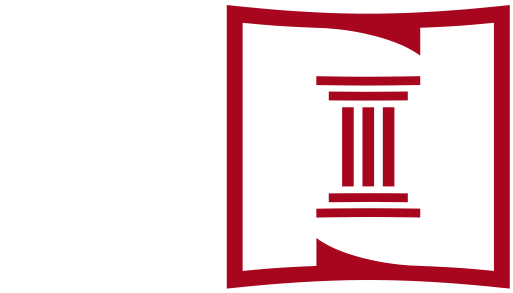

InfoNotary

PUBLIC KEY INFRASTRUCTURE STATEMENT

OF
QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

Version 2.3

Entry into force 02.06.2023

CONTENT

1. TRUST SERVICE PROVIDER CONTACT INFORMATION

INFONOTARY PLC is a Qualified Trust Service Provider under Regulation (EU) No 910/2014 and has been granted qualified status by the Bulgarian Supervisory Body in accordance with the conditions laid down in Regulation (EU) No 910/2014 and in accordance with national law.

INFONOTARY PLC is a commercial company registered in the Commercial Register at the Registry Agency under UIN 131276827. The company uses its registered trademark InfoNotary in its trade.

SEAT AND ADDRESS OF MANAGEMENT:

16 Ivan Vazov Str.

1000 Sofia

Bulgaria

Telephone number: +359 2 9210857

Web address: http://www.infonotary.com

e-mail: tsp@infonotary.com

2. CERTIFICATE TYPES, VERIFICATION PROCEDURES AND CERTIFICATES USAGE

As a Qualified Provider, INFONOTARY PLC declares that the current Statement relates to Qualified Certificates issued by its Certification Authority InfoNotary TSP Root under the following Certification Policies

Policy name	**Identifier (OID)**
InfoNotary TSP Root	1.3.6.1.4.1.22144.3
InfoNotary Qualified Natural Person Signature CP	1.3.6.1.4.1.22144.3.1.1
InfoNotary Qualified Delegated Signature CP	1.3.6.1.4.1.22144.3.1.2
InfoNotary Qualified Legal Person Seal CP	1.3.6.1.4.1.22144.3.2.1
InfoNotary Qualified Legal Person Seal for PSD2 Certificate	1.3.6.1.4.1.22144.3.2.2
InfoNotary Qualified Validated Domain CP	1.3.6.1.4.1.22144.3.3.1
InfoNotary Qualified Organization Validated CP	1.3.6.1.4.1.22144.3.3.2
InfoNotary Qualified PSD2 WA CP	1.3.6.1.4.1.22144.3.3.3

InfoNotary Q TSA CP	1.3.6.1.4.1.22144.3.4.1
InfoNotary Qualified OCSP CP	1.3.6.1.4.1.22144.3.5.1
InfoNotary Qualified Validation Service CP	1.3.6.1.4.1.22144.3.5.2
InfoNotary Qualified Certificate for Natural Person AESignature CP	1.3.6.1.4.1.22144.3.6.1
InfoNotary Qualified Certificate for Delegated AESignature CP	1.3.6.1.4.1.22144.3.6.2
InfoNotary Qualified Certificate for Legal Person AESeal CP	1.3.6.1.4.1.22144.3.7.1
InfoNotary Qualified Certificate for PSD2 AESeal CP	1.3.6.1.4.1.22144.3.7.2
InfoNotary TSP Registration Operator CP	1.3.6.1.4.1.22144.3.8.1
InfoNotary Mobile Device Authentication CP	1.3.6.1.4.1.22144.3.9.1
InfoNotary IoT Device Authentication CP	1.3.6.1.4.1.22144.3.9.2

2.1. End user certificates

INFONOTARY PLC as a Qualified Trust Service Provider, issues Qualified Certificates for Electronic Signature, Qualified Certificates for Electronic Seal, Qualified Certificates for Web Authentication, Electronic Time Stamps and performs validation services for electronic signatures and seals in full compliance with the provisions and the requirements of Regulation (EU) 910/2014.

