>
<td>3. IDENTIFICATION AND AUTHENTICATION</td>
<td>36</td>
</tr>
<tr>
<td>3.1. Naming</td>
<td>36</td>
</tr>
<tr>
<td>3.2. Initial identification and identity validation</td>
<td>39</td>
</tr>
<tr>
<td>3.3. Identity validation and authentication in requests for replacement of keys in a certificate</td>
<td>43</td>
</tr>
<tr>
<td>3.4. Identity validation and authentication for terminating a certificate</td>
<td>43</td>
</tr>
<tr>
<td>3.5. Identity validation and authentication for requests for suspending a certificate</td>
<td>44</td>
</tr>
<tr>
<td>4. EFFECTIVE CONDITIONS</td>
<td>46</td>
</tr>
<tr>
<td>4.1. Application for the issuance of a certificate</td>
<td>46</td>
</tr>
<tr>
<td>4.2. Procedure for submitting a request for a certificate</td>
<td>48</td>
</tr>
<tr>
<td>4.3. Issuing a Certificate</td>
<td>50</td>
</tr>
</tbody>
</table>
4.4. Accepting and publishing/publishing the certificate..............................52
4.5. Pairs of keys and use of the certificate ........................................52
4.6. Certificate Renewal........................................................................53
4.7. Changing a key in a certificate..........................................................56
4.8. Modifying a certificate .....................................................................56
4.9. Terminating a certificate ...................................................................57
4.10. Termination of the agreement for providing certification services ....64
4.11. Key recovery and Key escrow ..........................................................64
5. EQUIPMENT, PROCEDURES AND MANAGEMENT CONTROL.....66
5.1. Physical control................................................................................66
5.2. Procedure control ............................................................................68
5.3. Staff control, qualification and training ............................................70
5.4. Procedures for preparing and keeping an inspection data journal ....71
5.5. Repository.........................................................................................73
5.6. Modification of a certificate key........................................................75
5.7. Compromise and disaster recovery ....................................................75
5.8. Procedures for terminating the activity of the Provider ......................76
6. TECHNICAL SECURITY CONTROL...............................................78
6.1. Key pair generation and installation..................................................78
6.1.1. Key pair generation.......................................................................79
6.2. Private key protection and technical control of the cryptographic module ......................................................................................82
6.3. Other aspects of key pair control ......................................................83
6.4. Activation data..................................................................................84
6.5. Comuter security control.................................................................84
6.6. Technical control of the life-cycle.....................................................85
6.7. Network security control ..................................................................85
6.8. Time-stamping..................................................................................85
7. CERTIFICATE PROFILE, LIST OF SUSPENDED AND REVOKED CERTIFICATES AND ON-LINE STATUS CHECK PROTOCOL .......................... 88
7.1. Certificate profile ........................................................................................................ 88
7.2. Profile of the List of Suspended and Revoked Certificates ................................. 91
7.3. OCSP Profile ............................................................................................................. 93
8. AUDITING AND CONTROL OF THE ACTIVITY ................................................. 96
8.1. Scheduled or unscheduled audits ........................................................................... 96
8.2. Qualifications of the auditors .................................................................................. 96
8.3. Relationships between the auditor and the audited organization ...................... 96
8.4. Scope of the audit ..................................................................................................... 97
8.5. Measures for correcting established defects ......................................................... 97
8.6. Announcing the results .......................................................................................... 97
9. OTHER BUSINESS AND LEGAL PROVISIONS .............................................. 97
9.1. Fees and prices ......................................................................................................... 97
9.2. Financial responsibilities ......................................................................................... 99
9.3. Privacy of information ............................................................................................. 101
9.4. Privacy of personal data .......................................................................................... 102
9.5. Intellectual property rights ....................................................................................... 103
9.6. Responsibility and Warranties ............................................................................... 104
9.7. Waiver of responsibility ......................................................................................... 106
9.8. Limitations to the liability of the Provider .............................................................. 107
9.9. Indemnity of the Provider ....................................................................................... 108
9.10. Term and termination ............................................................................................ 108
9.11. Individual notification and correspondence between the participants ............. 109
9.13. Resolution of disputes and jurisdiction ................................................................. 110
9.15. Compliance with the governing law ...................................................................... 110
III. POLICY FOR PROVIDING UNIVERSAL ELECTRONIC SIGNATURE CERTIFICATION SERVICE
### Document History

#### Document Approval:

<table>
<thead>
<tr>
<th>Name and title</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Made up by:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verified by:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Document Distribution:

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Document Change Control:

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Name and title</th>
<th>Status and description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Document Information:

<table>
<thead>
<tr>
<th>File Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
ACKNOWLEDGMENTS

The current document "User Manual for Universal Electronic Signature Certification Services" of the Certification Services Provider INFONOTARY EAD was made up in compliance to the Law on Electronic Document and Electronic Signature (LEDES) and the Ordinance on the Activities of Certification Service Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services, the Ordinance on the Requirements to the Algorithms of Advanced Electronic Signature, the Ordinance on Certification Services Provider Registration and contains references to the whole or parts of the following generally accepted international standards and specifications:

- CWA 14167-1: security requirements for trustworthy system managing certificates for electronic signatures – Part 1: System Security Requirements;
- CWA 14167-2: security requirements for trustworthy system managing certificates for electronic signatures – Part 2: Cryptographic module for CSP signing certificates for signing operations – Protection Profile;
- RFC 2459: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile;
- RFC 3039: Internet X.509 Public Key Infrastructure – Qualified Certificates Profile;
- RFC 3279: Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile;
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates;
- ETSI TS 101 862: Qualified certificate profile;
I. User Manual

(1) This Document contains the terms and conditions under which INFONOTARY EAD renders to customers, against remuneration, universal electronic signature certification services through the Certification authority InfoNotary, in line with the requirements of Electronic Document and Electronic Signature Act.

(2) The main purpose of the Document is by detailed description of the rules and policies, which INFONOTARY EAD has introduced and follows in implementing its activity of certification services rendering to make them public for the users and to offer tools to all interested parties for establishing the compliance of the Provider's activity to the stipulations and requirements of the Electronic Document and Electronic Signature Act and the sub-laws concerning its implementation, and the reliability and security of the realized certification activity.

(3) The User Manual represents in its character general terms and conditions on the grounds of Art. 33, para 2 of the OACSP and in line with Art. 16 of the Act on Obligations and Contracts.

(4) Terms of the User Manual incorporated through referrals in the Certification Services Contract between INFONOTARY EAD and its customers, concluded in writing and in line with Art. 23 of the LEDES. The written contract may include specific terms, which supersede the general terms from the User Manual.

(5) The User Manual may be amended, and each amendment thereof shall be recorded upon approval by the Communications Regulation Commission and shall be publicly accessible by all interested parties at: http://www.infonotary.com.

(6) Any questions and information, concerning this document may be communicated to the Provider at the following address:
(7) The User Manual is comprised of the following documents:

1. Universal electronic signature certification services rendering practice of INFONOTARY EAD.

2. Universal electronic signature certification services rendering policy of INFONOTARY EAD.

1. CERTIFICATION PRACTICE STATEMENT (CPS)

(1) The document “Certification Practice Statement” of the InfoNotary Certification Authority, hereinafter referred to as InfoNotary CPS”, contains a detailed description of the terms and rules for security measures implementation during service rendering, issuance, discontinuation, restoration and termination of the validity of the certificates, as well as the terms and procedures for providing access to all certificates issued by the Certification Services Provider.

(2) InfoNotary CPS presents the technical and procedural practices for all provided services and followed certification policies.

(3) Certification Practice Statement is a public document, integral part of the User Manual and is subject to approval by the Communications Regulation Commission.
2. CERTIFICATION POLICY (CP)

(1) “Certification Policy” is a document, which is integral part of the User Manual, and describes the policy and procedures, followed by the Provider in certificate issuance, as well as the applicability of the issued certificates with view to the security of such procedures.

(2) For all types of issued certificates, the Provider develops and follows different certification policy.

(3) The certification policy for a particular type of certificate includes the rules for performing initial identification and authentication of electronic signature certificate Holders and Authors, as well as the issued certificate management policy – discontinuation, restoration and termination the action of a certificate issued by the Provider.

(4) The certification policy for each type of certificate defines as well the limitations in certificate applicability depending on the security level of check-ups and the degree of confidence in the facts certified in the issued document.
II. CERTIFICATION PRACTICE STATEMENT

1. INTRODUCTION

(1) The document “Certification Practice Statement”, hereinafter referred to as "InfoNotary CPS", contains detailed description of the terms and rules for security measures implementation during service rendering, issuance, discontinuation, restoration and termination of the validity of the certificates, as well as the terms and procedures for providing access to all certificates issued by the Certification Services Provider.

(2) InfoNotary CPS describes the technical and procedural practices for all provided services, related to the Provider's universal electronic signature certificates and the respective followed certification policies.

(3) InfoNotary CPS is developed in line with and covers the formal requirements to the content, structure and form of the generally accepted international specification of Internet Engineering Task Force (IETF) RFC 3647: “Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework” of November 2003, which replaces International Specification RFC 2527.

(4) The covering of RFC 3647 International Specification requirements provides a better guarantee of reliability to the users and enables the Provider to realize consistency and inter-operability with other Bulgarian and international certification service Providers.

(5) Within the document structure, the sections, which are not covered by the INFONOTARY management policy, are not filled-in and are marked as "Non-applicable", and where it is necessary to add more detailed information than the one, contained in the specification, additional sub-sections are added.

(6) The Certification Practice Statement is a public document, integral part of the User Manual and is approved by the Communication regulation commission.
1.1. GENERAL TERMS AND CONDITIONS

1.1.1. Certification Services Provider

(1) INFONOTARY EAD is a directoried Certification Service Provider under the Law on Electronic Document and Electronic Signature and the sub-laws regulating its implementation.

(2) As a directoried provider INFONOTARY EAD performs the following activities and provides the following universal electronic signature certification services, associated with:

1. Certificate issuance services:
   ▶ acceptance and review of applications for issuance of certificates;
   ▶ certificate generation, based on the established identity and valid data of the Holder and the Author;
   ▶ signing of certificates;
   ▶ issuance of universal electronic signature certificates;

2. Certificate management services:
   ▶ registration of the changes of the validity status of an issued certificate;
   ▶ services of discontinuation, renewal and termination of a certificate;
   ▶ directory-related services;
   ▶ maintenance of a directory of issued certificates;
   ▶ publishing of each issued certificate in the directory;
   ▶ publishing a list of the discontinued and terminated certificates in the directory.
3. Certificate access services:

► provision of third party access to the issued certificates directory;
► provision of third party access to the list of terminated certificates;
► provision of services for limiting access to the published certificates;
► provision of services for on-line certificate status protocol (OCSP).

4. Time Stamping services:

► Time stamping of signed electronic document date and time;
► provision of services of checking the electronic document date and time of a certification issued by the Provider;

5. Cryptographic key generation services:

► generation of a public and private key pair from asymmetric cryptosystem making use of Secure Signature Creation Device (SSCD) – smartcard.

1.1.2. Registration and voluntary accreditation

(1) The Certification Services Provider INFONOTARY EAD is directoried by the Communication regulation commission under the order of the LEDES and the OCSPR.

(2) For the purpose of attaining higher level of certification services rendered by the Provider and recognition of the legal force of the certificates issued thereby beyond the Bulgarian borders, INFONOTARY EAD may participate in organizations for voluntary accreditation.
(3) The Provider notifies the Electronic Signature Certificate Holders and Relying parties for its participation in organizations for voluntary accreditation.

1.2. Document Name and Identification

(1) The certification services provision practice of INFONOTARY EAD is named “InfoNotary qCPS” and is identified by the following object identifier in the issued certificates:

OID:1.3.6.1.4.1.22144.1

(2) The certification policies applicable to the different certificate types issued by the Provider to end-users are designated with the following object identifiers in the certificates:

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Name</th>
<th>Identifier (OID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Certification policy for natural person universal electronic signature certificate</td>
<td>i-Notary Personal Q Sign Certificate CP</td>
</tr>
<tr>
<td>2.</td>
<td>Certification policy for legal entity universal electronic signature certificate</td>
<td>i-Notary Company Q Sign Certificate CP</td>
</tr>
</tbody>
</table>

1.3. PKI Participants

1.3.1. Certification authority

(1) InfoNotary is the certification authority of the Certification services provider, performing the following activities: electronic signature certificate issuance, certificate management including certificate suspension, renewal and revocation, keeping of a directory of the issued certificates and ensuring access and the resources for limiting the access to the certificates.
(2) The certification authority (root CA) controls the Provider's certification policies, determining the information, contained in the different end-user certificate types identifying the Holder and the Author; the application constrains and responsibilities.

(3) The certification authority issues different types of certificates, in line with the certification policies, through its differentiated **Primary Certification Authorities** (primary CAs) and **Subordinate Certification Authorities** (subordinate CAs).

(4) The Provider's certification authority employs one- or two-level certification architecture for differentiation of the electronic signature certificate issuance and management activities, depending on the certification policy for the different certificate types, as shown in the table below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoNotary CSP Root CA</td>
<td>Root CA</td>
<td>1.3.6.1.4.1.22144.1</td>
</tr>
<tr>
<td>i-Notary Q Sign CA</td>
<td>primary CA</td>
<td>1.3.6.1.4.1.22144.1.1</td>
</tr>
<tr>
<td>i-Notary Personal Q Sign CA</td>
<td>subordinate CA</td>
<td>1.3.6.1.4.1.22144.1.1.1</td>
</tr>
<tr>
<td>i-Notary Company Q Sign CA</td>
<td>subordinate CA</td>
<td>1.3.6.1.4.1.22144.1.1.2</td>
</tr>
</tbody>
</table>

(5) In performing its activity the Provider's certification authority uses the following certification infrastructure model:

[Diagram of certification infrastructure model]
1.3.2. Registration authority

(1) The Provider renders its services to end users via a network of specified Registration Authorities.

(2) The Provider's Registration Authorities perform activities of:

► acceptance, checking, approval or rejection of applications for certificate issuance;

► registration of the applications submitted to the certification authority for certificate management certification services of:
  - suspension, renewal, revocation and update;

► performing of check-ups of the application with permissible resources, the identity data of the applicants (the Holder and the Author) and other data, depending on the certificate type and in line with the Provider's certification policies;

► certificate issuance initiation after positive results of the check-up and application approval, and notification of the certification authority;

► generation of a pair of keys for an asymmetric cryptosystem on a cryptographic carrier (smartcard) by request of the Holder or the Author;

► making a copy of the certificate and submission of the cryptographic carrier to the Author.

(3) The Provider may delegate rights and authorize third parties as well to perform activities of Registration Authority on the name and at the account of INFONOTARY EAD.

(4) The Provider assigns the performance of the activities of Registration Authority on the basis of a bilateral written contract.

(5) The Authorized Registration Authorities shall perform their activities in line with the User Manual, the Provider's certification policies and documented registration procedures.
(6) The Authorized Registration Authorities of the Provider shall be identified as such before all interested parties with Registration Authority Certificate by INFONOTARY EAD.

(7) Part of the Registration Authorities' functions may be performed by Local Registration Offices, acting under the supervision of the Registration Authorities.

1.3.3. Subscribers

(1) “A subscriber” is a natural person or legal entity that has concluded written contract with the Provider for provision of certification services.

(2) A subscriber, by whose application the Provider has issued an electronic signature certificate is an Electronic Signature Holder and is entered into the certificate as such.

1.3.4. Relying parties

(1) “Relying parties” are natural persons or legal entities to whom signed electronic statements are addressed, the authors of which have been issued electronic signature certificates by the Provider.

(2) The Relying parties should have skills to use the certificates electronic signature and to only place confidence in certificates issued by the Provider after checking the certificate status in the List of Suspended and Revoked certificates or the automated information submitted by the Provider by means of OCSP.

(3) The Relying parties are obliged to perform check-ups of the validity, suspension or revocation of a certificate from actual information about their status and to take into account and to accord their actions with all constrains for certificate usage, included in the certificate itself, or in the User Manual and the certification policies.
1.3.5. Holders

(1) “Holder” is a natural person or legal entity, owning electronic signature certificate issued by the Provider and is entered therein as such.

(2) The Holder keeps the electronic signature private key, corresponding to the public key, entered into the issued certificate.

(3) The Holder is also the owner of the cryptographic module - smartcard or token (Secure Signature Creation Deivse), issued for generation and storage of cryptographic keys, universal electronic signature certificate and electronic signature generation.

1.3.6. Authors

(1) “An Author” is a natural person, who makes electronic statements and generates electronic signatures on his/her behalf, or on behalf of the Holder, when duly authorized for that purpose and entered in the issued certificate as such.

(2) A Natural Person Holder is a person, who himself/herself makes electronic statements and generates electronic signatures on his/her behalf and is entered in the electronic signature certificate as the Author as well.

(3) When the Author is different from the Holder, the grounds for his/her empowerment is entered in the electronic signature certificate and he/she holds the private key for electronic signature, corresponding to the public key, entered in the certificate.

(4) When the empowerment of the Author is done by other empowered persons, the certificate contains information for these persons as well.

1.3.7. Representatives

(1) “A Representative” is a natural person duly empowered by the Holder, who performs on his/her behalf actions of electronic signature certificate issuance and management before the Provider.

(2) The Representative is a person, different from the Author; it is not entered in the certificate, it does not hold the private key and may not make electronic statements signed with the electronic signature of the Holder and on behalf of the Holder.
1.4. Certificate usage

1.4.1. Certificate types and usage

1.4.1.1. Certificates of the certification authority

1.4.1.1.1. Root certificate (Root)

(1) The root certificate for the public key of the Provider's certification authority, named InfoNotary CSP Root CA, is a self-issued and self-signed universal electronic signature certificate in line with Art. 33, para 1, cl. 2 of the LEDES.

(2) The certificate is signed with the root private key of the Provider.

(3) The root private key of the Provider, certified through a certificate for its public key InfoNotary CPS Root, is used to sign certificates of the Provider's international certification authorities and other data, related with the management of the certificates, issued by the Provider, including the list of suspended and revoked certificates, issued thereby (root-ca.crl).

(4) The Provider uses other root private keys as well and issues other self-signed certificates for their public keys for its activities and for the services provided to end-users beyond the scope of the certification services regulated in the LEDES.