INFONOTARY PLC, as a Qualified Trust Service Provider, issues Qualified Certificates for Qualified Electronic Signatures, Qualified Electronic Seals, Advanced Electronic Signatures and Advanced Electronic Seals, Qualified Electronic Time Stamps, Qualified Website Authentication Certificates and performs validation services for electronic signatures and seals in full compliance with the provisions and the requirements of the Regulation (EU) 910/2014.

InfoNotary Qualified Certificate for Qualified Natural Person Signature

The certificate is issued to a natural person (Holder) and can be used for personal identification to Internet applications, financial transactions, secured and encrypted communication, electronic correspondence, electronic document signing and making statements, authentication and data encryption activities. The certificate is associated with a pair of cryptographic keys that are generated and stored only on a qualified electronic signature creation device (QSCD). The device, the data for access to it (PIN, AIN) as well as the data for activation of the private key for creation of an electronic signature, are available and are only under the sole control of the Holder. The qualified certificate may be issued by the Provider as a Cloud Certificate for qualified electronic signature, when the Holder assigns the managment of the qualified electronic signature cration device to the Provider, who observs appropriate mechanisms

and procedures to ensure, that only the Holder has sole control over the use of his electronic signature creation data.

The pair of cryptographic keys associated with the cloud certificate are generated and stored only on a remote qualified electronic signature cration device (RQSCD), which is managed by the Provider on behalf of the Signatory. The data for access to the RQSCD and for remote activation of the private key for creating a remote electronic signature are solely under the control of the Holder.

InfoNotary Qualified Certificate for Qualified Delegated Signature

The certificate is issued to a natural person (Holder) and contains information about a legal entity that has delegated authority to the Holder and can be used for for personal identification to Internet applications, financial transactions, secured and encrypted communication, electronic correspondence, electronic document signing and making statements, authentication and data encryption activities. The certificate is associated with a pair of cryptographic keys that are generated and stored only on a qualified electronic signature creation device (QSCD). The device, the data for access to it (PIN, AIN) as well as the data for activation of the private key for creation of an electronic signature, are available and are only under the sole control of the Holder. The qualified certificate may be issued by the Provider as a Cloud Certificate for qualified electronic signature, when the Holder assigns the managment of the qualified electronic signature cration device to the Provider, who observs appropriate mechanisms and procedures to ensure, that only the Holder has sole control over the use of his electronic signature creation data.

The pair of cryptographic keys associated with the cloud certificate are generated and stored only on a remote qualified electronic signature cration device (RQSCD), which is managed by the Provider on behalf of the Signatory. The data for access to the RQSCD and for remote activation of the private key for creating a remote electronic signature are solely under the control of the Holder.

InfoNotary Qualified Certificate for Qualified Legal Person Seal

The certificate is issued to a Legal Person (Creator of a Seal) as a means of organization electronic identification to Internet applications, to perform financial transactions, secure and encrypted communication, electronic correspondence, stamping of electronic documents and performing warranty activities the integrity and origin of the sealed electronic data and information. The electronic seal can also be used to authenticate the legal person's digital assets such as software code, schemes and images. The certificate is associated with a pair of cryptographic keys that are generated and stored only on a qualified electronic seal creation device (QSCD). The device, the data for access to it (PIN, AIN) as well as the data for activation of the private key for creation of an electronic seal, are available and are only under the sole control

of the Creator of a seal. The qualified certificate may be issued by the Provider as a Cloud Certificate for qualified electronic seal, when the Holder assigns the managment of the qualified electronic seal cration device to the Provider, who observs appropriate mechanisms and procedures to ensure, that only the Creator of a seal has sole control over the use of his electronic seal creation data.

The pair of cryptographic keys associated with the cloud certificate are generated and stored only on a remote qualified electronic seal cration device (RQSCD), which is managed by the Provider on behalf of the Creator of a seal. The data for access to the RQSCD and for remote activation of the private key for creating a remote electronic seal are solely under the control of the seal Creator.

InfoNotary Qualified Validated Domain Certificate

The certificate is issued to a natural or legal person (Holder) and may be used to certify the authenticity of a website that is entered in the certificate. The certificate is issued in accordance with the requirements of Regulation (EU) 910/2014 and is used to create assurance in the visitors, that the website stakeholder is real and legitimate subject.

InfoNotary Qualified Organization Validated Certificate

The certificate is issued to a legal person/organization (Holder) and may be used to certify the authenticity of a website that is entered in the certificate. The certificate is issued in accordance with the requirements of Regulation (EU) 910/2014 and is used to create assurance in the visitors, that the website stakeholder is real and legitimate subject.

InfoNotary Qualified PSD2 WA Certificate

The certificate is issued to a legal person/organization (Holder) – Payment Service Provider PSP – PSD2 Directive and may be used to certify the authenticity of a website that is entered in the certificate. The certificate is issued in accordance with the requirements of Regulation (EU) 910/2014 and PSD2 Directive and is used to create assurance in the visitors, that the website stakeholder is real and legitimate subject. The Qualified Certificate contains specific attributes that provide the necessary information to identify the PSD2 Payment Service Provider.

InfoNotary Qualified TimeStamp Certificate

Electronic time stamps are data in electronic form that connect other data in electronic form at a specific point in time and represent evidence that the latest data existed at that time. The electronic time stamp issued by the Provider certifies the date and time of submission of an electronic document signed with a private key corresponding to the public key included in a qualified electronic signature certificate issued by the Provider. Qualified electronic time stamp is

issued to natural and legal persons who are holders or are a relying party.

InfoNotary Qualified Certificate for Advanced Natural Person Signature

The certificate is issued to a natural person (Holder) and can be used for personal identification to Internet applications, financial transactions, secured and encrypted communication, electronic correspondence, electronic document signing and making statements, authentication and data encryption activities.

InfoNotary Qualified Certificate for Advanced Delegated Signature

The certificate is issued to a natural person (Holder) and contains information about a legal entity that has delegated authority to the Holder and can be used for for personal identification to Internet applications, financial transactions, secured and encrypted communication, electronic correspondence, electronic document signing and making statements, authentication and data encryption activities.

InfoNotary Qualified Certificate for Advanced Legal Person Seal

The certificate is issued to a Legal Person (Creator of a Seal) as a means of organization electronic identification to Internet applications, to perform financial transactions, secure and encrypted communication, electronic correspondence, stamping of electronic documents and performing warranty activities the integrity and origin of the sealed electronic data and information. The electronic seal can also be used to authenticate the legal person's digital assets such as software code, schemes and images.

InfoNotary Qualified Certificate for PSD2 AESeal

The certificate is issued to a Legal Person (Creator of a Seal) Payment Service Provider PSP – PSD2 Directive as a means of organization electronic identification to Internet applications, to perform financial transactions, secure and encrypted communication, electronic correspondence, stamping of electronic documents and performing warranty activities the integrity and origin of the sealed electronic data and information. The electronic seal can also be used to authenticate the legal person's digital assets such as software code, schemes and images. The Qualified Certificate contains specific attributes that provide the necessary information to identify the PSD2 Payment Service Provider.

InfoNotary TSP Registration Authority Operator Certificate

The certificate is issued to a natural person (Holder), officially authorized to perform actions as an operator of the Provider's Registration Authority.

The certificate can be used for personal official identification before the portal for certification services of the Provider's Registration Authority, for secure and encrypted communication with the Provider's systems, electronic correspondence, signing electronic documents and making electronic statements, authentication and encryption of data only when the operater performя this activities as an authorized operator of the Provider's Registration Authority.

InfoNotary Mobile Device Authentication Certificate

The certificate is issued to a natural person, the owner/user of a mobile device, and can be used to authenticate the mobile device with a unique identifier that is recorded into it. The certificate is issued in the process of remote video identification, managed by the Provider, which is initiated by a natural person or a natural person, a representative of a legal entity through the Provider’s mobile application InfoNotary Mobile.