(5) The root certificate InfoNotary CPS Root contains the following basic information:

Root x509 attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3 (0x02)</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique for the Provider's directory; 8-byte number</td>
</tr>
</tbody>
</table>
### Issuer attributes (x509 Issuer DN):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>2.5.4.3</td>
<td>InfoNotary CSP</td>
</tr>
<tr>
<td>/countryName</td>
<td>2.5.4.6</td>
<td>BG</td>
</tr>
<tr>
<td>/postalCode</td>
<td>2.5.4.17</td>
<td>1000</td>
</tr>
<tr>
<td>/localityName</td>
<td>2.5.4.7</td>
<td>Sofia</td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>2.5.4.9</td>
<td>16 Ivan Vasov Street, 6th fl.</td>
</tr>
<tr>
<td>/organizationName</td>
<td>2.5.4.10</td>
<td>InfoNotary PLC</td>
</tr>
<tr>
<td>/organizationalUnitName</td>
<td>2.5.4.11</td>
<td>InfoNotary CSP Root</td>
</tr>
<tr>
<td>/emailAddress</td>
<td>1.2.840.113549.1.9.1</td>
<td><a href="mailto:csp@infonotary.com">csp@infonotary.com</a></td>
</tr>
</tbody>
</table>

**Additionally defined organization attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/telephoneNumber</td>
<td>2.5.4.20</td>
<td>35929875717</td>
</tr>
<tr>
<td>/bgBulstatNumber</td>
<td>2.5.4.10.100.1.2</td>
<td>131276827</td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>2.5.4.10.100.1.1</td>
<td>1220187884</td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>2.5.4.10.100.1.3</td>
<td>SGS 7719/2004</td>
</tr>
</tbody>
</table>

### Holder attributes (x509 Subject DN):

*(They coincide with the issuer attributes)*

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>Value</th>
</tr>
</thead>
</table>
Additionally defined organization attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/telephoneNumber</td>
<td>2.5.4.20</td>
<td>35929875717</td>
</tr>
<tr>
<td>/bgBulstatNumber</td>
<td>2.5.4.10.100.1.2</td>
<td>131276827</td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>2.5.4.10.100.1.1</td>
<td>1220187884</td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>2.5.4.10.100.1.3</td>
<td>SGS 7719/2004</td>
</tr>
</tbody>
</table>

Additional attributes x509 extensions (x509v3 extensions):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/basicConstraints</td>
<td>2.5.29.19</td>
<td>CA=true</td>
</tr>
<tr>
<td>/keyUsage</td>
<td>2.5.29.15</td>
<td>KeyCertSign, CRLSign</td>
</tr>
<tr>
<td>/authorityKeyIdentifier</td>
<td>2.5.29.35</td>
<td>Coincides with “subjectKeyIdentifier”</td>
</tr>
<tr>
<td>/subjectKeyIdentifier</td>
<td>2.5.29.14</td>
<td>SHA1 of DER-coded public key</td>
</tr>
<tr>
<td>/cRLDistributionPoints</td>
<td>2.5.29.25</td>
<td></td>
</tr>
</tbody>
</table>

Additional certificate policies attributes (x509v3 extension):
| **OID:** | 1.3.6.1.4.1.22144.0 |
| **Value:** | http://www.crc.bg |
| **Text:** | Registration Resolution № .......by the Communications Regulation Commission |

| **OID:** | 1.3.6.1.4.1.22144.1 |
| **Value:** | http://repository.infonotary.com/cps/qcps.html |
| **Text:** | Qualified Certificates Certification Practice Statement |
1.4.1.1.2. Certificates of primary certification authorities (i-Notary primary CAs)

The primary certification authorities of the Provider issue and sign certificates of the subordinate certification authorities of the Provider and of the data for the status of certificates issued by them.

1.4.1.1.2.1. Primary certification authority for universal electronic signature certificates (i-Notary Q Sign CA)

(1) Certificate for the public key of the primary certification authority for universal electronic signature certificates (i-Notary Q Sign CA), OID: 1.3.6.1.4.1.22144.1.1, is issued and signed with the root private key of the certification authority.

(2) The certificates of the subordinate authorities of the Provider, who issue universal electronic signature certificates to end-users are signed with the private key of the primary authority (i-Notary Q Sign CA):

- Operative Certification Authority for universal electronic signature certificates of natural persons (i-Notary Personal Q Sign CA);

- Operative Certification Authority for universal electronic signature certificates of legal entities (i-Notary Company Q Sign CA).

(3) The list of suspended and revoked subordinate certificates (qsign-ca.crl) issued by the primary authority (i-Notary Q Sign CA) is signed with its private key.
1.4.1.1.3. Operative Certification Authorities (i-Notary subordinate CAs)

1.4.1.1.3.1. Operative Certification Authority (i-Notary Personal Q Sign CA)

(1) A certificate for the public key of the Operative Certification Authority for universal electronic signature certificates of natural persons (i-Notary Personal Q Sign CA), OID: 1.3.6.1.4.1.22144.1.1.1, is signed by the private key of the primary authority (i-Notary Q Sign CA).

(2) In line with the respective certification policy and the User Manual, universal electronic signature certificates of natural persons (i-Notary Personal Q Sign certificate) for end-users are signed with the private key of the subordinate authority (i-Notary Personal Q Sign CA).

(3) The list of suspended and revoked certificates of end-users (qsign-personal-ca.crl) issued by the subordinate authority (i-Notary Personal Q Sign CA) is signed with its private key.

1.4.1.1.4. Operative Certification Authority (i-Notary Company Q Sign CA)

(1) A certificate for the public key of the Operative Certification Authority for universal electronic signature certificates of legal entities (i-Notary Company Q Sign CA), OID: 1.3.6.1.4.1.22144.1.2.1, is signed by the private key of the primary authority (i-Notary Q Sign CA).

(2) In line with the respective certification policy and the User Manual, universal electronic signature certificates of legal entities (i-Notary Company Q Sign certificate) for end-users are signed with the private key of the subordinate authority (i-Notary Company Q Sign CA).

(3) The list of suspended and revoked certificates of end-users (qsign-company-ca.crl) issued by the subordinate authority (i-Notary Company Q Sign CA) is signed with its private key.
1.4.1.2. End-User Certificates

(1) The universal electronic signature certificates issued by the Provider to end users, may be with different designation, depending on the policies on such certificates.

(2) The universal signature certificates issued by the Provider, contain the extensions defined by the X.509 v.3 standard, as well as additional constrains and extension in line with those defined by the International Organization for Standardization (ISO).

(3) The universal signature certificates contain the extension “Key Usage” defining certificate application constraints. The attribute is of category of “critical”.

(4) Certificates issued by the Provider in line with its certification policy may be used for the following designations:

► authentication – authorship certification;

► confidentiality – usage for data encryption and decrypting;

► integrity – ensuring the entirety and invariability of the signed data;

► non-repudiation – impossibility for signing rejection.

(5) The universal signature certificates contain the extension “Extended Key Usage” which details the certificate application with view to its designation. This attribute belongs to the category of “non critical”.

1.4.1.2.1. End-user universal electronic signature certificates

The universal electronic signature certificates issued by the Provider are of two types according to the Holder type – natural person or legal entity, entered therein and may be used in the following applications:

► Natural person universal electronic signature certificate (i-Notary Personal Q Sign certificate):
it may be used as a means of personal electronic identification in e-trade, financial transactions, electronic correspondence, electronic document signing and making statements from and to public authorities or local self-government authorities in line with the LEDES.

Legal entity universal electronic signature certificate (i-Notary Company Q Sign certificate):

it may be used as a means of company/ professional electronic identification, e-trade, financial transactions, electronic correspondence, electronic document signing, making statements from and to public authorities or local self-government authorities in line with the LEDES.

### 1.4.2. Signature action constraints

(1) The certificates issued by the Provider, depending on their type and certification policy may be limited with respect to the value of the transactions that might be concluded by their application – for electronic signature certification and electronic identification.

(2) For universal electronic signature certificates the limitation with respect to transaction amount shall be put by the Holder and shall be directoried in the certificate by the Provider on the basis of the certificate issuance application. The constraints are recorded in the certificate extension “bgFinancialObligationsStatement”, OID: 2.5.4.3.100.1.3.

(3) If the Holder has specified nothing else in the issuance application and no agreement exists for the certificate to be issued without constrains of the action with respect to the property interest value, the certificate is issued with directoried constrains for usage of the certificate up to a specific property interest according to the limits specified in cl. 9.8, para 2 of the User Manual.

(4) The Provider shall not be held liable for damages, incurred as a result of the use of certificates issued thereby beyond their permitted use and application constraints with respect to the designation and transaction amount and such usage shall invalidate the guarantees given by INFONOTARY EAD to the Holder and the trusting parties.
1.5. Policy Administration

(1) The certification policy of the Provider shall be defined by the Board of Directors of INFONOTARY EAD.

(2) Any and all amendments, editions and additions to the universal electronic signature certification services provision practice and certification policies for the different universal electronic signature certificate types shall be adopted by the Board of Directors of INFONOTARY EAD.

(3) The new versions of the documents shall be published in the Provider's Document Directory immediately after their approval by the Communication regulation commission and shall be publicly accessible at: http://repository.infonotary.com.

(4) Any and all comments, requests for information and clarification of the universal electronic signature certification services provision practice and certification policies may be addressed to:

<table>
<thead>
<tr>
<th>INFONOTARY EAD</th>
<th>Tel./Fax: 00359 2 987 57 17</th>
</tr>
</thead>
<tbody>
<tr>
<td>16, Ivan Vazov St, floor 6</td>
<td>e-mail: <a href="mailto:legal@infonotary.com">legal@infonotary.com</a></td>
</tr>
<tr>
<td>1000 Sofia, Bulgaria</td>
<td>URL: <a href="http://www.infonotary.com">www.infonotary.com</a></td>
</tr>
</tbody>
</table>
1.6. Acronyms

**ENGLISH LANGUAGE ACRONYMS**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1</td>
<td>Abstract Syntax Notation One – Abstract object-description language for certificates</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria</td>
</tr>
<tr>
<td>CEN</td>
<td>European Committee for Standardization</td>
</tr>
<tr>
<td>CENELEC</td>
<td>European Committee for Electrotechnical Standardization</td>
</tr>
<tr>
<td>CP</td>
<td>Certificate Policy – certification services provision policy</td>
</tr>
<tr>
<td>CPS</td>
<td>Certification Practice Statement – certification services provision practice</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List – List of suspended and revoked certificates</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm – A kind of cryptographic algorithm for signature generation</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name – Unique name</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm – A kind of cryptographic algorithm for signature generation</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standardization Organization</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol – A protocol for simplified directory access</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>OCSP</td>
<td>On-line Certificate Status Protocol – Protocol for real-time checking of certificate status</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public Key Cryptography Standards – Cryptographic standard for public key transfer</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest-Shamir-Adelman – Cryptographic algorithm for signature generation</td>
</tr>
<tr>
<td>SSCD</td>
<td>Secure Signature Creation Device</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm – Hash Algorithm for hash identifier extraction</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer – Secure data transmission channel</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
</tbody>
</table>

**BULGARIAN LANGUAGE ACRONYMS**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Joint-Stock Company</td>
</tr>
<tr>
<td>EAD</td>
<td>Sole Joint-Stock Company</td>
</tr>
<tr>
<td>PN</td>
<td>Personal number</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>LEDES</td>
<td>Law on Electronic Document and Electronic Signature</td>
</tr>
<tr>
<td>CRC</td>
<td>Communication Regulation Commission</td>
</tr>
<tr>
<td>OACSP</td>
<td>Ordinance on the Activities of Certification Service Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services</td>
</tr>
<tr>
<td>ORAESA</td>
<td>Ordinance on the Requirements to Advanced Electronic Signature Algorithms</td>
</tr>
<tr>
<td>OCSPR</td>
<td>Ordinance on Certification Services Provider Registration</td>
</tr>
<tr>
<td>Manual</td>
<td>Universal Electronic Signature Certification Services User Manual</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>Practice</td>
<td>Universal Electronic Signature Certification Services Provision Practice</td>
</tr>
<tr>
<td>Policy</td>
<td>Universal Electronic Signature Certification Services Provision Policy</td>
</tr>
</tbody>
</table>
2. Publication and Repository Responsibilities

The Provider publishes information on the certification services for universal electronic signature which is available in electronic directories accessible to the public.

2.1. Repositories

2.1.1. Public Documental Repository

(1) All the public information, connected with the activity of the Provider is published and updated regularly in an Electronic documental directory, publicly accessible on: http://repository.infonotary.com

(2) The published versions and updated editions of the following documents of the Provider are maintained in the documental directory:

► User Manual for Certification services for universal electronic signature;

► Contract for Certification services;

► Price-list for providing certification services for universal electronic signature;

► Regulations for issuing certificates, including regulations for establishing the identity of the holder of the universal electronic signature”;

► Terms and conditions for using the universal electronic signature, including requirements for storing the private key;

► Other documents and information, provided in the LEDES.

(3) The access to the documents published in the document directory for the purpose of reading and retrieving them is unlimited and free.
2.1.2. Certificates Directory

(1) The Provider of certification services keeps electronic directory of certificates in which it publishes the certificate for its electronic signature in accordance with Art.22, cl. 8 of LEDES as well as all certificates issued by the Provider.

(2) The Provider also keeps and publishes in the electronic directory a separate list of suspended or revoked certificates.

2.2. Publishing information for the certificates

(1) The issued certificates are published in the Certificates directory not later than 5 minutes of their being signed by the Certification authority of the Provider.

(2) Suspended or revoked certificates are published in the List of Suspended or Revoked certificates by the Certification authority of the Provider not later than 5 minutes of their being suspended or revoked.

(3) Renewed certificates are deleted from the List of Suspended or Revoked Certificates by the Certification authority in the order provided in cl. 4.9.15.

2.3. Frequency of publications

(1) The lists of the valid certificates are updated automatically when a newly issued certificate is published.

(2) The lists of the suspended or revoked certificates are updated automatically within 5 minutes of a suspended certificate, revoked certificate, or expired certificate being listed and of a renewed certificate being deleted from the list.

(3) The lists of suspended and revoked certificates are as well updated within 3 hours of the last publishing if they have not been updated in accordance with cl. 2.
(4) The term of validity of a published list of suspended or revoked certificates is 3 hours.

(5) All published lists of suspended and revoked certificates are stored in the Archives of lists of expired certificates and are available at the following address: http://crl.infonotary.com/archives/.

(6) Any changes to documents published in the Documental directory are published immediately after they are accepted in the order provided in cl. 1.5.

2.4. **Access to the directory of certificates**

2.4.1. **Public access to the directory**

(1) The electronic directory of the certificates of the Provider is also accessible to the public through LDAP-based access at: ldap://ldap.infonotary.com/dc=infonotary,dc=com

(2) Any interested party may initiate a search in the Certificates Directory according to certain criteria and may read and retrieve/download published certificates from: http://repository.infonotary.com/.

(3) The Provider does not in any way and in any form restrict the access to the Certificates Directory. The Directory is constantly accessible except under force majeure circumstances or events beyond the Provider's control.

(4) Upon explicit request of the Author, the Provider may restrict the access for reading and downloading his electronic signature certificate.

2.4.2. **Access control in keeping the directory**

The Provider ensures complete physical, technological and procedure control in keeping the directory ensuring that:

- only duly authorized personnel may enter data into the directory;
- changes to the data in the directory are not possible;
the possibility of unauthorized interference is kept to a minimum.
3. IDENTIFICATION AND AUTHENTICATION

(1) The Provider supports Registration authorities which check and verify the identity and/or other data included in the electronic signature certificates.

(2) Before the issuance of a certificate is validated by the Authentication authority of the Provider, the Registration authority verifies the identity of the Holder and Author.

(3) The Registration authorities of the Provider follow specific procedures in checking the names, including the protected data in some names.

(4) The Registration authorities authenticate the requests for terminating the validity of certificates in compliance with the provisions in cl. 3.4.

3.1. Naming

3.1.1. Types of names

(1) In identifying the Holder and Author in the certificates, the Provider uses different kinds of names for the name and its individualizing data, such as X.500 unique names and RFC – 822 names.

(2) The names assumed by the Holder and Author of a certificate issued by the Provider are unique and are always used together with the unique number of the certificate.

3.1.2. Pseudonyms

The Provider does not issue universal electronic signature certificates on the basis of a used pseudonym as a means of naming the Holder or Author.
3.1.3. Rules for interpreting different forms of names

(1) Only the information contained in the request and duly supported by documentation, identifying the Holder and Author, is included in the universal electronic signature certificate issued by the Provider.

(2) To identify an Holder – a physical person, the following data is included in the name attribute on the certificate (CommonName) of (x509 Subject DN):

- First name, middle name and surname of the Holder.

(3) When the Author of the certificate is not the Holder, then in the name box/space (CommonName) of (x509 Subject DN) the identification data of the physical person – Author is included:

- First name, middle name and surname of the Author.

(4) The information for identification of the Holder, when different from the Author, is included in the space provided for the name of the organization (OrganizationName) and includes:

□ For Legal entities:

- The full name of the organization as it appears on its registration documents

□ For Physical persons:

- First name, middle name and surname of the person.

(5) In a certificate of a legal entity, the unique name (DN) necessarily contains information on the authorization of the Author by the Holder such as details including the identity of the legal entity – Holder of the certificate.
(6) Additional information identifying the Holder, different from the Author, is included as additionally defined attributes of (x509 Subject DN) and includes:

□ For Legal entities:

- BULSTAT;
- Tax registration number;
- Court Registration or articles of association.

□ For Physical persons:

- Personal Identification Number;
- ID number;
- Identification of a document evidencing the representative powers of the Author.

### 3.1.4. Uniqueness of the names

(1) The Provider issues certificates filed under unique numbers in its directory.

(2) The unique number of the certificate is a 16-symbol/digit number, generated by a unique counter.

(3) The combination of the name of the Holder, the name of the Author and the authorization of the Author, together with the type of the certificate are unique for the valid certificates.

(4) The Provider issues only one universal electronic signature certificate of a type to a Holder for an Author.

### 3.1.5. Recognition, authenticity and role of trade marks

(1) The Provider complies adheres to established validation and verification procedures when issuing certificates with regard to the right of the
Holders and Authors over reserved trade marks, brand names, Internet domains, etc., stated to be included in a certificate.

(2) Holders of rights to such names or marks, etc., prove such rights in the registration procedure by presenting the relevant official documents to the Registration authority of the Provider.

(3) When information, authenticated property of third parties, is requested to be included in a certificate, the Provider may withhold the issuance of the certificate.

(4) The Provider shall not be held responsible if data included in the certificate violates copyright or right of ownership of a name, mark, etc.

(5) The Provider shall not include any graphic reserved symbols, logos or other graphic materials subject to copyright in the certificates issued by the Provider.

3.2. Initial identification and identity validation

(1) For initial identification and authentication of the Holder and Author of the universal electronic certificate requested to be issued, the Provider performs the following checks for:

► Holding the private key corresponding to the public key submitted to the Provider by the physical person, indicated as Author in the certificate;

► Verification of the identity of the Physical person – Holder and Author.

3.2.1. Method of verifying the holding of the Private Key

(1) The holding of the Private Key, corresponding to the public key submitted to the Provider to be included in the certificate, is subject to verification in different ways depending on the Verification and Validation policy for a certain type of certificate.
(2) When a request for issuing a universal electronic certificate is submitted, the verification/check of the holding/possession of the private key is performed by the Registration authority by means of a check of the electronic signature with which the request for the issuance of a certificate in the PKCS#10 format is signed.

(3) The Registration authority also verifies the holding of the private key before initiating the issuance of a certificate and forwarding it to the Certification authority of the Provider, regardless of whether the pair of keys involved in the request is generated by the Author, respectively the Holder individually, or the pair of keys is generated by the Provider, respectively, the Registration authority.

(4) When issuing a universal electronic signature certificate, the Registration authority also checks the availability in the cryptographic device (smart card) of the private key corresponding to the public key submitted to be included in the certificate.