The certificate can be used to authenticate the mobile device before information systems, Internet applications, when performing secure and encrypted communication and to guarantee the origin of electronic data and information that are accessible through the Provider’s mobile application InfoNotary Mobile. A qualified certificate may also contain specific attributes providing the necessary information to identify the device.

InfoNotary IoT Device Authentication Certificate

The certificate is issued to a natural or legal person, the owner/user of an IoT device and can be used to authenticate such device with a unique identifier that is recorded into it. The certificate can be used to authenticate an IoT device to information systems, Internet applications, when performing secure and encrypted communication and to guarantee the origin of electronic data and information. A qualified certificate may also contain specific attributes providing the necessary information to identify the device.

2.2. Identification and verification when issuing qualified certificates

Qualified certificates are issued to physical and legal persons after their identity has been verified. Identity verification is done by the Provider's Registration Authority and the request for issuance/management of a qualified certificate can be made directly by the person or by his authorized representative.

The natural persons shall prove their identity by means of a national identity document, Legal persons, by a document of good standing and all forms of authorization shall be proved by a notarized power of attorney and other documents defining the relationship between the authorizer and the representative and his rights.

The procedure for verification and confirmation the natural person's identity (applicant for a trusted service) in a personal capacity, as an authorized representative of another natural person, as an authorized representative of a legal entity/organization or as a legal representative of a legal entity/ organization is carried out by the Registration Authority, in a personal presence of the natural person at the office, or remotely by means of secure video identification, electronic identification, qualified certificate for the qualified electronic signature and other legal means of secure remote identification in line with the requirements of Regulation (EU) 910/2014.

The confirmation of the personal identity of the natural person and the identity of the legal entity is carried out on the basis of submitted documents and/or by checking/referring to the state registers maintained by primary data administratiors.

3. SERVICES ACCESS AND USAGE

Qualified Certificates for Electronic Signature, Qualified Certificates for Electronic Seal, Qualified Certificates for Web Authentication and Qualified TimeStamp Certificates should be used in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Where practicable and depending on the certification service that is requested or provided to the Subscriber, as well as products related to its receipt, the Provider shall provide the opportunity for use by persons with disabilities. Accessibility to services and products is provided without prejudice to or exclusion of compliance with the requirements of security, relevance and compliance with the provisions of Regulation (EU) No 910/2014, the national legislation and internal policies and procedures of the Provider.

4. CERTIFICATE ACTIVITY LIMITATIONS

Qualified certificates issued by the Provider, depending on their type and certification policy, may have limited effect on the purposes and/or value of the transactions - for electronic signature, electronic seal or electronic identification and authentication and / or the value of transactions and financial interest.

The limit on the value of transactions for Qualified Electronic Signature Certificates/Seals is determined by the Holder/ Creator of the seal and entered by the Provider in the Certificate on the basis of the certificate issuance application. The limitations are entered in the certificate in the additional extension QcLimitValue: id-etsi-qcs-QcLimitValue, OID: 0.4.0.1862.1.2.

The Provider is not responsible for damages resulting from the use of the

certificates issued by him beyond their authorized use and according to the limitations of the application regarding the purpose and the value of the transactions and financial interest and will lead to the cancellation of the guarantees, which INFONOTARY PLC gives the Holder/ Creator of the seal and the relying parties.

5. APPLICABLE AGREEMENTS, PRACTICES IN PROVISION OF CERTIFICATES, CERTIFICATE POLICIES

- Certification Practice Statement for Qualified Certification Services;
- Policy for Providing Qualified Certification Services for Qualified Electronic Signature;
- Policy for Providing Qualified Certification Services for Qualified Electronic Seal;
- Policy for providing Qualified Certification Services for Website Authentication Certificate;
- Policy for Providing Qualified Certification Services for Advanced Electronic Signature;
- Policy for Providing Qualified Certification Services for Advanced Electronic Seal;
- Policy for providing Qualified Time Stamp Services;
- Policy for providing Qualified Validation Services;
- Policy and practice for providing remote video identification service;
- Policy and practice for providing qualified service for remote signing and sealing of electronic documents;
- Qualified Certification Services Agreements.

6. PAYMENT REFUNDING POLICY

In case of objections raised by the Subscriber to a Qualified Certificate within 3 days of its publication in the certificate Register of incompleteness or inaccuracies contained therein, the Provider shall terminate the issued certificate and issue a new one free of charge or refund the payment made for the issuance of the certificate.

InfoNotary PLC provides the highest quality of its services. If the Subscriber is not satisfied with the certification service used, he may request termination of the certificate and refunding of the paid amount (respectively the value for the period of validity of the certificate that will not be used) only if InfoNotary PLC has not fulfilled its commitments and obligations, arising from the Qualified Certification Services Agreement and the Certification Practice Statement for Qualified Certification Services, and in this document

7. FINANCIAL RESPONSIBILITY

INFONOTARY PLC is responsible to the Holder/The Creator of a Seal, the Subscriber and all third parties who trust the qualified certificates issued by the Provider.

INFONOTARY PLC is liable only for damages resulting from usage of a qualified certificate during its period of validity and only if there are no circumstances excluding the Provider's liability.

8. INSURANCE OF THE PROVIDER'S ACTIVITY

INFONOTARY PLC has an appropriate insurance policy that deals with the liability of the Provider for Qualified Trust Services for damage in accordance with Regulation (EU) 910/2014 and with national law.

All sums not exceeding the maximum limit of compensation under national law which the Provider is obliged to pay as compensation for non-pecuniary and/or pecuniary damage caused to the Holder/Creator of the seal of a qualified certificate and to all third parties are liable to indemnity under the Provider's insurance due to negligence, errors or omissions in the performance of the insurance activity for which the Provider is responsible under the Bulgarian legislation or the legislation of a Party in which the damage occurred.

The Provider has the right to refuse to pay compensation for damages exceeding the maximum limit of compensation.

For the relation between the Provider and the Subscribers and all third parties, the limits of compensation and conditions are applied since the date of the occurrence of the damage.

The insurance does not cover and the Provider is not liable for any damages suffered as a consequence of:

- Qualified certificates Holders, Creators of a Seal and Subscribers failure to comply with the obligations in accordance with the Certification Practice Statement for Qualified Certification Services, the respective certification policy for qualified certification services and the Qualified Certification Services Agreement;
- compromise or loss of a private key of the Holder, respectively Creator, due to the failure to exercise the due care for its preservation or use;
- non-compliance with the requirements of due diligence for verifying the validity of the electronic signature certificate, the electronic seal

certificate and the qualified electronic time stamp of the Relying Parties;

- non-compliance with the obligations of users of the Remote Video Identification Service resulting from the terms of the relevant policy, the Provider's practice for providing qualified trust services and the General Terms and Conditions for use of InfoNotary Mobile application;
- loss of a mobile device or compromise of the created secret code (PIN code) for entering the application by the user, because of failure to take reliable care for its protection or use;
- malicious actions of third parties (hacking attacks, stealing a mobile device, access to identification means, etc.)
- force majeure, accidents and other events beyond the control of the Provider.

9. INFORMATION CONFIDENTIALITY

The Provider complies with all applicable rules for the protection of personal data and confidential information collected regarding its activities.

The Provider considers as confidential the information contained in and related to:

- any information regarding the Holder/Creator and Subscriber beyond the published in the certificate;
- the reason for suspending or terminating the validity of certificates, beyond the published status information of the certificate;
- correspondence related to the Provider’s activity;
- the Provider’s private keys;
- the Holder’s/ Creator’s private key when the Provider stores them on assignment by the Holder/Creator of the seal;
- the Agreement for Qualified Certification Services;
- archives of requests for issuance, suspension, resumption and termination of certificates;
- transaction archives;
- records of external and internal audits and reports;
- disaster and unforeseen cases recovery plans.
- reports of the conformity assessment body, of the other external auditors and the Supervisory Authority

10. PERSONAL DATA CONFIDENTIALITY

The provider is a controller of personal data and ensures the storage and processing of personal data provided to him as a Qualified trust service

provider, providing qualified trust services[1] pursuant to the Personal Data Protection Act and Regulation (EU) 2016/679 (GDPR)

The type and amount of personal data collected is proportionate to the purposes and their use. Personal data is only used in connection with the provision of qualified certification services.