3.2.2. Identity Validation of an Holder – Legal Entity

(1) To establish and verify the identity of a legal entity that has requested to be issued a certificate, certain procedures are applied and rules, determined/established by the Provider, are observed, depending on the type of the requested certificate and the conditions for its issuance.

(2) The Provider reserves the right to alter the requirements regarding the information and documents needed for the identity validation of the Holder-Legal entity, if necessary in view of its verification policy or the provisions and requirements of applicable laws.

(3) When a universal electronic signature certificate is issued, the Registration authority checks and verifies the information in accordance with the rules and procedures established by the Provider and in full compliance with the User Manual and other interior regulations and documents.

(4) The Registration authority checks and verifies the following information identifying the Holder-Legal entity:

□ Name of the legal entity;
□ Address, city, country, postal code;
□ Number in the national tax register and/or
□ BULSTAT number;
□ Name of the domain;
□ Legal statute and current status;
□ Right to a brand name, trade mark, domain, etc;
□ Information for contacts and invoicing.

(5) The Holder, respectively an authorized representative of the Holder, personally submits to the Registration authority the following documents:

□ Court Resolution for registration or Articles of Association;
□ Certificate of current status, issued not earlier than 1 month prior to the date of submission;
□ BULSTAT registration certificate;
□ Tax registration certificate;
□ Document evidencing the right to use a name, etc.

3.2.3. Identity Validation of a Physical Person – Holder, Author or Authorized Representative

(1) Certain procedures are applied and rules, established by the Provider, are adhered to in establishing and validating the identity of a physical person applying for a certificate, depending on the type of the requested certificate and the terms and conditions for its issuance.

(2) The Provider reserves the right to change his requirements regarding the information and documents necessary for the identity validation of a Physical person – Holder or Author, if this is required by the law or in accordance with his certification policies.

(3) When a universal electronic signature is issued, the information check and verification is performed by the Registration Authority in accordance with
the rules and procedures of the Provider and in full compliance with the User Manual and other internal regulations.

(4) The Registration Authority checks and verifies the following information identifying the Physical person – Holder or Author, or an Authorized representative:

- First name, middle name, surname;
- date of birth;
- place of birth;
- nationality;
- sex;
- address, city, country, postal code;
- Personal Identification Number (PIN);
- ID number: identification card, passport;
- issuing authority, date of issue and expiry date of the identification document;
- representative power of the Author or the Authorized representative;
- information for contacts and invoicing.

(5) The Holder, Author or Authorized representative of the Holder personally submits to the Registration Authority the following documents:

- valid identification document: ID card or passport;
- notarized Power of Attorney pursuant to which the Representative is empowered to represent the Holder before the Provider for the issuance and management of certificates;
- a document evidencing the representative power of the Author – court resolution, current status certificate, notarized Power of Attorney or some other authorizing instrument.
3.2.4. Unconfirmed information

(1) In some cases the Provider includes in the issued certificates unconfirmed information about the Holder or Author, such as position of the empowered physical person, department or organization, telephone, fax, email, etc.

(2) Unconfirmed information is information which is outside the range of mandatory details, included in the content of the certificate in accordance with Art.24 of LEDES, and cannot be verified by the Provider on the basis of official documents or in another way provided by the law.

(3) The Provider shall not be held responsible for any such unconfirmed information included in the certificate.

3.3. Identity validation and authentication in requests for replacement of keys in a certificate

Not supported by the Provider.

3.4. Identity validation and authentication for terminating a certificate

(1) The validity of a certificate is revoked by the Certification Authority of the Provider after the Registration Authority of the Provider initiates the termination in accordance with the provisions of cl. 4.9.3.

(2) The Registration Authority makes a request for termination to the Provider after receiving a request for termination from the Holder or Author of an electronic signature certificate and performing identity validation and authentication of the applicants and their confirmation.

(3) The Holder, Author or the Authorized representative of the Holder, who has submitted a request for terminating a certificate, personally presents to the Registration Authority the following documents:
□ valid identification document: ID card or passport;

□ notarized Power of Attorney pursuant to which the Representative is empowered to represent the Holder before the Provider for the issuance and management of certificates;

□ a document evidencing the representative power of the Author – court resolution, current status certificate, notarized Power of Attorney or some other authorizing instrument.

□ signed Request for terminating a certificate.

3.5. Identity validation and authentication for requests for suspending a certificate

(1) The request for suspending the term of validity of a certificate can be submitted to the Provider in accordance with the conditions and order provided in cl. 4.9.13.

(2) A valid certificate is suspended by the Certification Authority of the Provider for the term needed according to the circumstances but not for more than 48 hours.

(3) The Provider suspends a certificate without performing any identity validation and authentication of the applicant in the following events:

► By request of the Holder, respectively the Author;

► By request of the Communications Regulating Commission for universal electronic signature certificates;

► By order of the Chairman of the Communications Regulating Commission, when there is a risk for the interests of third parties or when there is sufficient evidence of violation of the law.

(4) The validity of a certificate is renewed by the Certification Authority of the Provider in the order of cl. 4.9.15 and after the renewal is initiated by the Registration Authority.
(5) The Registration Authority performs identity validation and authentication of the Holder when the latter has submitted personally or through an authorized representative the request for the renewal of a certificate.

(6) The Holder, or his authorized representative, who has requested the renewal of a certificate, personally presents to the Registration Authority the following documents:

- valid identification document: ID card or passport;

- notarized Power of Attorney pursuant to which the Representative is empowered to represent the Holder before the Provider for the issuance and management of certificates;

- a signed Request for the renewal of a certificate containing a statement that the Holder is aware of the reason and grounds for the suspension of the certificate and the request for renewal is submitted as a result of this.
4. EFFECTIVE CONDITIONS

(1) Holders, Registration Authorities and other participants in the certification infrastructure of the Provider shall inform him immediately if there are any changes to the information contained in and concerning the certificate issued, during the term of its validity and until it is revoked.

(2) The Certification Authority of the Provider issues, suspends and revokes a certificate pursuant to duly signed request to that effect from his Registration Authority.

4.1. Application for the issuance of a certificate

The Registration Authority of the Provider accepts and processes all applications for the issuance of a certificate and has to submit to the Certification Authority truthful and correct information concerning the received applications for issuance from ultimate users.

4.1.1. Applicants

(1) An application for the issuance of a certificate can be submitted to the Provider by every person who:

► Fills in an application form for the issuance of a certificate;

► Generates a pair of cryptographic keys, personally or through the Provider;

► Submits to the Certification Authority of the Provider the public key corresponding to the private key;

► Accepts the conditions of the Provision of Certification services Agreement and the User Manual of the Provider;

(2) The application for the issuance of a certificate can be submitted personally by the Holder or by his authorized representative.
4.1.2. Process of applying for the issuance of a certificate

(1) The application for the issuance of a certificate has to contain the following data:

- information, identifying the Holder, and, if the Holder is not the Author, information about the Author;
- the public key corresponding to the private key from the pair of cryptographic keys generated by the Author;
- the type of the selected certificate.

(2) The application for the issuance of a certificate is an electronic document in PKCS #10 format, signed with the private key corresponding to the public one contained in the document.

(3) Depending on the certification policy for the different types of certificates issued by the Provider, it may be necessary that some additional information be included in the application for the issuance of a certificate.

(4) The application for the issuance of a certificate can be generated through the Provider’s website or submitted to him through an encrypted communication channel at https://www.infonotary.com.

(5) The Registration Authority of the Provider provides assistance in generating the pair of cryptographic keys, the creation of an application for the issuance of a certificate and their submitting to the Provider.

(6) When the Registration Authority, upon the request of the Holder, generates the pair of cryptographic keys, it uses a protection mechanism for generating the keys, and submits them to the Author recorded on a secure cryptographic device – smart card, etc.

(7) Rights of access to the private key – PIN code or password, are granted by the Registration Authority to the Holder in a protected form.
(8) After the Registration Authority delivers the device on which the private key is recorded and the rights of access to it, the Holder and the Author are fully responsible for preventing the compromising, loss, disclosure, modification or some other unauthorized use of their private keys.

4.2. Procedure for submitting a request for a certificate

4.2.1. Performing the functions for identity validation and authentication

(1) The functions for identity validation and authentication of applicants for the issuance of a universal electronic signature certificate are performed by an authorized Registration Authority of the Provider.

(2) Adhering to the procedures established by the Provider and in accordance with cl. 3.2., on the basis of the received application for issuance of a certificate and the presented documents, and in the presence of the Applicant – Author, Holder or a person authorized by him, the Registration Authority checks and verifies before the Certification Authority:

- The identity of the Author, Holder or his authorized representative;
- The representative power of the Author and the person authorized by the Holder;
- The possession of the private key corresponding to the public key, included in the application at the time of its generating;
- Additional information to be included in the certificate, with the exception of unconfirmed information;
- The Holder’s and the Author’s acceptance of the conditions of this User Manual and the signing of an agreement for the provision of certification services.
4.2.2. Granting or denying applications for certificates

(1) Prior to granting a submitted application for issuance of a certificate, the Registration Authority of the Provider performs the necessary checks in accordance with the provisions of cl. 3.2.:

- Validates and authenticates the identity of the Applicant – Author, Holder or a person authorized by him, on the basis of the presented documents;
- Checks and validates the representative powers of the Author and the person authorized by the Holder to represent him;
- Checks the correctness of the received or generated signed electronic application (in PKCS#10 format) for issuance of a certificate;
- Presents to the Holder or Author the information which is confirmed and will be included in the issued certificate for approval of its content.

(2) After the Registration Authority performs the respective checks and the Holder and Author approve the content of the certificate, the Registration Authority confirms the application for issuance of a certificate and forwards it to the Certification Authority, guaranteeing that:

□ The application is from the Holder or a person duly authorized by him, or from the Author;
□ The information regarding the Holder and the Author, provided to be included in the certificate, is correct and complete;
□ The private key is technically appropriate to be used for the generation of an improved electronic signature and corresponds to the public key, so that it is possible, through the public key, to verify the fact that a certain electronic signature is generated with the private key, and
□ The private key is in the possession of the Holder.

(3) If the process for validating the application for issuance of a certificate finishes unsuccessfully, the Registration Authority delays the application for issuance of a certificate.
(4) The Registration Authority immediately notifies the Applicant and points out the reasons and grounds for the denial.

(5) Applicants whose applications for issuance of a certificate have been denied, they may apply for the issuance of a certificate again.

(6) The Registration Authority files and stores the documents presented by the Holder, Author or the authorized representative, together with the application for the issuance of a certificate and a signed agreement for the provision of certification services (certification services).

(7) The Provider controls the correctness of the information, presented by the Holder and Author and included in the certificates to the date of issuing the certificate.

(8) In all cases and for all types of certificates issued by the Provider, the Holder and Author have the permanent obligation to monitor the correctness of the presented information and to inform the Provider of any changes that have become effective after the issuance of the certificate.

4.2.3. Term for processing the applications for certificates

The check and validation of the information provided in the application for the issuance of a certificate are performed processed within a reasonable period of time, and the Provider issues the certificates within 5 days of receiving the documents.

4.3. Issuing a Certificate

4.3.1. Functions of the Certification Authority in issuing a certificate

(1) The Certification Authority of the Provider issues the certificate on the basis of a request for issuing a certificate from the Registration Authority.
(2) The request for the issuance of a certificate from the Registration Authority is a guarantee that the validity of the application has been confirmed, the data contained in it is also verified, and it is signed by the administrator of the Registration Authority performing the checks and validations.

(3) The Certification Authority of the Provider performs identity validation of the Registration Authority and authentication of the administrator of the Registration Authority on the basis of presented commission (special administrative certificate of the administrator of the Registration Authority).

4.3.2. Notifying the Holder by the Certification Authority of the issuance of the certificate and its delivery

(1) The Provider shall immediately notify the Holder, respectively the Author, of the issuance of a universal signature certificate by:

► Sending an electronic letter to the Holder, respectively the Author, and

► Publishing the information for the issuance of the certificate on the Provider’s website, when the Holder or the Author is a registered user and has valid rights of access to the website at:: http://www.infonotary.com.

(2) After issuing the certificate, the Provider delivers it to the Holder, respectively the Author:

► By publishing a link for downloading the certificate on the Provider’s website when the Holder, respectively the Author, is a registered user and has valid rights of access to the website at:: http://www.infonotary.com

► Or through the Registration Authority.
4.4. Accepting and publishing/publishing the certificate

4.4.1. Accepting the certificate

(1) The Provider issues the certificate in accordance with the consent of the Holder, respectively the Author.

(2) The Holder, respectively the Author, accepts/approves the content of the universal electronic signature certificate prior to publishing of the said certificate on the Certificates Directory of the Provider, and certifies it by signing a Protocol of acceptance of the certificate.

4.4.2. Publishing/publishing the certificate by the Certification authority

The Provider immediately publishes the issued universal electronic signature certificate on its Certificates Directory.

4.5. Pairs of keys and use of the certificate

4.5.1. Private key of the Holder/Author

(1) No one apart from the Author has the right of access to the private key.

(2) The Holder, respectively the Author, is fully responsible for storing and using the private key, as well as for preventing any discredit, loss, disclosure, modification or any other unauthorized use of his private key.

(3) The Holder, respectively the Author, is fully responsible for the actions or faults of parties authorized by them to generate, keep, store or destroy their private keys.
4.5.2. Use of the public key by the Relying Parties and use of the certificate

The Relying Parties the public key included in the universal electronic signature certificate issued by the Provider to check the validity of the electronic signature generated by means of the private key corresponding to the public key in the certificate.

4.6. Certificate Renewal

4.6.1. Conditions for renewal of a certificate

(1) The certificates issued by the Provider have different terms of validity depending on their type and on the certification policy. The term of validity is entered as a requisite in the issued certificate.

(2) Certificate renewal – the issuance of a certificate with a renewed term of validity without any change to the data included in it and to the respective pair of keys, is a service supported by the Provider on conditions and requirements depending on the type of the certificate and its application.

(3) A valid, not suspended, universal electronic signature certificate of a physical person or a legal entity may be renewed once only for another term of validity – 1 year (365 days).

(4) A certificate issued by the Provider may be renewed only if all data contained in the certificate is unchanged and the content of the certificate is identical with the valid certificate, and the new term of validity is entered in the new certificate.

4.6.2. Who may submit a request for renewal

The Holder or the Author entered in the valid certificate may submit a request for renewal at least 10 (ten) days prior to the expiry of the term of validity of the certificate.
4.6.3. Procedure for submitting a request for renewal

(1) The request for renewal is made by submitting a request for the renewal of a valid certificate with the Registration Authority or through the Provider’s website with a signed electronic request/application form, if the Holder or the Author is a registered user and has valid rights of access to the website at: http://www.infonotary.com.

(2) The electronic request/application form has to be signed by the Author with the valid electronic signature certificate, for which renewal is requested.

(3) The Registration Authority of the Provider may require that the Applicant provide updated documents evidencing the truthfulness and correctness of the information included in the certificate as of the time of submitting the request for renewal.

(4) The Applicant signs a statement that the information provided at the initial issuance and the information included in the certificate is true, correct and unchanged to date.

(5) Before granting the submitted certificate renewal request, the Registration Authority of the Provider carries out the necessary checks and validations in compliance with cl. 3.2. and 4.2.

(6) After carrying out the necessary checks and accepting the content of the certificate, certified by the Holder or Author in compliance with cl. 4 with a signed statement, the Registration Authority confirms the certificate renewal request to the Certification Authority of the Provider and guarantees that:

► The renewal request is submitted by /comes from/ the Holder, or a party duly authorized by him, or the Author;

► The information concerning the Holder and the Author included in the certificate is correct, true and updated;

► The private key is in the possession of the Holder;

► The certificate whose renewal is requested is valid.
(7) If the process of confirming the certificate renewal request is completed unsuccessfully, the Registration Authority denies the certificate renewal request.

(8) The Registration Authority immediately notifies the Applicant and states the grounds for the denial.

(9) Applicants whose request for renewal of certificates have been denied may apply for a new certificate.

(10) The Registration Authority files and stores the documents submitted by the Holder and the Author together with the request for renewal of a certificate and the signed statement.

(11) The check and validation of the information provided in the requests are carried out within a reasonable term and the Provider issues the certificate within 5 days of the date of receiving the documents.

(12) The Certification Authority of the Provider issues the new certificate on the basis of the request for renewal received from the Registration Authority.

(13) The request for the renewal of a certificate from the Registration Authority guarantees the validation of the request submitted by the Applicant, the validity of the information contained in it, and is signed by the administrator of the Registration Authority who has carried out the checks.

(14) The Certification Authority of the Provider checks the identity of the Registration Authority and that of the Registration Authority administrator on the basis of a presented commission (a special administrative certificate of the Registration Authority administrator).

4.6.4. Informing the Holder about the issuance of the new certificate by the Certification Authority

(1) The provider immediately informs the holder, respectively the Author about the new universal electronic signature certificate issued, by:

- sending an e-mail to the Holder, respectively the Author and
► publishing information about the issuance on the Provider’s website, when the Holder and the Author are registered users and have valid website access rights on: http://www.infonotary.com.

(2) After issuing the new certificate the Provider provides it to the Holder, respectively to the Author:

► by publishing a link for downloading the certificate on the Provider’s website, when the Holder and the Author are registered users and have valid website access rights on: http://www.infonotary.com

► or by the Registration Authority.

4.6.5. Agreeing on the renewed certificate

The Holder, respectively the Author agree on the contents of the renewed certificate before issuing it by signing the Information Validity Declaration according to section 4.6.3, paragraph 4.

4.6.6. Issuance of the renewed certificate by the Certification Authority

The Provider immediately publishes the issued certificate in the Directory of his certificates.

4.7. Changing a key in a certificate

Not supported by the Provider.

4.8. Modifying a certificate

Not supported by the Provider.
4.9. Terminating a certificate

When terminating the basis or operating certificates of the Certification Authority of the Provider due to discrediting of their private keys all certificates, signed by the Provider with these keys are no longer valid.

4.9.1. Conditions for terminating a certificate

(1) The validity of issued valid certificates by the Provider is automatically revoked:

- when the certificate validity date expires;

- when the Provider’s legal entity revokes the certification services without transferring the activity to another certification services provider.

(2) The Provider of certification services revokes the certificate validity in case of:

- death or when the Holder or the Author are under judicial disability;

- termination of the legal entity of the Holder;

- termination of the representative rights of the Author regarding the Holder;

- verifying that the certificate was issued on the basis of false information.

(3) The Provider takes immediate actions on the termination of the certificate validity when there is justification for doing so.

(4) The Certification Authority of the Provider revokes the validity of certificates issued by him.

(5) The Provider immediately informs the Author and the Holder on the circumstances regarding the validity and reliability of the certificate issued.
4.9.2. Who can ask for a certificate termination

The certification services Provider is obliged to terminate the validity of a certificate when the Holder or the Author asks for it after checking the identity and the legal entity of the Holder, respectively the Author.

4.9.3. Procedure for termination request

(1) To take actions on terminating a certificate by the Certification Authority of the Provider it is necessary:

- to make a written request for terminating a certificate from the Holder, respectively the Author to the Provider;
- the Registration Authority to verify the identity and the representative rights of the Holder, respectively the Author.

(2) The Holder or the properly authorized by him person file a petition for terminating a certificate:

- via e-mail, through the Provider’s website if he is a registered user and has the corresponding access rights on the following address: http://www.infonotary.com and

- personally in the office of a Registration Authority of the Provider signing a “Petition for terminating a certificate”.

(3) The identification and the authentication of the applicants who have requested for a certificate termination are done by the Registration Authority of the Provider according to section 3.4.

(4) The Certification Authority of the Provider revokes the certificate on the grounds of the received request for termination from the Registration Authority.

(5) The certificate termination request from the Registration Authority guarantees the validity confirmation of the request made by the Applicant, the
validity of the information in the request, and it is signed by the administrator of the Registration Authority who has lead the check-ups.

(6) The Certification Authority of the Provider checks the identity of the Registration Authority and the identity of the administrator of the Registration Authority on the grounds of presented powers (a special administrative certificate of an administrator of a Registration Authority) and revokes the certificate.

(7) After terminating the certificate the Provider includes it in the List of the suspended and revoked certificates and updates publicly the available electronic certificate directory.

(8) After terminating the certificate the Provider informs the Holder and the Author directly or through the Registration Authority about the actions taken.

(9) The certificates revoked by the Provider cannot be renewed.

### 4.9.4. Grace period before termination

(1) The validity of the certificate is ended in a period up to 48 hours from the time of receiving the termination request.

(2) In case of a successful examination done by the Registration Authority and after the 48-hour grace period expires the certificate is revoked.

(3) In case of an unconfirmed Registration Authority check-up or at the explicit request of the Holder, respectively the Author, within the grace period the validity of the certificate is renewed.

### 4.9.5. Period in which the Certification Authority has to process the request for termination

The check and validation of the information provided in the requests for termination of certificates are carried out within a reasonable period of time and the Provider revokes the certificates within 48 hours of accepting the request.
4.9.6. Requirements for validation of the termination of a certificate for the Relying Parties

(1) The Relying Parties shall rely on certificates issued by the Provider only after they have validated the status of the certificate in the List of suspended or revoked certificates or through the automatic information provided by the Provider through an OCSP protocol.

(2) If the Relying Party does not carry out the due check of the status of a certificate, the Provider shall not be held responsible for any ensuing damage to the Relying Party.

4.9.7. Frequency of updating the List of revoked certificates

(1) The List of revoked certificates is updated automatically after a certificate is listed.

(2) The term of validity of the List of suspended and revoked certificates is 3 astronomic hours.

4.9.8. Maximum delay of publishing the List of suspended and revoked certificates

The List of suspended and revoked certificates is updated automatically within 5 minutes of the listing of a suspended or revoked certificate, or the delisting of a renewed certificate.

4.9.9. Option for checking the status of a certificate in real time (OCSP)

The Provider offers the service of checking the status of certificates issued by him in real time through an OCSP protocol.
4.9.10. Requirements for using OCSP

The Relying Parties may use the information provided by the automatic system through an OCSP protocol to check the status of a certificate, in accordance with cl. 7.3.

4.9.11. Conditions for suspending a certificate

(1) The Certification Authority of the Provider suspends the validity of certificates issued by him if there are reasonable grounds for that, for the term according to the circumstances.

(2) The Provider takes immediate steps regarding the suspension of a certificate if the circumstances for that are established.

(3) The Provider promptly notifies the Author and the Holder of circumstances concerning the validity or trustworthiness of the certificate issued to him.

(4) For the period of suspension of a certificate, the same certificate is deemed invalid.

4.9.12. Who may file a request for suspending a certificate

The Provider shall suspend the validity of a universal electronic signature certificate issued by him:

- Upon the request of the Holder, respectively the Author, in which case the Provider is not obliged to verify his identity or representative power;

- By order of the Communications Regulating Commission if there are reasons to believe that the validity of the certificate is to be terminated, and

- By order of the Chairman of the Communications Regulating Commission in case of immediate risk for the interests of third parties, or in case of sufficient evidence of violation of the law.
4.9.13. Termination request procedure

(1) To execute all actions involved in suspending a certificate, the certification Authority of the Provider has to obtain/receive:

- □ A request for the suspension of a certificate from the Holder, respectively the Author, to the Provider;
- □ A written order for suspending the certificate, issued by the Communications Regulating Commission, if there are reasonable grounds for the certificate to be revoked, and
- □ An order from the Chairman of the Communications Regulating Commission, if there is a risk for the interests of third parties or sufficient evidence of violation of the law.

(2) The Author, the Holder or a duly authorized party files the request for suspension:

► Through the Provider’s website, if the Claimant is a registered user and has the necessary access rights;

► By telephone, using the IVR service provided by the Provider, using Personal Identification Code received upon the initial registration of the Holder or the Author;

► By fax or email, or

► Personally with the Registration Authority of the Provider.

(3) No prior identification and authentication of the claimant filing the request for suspending a certificate, or of their representative power, is required.

(4) The Certification Authority suspends the validity of a certificate within a reasonable term, according to the circumstances, of receiving the request, and publishes it on the List of suspended and revoked certificates.
4.9.14. Limits to the term for suspending a certificate

The Provider shall suspend the validity of a certificate, issued by him, within a reasonable term, according to the circumstances, but this term shall not exceed 48 hours of receiving the request for suspension.

4.9.15. Renewal of a suspended certificate

(1) The Provider shall renew the validity of a suspended certificate:

   □ When the term for suspension expires (48 hours);

   □ When the grounds and circumstances for the suspension no longer exist;

   □ Upon the request of the Holder, after the Provider, respectively the CRC, has made certain that the former has found out the reason for the suspension, and that the request for renewal is made after this finding.

(2) A certificate is deemed valid as of the moment of its renewal by the certification Authority of the Provider.

4.9.16. Procedure for renewal of a suspended certificate

4.9.16.1. Renewal upon the request of the Holder

(1) When the renewal is made upon the request of the Holder, the Registration Authority of the Provider shall verify the request and validate the identity of the Holder in accordance with cl. 3.5.

(2) After receiving a confirmation of a verified request for renewal and of an identity validation from the Registration Authority of the Provider, the
Certification Authority shall delete the suspended certificate from the List of suspended and revoked certificates, and publishes it.

4.9.16.2. Renewal by order of the Communications Regulating Commission (CRC)

The Certification Authority of the Provider renews the validity of a certificate and deletes it from the List of suspended and revoked certificates upon receiving:

- □ A written order for renewing the certificate, issued by the Communications Regulating Commission, if there were reasonable grounds for the certificate to be revoked, and
- □ An order from the Chairman of the Communications Regulating Commission for renewing a certificate which has been suspended, on account of an immediate threat to the interests of third parties or sufficient evidence of violation of the law.

4.9.16.3. Renewal after the suspension term expires

After the term for suspending the validity of a certificate expires – 48 hours of the moment of suspending the validity of a certificate, the Certification Authority of the Provider automatically renews the validity of the certificate and deletes it from the List of suspended and revoked certificates, except in the cases provided in cl. 4.9.4., (1) and (2).

4.10. Termination of the agreement for providing certification services

The agreement for providing certification services, concluded between the Provider and the Subscriber shall be terminated if the certificates issued by the former have expired or have been revoked.

4.11. Key recovery and Key escrow

Not supported by the Provider.
5. EQUIPMENT, PROCEDURES AND MANAGEMENT CONTROL

5.1. Physical control

(1) The Provider ensures physical protection and control of the access to all critical parts of its/his infrastructure, located rooms owned, rented or leased by him.

(2) The infrastructure of the Certification Authority of the Provider is logically and physically separated and is not used by any other departments or organizations of the Provider.

5.1.1. Layout and design of the rooms

The rooms in which the critical components of the system are located are specially designed, constructed and equipped to store objects and information in conditions of strict admission and access control.

5.1.2. Physical access

(1) The Provider ensures strict control of the access to all his rooms and information resources by means 24-hour security guards, system for electronic control of access, video surveillance systems and alarm systems, etc.

(2) The access control procedures, as well as the systems for controlling physical access – surveillance, admission and signalling, are subjected to scheduled and unscheduled audit and control.

(3) Only authorized members the staff of the Provider, who strictly adhere to and follow the established internal procedures for identification, verification and documenting access, have access to certain rooms and information resources.
5.1.3. Power supply and ambient conditions

(1) The Provider makes sure that the power supply for the whole equipment of the infrastructure of the Provider is protected from power cuts by additional/emergency power supply provided by backed-up sources.

(2) The Provider adheres to all the requirements of the manufacturers of his technical equipment regarding the conditions for its storage and operation, and provides means of monitoring and maintaining the necessary ambient conditions.

(3) The antenna systems used by the Provider are equipped and protected with overload protection systems.

5.1.4. Floods

The Provider ensures a system for monitoring and signalling in case of flooding in the rooms.

5.1.5. Fire alarm and protection

The Provider ensures fire alarm devices and a system for protection in case of fire in his rooms.

5.1.6. Data storage devices

The Provider uses reliable means and devices for the physical storage of data and confidential information, such as safes and metal cases with different degree of protection.
5.1.7. Taking a technical component out of use and operation

The Provider ensures measures for the safe taking of technical components and data and confidential information carriers out of operation and use.

5.1.8. Backing up of components

The Provider ensures back-up copies/parts of all critical components of the infrastructure of the Certification Authority, as well as means and devices for monitoring and automatic replacement of the critical components, if necessary.

5.2. Procedure control

(1) The Provider pursues in his activity such a policy of management and human resource management as to guarantee reliability and trustworthiness in fulfilling all obligations assumed by him as well as competence for providing certification services in accordance with LEDES.

(2) The Procedures described in the User Manual, connected with the activity of the Certification Authority of the Provider, are implemented in accordance with the established internal rules and regulations of the Provider.

(3) Every member of the staff of the Provider shall sign a statement for lack of conflicting interests, protection of the privacy of the information, and personal data protection.

(4) The Provider ensures double control of all critical functions of the Certification Authority.

(5) For some activities, including the ones described in cl. 5 of OACSP, the Provider may use hired services.
5.2.1. Positions and functions

The Provider has at his disposal the necessary number of qualified staff who, at any time of the execution of his activity, shall ensure the fulfilment of his obligations.

5.2.2. Number of employees involved in a certain task

The assigned tasks connected with the functioning of the Certification Authority of the Provider are performed by at least two members of the staff.

5.2.3. Identification and authentication of each position

The Provider has developed a job description for each of the positions of his staff.

5.2.4. Requirements for division of responsibilities for the separate functions

The positions under cl. 5.2.1, par. 2 are performed by different members of the staff of the Provider.
5.3. **Staff control, qualification and training**

(1) The technical staff of the Provider is carefully selected and possesses professional knowledge in the following fields:

- security technologies, cryptography, public key infrastructure (PKI);
- technical norms for security assessment;
- information systems;
- administrating large data base;
- network security;
- auditing, etc.

(2) The Provider checks his future employees on the basis of references issued by competent authorities or third parties, and on the basis of statements.

(3) The Provider ensures training for his staff for the implementation of the activities and functions of the Registration Authority of the Provider.

(4) The Provider organizes regular refresher training so as to ensure continuity and currency of the knowledge of the staff and the procedures.

(5) The Provider imposes sanctions on the staff for unauthorized actions, malpractice and unauthorized use of the systems of the Provider.

5.3.1. **Requirements to independent providers**

The independent providers whose services the Provider uses adhere to the same rules for information privacy and personal data protection as the staff of the Provider.
5.3.2. Documentation provided to the staff

The Provider provides documentation – procedures, rules and regulations to the staff of the Certification Authority and the Registrations Authority for the purpose of initial training, qualification improvement, etc.

5.4. Procedures for preparing and keeping an inspection data journal

(1) The procedures for preparing and keeping an inspection data journal include documenting/reporting events, reporting system checks and inspections, implementing the objectives and maintaining a secure environment.

(2) The Provider keeps record of all events connected with the activity of the Certification Authority, including but not limited to:

□ Issuing a certificate;
□ Signing a certificate;
□ Terminating a certificate;
□ Suspending a certificate;
□ Publishing /publishing/ a certificate;
□ Publishing /publishing/ a List of suspended and revoked certificates.

(3) The records under cl. 2 contain the following information:

□ Identification of the operation;
□ Time and date of the operation;
□ Identification of the certificate involved in the operation;
□ Identification of the person performing the operation;
□ A reference to the request for the operation.

(4) The Provider keeps record of all events connected with the use of the hardware and software platforms, as follows:
□ In cases of installing a new and/or additional software;
□ In cases of shutting down or launching the systems and their applications;
□ In cases of successful or unsuccessful attempts to launch or gain access to the software PKI components of the systems;
□ In cases of regular software and hardware failures of the systems, etc.;
□ In cases of managing and using the hardware cryptomodules.

(5) Records of actions performed by the Registration Authorities in the process of registering Subscribers, identifying Holders and Authors, etc., are also stored.

(6) Records generated by the communication devices of the Provider are also stored.

5.4.1. Frequency of generating records

(1) Records are generated automatically and stored at discrete intervals for the different modules.

(2) Authorized personnel of the Provider checks the records and logs at regular intervals and establishes and reports irregularities.

5.4.2. Record storage period

The records and logs are stored for a period of 20 (twenty) years.

5.4.3. Record security and protection

(1) All records and logs generated by the components of the infrastructure are stored electronically signed.

(2) Only qualified authorized members of the staff of the Provider have the right of access and work with these records and logs.
5.4.4. Procedures for generating back-up copies of the records

(1) Back-up copies of the records and logs are generated at discrete intervals of several hours up to 24 hours for the different modules.

(2) Back-up copies are saved on material carriers and stored in a room with a high level of protection, security and access control.

5.5. Repository

(1) The Provider stores as internal repository the following documents:

- All issued electronic signature certificates for a period of at least 30 years as of the expiry of the term of validity of a certificate;
- All records and logs connected with the issuance of a certificate for a period of at least 30 years as of the issuance of the certificate;
- All records and logs connected with the termination of a certificate for a period of at least 30 years as of the termination of the certificate;
- Lists of suspended and revoked certificates for a period of at least 30 years as of the termination or expiry of the term of validity of the certificate;
- All documents connected with the issuance and management of the certificates (requests, identification and authentication documents, contracts, etc.) for a period of at least 30 years as of the expiry of the term of validity of a certificate.

(2) The Provider stores the records repository in a format that can be restored.

(3) The Provider ensures the integrity of the material carriers and implements a mechanism for their copying as a way to prevent loss of data.

(4) The repository is accessible only to authorized personnel of the Provider and the Registration Authorities, if necessary.
5.5.1. Types of repositories

The Provider keeps a repository for electronic signature certificates, inspection and check data, information regarding the request for the issuance and management of certificates, logs, records and documents facilitating the certification services.

5.5.2. Storage period

The Provider keeps the repository for a period of 30 years.

5.5.3. Repository protection and security

The protection and security of the repository is ensured by the following measures:

- Only personnel authorized to keep the repository has access to it;
- Protection of the repository from modifications by recording the data on devices which are not rewritable;
- Protection of the repository from erasing;
- Protection ensuring the destruction of carriers on which the repository has been stored, after the regular transfer of data to a new carrier.

5.5.4. Procedures for restoring the repository

Not supported by the Provider.

5.5.5. Requirements for verification of the time and date of records

The time of generating certain records and documents by the systems of the Provider is verified by certifying the date and time of their generating and signing through the TimeStamp server of the Provider.
5.5.6. Storing repositories

The repository information is stored in rooms with a high level of physical protection and in conditions allowing the safe long-term storage of paper, magnetic, optical and other carriers.

5.5.7. Procedures for obtaining and checking information from the repository

The repository information, which is public is published and available on the Public electronic directories of the Provider in a readable form.

5.6. Modification of a certificate key

Not supported by the Provider.

5.7. Compromise and disaster recovery

(1) To maintain the continuity and integrity of the services, the Provider introduces, documents and regularly tests suitable plans and procedures for unforeseen events and recovery after disasters.

(2) The Provider does his best to ensure the full and automatic recovery of his services in cases of disasters, computer resources failures, software or information corruption.

(3) With priority the Provider ensures the recovery of the support and the public access to the Certificate Register and the List of suspended and revoked certificates.

(4) If the private key of the Certification Authority of the Provider is compromised, the following measures are taken:

► The electronic signature certificate of the Provider is revoked immediately;

► The Communications Regulating Commission is notified of the revocation of the Provider’s certificate, entered in its register of certificates;
The Certification Authority of the Provider is suspended;

A procedure for generating a new pair of cryptographic keys is initiated;

A new certificate for the electronic signature of the Provider is issued;

All valid certificates issued before the key compromise are re-issued.

(5) If the private key of the Holder, respectively the Author, is compromised, he shall immediately notify the Provider to start the procedure for the revocation of the effective certificate.

5.8. Procedures for terminating the activity of the Provider

(1) The activity of the Provider is terminated in the order provided in OASCP.

(2) If the Provider plans to terminate his activity, he shall notify CRC of his intentions at least 4 months prior to the date of termination.

(3) The Provider notifies CRC if there is a claim for declaring the company insolvent, for declaring the company inoperative, or there is some other claim for dissolving or starting liquidation procedures.

(4) The Provider does his best to continue the validity of the certificates issued by him by transferring them to an operative Certification Services Provider.

(5) The Provider sends written notices to CRC and the users if the service of the Provider is transferred to another registered provider prior to terminating his activity at the latest.

(6) The written notice is also published on the web site of the Provider and contains information about the name and contact details of the provider-successor.
(7) The Provider informs the users of the terms of support of their certificates transferred to the provider-successor.

(8) The Provider duly submits the whole documentation on his activity to the provider-successor, together with all repositories and all issued certificates (valid, revoked and suspended).

(9) If the Provider fails to transfer his activity to another registered provider, he revokes all certificates issued by him and submits the documentation under par.8 to CRC.

(10) CRC keeps a register with the list of the revoked certificates of the Provider.
6. TECHNICAL SECURITY CONTROL

6.1. Key pair generation and installation

(1) The Provider protects its private keys in accordance with the provisions of this User Manual.

(2) The provider uses the middle and operational private keys of the Certification Authority only to sign certificates and the Lists of suspended and revoked certificates in accordance with the authorized use of these keys under cl.1.4 of this document.

(3) The Provider will refrain from using his private keys used by the Certification Authority for purposes outside the range of activities of the Certification Authority.

(4) The users of the certification services of the Provider generate their pair of cryptographic keys – private and public, for electronic signature certificates:

- Personally, with the Holder or Author – using hardware and software under their control,
- With the Provider, respectively with the Registration Authority authorized by him – using hardware and software, part of the infrastructure of the Provider.

(5) When the key pair is generated by the Provider, a “Secure Signature Creation Device” – SSCD, is used. SSCD has secure, protected profile determined in compliance with the Common Criteria, security level EAL 3 or higher in conformity with the standard ISO 15408 or another specification, determining equivalent security levels.