The information collected by the Holder/Creator of a Seal/Authorized Representative and Subscriber is only for the purpose of providing a qualified certification service.

The information included in the qualified certificates may contain personal data of the Holder/Creator of the seal pursuant to the Personal Data Protection Act and Regulation (EU) 2016/679 (GDPR). This data is stored and processed in the Provider's databases.

The Register of the issued certificates and the Certificates Revocation List, maintened by the Provider are publicy avaiable to third parties.

At the explicit request of the Holder/Creator of the seal, the Provider restricts the access for reading and downloading of the issued certificate from the Register of issued certificates. In this case, only information about the issued certificate and its status is available in the Register.

The information collected by the Holder/Creator of a Seal/Authorized Representative and Subscriber and not included in the Qualified Certificates and the information on their status and constituting personal data within the meaning of the Personal Data Protection Act and Regulation (EU) 2016/679 (GDPR) shall be collected only as far as it is required for the purpose of issuing and maintaining Qualified Certificates or use of another Certification Service and may not be used for any other purpose or provided to third parties without the express consent of the Providers or what is permitted by law.

The Provider shall inform in advance the Holder/Creator of a Seal/Authorized Representative and Subscriber of Qualified Certification Services of the types of information it collects for them, how it is provided and stored and accessed to third parties.

The Holder / Creator of the seal, when signing the Contract for qualified certification services and accepting the terms and conditions of the Practice in providing qualified certification services and of the Certification policies, agrees that the qualified certificate shall contain personal data that identifies him, and which are avaiable to the third parties from the Register of the issued certificates.

---

[1] *in accordance with REGULATION (EU) No 910/2014 and national law*

11. INTELLECTUAL PROPERTY RIGHTS

The Provider owns and reserves all intellectual property rights to databases, websites, mobile applocations, Qualified Certificates issued by the Provider, and any other documents and information originating from the Provider and included in the Provider's Documentary repository.

The Provider allows the certificates issued by him and without any limitation of access to them by the Holder to be reproduced and distributed, provided that they are entirely reproduced and distributed.

All trademark and trademark rights are retained by the owners of these rights. The Provider uses the objects of such rights only for the purpose of providing Qualified Certification Services.

Private and public keys, as well as the means of access to them (PIN codes, passwords, etc.) are owned by their Holders, who use them and store them in the correct manner.

Key pairs as well as secret parts of Provider's private keys are property of the Provider.

12. OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES

The obligations, responsibilities and warranties of the Provider, Registration Authorities, Holder, Creator of a Seal, Subscribers of Qualified Certification Services and Relying Parties are governed by Regulation (EU) 910/2014, in national legislation, Certification Practice Statement for Qualified Certification Services, the Certification policies of the Provider and the Qualified Certification Services Agreement.

12.1. Obligations, Responsibilities and Warranties of the Provider

The Provider ensures that he complies with all the provisions of Regulation (EU) No 910/2014, the national legislation and current document, strictly enforces the procedures and observes the policies established in Certification Policies for different types of Qualified Certificates.

When issuing Qualified Certificates, the Provider ensures the accuracy and timeliness of the information included in the content of the certificate at the time of its verification and according to the policy of issuing the certificate.

The Provider is responsible to the Holder/Creator and to any third party for

damages caused by:

- failure to comply with the Provider's obligations under Regulation (EU) 910/2014 and national law governing the issue, management and content of the Qualified Certificate;
- from false or missing data in the Qualified Certificate at the time of issuance;
- if during the issuance of the Qualified Certificate the person named as Holder/Creator did not have the private key corresponding to the public key included in a certificate issued by the Provider;
- the algorithmic discrepancy between the private key and the public key entered in the Qualified Certificate;
- identity gaps of the Holder/Creator of a seal.