(6) Pursuant to a contract, the Provider may provide the Holders with technical means approved by him (software, smart cards and other cryptographic devices) which meet the requirements for level of security under par.5.
(7) The Holder, respectively the Author, may use other cryptographic devices and software which suit the requirements of par.5., other than the ones provided by the Provider, and in this case the Provider shall not be held responsible for the quality and reliability of the provided certification services.

(8) Only signatures generated with the private key from a key pair in the order provided in par.4 and in accordance with the provisions of par.5 may have the characteristics and validity of universal signatures under LEDES.

(9) If the cryptographic keys for an electronic signature certificate issued by the Provider are generated and installed personally by the Holder, respectively the Author, it is mandatory to use licensed software of a certain manufacturer.

6.1.1. Key pair generation

6.1.1.1. Generation of a private key to be used by the Certification Authority of the Provider

(1) To generate and install the private keys of the Certification Authority, the Provider uses a high-level reliability and security system and adheres to the documented internal procedure.

(2) Hardware protection modules, certified at a level of security FIPS 140-2 Level 3 or higher, are used for generating and using the private keys of the Certification Authority of the Provider.

(3) The implementation of the documented procedure for generating and installing the root key pair of the Certification Authority of the Provider is performed by a specially authorized employee of the Provider in the presence of the members of the Board of Directors of ‘INFONOTARY’ EAD.

(4) The secret components of the root private key, as well as of all operational private keys of the Certification Authority, are separated and stored, and, provided, if they need to be used by persons authorized by the Provider.
(5) Additional protection from compromise and unauthorized use of the private keys of the Certification Authority of the Provider is guaranteed by the additional policy, implemented by the Provider, of control of the access to:

□ The control of the hardware module through secret data, accessible to authorized persons only;

□ The control and use of the private middle and operational keys of the Certification Authority through certain secret data, accessible to authorized persons only.

6.1.1.2. Generation of a key pair of a Subscriber

(1) The Provider offers the service of generating a key pair of a Subscriber, and in the process of generating a protection device is used - "Secure Signature Creation Device" – SSCD, with a protected profile, determined in accordance with the Common Criteria, security level EAL 3 or higher, in compliance with ISO 15408 or another specification, determining equivalent security levels.

(2) Upon the request of the Subscriber, the Provider provides technical devices for the secure generation and storage of the key pair, corresponding to the security levels under par.1 – cryptographic smart cards and other cryptographic devices.

(3) A private key of a Holder, respectively of an Author, generated by the Provider, to be used for the generation of a universal electronic signature, is recorded on a technical device under par.2 – smart card, token, etc., and automatically and irreversibly deleted from the devices of the Provider, used in the process of generating.

(4) The Holder, respectively the Author, may use other cryptographic devices, different from the ones provided by the Provider, but they have to meet the security requirements under par.1 regarding the security level, and must be approved by the Provider, if they are used for generating and installing a key pair with the Provider.

(5) For issuing electronic signature certificates, a protection device – Secure Signature Creation Device – SSCD, with the required level of security
under par.1, has to be used for the generation and storage of the private key of the Holder, respectively the Author of an electronic signature, approved by the Provider. The minimum key length has to be RSA - 1024 bits.

(6) When the key pair generation and storage by the Holder, respectively the Author, for which the issuance of a certificate by the Provider is requested, is performed through software, the Provider requires that the Holder, respectively the Author, always use licensed software of a certain producer in the process of key pair software generation and installation.

6.1.2. Private key delivery

(1) When the Provider, upon the request of the Holder, respectively the Author, generates the key pair, the private key from this pair is recorded on a smart card or another technical device which meets the requirements of cl.6.1.1.2., and the access to it is protected by PIN or password.

(2) The Holder, respectively the Author, is provided with the technical device together with the rights of access.

6.1.3. Delivery of the public key to the party issuing the Certificate

(1) This procedure is performed only by the Holder, respectively the Author, who generates the key pair and who has to deliver the public key to the Provider so that a certificate can be issued.

(2) The electronic request form for the issuance of a certificate, through which the public key is delivered to the Provider, has to be a PKCS#10 file, in DER format.

(3) The Holder, respectively the Author, may submit the electronic request form:

► Through the web site of the Provider at: http://www.infonotary.com;

► Stored on a floppy, CD or another external carrier personally with the Registration Authority.
6.1.4. Delivery of the public key of the Certification Authority to the Relying Parties

The public keys of the Certification Authority are available and accessible on the Provider’s web site at: http://www.infonotary.com.

6.1.5. Key length

(1) The length of the private key of the root certificate of the Certification Authority – InfoNotary CPS Root CA is DSA - 1024 bits, or RSA - 4096 bits.

(2) The length of the private key of the intermediate and operative Certification authority certificate DSA is 1024 bits and RSA - 2048 bits.

(3) For the issuance of a universal electronic signature certificate the private key of the Holder, respectively the Author should be at least 1024 bits long for the RSA and DSA algorithms and 160 bits for the ECDSA algorithms.

6.2. Private key protection and technical control of the cryptographic module

6.2.1. Cryptographic module standards

(1) The Certification Authority of the Provider uses secure and reliable hardware cryptographic modules in compliance with the regulations.

(2) The hardware cryptographic modules used by the Provider for storing the private keys of the Certification Authority are certified for a high level of security and reliability in conformity with FIPS 140-2, Level 3, FIPS 140-1 Level 2, etc..
6.2.2. Private key storage and use control

(1) Together with the procedure for generating and installing the keys of the Certification Authority of the Provider, a procedure for storing and archiving the private keys is performed.

(2) The secret parts for access to the root private key, as well as of all operational private keys of the Certification Authority, are stored separately.

(3) The delivery of the shared parts to persons authorized to store and present them is recorded in a written form.

(4) The procedure for the destruction of the private keys of the Certification Authority of the Provider, performed by the Provider following the expiry of their period of validity guarantees their final destruction and the impossibility for them to be retrieved and used. The process of destroying the keys is documented and all relevant records are stored on the repository of the Provider.

6.3. Other aspects of key pair control

6.3.1. Archiving of the public key

The Provider archives all his public keys and stores them for a period of 30 years after the expiry of their term of validity or following their revocation.

6.3.2. Term of validity of a certificate and term of use (lifetime) of the key pair

(1) The Provider issues electronic signature certificates to the end users for a certain term of validity, stated in the certificate.

(2) Certificates issued by the Certification Authority of the Provider for the root public key and the middle and operational public keys are issued for a certain term of validity, stated in the certificate.
(3) The term of validity of the certificate is the term of use (lifetime) of the key pair connected with it.

(4) The creation of signatures by using a private key of a certificate with an expired term of validity is invalid.

### 6.4. Activation data

(1) The Provider stores on secure and reliable carriers and archives with a high level of protection the activation data concerning the private keys of the Certification Authority and its activity.

(2) An Author using a smart card for storing his private key has to store and protect from compromise the personal activation data for his smart card or token – PIN or password.

### 6.5. Computer security control

#### 6.5.1. Specific requirements for computer security

The Provider implements and uses procedures and methods of control of the security of the technical and technological equipment in his infrastructure in compliance with the established international standards for information security control. The Provider also performs tests and inspections of the technical equipment and technologies implementing methods of security assessment, based on the general methods of security assessment included in ISO Standard 15408.

#### 6.5.2. Computer security rating

The security rating of the technical equipment, technologies and systems, used by the Provider, has to meet the requirements of the regulations for performing the activity of Certification Services Provider.
6.6. Technical control of the life-cycle

(1) The Provider ensures thorough technical control of the life-cycle of the systems through which the certification services are provided by the Provider.

(2) Procedures and rules, set out in the internal documents and regulations of the Provider, are adhered to at any stage of the development and operation of the systems.

(3) The results from the tests are documented and stored in the repository of the Provider.

6.7. Network security control

The Provider maintains a high level of security of the network as well as devices for detecting and recording unauthorized access.

6.8. Time-stamping

(1) The Provider provides Subscribers with the service of time and date stamping of the submission of an electronic document signed with a private key corresponding to the public key, included in the certificate issued by the Provider.

(2) The procedure of time stamping and the provision of an independent time source are performed personally by the Provider.

(3) The system of the Provider for time-stamping (Time Stamp Server) is developed in accordance with IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) and the service is also provided in compliance with IETF RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs).

6.8.1. Procedure for providing the time stamping service

(1) The system of the Provider, which ensures the time-stamping service (Time Stamp Server), accepts requests and sends back replies in a format
defined in RFC 3161 - „Internet X.509 Public Key Infrastructure - Time-Stamp Protocol“.

(2) The request must include hash of the electronic signature on the certificate to be time stamped, and a version of the request form.

(3) Optionally, it may include also a request for inclusion in the reply to the signing certificate together with the chain of certificates of the Certification Authority.

(4) The request for time-stamping can be generated through the web site of the Provider at: http://www.infonotary.com or through specialized client software of “INFONOTARY” Ltd.

(5) The submitted requests are processed consecutively.

(6) The time stamp provided by the Provider certifies the exact time and date of the registration of the client’s electronic document in the Time Stamp Server of the Provider.

(7) The time stamp issued by the Provider is with an allowance of 1 second only.

(8) The time stamp certificate issued by the Provider includes the following:

□ status – a whole number indicating if the signing has been completed successfully.
□ Version of the time-stamp certificate (version 1);
□ The hash of the signature contained in the request;
□ Unique consecutive serial number;
□ Time of signing - GMT;
□ Identification of the Timestamp certifying authority – the Provider.

(9) The time-stamp certificate is signed with a private key of the Provider, designed only for this activity.

(10) The whole process of signing the time stamp certificates is performed by a hardware protected module with a high level of reliability and security.
(11) The system of the Provider for creating time-stamp certificates is in a high physical and technological access control mode, and is stored in a special room with control of the access of unauthorized employees.

6.8.2. Independent Time Synchronizer

(1) The Provider operates its own Independent Time Synchronizer, maintaining the following protocols:

- NTPv2 (RFC 1119)
- NTPv3 (RFC 1305)
- NTPv4 (IETF Draft Standard)
- SNTP (RFC 2030)
- Daytime Protocol (RFC 876)
- Time Protocol (RFC 868)
- SNMPv1 (RFC 1157), SNMPv3 (RFC 3411-3415)

(2) The system is synchronized with respect to accuracy via GPS, synchronization by other NTP servers or Dial-up connections.

(3) All data about the exact time transmitted by the Time Synchronizer to the TimeStamp server are encrypted by the synchronizer itself and modification- and discreditation-protected.

(4) The Independent Time Synchronizer System of the Provider is under high control of physical and technological access regime and is kept in specialized premises with authorized person access control.
7. CERTIFICATE PROFILE, LIST OF SUSPENDED AND REVOKED CERTIFICATES AND ON-LINE STATUS CHECK PROTOCOL

7.1. Certificate profile

(1) The certificates, issued by the Provider in line with the User Manual comply with the requirements of the Law on Electronic document and electronic signature and the ordinances related thereto on advanced electronic signature certificates.

(2) The following standards are implemented and used in universal electronic signature certificates issued by the Provider:

- ETSI TS 456 (2002-04) “Policy requirements for certification authorities issuing qualified certificates”;
- ETSI TS 101 862 V1.2.1 (2001-06) “Qualified Certificate Profile”;
- ETSI TR 102 153 V1.1.1 (2003-02) “Electronic Signatures and Infrastructures (ESI); Prestudy on certificate profiles”;
- IETF PKIX RFC 3039 “Internet X.509 Public Key Infrastructure Qualified Certificates profile”;
- IETF PKIX RFC 3279 “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profiles”;

7.1.1. Version Number

(1) The Provider issues certificates in X.509 v.3 format.

(2) The certificate version number is written in the certificate itself.
7.1.2. Certificate Extensions

7.1.2.1. Mandatory Extensions

7.1.2.1.1. “Basic Constraints” Attribute

This attribute specifies the certificate holder type – Certification Authority or end user. The attribute is “Critical”.

7.1.2.1.2. “Key Usage” Attribute

(1) It defines the constraints in certificate usage according to the key use designation. This attribute is “Critical”.

(2) The attribute is used to limit the key use according to the possible usages:

- Digital Signature – for authentication;
- Non-repudiation – to prove the electronic signature use;
- Key encipherment – for key encipherment;
- Data encipherment – for data encipherment;
- Key Certificate Signing (electronic certificate signing) – only used by Provider's Certification Authorities;
- CRL Signing (electronic signing of a List of Suspended and Revoked Certificates) – for CRLs signing, only used by Certification Authorities.

7.1.2.1.3. “Extended Key Usage” Attribute

The attribute is used to specify the applications in which the key may be used – protection of electronic correspondence, electronic authentication, etc.

7.1.2.1.4. “Subject Key Identifier” Attribute

The attribute contains SHA1 of the DER-coded public key.
7.1.2.1.5. “cRL Distribution Points” Attribute

The attribute contains a link to the List of Suspended and Revoked Certificates, maintained by the Provider.

7.1.2.1.6. “Authority Info Access” Attribute

The attribute contains a link to the OCSP service maintained by the Provider and submitting certificate status information through OCSP.

7.1.2.1.7. “Qualified Certificate Statement” Attribute

The attribute is mandatory for universal electronic signature certificates, issued by the Provider and contains information whether the certificate is issued for universal electronic signature.

7.1.2.1.8. “Certificate Policy” Attribute

(1) The attribute specifies the certificate issuance policies of the Provider.

(2) The attribute contains identifier (OID) of the respective certification policy according to the certificate type.

(3) In universal electronic signature certificates this attribute contains as well OID marked information concerning:

- Provider registration by the Communication Regulation Commission;
- link to the Provider's certificate included in the Directory of Certification Service Provider Certificates, maintained by the CRC;
- certificate type – universal electronic signature certificate with Secure Signature Creation Device (SSCD).

7.1.3. Electronic Signature Algorithm Identifiers

The electronic signature algorithm identifier identifies:

1. Hash-function: sha1;

2. Encryption algorithm: RSA/DSS.
7.1.4. Naming Forms
See cl. 3.1.3 of the Document.

7.1.5. Name limitations
See cl. 3.1.4 of the Document.

7.2. Profile of the List of Suspended and Revoked Certificates

7.2.1. Version number
(1) The lists of suspended and revoked certificates maintained by the Provider in the Public Directory of Certificates are in X.509 v.2 format.

(2) The version number is written in the certificate.

7.2.2. Attributes of the List and of the certificates published therein

7.2.2.1. List attributes

7.2.2.1.1. Main x509 CRL attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2 (0x01)</td>
</tr>
<tr>
<td>Publication date</td>
<td>Date and time of signing of the CRL</td>
</tr>
<tr>
<td>Subsequent publication date</td>
<td>Date and time of signing of the CRL + 24 hours</td>
</tr>
<tr>
<td>Electronic signature algorithm on CRL</td>
<td>rsaWithSHA1</td>
</tr>
</tbody>
</table>
7.2.2.1.2. Additional List Attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/authorityKeyIdentifier</td>
<td>2.5.29.35</td>
<td>&quot;subjectKeyIdentifier&quot; of the signing certificate of the issuer</td>
</tr>
<tr>
<td>/cRLNumber</td>
<td>2.5.29.20</td>
<td>Number of the CRL published in the Public Certificate Directory of the Provider; 20-byte number</td>
</tr>
</tbody>
</table>

7.2.2.1.3. Attributes of the certificates included in the list:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial number</td>
<td>Unique certificate number in the Provider's directory; 8-byte number</td>
</tr>
<tr>
<td>Revocation date</td>
<td>Date, hour and minute of certificate revocation</td>
</tr>
<tr>
<td>Reason for revocation</td>
<td>KeyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, privilegeWithdraw</td>
</tr>
</tbody>
</table>

Meaning of the certificate suspension and revocation keys:

- **KeyCompromise** – compromised private key of the Author;
- **cACompromise** – compromised private key of the certification authority;
- affiliationChanged – changed status of the Author with respect to the Holder – change in the representative power, deprivation of the representative power, discontinuation of the labour contract, etc.;
- superseded – the certificate is replaced with another one;
- cessationOfOperation – with expired validity term;
- certificateHold – the certificate is suspended;
- privilegeWithdrawn – the certificate is with access limitation.

7.3. OCSP Profile

7.3.1. OCSP Order Profile

7.3.1.1. Order Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1 (0x00)</td>
</tr>
<tr>
<td>Ordering person</td>
<td>Ignored</td>
</tr>
<tr>
<td>List of certificate identifiers</td>
<td>according to RFC 2560 (see 1.2)</td>
</tr>
<tr>
<td>Order extensions</td>
<td>Ignored</td>
</tr>
</tbody>
</table>

7.3.1.1.1. Certificate Identifier (ESC)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic check-sum (CCS) algorithm</td>
<td>SHA-1</td>
</tr>
<tr>
<td>ESC issuer</td>
<td>SHA-1 of the DER-coded DN of issuer</td>
</tr>
<tr>
<td>ESC issuer CCS key</td>
<td>SHA-1 of the DER-coded subjectPublicKeyInfo of issuer (without T and L).</td>
</tr>
<tr>
<td>ESC serial number</td>
<td>Unique for the Provider's directory; 8-byte number</td>
</tr>
</tbody>
</table>
7.3.2. OCSP Response Profile

7.3.2.1. Common attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>successful – in line with RFC 2560</td>
</tr>
<tr>
<td></td>
<td>malformedRequest – in line with RFC 2560</td>
</tr>
<tr>
<td></td>
<td>internalError – not used</td>
</tr>
<tr>
<td></td>
<td>tryLater – not used</td>
</tr>
<tr>
<td></td>
<td>sigRequired – not used</td>
</tr>
<tr>
<td></td>
<td>unauthorized – not used</td>
</tr>
<tr>
<td>Response type</td>
<td>id-pkix-ocsp-basic (1.3.6.1.5.5.7.48.1.1)</td>
</tr>
<tr>
<td>Response (see 2.2)</td>
<td>in line with RFC 2560</td>
</tr>
</tbody>
</table>

7.3.2.2. Response attributes in line with id-pkix-ocsp-basic (1.3.6.1.5.5.7.48.1.1)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data to the response (see 7.3.3)</td>
<td>in line with RFC 2560</td>
</tr>
<tr>
<td>Algorithm of electronic signature on the response</td>
<td>FIPS-186 DSS;</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>in line with RFC 2560</td>
</tr>
<tr>
<td>List of issuer’s certificates</td>
<td>not used</td>
</tr>
</tbody>
</table>

7.3.3. Data to the OCSP Response

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1 (0x00)</td>
</tr>
<tr>
<td>OCSP Responder identifier</td>
<td>DN of the signing ESC</td>
</tr>
<tr>
<td>Publication date</td>
<td>Date, hour and minute of signing of the response</td>
</tr>
<tr>
<td>Individual responses (see 2.4)</td>
<td>in line with RFC 2560</td>
</tr>
<tr>
<td>Extensions</td>
<td>not used</td>
</tr>
</tbody>
</table>
### 7.3.4. Individual OCSP responses

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESC identifier</td>
<td><em>in line with RFC 2560 (see 7.3.1.1.1)</em></td>
</tr>
<tr>
<td>Status</td>
<td><em>good – in line with RFC 2560</em></td>
</tr>
<tr>
<td></td>
<td><em>revoked – in line with RFC 2560</em></td>
</tr>
<tr>
<td></td>
<td><em>unknown – in line with RFC 2560</em></td>
</tr>
<tr>
<td>Publication date</td>
<td><em>Date, hour and minute of signing of the CRL</em></td>
</tr>
<tr>
<td>Subsequent publication date</td>
<td><em>Date and time of signing of the CRL + 24 hours</em></td>
</tr>
<tr>
<td>Extensions</td>
<td><em>not used</em></td>
</tr>
</tbody>
</table>
8. AUDITING AND CONTROL OF THE ACTIVITY

8.1. Scheduled or unscheduled audits

(1) Under LEDES, the Communications Regulating Commission exercises control of the activity of the Provider as a registered certification services provider.

(2) The activity of the Provider is subject to constant internal control exercised by the Board of Directors of ‘INFONOTARY’ Ltd.

(3) For the purposes of internal control, the Board of Directors of ‘INFONOTARY’ Ltd. appoints scheduled (routine) or unscheduled audits in the order and range according to the internal regulations of the Provider.

(4) The Provider exercises constant control of the activity of the Registration Authorities..

8.2. Qualifications of the auditors

(1) For the purpose of exercising internal control, parties that meet the requirements of Art.32, par.2.4 of LEDES and Part 5 of OACSP, or auditors, licensed by an international accreditation organization, may be appointed to perform the audit.

(2) The activity of the Registration Authorities is audited by employees of the Provider, especially authorized by the governing body of the Provider, or by independent auditors not affiliated with the Provider.

8.3. Relationships between the auditor and the audited organization

(1) The auditors appointed to perform an audit have to be independent, directly or indirectly not affiliated with the Provider and having no conflicting interests with the Provider.
(2) The relationships between the independent auditors and the Provider are regulated by a written agreement.

8.4. Scope of the audit

(1) The scope of the performed audits depends on the type of exercised control and the audited authorities.

(2) All activities, documents and circumstances concerning the functioning of the Provider are within the scope of the audit. The may include, but not be limited to:

- Compliance of the operational procedures and principles of work of the Provider with the procedures and policies set out in the User Manual;
- The management of the infrastructure included in the provision of certification services.

8.5. Measures for correcting established defects

The Board of Directors of ‘INFONOTARY’ Ltd. determines the measures that need to be taken for the correction of the established customers and the terms for their correction.

8.6. Announcing the results

The results from the audits are stored under the conditions and in the order provided in the User Manual.

9. OTHER BUSINESS AND LEGAL PROVISIONS

9.1. Fees and prices

(1) The Provider determines the prices and the subscription fees for using the universal electronic signature certification services provided by him, and

(2) The Provider reserves the right to change unilaterally the Tariff for providing electronic signature certification services at any time during the term of the contract; the changes are approved by the Board of Directors of ‘INFO NOTARY’ Ltd. and are published and available at the following URL address: http://www.infonotary.com/.

(3) The Provider notifies the Holders of such changes individually or by publishing the said changes. These changes become effective with regard to the Holder as of the day following the day of notification or publication.

(4) The changes are in force from the date they become effective onwards, and do not apply to single or subscription fees already paid in advance prior to the date on which the change becomes effective.

9.1.1. Remuneration under Contract for providing certification services

(1) The remuneration under Contract for providing certification services, concluded between the Holder and the Provider, is formed by the amounts payable by the Holder for the provision of the services he has requested, on the basis of the Tariff for providing electronic signature certification services and the request form signed by the Holder.

(2) Subscription fees or amounts paid in advance are not refundable, if for the period for which they have been paid the provided services have not been used.

(3) All amounts due pursuant to the Contract are paid by the Holder as bank transfer. The transfer is deemed effected upon receiving a bank statement certifying that the whole amount due has been transferred into the specified account of the Provider.
9.1.2. Invoicing

The Provider issues to the Holder a tax invoice for the provided services within 5 days of the payment.

9.1.3. Certificate returning and payment refunding policy

If, within 3 days of publishing a certificate in the Register, the Holder or the Author of a universal electronic signature certificate makes claims regarding incorrect or incorrect information contained in the certificate, the Provider suspends the said certificate and issues a free new one, or refunds the amount paid for the issuance of the certificate, subject of the claim.

9.2. Financial responsibilities

9.2.1. Insurance of the activity

(1) The Provider holds a valid mandatory insurance policy as of the time of submitting the application form for registration as a Provider of certification services to CRC.

(2) The subject of the mandatory insurance policy is the responsibility of the Certification Services Provider, issuing universal electronic signature certificates for the activity exercised by him under LEDES, in accordance with the requirements of Art.29 of the Law for electronic document and the electronic signature:

(3) The mandatory insurance covers the liability of the Provider for property or non-property damage caused to the Holder and to all Relying Parties within the scope under cl.9.6.1 of the User Manual and the limits set out in Art.29 of LEDES.

(4) The Provider holds an insurance policy for 600 000 (six hundred thousand) leva for each affected party by any circumstance for each electronic
signature certificate issued without limitations to the validity of the signature to a certain property interest.

(5) In case of event that may result in a claim covered by the insurance policy, the affected party has to notify the Provider and the Insurer immediately, within 7 days of becoming aware of the event.

9.2.2. Insurance contract cover for the end users

(1) Under the insurance policy of the Provider, all sums which do not exceed the indemnity limit are subject to indemnity. The Provider shall pay these sums as compensation for property and/or non-property damage, caused to the Holder of the universal electronic signature certificate and to all third parties as a result of negligence or fault in performing the insured activity for which the Provider is responsible in accordance with the Bulgarian legislation or the legislation of the country in which the damage has occurred.

(2) The insurance policy does not cover, and the Provider is not responsible for the events under cl.9.7. of the User Manual, in particular for damage resulting from:

- Failure on behalf of Holders and Authors to fulfil their obligations according to the User Manual;

- Compromise or loss of a private key of a Holder, respectively Author, due to negligence in keeping or using it;

- Failure on behalf of the Relying Parties to comply with the requirements for taking due care to check the validity of the electronic signature and of the certificate issued by the Provider;

- Force majeure circumstances, accidents and other events beyond the control of the Provider.
9.3. Privacy of information

The Provider adheres to all applicable rules for personal data protection and privacy of information gathered in view of his activity, as set out in the User Manual.

9.3.1. Scope of confidential information

The Provider deems confidential any information obtained in and concerning:

► Any information about the Holder apart from the information provided in the certificate;
► The reason for suspending or revoking certificates other than the published information about the status of the certificate;
► Correspondence connected with the activity of the Provider;
► The private keys of the Provider;
► The contract for providing certification services;
► Repositories for applications for issuance, suspension, renewal and revocation of certificates;
► Records of transactions;
► Records of internal and external audits and reports;
► Plans for recovery after disasters and unforeseen events.

9.3.2. Information outside the scope of the confidential information

The following are not deemed confidential:

☐ Certificates published in the register of the Provider;
□ Data provided in the certificates;

□ Information on the status of the certificates published in the List of suspended and revoked certificates.

9.3.3. Obligation to protect confidential information

(1) The Provider does not disclose and cannot be asked to disclose or submit to third parties any confidential information, unless he is obliged to disclose such information to a competent authority in accordance with a special law.

(2) The Registration Authorities, Authors and Holders or persons authorized by them, have no right to disclose, or allow to be disclosed, information that has come to their knowledge in the process of fulfilling or in connection with their obligations under contracts with the Provider, without the prior written consent of the other party.

9.4. Privacy of personal data

(1) The information gathered by the Provider about the Holder and Author is only for the purposes of issuing and maintaining electronic signature certificates.

(2) Information included in the electronic signature certificates and information on the status of the certificates may contain personal data about the Author and Holder in the meaning of the Personal Data Protection Act.

(3) The Provider stores and processes the personal data about the Holder and the Author in data bases and ensures access of third parties to the data.

(4) The Provider is registered as personal data administrator by the Personal Data Protection Commission in the order provided by PDPA.

(5) Information about the Author and the Holder gathered by the Provider but not included in the universal electronic signature certificate and the
information about the status of a certificate is deemed personal data in the meaning of the Personal Data Protection Act. It is gathered only for the purpose of issuing and maintaining a certificate and cannot be used for other purposes or disclosed to third parties without the explicit consent of the persons who have provided the information, or if permitted by the law.

(6) The Provider informs the Author or Holder of a universal electronic signature certificate in advance about the kinds of information gathered on them, the way of storing it and the access of third parties to it.

(7) By signing the Contract for providing certification services and the acceptance of the provisions of the User Manual, the Holder and Author agree their personal data gathered by the Provider to be included in the universal electronic signature certificate and to be accessible and available to all interested parties in the Register of certificates and the List of suspended and revoked certificates.

9.5. Intellectual property rights

(1) The Provider has and retains all intellectual property rights on the database, Internet sites, electronic signature certificates, issued by the Provider, as well as on all other documents generated by the Provider, including the User Manual.

(2) The Provider permits the download, copy and distribution of the certificates issued by him, the access to which is not restricted by the Holder, on condition that they are copied and distributed in full.

(3) All rights to trade marks, brand names and logos are reserved by the holders of these rights. The Provider uses the subjects of these rights only for the purpose of providing certification services.

(4) The private and public keys, as well as the means of access to them (PIN codes, passwords, etc.) are property of their Holders who use and store them in an appropriate way.

(5) Key pairs, as well as the shared secrets of the private keys, are property of the Provider.
9.6. Responsibility and Warranties

9.6.1. Responsibility and warranty of the Provider

(1) The Provider warrants that he adheres to all the provisions and requirements of the User Manual, strictly follows the procedures provided hereunder, and pursues the policies established in the Certification policies for the different kinds of certificates regarding their issuance and management.

(2) When issuing a certificate, the Provider guarantees the correctness and currency of the information contained in the certificate at the time of its validation and in accordance with the policy of issuing the certificate.

(3) For the issuance of universal electronic signature certificates, the Provider is responsible to the Holder and the Relying Parties for damage:

1. resulting from failure to meet the requirements under Art.21 of LEDES and his obligations under Art.22 and 25 of LEDES and the User Manual.

2. resulting from incorrect or missing information in the certificate at the time of its issuance.

3. incurred by them, in the case that at the time of issue of the certificate the person nominated as Author did not have the private key corresponding to the public key included in the certificate issued by the Provider, if the Provider has shown negligence in validating this circumstance.

4. resulting from discrepancies between the data for validating the use of the private key, and the data provided to the person using the public key.

9.6.2. Warranty and responsibility of the Registration Authority

The Provider guarantees that the Registration Authorities perform their functions and obligations in compliance with the User Manual, the applicable policies for the issuance of the certificates and the respective internal procedures and documents.
9.6.3. Responsibility of the Holder and the Author to third parties

(1) The Holder is responsible to third conscientious parties, when, in generating the public and private key pair he has used an algorithm which does not meet the requirements of OACSP.

(2) The Holder is responsible to third conscientious parties if the Author:

□ does not adhere strictly to the security requirements, determined by the Provider;

□ does not request that the Provider revoke the certificate, when he has established an unauthorized use of the private key, or there is a possibility of such unauthorized use.

(3) The Holder who has accepted the certificate upon its issuance is responsible to third conscientious parties and to the Provider:

□ if the Author is not authorized to keep the private key corresponding to the public key included in the certificate;

□ for misrepresentation before the Provider concerning the content of the certificate.

(4) The Author who has accepted the certificate upon its issuance is responsible to third conscientious parties and to the Provider, if he has not been authorized to request the issuance of the certificate.

(5) The Holder, respectively the Author, is responsible to the Provider if he has accepted the certificate issued by the Provider on the basis of false information presented by him, respectively on the basis of incomplete or concealed information.

(6) In all cases of failure on behalf of the Holder, respectively the Author, to fulfil his obligations pursuant to the User Manual or the Contract for providing certification services, the Provider shall hold the Holder responsible for damage.
9.6.4. Care provided by the Relying Parties

(1) The parties, relying on the universal electronic signature certification services of the Provider have to take due care by:

- having technical skills to use the electronic signature certificates;
- being informed about the conditions on which they have to rely on the certificates, in accordance with the policy for issuing the certificates and the procedures for validating the information by the Provider;
- validating certificates issued by the Provider through the data about the status of the certificates published by the Provider – the List of suspended and revoked certificates;
- relying on the certificates issued by the Provider only if the result from their validation is correct and up-to-date..

(2) The Relying Parties have to verify the validity, suspension or revocation of the certificate through the updated information about their status and has to take into consideration and comply their actions with all the restrictions to the use of the certificate included in the certificate itself.

9.7. Waiver of responsibility

(1) The Provider shall not be held responsible for damage which has resulted from negligence, lack of care or lack of basic knowledge concerning the use of and work with the electronic signature certificates on behalf of the Holder, the Author or the Relying Parties.

(2) The Provider shall not be held responsible for damage resulting from the untimely revocation and suspension of certificates and verification of the status of the certificates for reasons beyond his control.
(3) The Provider shall not be held responsible if a certificate is used beyond the range of its purposes and restrictions to its use, included in the certificate.

(4) The Provider shall not be held responsible for any violation of the rights of third parties with regard to their trade marks, brand names or other property and non-property rights, when the information, provided in the certificate issued, has led to such violations.

(5) The Provider shall not be held responsible for any direct or indirect, predictable or unpredictable damage, ensuing from the use of or reliance on suspended, revoked or expired certificates.

(6) The Provider shall not be held responsible for the way of use and for the correctness, authenticity and completeness of information included in trial, free or demo certificates.

(7) The Provider shall not be held responsible for the security, integrity and use of the software products and hardware devices used by the Holder, the Author or the Relying Parties.

9.8. Limitations to the liability of the Provider

(1) The Provider sets limitations to the application of the certificates he issues to a certain material interest, in accordance with cl.1.4.2. of the User Manual and with reference to Art.24, par.1.8 of LEDES, and Art.29, par.3 of LEDES, and limits his liability for damage caused by the use of these certificates outside the scope of the restrictions, included in the certificates, to the effect of the signature.

(2) The limits to the universal electronic signature certificates in accordance with cl.3 must be included in the certificate, unless it is agreed that the certificate should be issued without limitations to its effect with regard to the value of the material interest, or the Holder has set a limit to the value of the transactions in which the certificate is used in the order provided in cl.1.4.2 of the User Manual.
(3) The maximum limits, within which the Provider shall be held responsible for damage ensuing from the use of universal electronic signature certificates issued by him with included limitations to its effect, are determined according to the type of certificates offered by the Provider, as shown in the table below:

<table>
<thead>
<tr>
<th>Type of certificate</th>
<th>Maximum limit to the liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal electronic signature certificate of a Physical person</td>
<td>100 000 leva</td>
</tr>
<tr>
<td>Universal electronic signature certificate of a Legal entity</td>
<td>100 000 leva</td>
</tr>
</tbody>
</table>

9.9. **Indemnity of the Provider**

In all cases of failure on behalf of the Holder, respectively the Author, to fulfil their obligations pursuant to the User Manual or the Contract for providing certification services, the Provider shall hold the Holder responsible for damage.

9.10. **Term and termination**

9.10.1. **Term**

(1) The provisions of the User Manual as well as the Practice for providing certification services and the Policy for certification services, included in the Manual, are in force till amended or information about their infirmity is published in the Document register and on the web site of the Provider.

(2) The term of validity of the Contract for providing certification services is 1 year, or until the expiry of the term of validity of all certificates issued pursuant to it.
9.10.2. Termination and invalidity

(1) The term of validity of the User Manual is terminated upon the termination of the activity of the Provider.

(2) If any of the clauses of this Manual proves to be invalid, this will not affect the validity of other clauses or parts of the Manual, nor will it result in the invalidation of the whole contract with an end user. The invalid clause will be replaced in compliance with the laws and regulations.

(3) The Contract for providing certification services is terminated upon the termination or expiry of all certificates issued pursuant to the contract, or if there are other reasons for its termination, set out in the User Manual.

9.10.3. Termination effect

After the term of validity of the User Manual is terminated, the provisions concerning the obligations of the Provider to keep archives of the documents and certificates in the scope and for the period of time specified in the Manual, remain effective.

9.11. Individual notification and correspondence between the participants

(1) All interested parties may send notifications to the Provider in connection with the provisions of the User Manual and the contracts in the form of signed electronic messages with a universal or an improved electronic signature, registered mail, our via couriers to the Provider.

(2) Individual notification of the Provider may be sent to the address for electronic correspondence: legal@infonotary.com or to the following mailing address: Sofia 1000, 16 ‘Ivan Vazov’ Street, 6 floor.

(3) For his correspondence with the Holders, the Provider uses electronic letters, signed with a universal electronic signature, registered mail, or letters sent via a courier.

(1) The User Manual can be modified at any time, and each modification is made after it is approved by the Communications Regulating Commission and is available and accessible to all interested parties at:: http://www.infonotary.com.

(2) Anyone can propose changes or modifications (to the structure and to the contents) or comment on established errors in the electronic and mailing addresses for contacts with the Provider, provided in cl.9.11.

9.13. Resolution of disputes and jurisdiction

All disputes which arise between the Parties in connection with the Contract for providing certification services, shall be settled through negotiations between the Parties in the spirit of good will, but if no agreement is reached, the disputes shall be resolved by the competent Bulgarian court.


All issues which are not settled in this User Manual shall be interpreted and resolved in compliance with the Bulgarian laws.

9.15. Compliance with the governing law

This User Manual is elaborated in compliance with the provisions of the Law for Electronic Document and Electronic Signature, the Ordinance for the Activity of Certification Services Providers, the order for its termination and the conditions for providing certification services, the Ordinance for Registration of Certification Services Providers, the Ordinance for Algorithms for Improved Electronic Signature, and the effective Bulgarian laws.
III. POLICY FOR PROVIDING UNIVERSAL ELECTRONIC SIGNATURE CERTIFICATION SERVICE

(1) The “Policy for providing universal electronic signature certification service” is a document which is an integral part of the User Manual, in which the policy and procedures followed by the Provider when issuing certificates, as well as the application and use of the issued certificates in view of the security of these procedures, are set out.

(2) The Provider develops and follows a different certification policy for each type of certificates he issues.

(3) The certification policy for a certain type of certificate includes the rules for performing the initial validation and authentication of the Holders and Authors of electronic signature certificates, as well as the policy of management of the issued certificates – suspension, revocation and renewal of the certificates issued by the Provider.

(4) The certification policy for each type of certificate also determines the limitations to the application of the certificates depending on the security levels during the checks and the level of reliance on the facts certified in the issued document.

(5) The certification policies of the universal electronic signature certificates also contain the conditions and order for using the universal electronic signature and the requirements for storing the private key.

I.1. Policy for issuing and management of a universal electronic signature certificate of a Physical person

I.1.1. General characteristics of the certificate
(1) The i-Notary Personal Q Sign Certificate has the characteristics of a universal electronic signature certificate in the meaning of Art.24 of LEDES, and every electronic signature accompanied by this certificate has the effect of a universal signature.

(2) The universal electronic signature certificate of a Physical person (i-Notary Personal Q Sign) is issued to a physical person – Holder or Author, and certifies the identity and connection with his public key.