12.2. Responsibility of the Holder/Creator of the seal to relying parties

The Holder/Creator of a Seal is responsible for the relying parties:

- when creating the pair (public and private keys) the algorithm and devices for creation of electronic signature/seal does not meet the requirements of Regulation (EU) 910/2014;
- does not strictly meet the security requirements specified by the Provider;
- does not require the Provider to suspend or terminate the certificate in case of finding out that the private key is compromised, has been misused or is at risk of being misused;
- for false statements made to the Registration Authority and the Provider concerning the content or issuance of the certificate.

The Holder/Creator of a Seal is responsible before the Provider if it has provided false data, or has skipped data relevant to the content or issuance of the certificate, and when it did not hold the private key corresponding to the public key specified in the certificate.

In all cases of non-compliance by the Holder, respectively the Creator, resulting from the Certification Practice Statement for Qualified Certification Services, the Provider will hold responsibility for damages of the Holder, respectively the Creator.

13. RELYING PARTIES CARE

Persons who trust the Qualified Certification Services of the Provider should exercise due care, such as:

- have the technical skills to use qualified certificates;
- be aware of the conditions under which they must rely on qualified certificates, in accordance with the policies under which they are issued and the procedures for the inspections of the information provided by the Provider detailed in the Provider's Certification Practice Statement for Qualified Certification Services;
- validate Qualified Certificates issued by the Provider by means of the published status data of the Certificates from the Provider - Certificate Revocation List;
- use a secure electronic signature/electronic seal verification mechanism that guarantees:
- public key, private key and content of the signed electronic document check; verification of the authenticity and validity of the qualified certificate at the time of signing, correct presentation of the results of the inspection and the possibility of any changes being identified;
- trust the qualified certificates issued by the Provider only if the result of the validity checks made is correct and up-to-date.

Relying parties are required to check the validity, suspension or termination of a qualified certificate by updating their status and to take account of and take action with all limitations on the use of the certificate included in the certificate itself.

14. RESPONSIBILITY DISCLAIMER

The Provider does not respond in cases where the damages are due to negligence, lack of care or basic knowledge of usage with Qualified Certificates by the Holder, Creator or Relying party.

The Provider is not liable for any damages caused by the untimely termination and suspension of certificates and verification of the status of certificates for reasons beyond his control.

The Provider is not responsible for the use of a certificate beyond the limits of use and the usage restrictions included in the certificate.

The Provider is not responsible for violating third party rights regarding their trademarks, trade names or other proprietary or non-proprietary rights where the information contained in the certificates issued has led to such breaches.

The Provider is not responsible for any direct or indirect, predictable or unpredictable damages occurred as a result of using or trusting suspended, terminated or expired certificates.

The Provider is not responsible for the manner of use and for the accuracy, authenticity and completeness of the information included in test, free or demonstration certificates.

The Provider is not responsible for the security, integrity and use of software products and hardware devices used by Holder, Creator of a Seal or Relying party.

15. CONFLICT MANAGEMENT AND JURISDICTION

Any disputes arising between the parties regarding the Qualified Certification Services Agreement shall be settled by agreement between the parties through understanding and a spirit of goodwill, and if not possible otherwise, shall be settled by the competent Bulgarian court.

All complaints or claims by Subscribers must be addressed to the Provider in writing and sent to: 1000, 16 Ivan Vazov Str. or electronically signed at legal@infonotary.com.

Complaints and claims will be reviewed promptly and the complainant shall receive a response within 14 days of receiving the complaint from the Provider.

16. APPLICABLE LAW

For all matters not settled in the Certification Practice Statement for Qualified Certification Services of Infonotary PLC, the provisions of the national and European legislation are in force.

17. CERTIFICATION AUTHORITY, LICENSES, REPOSITORIES, CONFIDENTIAL MARKS AND AUDITS

Further information about results of audits, certifications and accreditations of the Provider is kept up-to-date at: http://www.infonotary.com.