(3) The i-Notary Personal Q Sign Certificate is issued with generated and stored on a cryptographic device (smart card) pair of cryptographic keys – private and public, used for the creation and verification of a universal electronic signature.

(4) For the issuance of i-Notary Personal Q Sign Certificate, different procedures are applied which ensure high level of reliability and security of the certified information identifying the Holder and Author and the possession of the means for creating an electronic signature – the private key.

(5) The procedures of identification and establishing the identity of the Holder and the Author require submission of evidence of the identity of the Holder, the identity of the Author, as well as of the representative authority of the Author and their personal appearance before Suppliers’ registration authority.

I.1.2. Purpose and application of the certificate

(1) The i-Notary Personal Q Sign Certificate can be used as a means of personal electronic identification in electronic trading, financial transactions, electronic correspondence, electronic signing of documents, notifications from and to government authorities and local authorities in the meaning of LEDES.

(2) It is within the responsibilities of the relying Party to check the purpose and application of this certificate when relying on the electronic signature, accompanied by the certificate.

(3) For the purpose of the check and verification by the relying Party, the certificate includes the policy applicable to this certificate (“Certificate Policy”), and additions to it and the application and limitations to the usage of the
certificate, described in the attributes “Key Usage”, “Extended Key Usage”, “Qualified Statements”.

I.1.3. Denotation and designation

(1) The policy applicable to this certificate is denoted in the following way:

<table>
<thead>
<tr>
<th>Type of policy</th>
<th>Denotation</th>
<th>Designation (OID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification policy for a universal electronic signature certificate of a physical person</td>
<td>i-Notary Personal Q Sign Certificate CP</td>
<td>1.3.6.1.4.1.22144.1.1.1.1</td>
</tr>
</tbody>
</table>

(2) The policy is published in the Public document register of the Provider and is available at the following address: http://repository.infonotary.com/certpolicy_qsign_personal.html

I.1.4. Personal Q Sign Certificate Profile

Root x509 attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3 (0x02)</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique in the Provider’s directory; 8-byte number</td>
</tr>
<tr>
<td>Beginning of the validity period</td>
<td>Date and hour of signing the ESC</td>
</tr>
<tr>
<td>End of the validity period</td>
<td>Date and hour of signing the ESC + 1 year</td>
</tr>
<tr>
<td>Algorithm of electronic signature on ESC</td>
<td>FIPS DSS; dsaWithSHA1 (1.3.14.3.2.27) or RSA – 2048 bits</td>
</tr>
</tbody>
</table>

Issuer Attributes (x509 Issuer DN)
The issuer attributes coincide with the attributes of the signing electronic signature certificate Holder (ESC).

Attributes of the Holder/Author (x509 Subject DN):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M¹</th>
<th>T/A²</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>2.5.4.3</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/countryName</td>
<td>2.5.4.6</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/postalCode</td>
<td>2.5.4.17</td>
<td></td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/localityName</td>
<td>2.5.4.7</td>
<td></td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>2.5.4.9</td>
<td>+</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/organizationName</td>
<td>2.5.4.10</td>
<td>+</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/organizationalUnitName</td>
<td>2.5.4.11</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/emailAddress</td>
<td>1.2.840.113549.1.9.1</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/telephoneNumber</td>
<td>2.5.4.20</td>
<td></td>
<td>T</td>
<td></td>
</tr>
</tbody>
</table>

Additionally defined organization attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgBulstatNumber</td>
<td>2.5.4.10.100.1.1</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>2.5.4.10.100.1.2</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgBankAddressableUnit</td>
<td>2.5.4.11.100.1.2</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgBudgetIdentificationNumber</td>
<td>2.5.4.11.100.1.1</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>2.5.4.10.100.1.3</td>
<td></td>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>

Additionally defined natural person attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M¹</th>
<th>T/A²</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgUnifiedCitizenNumber</td>
<td>2.5.4.3.100.1.1</td>
<td>+</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/bgIdentificationCardNumber</td>
<td>2.5.4.3.100.1.2</td>
<td></td>
<td>T</td>
<td></td>
</tr>
</tbody>
</table>

¹ Mandatory
² Holder/Author
### Attributes of the Author (x509v3 subjectAltName extension DN):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>T/A</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>2.5.4.3</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/countryName</td>
<td>2.5.4.6</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/postalCode</td>
<td>2.5.4.17</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/localityName</td>
<td>2.5.4.7</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>2.5.4.9</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/organizationName</td>
<td>2.5.4.10</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/organizationalUnitName</td>
<td>2.5.4.11</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/emailAddress</td>
<td>1.2.840.113549.1.9.1</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/telephoneNumber</td>
<td>2.5.4.20</td>
<td></td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

**Additionally defined organization attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>T/A</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgBulstatNumber</td>
<td>2.5.4.10.100.1.1</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>2.5.4.10.100.1.2</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgBankAddressableUnit</td>
<td>2.5.4.11.100.1.2</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgBudgetIdentificationNumber</td>
<td>2.5.4.11.100.1.1</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>2.5.4.10.100.1.3</td>
<td></td>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>

**Additionally defined natural person attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>T/A</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgUnifiedCitizenNumber</td>
<td>2.5.4.3.100.1.1</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/bgIdentificationCardNumber</td>
<td>2.5.4.3.100.1.2</td>
<td></td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>
### Additional x509 attributes (x509v3 extensions):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>C³</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/basicConstraints</td>
<td>2.5.29.19</td>
<td>+</td>
<td>+</td>
<td>CA=false</td>
</tr>
<tr>
<td>/keyUsage</td>
<td>2.5.29.15</td>
<td>+</td>
<td>+</td>
<td>Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment</td>
</tr>
<tr>
<td>/extKeyUsage</td>
<td>2.5.29.37</td>
<td>+</td>
<td></td>
<td>emailProtection, clientAuth</td>
</tr>
<tr>
<td>/authorityKeyIdentifier</td>
<td>2.5.29.35</td>
<td></td>
<td></td>
<td>subjectKeyIdentifier of the signing ESC</td>
</tr>
<tr>
<td>/subjectKeyIdentifier</td>
<td>2.5.29.14</td>
<td>+</td>
<td></td>
<td>SHA1 of the DER-coded public key</td>
</tr>
<tr>
<td>/cRLDistributionPoints</td>
<td>2.5.29.25</td>
<td>+</td>
<td></td>
<td><a href="http://crl.infonotary.com/crl/qsign-personal-ca.crl">http://crl.infonotary.com/crl/qsign-personal-ca.crl</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ldap://ldap.infonotary.com/dc=qsign-personal-ca,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dc=infonotary,dc=com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://crl.infonotary.com/crl/qsign-personal-ca.crl">http://crl.infonotary.com/crl/qsign-personal-ca.crl</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ldap://ldap.infonotary.com/dc=qsign-personal-ca,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dc=infonotary,dc=com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://ocsp.infonotary.com/responder.cgi">http://ocsp.infonotary.com/responder.cgi</a></td>
</tr>
<tr>
<td>/qcStatements</td>
<td>1.3.6.1.5.5.7.1.3</td>
<td>+</td>
<td></td>
<td>0.4.0.1862.1.1</td>
</tr>
</tbody>
</table>

**Certificate Policies x509v3 extension:**

³ Critical
Identifier (OID) | 1.3.6.1.4.1.22144.0
---|---
CPS | http://www.crc.bg
Text | Registration Resolution № ……by the Communications Regulation Commission

Identifier (OID) | 1.3.6.1.4.1.22144.1.1.1.1
---|---
CPS | http://repository.infonotary.com/certpolicy_qsign_personal.html
Text | InfoNotary personal qualified certificate

Identifier (OID) | 0.4.0.1456.1.1
---|---
CPS | http://www.infonotary.com/qcp-sscd.html
Text | This certificate is issued as qualified certificate for advanced electronic signature using secure storage cryptographic device

**Description and application of the attributive OID, used in Certificate RDN**

**Attribute description**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>P&lt;sup&gt;i&lt;/sup&gt;</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>2.5.4.3</td>
<td></td>
<td>Subject name</td>
</tr>
<tr>
<td>/countryName</td>
<td>2.5.4.6</td>
<td></td>
<td>Country code</td>
</tr>
<tr>
<td>/postalCode</td>
<td>2.5.4.17</td>
<td></td>
<td>Postal code</td>
</tr>
<tr>
<td>/localityName</td>
<td>2.5.4.7</td>
<td></td>
<td>City/District</td>
</tr>
</tbody>
</table>

<sup>i</sup>Own (Provider-defined as an extension of existing X.500 attribute)
### Format description and attribute formation

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Format</th>
<th>S</th>
<th>Pr</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>A+</td>
<td></td>
<td></td>
<td>Author’s full name</td>
</tr>
<tr>
<td>/countryName</td>
<td>A2</td>
<td></td>
<td></td>
<td>Two-symbol country code</td>
</tr>
<tr>
<td>/postalCode</td>
<td>N4</td>
<td></td>
<td></td>
<td>Holder’s/Author’s postal code</td>
</tr>
<tr>
<td>/localityName</td>
<td>AN+</td>
<td></td>
<td></td>
<td>Holder’s/Author’s city</td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>AN+</td>
<td></td>
<td></td>
<td>Holder’s/Author’s address data</td>
</tr>
</tbody>
</table>

*S: Separator,*  
*Pr: Prefix*
### Format Table

<table>
<thead>
<tr>
<th>Format</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>The attribute may only take alphabetic character values</td>
</tr>
<tr>
<td>N</td>
<td>The attribute may only take numeric values</td>
</tr>
<tr>
<td>AN</td>
<td>The attribute may take alpha-numeric values</td>
</tr>
<tr>
<td>IA5</td>
<td>The attribute may take valid IA5 character values (e-mail/url)</td>
</tr>
</tbody>
</table>

- The number following the format designation gives the maximum permitted number of characters.
- The character " + " stands for one or more characters.
Each field except those marked as IA5, contains data in UTF-8 encoding.

The data in the validity fields are presented as ASN1 GeneralTime.

I.1.5. Application Procedure for Certificate Issuance

(1) The registration authorities of the Provider accept and process all applications for universal electronic signature certificate issuance by end users.

(2) All persons may submit application to the Provider for certificate issuance, who:

► fill-in Certificate Issuance Application Form;

► generate a pair of cryptographic keys, either independently, or through the Provider;

► submit to the Provider’s certification authority the public key, corresponding to the private key;
► accept the terms and conditions of the Certification Services Provision Contract and the User Manual of the Provider.

(3) The Certificate Issuance Application should contain the following data:

- information identifying the Holder and, if the Author is different from the Holder – information about the Author as well;

- the public key, corresponding to the private key of the pair of cryptographic keys, generated by the Holder;

- the selected certificate type.

(4) The Certificate Issuance Application is an electronic document in PKCS #10 format, signed with the private key, corresponding to the public one included in the document.

(5) The Certificate Issuance Application may be generated via the Provider’s website and submitted to it via an encrypted communication channel to: https://www.infonotary.com.

(6) The registration authorities of the Provider render to all persons the service of cryptographic key pair generation, generation of application for certificate issuance and their submission to the Provider.

(7) When the registration authority of the Provider performs cryptographic key pair generation by request of the Holder, it makes use of a protective mechanism for their generation and submits them to the Author recorded on cryptographically protected device – smartcard, etc.

(8) The private key access rights – PIN-code or password are submitted by the registration authority of the Author in protected form.

(9) After the registration authority submits the device, on which the private key and the access rights thereto are recorded, the Holder and the Author are fully responsible for prevention of compromising, loss, disclosure, modification or other unauthorized use of their private key.

I.1.6. Approval or Rejection of Certificate Applications
(1) In order to establish and confirm the identity of a natural person who has submitted application for issuance of a certificate, Provider-defined procedures and rules are applied.

(2) The checking and confirmation of the information are performed by the registration authority in line with the Provider's rules and procedures and in full compliance with the User Manual and other internal documents.

(3) The registration authority checks and confirms the following information, identifying the natural person – Holder, Author or authorized representative of the Holder:

- Christian name, parental name and surname;
- date of birth;
- place of birth;
- nationality;
- gender;
- address, city, country, postal code;
- Personal number (PN);
- number of identity document: identity card, passport;
- issuing authority, date of issuance and validity of the identity document;
- the representative authority of the Author and/or Representative;
- contact and invoicing information.

(4) The Holder, the Author or the authorized representative of the Holder submits personally before the Registration authority the following documents:

- valid identity document: identity card or passport;

- notarized power of attorney authorizing the Representative to represent the Holder before the Provider for certificate issuance and management;
□ document certifying the representative power of the Author – court ruling, certificate of current status, notarized power of attorney or other empowering act.

(5) Prior to approval of a submitted application for issuance of a certificate the Registration authority of the Provider performs the necessary check-ups, namely:

► checks-up and confirms the identity of the Applicant, Author, Holder or the person representing him/her on the basis of the documents, submitted thereby;

► checks-up and confirms the representative authority of the Author and of the person, authorized to represent the Holder;

► checks-up the correctness of the received or filled-in and signed electronic application (in PKCS#10 format) for issuance of certificate;

► submits to the Holder or the Author the information, which is confirmed and will be included in the issued certificate for acceptance of its content.

(6) After making the check-ups and acceptance of the certificate content by the Holder or the Author the Registration authority confirms the application for issuance of a certificate to the Provider's certification authority and guarantees that:

□ the application for issuance comes from the Holder or by a person duly authorized thereby, or by the Author;

□ the information about the Holder and the Author, presented for inclusion in the certificate, is true and complete;

□ the private key is technically appropriate to be used for generation of advanced electronic signature and corresponds to the public key, so that by the public key it could be certified that a particular electronic signature is generated with the private key, and

□ the private key is held by the Author.
(7) If the process of approval of the application for issuance of a certificate fails, the Registration authority rejects the application for issuance of a certificate.

(8) The Registration authority immediately notifies the Applicant and states the reason for rejection directly or by:

► sending an e-mail to the Holder, respectively the Author, and

► publishing information about the issuance on the website of the Provider, if the Holder or the Author is registered user and has valid rights for access to the website on: http://www.infonotary.com.

(9) Applicants, whose applications for issuance of a certificate have been rejected, may again submit application for issuance of a certificate.

(10) The Registration authority completes and keeps the documents, submitted by the Holder, Author or Applicant, together with the application for issuance of a certificate and a signed contract for certification services.

(11) The Provider controls the accuracy of the information included in the certificate, which is submitted to the Holder and Author upon the issuance of the certificate.

(12) The check-up and confirmation of the information in the submitted applications for issuance of a certificates are processed within a reasonable term and the Provider issues the certificates within 5 business days as of the date of acceptance of the documents.

I.1.7. Certificate Issuance

(1) The Provider’s certification authority issues the certificate on the basis of received request for issuance by the Registration authority.

(2) The request for certificate issuance of the Registration authority guarantees confirmation of the validity of the application made by the Applicant, the validity of the data, contained therein, and is signed by the administrator of the Registration authority, which has made the check-ups.
(3) The Provider's certification authority checks the identity of the Registration authority and the identity of the Registration authority's administrator on the basis of submitted authorizations (special administrative certificate for Registration authority's administrator).

(4) After the issuance of the certificate the Provider submits it to the Holder, respectively to the Author:

► by publishing a link for download of the certificate on the website of the Provider, when the Holder or the Author are authorized users and have valid access rights for the website on: http://www.infonotary.com

► or through the Registration authority.

I.1.8. Certificate Acceptance

(1) The Provider issues the certificate based on the consent of the Holder, respectively the Author.

(2) Acceptance of the certificate content is certified with the signing of a Written Statement of Acceptance of the universal electronic signature certificate by the Holder, respectively the Author prior to its publication in the Certificates Directory of the Provider.

I.1.9. Certificate Publishing by the Certification Authority

The Provider publishes immediately the issued universal electronic signature certificate in its Certificates Directory.

I.1.10. Certificate Suspension and Renewal

Certificate suspension and renewal is performed based on the common certificate suspension and renewal procedures in line with cls. 4.9.11 and 4.9.16 of the User Manual.

I.1.11. Certificate Revocation
Certificate revocation is performed based on the common certificate revocation procedures in line with cl. 4.9 of the User Manual.

**I.1.12. Certificate Update**

The certificate update is performed under the common certificate revocation procedures in line with cl. 4.6 of the User Manual.

**I.2. Policy of Issuance and Management of Universal Electronic Signature Certificate for a Legal entity**

**I.2.1. Certificate General Characteristics**

(1) Certificate i-Notary Company Q Sign is a universal electronic signature certificate in line with Art. 24 of LEDES and each electronic signature, accompanied with such certificate is a universal signature.

(2) Universal electronic signature certificate of a legal entity (i-Notary Company Q Sign) is issued to legal entity – Holder and certifies the identity and the connection with its public key.

(3) Certificate i-Notary Company Q Sign is issued obligatorily with cryptographic keys – private and public, which are used for universal electronic signature generation and check-up, and are generated and stored in a cryptographic device (smartcard) of the pair.

(4) For the issuance of i-Notary Company Q Sign certificate procedures are implemented, ensuring high level of reliability and security of the certified information, identifying the Holder and the Author and the keeping of the resources for generation of electronic signature – the private key.

(5) The procedures of identification and establishing the identity of the Holder and the Author require submission of evidence for the identity of the Holder, the identity of the Author, as well as of the representative authority of the Author and their personal appearance before the Providers Registration authority.
I.2.2. Designation

(1) The policy applicable to this certificate, is designated as follows:

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Name</th>
<th>Designation (OID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal entity universal electronic signature certificate certification policy</td>
<td>i-Notary Company Q Sign Certificate CP</td>
<td>1.3.6.1.4.1.22144.1.1.2.1</td>
</tr>
</tbody>
</table>

(2) The policy is published in the Public Document Directory of the Provider and could be accessed at:

http://repository.infonotary.com/certpolicy_qsign-company.html.

I.2.3. Certificate Purpose and Applicability

(1) The legal entity universal electronic signature certificate (i-Notary Company Q Sign certificate) may be used as a means of company/professional electronic identification, e-trade, financial transactions, electronic correspondence, electronic document signing, making statements from and to public authorities and local self-governing authorities under the sense of the LEDES.

(2) The due care of the trusting party includes checking of the purpose and applicability of this certificate, when placing confidence in the electronic signature, accompanied by the certificate.

(3) For the purpose of check-up by the trusting party the certificate designates the policy applicable to such certificate (“Certificate Policy”), and the additional extensions thereto, as well as the purpose and the action restrictions of the certificate, listed in the attributes “Key Usage”, “Extended Key Usage”, “Qualified Statements”.
I.2.4. Company Q Sign Certificate Profile

I.2.5. Main Attributes (x509)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3 (0x02)</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique in the Provider’s directory; 8-byte number</td>
</tr>
<tr>
<td>Beginning of the validity term</td>
<td>Date and time of signing of ESC</td>
</tr>
<tr>
<td>End of the validity term</td>
<td>Date and time of signing of ESC+ 1 year</td>
</tr>
<tr>
<td>Electronic signature algorithm on ESC</td>
<td>FIPS DSS; dsaWithSHA1 (1.3.14.3.2.27) or RSA – 2048 bits</td>
</tr>
</tbody>
</table>

Issuer Attributes (x509 Issuer DN)

The issuer attributes coincide with the attributes of the signing electronic signature certificate Holder (ESC).

Attributes of the Holder/Author (x509 Subject DN):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M(^7)</th>
<th>T/A(^8)</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>2.5.4.3</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

\(^7\) Mandatory  
\(^8\) Holder/Author
<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>T/A</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/countryName</td>
<td>2.5.4.6</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/postalCode</td>
<td>2.5.4.17</td>
<td>T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/localityName</td>
<td>2.5.4.7</td>
<td>T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>2.5.4.9</td>
<td>+</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/organizationName</td>
<td>2.5.4.10</td>
<td>+</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/organizationalUnitName</td>
<td>2.5.4.11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/emailAddress</td>
<td>1.2.840.113549.1.9.1</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/telephoneNumber</td>
<td>2.5.4.20</td>
<td>T</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additionally defined organization attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgBulstatNumber</td>
<td>2.5.4.10.100.1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>2.5.4.10.100.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/bgBankAddressableUnit</td>
<td>2.5.4.11.100.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/bgBudgetIdentificationNumber</td>
<td>2.5.4.11.100.1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>2.5.4.10.100.1.3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additionally defined natural person attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>T/A</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgUnifiedCitizenNumber</td>
<td>2.5.4.3.100.1.1</td>
<td>+</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/bgIdentificationCardNumber</td>
<td>2.5.4.3.100.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/bgFinancialObligationsStatement</td>
<td>2.5.4.3.100.1.3</td>
<td></td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>/bgRepresentativeDocumentNumber</td>
<td>2.5.4.3.100.1.4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Attributes of the Author (x509v3 subjectAltName extension DN):**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>T/A</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>2.5.4.3</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Attribute</td>
<td>OID</td>
<td>M</td>
<td>C⁹</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------</td>
<td>---</td>
<td>----</td>
<td>------------------------</td>
</tr>
<tr>
<td>/countryName</td>
<td>2.5.4.6</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/postalCode</td>
<td>2.5.4.17</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/localityName</td>
<td>2.5.4.7</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>2.5.4.9</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/organizationName</td>
<td>2.5.4.10</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/organizationalUnitName</td>
<td>2.5.4.11</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/emailAddress</td>
<td>1.2.840.113549.1.9.1</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/telephoneNumber</td>
<td>2.5.4.20</td>
<td></td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

### Additionally defined organization attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>C⁹</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgBulstatNumber</td>
<td>2.5.4.10.100.1.1</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>2.5.4.10.100.1.2</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/bgBankAddressableUnit</td>
<td>2.5.4.11.100.1.2</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/bgBudgetIdentificationNumber</td>
<td>2.5.4.11.100.1.1</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>2.5.4.10.100.1.3</td>
<td></td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

### Additionally defined natural person attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>C⁹</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bgUnifiedCitizenNumber</td>
<td>2.5.4.3.100.1.1</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/bgIdentificationCardNumber</td>
<td>2.5.4.3.100.1.2</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>/bgFinancialObligationsStatement</td>
<td>2.5.4.3.100.1.3</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/bgRepresentativeDocumentNumber</td>
<td>2.5.4.3.100.1.4</td>
<td>+</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

### Additional x509 attributes (x509v3 extensions):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>M</th>
<th>C⁹</th>
<th>Value</th>
</tr>
</thead>
</table>

⁹ Critical
<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>Flags</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/basicConstraints</td>
<td>2.5.29.19</td>
<td>+</td>
<td>CA=false</td>
</tr>
<tr>
<td>/keyUsage</td>
<td>2.5.29.15</td>
<td>+</td>
<td>Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment</td>
</tr>
<tr>
<td>/extKeyUsage</td>
<td>2.5.29.37</td>
<td>+</td>
<td>emailProtection, clientAuth</td>
</tr>
<tr>
<td>/authorityKeyIdentifier</td>
<td>2.5.29.35</td>
<td></td>
<td>subjectKeyIdentifier of the signing ESC.</td>
</tr>
<tr>
<td>/subjectKeyIdentifier</td>
<td>2.5.29.14</td>
<td>+</td>
<td>SHA1 of DER- coded public key</td>
</tr>
<tr>
<td>/cRLDistributionPoints</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://crl.infonotary.com/crl/qsign-company-ca.crl">http://crl.infonotary.com/crl/qsign-company-ca.crl</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ldap://ldap.infonotary.com/</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>dc=qsign-corporate-ca,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>dc=infonotary.dc=com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/authorityInfoAccess</td>
<td>1.3.6.1.5.5.7.1.1</td>
<td>+</td>
<td><a href="http://ocsp.infonotary.com/responder.cgi">http://ocsp.infonotary.com/responder.cgi</a></td>
</tr>
<tr>
<td>/qcStatements</td>
<td>1.3.6.1.5.5.7.1.3</td>
<td>0.4.0.1862.1.1</td>
<td></td>
</tr>
</tbody>
</table>

**Certificate Policies x509v3 extension:**

| Identifier (OID)          | 1.3.6.1.4.1.22144.0          | CPS   | http://www.crc.bg                                                        |
|                          |                             | Text  | Registration Resolution № …….by the Communications Regulation Commission |

| Identifier (OID)          | 1.3.6.1.4.1.22144.1.1.2.1   | CPS   | http://repository.infonotary.com/certpolicy_qsign-company.html          |
|                          |                             | Text  | This certificate is issued to the subject in order to legally represent the organization as stated above |

| Identifier (OID)          | 0.4.0.1456.1.1              | CPS   | http://www.infonotary.com/qcp-sscd.html                                  |
|                          |                             | Text  | This certificate is issued as qualified certificate for advanced electronic signature using secure storage cryptographic device |

**Description and application of the attributive OID, used in Certificate RDN**

**Attribute description**
<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
<th>( p^{10} )</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>2.5.4.3</td>
<td></td>
<td>Subject name</td>
</tr>
<tr>
<td>/countryName</td>
<td>2.5.4.6</td>
<td></td>
<td>Country code</td>
</tr>
<tr>
<td>/postalCode</td>
<td>2.5.4.17</td>
<td></td>
<td>Postal code</td>
</tr>
<tr>
<td>/localityName</td>
<td>2.5.4.7</td>
<td></td>
<td>City/District</td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>2.5.4.9</td>
<td></td>
<td>Address</td>
</tr>
<tr>
<td>/organizationName</td>
<td>2.5.4.10</td>
<td></td>
<td>Organization name</td>
</tr>
<tr>
<td>/organizationalUnitName</td>
<td>2.5.4.11</td>
<td></td>
<td>Name of subdivision within the organization</td>
</tr>
<tr>
<td>/emailAddress</td>
<td>1.2.840.113549.1.9.1</td>
<td></td>
<td>e-mail address</td>
</tr>
<tr>
<td>/phoneNumber</td>
<td>2.5.4.20</td>
<td></td>
<td>Telephone number</td>
</tr>
<tr>
<td>/bgBulstatNumber</td>
<td>2.5.4.10.100.1.1</td>
<td>+</td>
<td>BULSTAT</td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>2.5.4.10.100.1.2</td>
<td>+</td>
<td>Organization taxation number</td>
</tr>
<tr>
<td>/bgBankAddressableUnit</td>
<td>2.5.4.11.100.1.2</td>
<td>+</td>
<td>Bank addressable unit</td>
</tr>
<tr>
<td>/bgBudgetIdentificationNumber</td>
<td>2.5.4.11.100.1.1</td>
<td>+</td>
<td>Budget identification number</td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>2.5.4.10.100.1.3</td>
<td>+</td>
<td>Information about the court registration of the organization</td>
</tr>
<tr>
<td>/bgUnifiedCitizenNumber</td>
<td>2.5.4.3.100.1.1</td>
<td>+</td>
<td>Personal number</td>
</tr>
<tr>
<td>/bgIdentificationCardNumber</td>
<td>2.5.4.3.100.1.2</td>
<td>+</td>
<td>ID card number</td>
</tr>
<tr>
<td>/bgFinancialObligationsStatement</td>
<td>2.5.4.3.100.1.3</td>
<td>+</td>
<td>Financial limitations for the documents, signed with ESC</td>
</tr>
<tr>
<td>/bgRepresentativeDocumentNumber</td>
<td>2.5.4.3.100.1.4</td>
<td>+</td>
<td>Information about the number and issuer of the representative power document</td>
</tr>
</tbody>
</table>

**Format description and attribute formation**

\(^{10}\)Own (Provider-defined as an extension of existing X.500 attribute)
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Format</th>
<th>S&lt;sup&gt;11&lt;/sup&gt;</th>
<th>P&lt;sup&gt;12&lt;/sup&gt;</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>/commonName</td>
<td>A+</td>
<td>,</td>
<td></td>
<td>Author’s full name</td>
</tr>
<tr>
<td>/countryName</td>
<td>A2</td>
<td></td>
<td></td>
<td>Two-symbol country code</td>
</tr>
<tr>
<td>/postalCode</td>
<td>N4</td>
<td></td>
<td></td>
<td>Holder’s/Author’s postal code</td>
</tr>
<tr>
<td>/localityName</td>
<td>AN+</td>
<td>,</td>
<td></td>
<td>Holder’s/Author’s city</td>
</tr>
<tr>
<td>/unstructuredAddress</td>
<td>AN+</td>
<td>,</td>
<td></td>
<td>Holder’s/Author’s address data</td>
</tr>
<tr>
<td>/organizationName</td>
<td>AN+</td>
<td></td>
<td></td>
<td>Holder’s organization name/Holder’s full name in the case of natural person</td>
</tr>
<tr>
<td>/organizationalUnitName</td>
<td>AN+</td>
<td></td>
<td></td>
<td>Name of subdivision within the organization</td>
</tr>
<tr>
<td>/emailAddress</td>
<td>IA5+</td>
<td></td>
<td></td>
<td>Author’s e-mail address</td>
</tr>
<tr>
<td>/telephoneNumber</td>
<td>AN+</td>
<td></td>
<td></td>
<td>Holder’s/Author’s telephone number</td>
</tr>
<tr>
<td>/bgBulstatNumber</td>
<td>N+</td>
<td>BULSTAT:</td>
<td></td>
<td>BULSTAT number</td>
</tr>
<tr>
<td>/bgTaxationNumber</td>
<td>N+</td>
<td>TAXNUM:</td>
<td></td>
<td>Taxation number</td>
</tr>
<tr>
<td>/bgBankAddressableUnit</td>
<td>N+</td>
<td>BAU:</td>
<td></td>
<td>Bank addressable unit</td>
</tr>
<tr>
<td>/bgBudgetIdentificationNumber</td>
<td>N+</td>
<td>BIN:</td>
<td></td>
<td>Budget identification number</td>
</tr>
<tr>
<td>/bgLegalRegistration</td>
<td>AN+</td>
<td>,</td>
<td>LEGAL:</td>
<td>Information about the court registration of the organization</td>
</tr>
<tr>
<td>/bgUnifiedCitizenNumber</td>
<td>N+</td>
<td>UCN:</td>
<td></td>
<td>Holder’s/Author’s personal number</td>
</tr>
<tr>
<td>/bgIdentificationCardNumber</td>
<td>N+</td>
<td>IDCARD:</td>
<td></td>
<td>Holder’s/Author’s ID card number</td>
</tr>
<tr>
<td>/bgFinancialObligationsStatement</td>
<td>AN+</td>
<td>:</td>
<td>FO:</td>
<td>Minimum value, maximum value and ISO currency code of the constraint</td>
</tr>
<tr>
<td>/bgRepresentativeDocumentNumber</td>
<td>AN+</td>
<td>REPDN:</td>
<td></td>
<td>Information about the number and issuer of the representative power document</td>
</tr>
</tbody>
</table>

The Format column has the following meaning:

---

<sup>11</sup> Separator  
<sup>12</sup> Prefix
<table>
<thead>
<tr>
<th>Format</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>The attribute may only take alphabetic character values</td>
</tr>
<tr>
<td>N</td>
<td>The attribute may only take numeric values</td>
</tr>
<tr>
<td>AN</td>
<td>The attribute may take alpha-numeric values</td>
</tr>
<tr>
<td>IA5</td>
<td>The attribute may take valid IA5 character values (e-mail/url)</td>
</tr>
</tbody>
</table>

- The number following the format designation gives the maximum permitted number of characters.
- The character " + " stands for one or more characters.
- Each field except those marked as IA5, contains data in UTF-8 encoding.
- The data in the validity fields are presented as ASN1 GeneralTime.

### I.2.6. Application Procedure for Certificate Issuance

(1) The registration authorities of the Provider accept and process all applications for universal electronic signature certificate issuance by end users.

(2) All persons may submit application to the Provider for certificate issuance, who:

- fill-in Certificate Issuance Application Form;
- generate a pair of cryptographic keys, either independently, or through the Provider;
- submit to the Provider’s certification authority the public key, corresponding to the private key;
- accept the terms and conditions of the Certification Services Provision Contract and the User Manual of the Provider.
(3) The Certificate Issuance Application should contain the following data:

- information identifying the Holder and, if the Author is different from the Holder – information about the Author as well;
- the public key, corresponding to the private key of the pair of cryptographic keys, generated by the Holder;
- the selected certificate type.

(4) The Certificate Issuance Application is an electronic document in PKCS #10 format, signed with the private key, corresponding to the public one included in the document.

(5) The Certificate Issuance Application may be generated via the Provider’s website and submitted to it via an encrypted communication channel to: https://www.infonotary.com.

(6) The registration authorities of the Provider render to all persons the service of cryptographic key pair generation, generation of application for certificate issuance and their submission to the Provider.

(7) When the registration authority of the Provider performs cryptographic key pair generation by request of the Holder, it makes use of a protective mechanism for their generation and submits them to the Author recorded on cryptographically protected device – smartcard, etc.

(8) The private key access rights – PIN-code or password are submitted by the registration authority of the Author in protected form.

(9) After the registration authority submits the device, on which the private key and the access rights thereto are recorded, the Holder and the Author are fully responsible for prevention of compromising, loss, disclosure, modification or other unauthorized use of their private key.

I.2.7. Approval or Rejection of Certificate Applications
(1) In order to establish and confirm the identity of a legal entity that has submitted application for issuance of a certificate, procedures and rules are applied, defined by the Provider in the User Manual.

(2) The Provider reserves the right to amend the requirements to the information and documents necessary for confirmation of the identification of the Holder – legal entity, whenever necessary in implementation of its certification policies or legal requirements.

(3) The checking and confirmation of the information are performed by the registration authority in line with the Provider's rules and procedures and in full compliance with the User Manual and other internal documents.

(4) The registration authority checks and confirms the following information, identifying the legal entity – Holder:

- name of the legal entity;
- address, city, country, postal code;
- number in national tax register and/or
- BULSTAT number;
- domain name;
- legal status and current state;
- right upon the trade name, mark, domain, etc.;
- contact and invoicing information.

(5) The Holder, respectively authorized representative of the Holder submits personally before the Registration authority the following documents:

- court decision for registration or incorporation deed;
- current state certificate issued not earlier than 1 month prior to the date of submission;
- document for BULSTAT registration;
- document for taxation registration;
- document proving the right to use a name, etc.
(4) The Holder, the Author or the authorized representative of the Holder submits personally before the Registration authority the following documents:

- valid identity document: identity card or passport;

- notarized power of attorney authorizing the Representative to represent the Holder before the Provider for certificate issuance and management;

- document certifying the representative power of the Author – court ruling, certificate of current status, notarized power of attorney or other empowering act.

(5) Prior to approval of a submitted application for issuance of a certificate the Registration authority of the Provider performs the necessary check-ups, namely:

- checks-up and confirms the identity of the Applicant, Author, Holder or the person representing him/her on the basis of the documents, submitted thereby;

- checks-up and confirms the representative authority of the Author and of the person, authorized to represent the Holder;

- checks-up the correctness of the received or filled-in and signed electronic application (in PKCS#10 format) for issuance of certificate;

submits to the Holder or the Author the information, which is confirmed and will be included in the issued certificate for acceptance of its content.

(6) After making the check-ups and acceptance of the certificate content by the Holder or the Author the Registration authority confirms the application for issuance of a certificate to the Provider's certification authority and guarantees that:
□ the application for issuance comes from the Holder or by a person duly authorized thereby, or by the Author;

□ the information about the Holder and the Author, presented for inclusion in the certificate, is true and complete;

□ the private key is technically appropriate to be used for generation of advanced electronic signature and corresponds to the public key, so that by the public key it could be certified that a particular electronic signature is generated with the private key, and

□ the private key is held by the Holder, or respectively by the Author.

(7) If the process of approval of the application for issuance of a certificate fails, the Registration authority rejects the application for issuance of a certificate.

(8) The Registration authority immediately notifies the Applicant and states the reason for rejection directly or by:

sending an e-mail to the Holder, respectively the Author, and

publishing information about the issuance on the website of the Provider, if the Holder or the Author is registered user and has valid rights for access to the website on: http://www.infonotary.com.

(9) Applicants, whose applications for issuance of a certificate have been rejected, may again submit application for issuance of a certificate.

(10) The Registration authority completes and keeps the documents, submitted by the Holder, Author or Applicant, together with the application for issuance of a certificate and a signed contract for certification services.

(11) The Provider controls the accuracy of the information included in the certificate, which is submitted to the Holder and Author upon the issuance of the certificate.

(12) The check-up and confirmation of the information in the submitted applications for issuance of a certificates are processed within a reasonable
term and the Provider issues the certificates within 5 business days as of the date of acceptance of the documents.

**I.2.8. Certificate Issuance**

(1) The Provider's certification authority issues the certificate on the basis of received request for issuance by the Registration authority.

(2) The request for certificate issuance of the Registration authority guarantees confirmation of the validity of the application made by the Applicant, the validity of the data, contained therein, and is signed by the administrator of the Registration authority, which has made the check-ups.

(3) The Provider's certification authority checks the identity of the Registration authority and the identity of the Registration authority's administrator on the basis of submitted authorizations (special administrative certificate for Registration authority's administrator).

(4) After the issuance of the certificate the Provider submits it to the Holder, respectively to the Author:

by publishing a link for download of the certificate on the website of the Provider, when the Holder or the Author are authorized users and have valid access rights for the website on: [http://www.infonotary.com](http://www.infonotary.com) or through the directories.

**I.2.9. Certificate Acceptance**

(1) The Provider issues the certificate based on the consent of the Holder, respectively the Author.

(2) Acceptance of the certificate content is certified with the signing of a Written Statement of Acceptance of the certificate by the Holder, respectively the Author prior to its publication in the Certificates Directory of the Provider.

**I.2.10. Certificate Publishing by the Certification Authority**

The Provider publishes immediately the issued certificate in its Certificates Directory.
I.2.11. Certificate Suspension and Renewal

Certificate suspension and renewal is performed based on the common certificate suspension and renewal procedures in line with cls. 4.9.11 and 4.9.16 of the User Manual.

I.2.12. Certificate Revocation

Certificate revocation is performed based on the common certificate revocation procedures in line with cl. 4.9 of the User Manual.

I.2.13. Certificate Update

The certificate update is performed under the common certificate revocation procedures in line with cl. 4.6 of the User Manual.