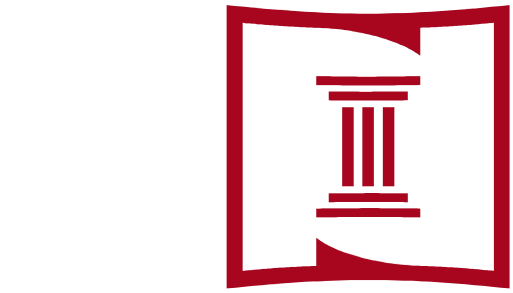

InfoNotary

PUBLIC KEY INFRASTRUCTURE STATEMENT

OF
QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

Version 1.0

Entry into force 01.06.2017

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 Validated Domain CP	1.3.6.1.4.1.22144.3.3.1

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.

2.1.1. InfoNotary Qualified Natural Person Signature

The certificate is issued to an individual (Holder) and can be used for personal identification in front of Internet applications, for financial transactions, secure and encrypted communication, electronic correspondence, signing of electronic documents and electronic statements, authentication and data encryption.

2.1.2. InfoNotary Qualified Delegated Signature Certificate

The certificate is issued to an individual (Holder) and contains information about a legal entity that has delegated authority to the Holder and can be used for personal identification before Internet applications, for financial transactions, secure and encrypted communication, electronic correspondence, signing electronic documents and electronic statements, authentication and data encryption.

2.1.3. InfoNotary Qualified Legal Person Seal Certificate

The certificate is issued to a Legal Entity (Creator of an Electronic Seal) and can be used to identify the Entity in front of Internet applications, to perform financial transactions, secure and encrypted communication, electronic correspondence, sealing of electronic documents and performing warranty activities the integrity and the origin of the electronic sealed data and information. Electronic seal can also be used to authenticate the legal entity's digital assets such as software code, schemes and images.

2.1.4. InfoNotary Qualified Validated Domain Certificate

The certificate is issued to a physical or legal entity (Holder) and may be used for website authentication that is entered on it. The certificate is issued in accordance with the requirements of Regulation (EU) 910/2014 and can be used as a verification by which a visitor to the website can be sure that behind the website is a real and legitimate subject.

2.1.5. InfoNotary Qualified TimeStamp Certificate

Electronic time stamps are data in electronic form that connect other data in electronic form at a particular 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 physical and legal persons who are holders or relying party.

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.

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.

The limit on the value of transactions for Qualified Electronic Signature Certificates is determined by the Holder 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 will lead to the cancellation of the guarantees, which INFONOTARY PLC gives the Holder 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;
- Qualified Certification Services Agreement

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;
- 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 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.

10. PERSONAL DATA CONFIDENTIALITY

The Provider is registered as a personal data controller by the Personal Data Protection Commission under LPPD (Personal data protection act) and provides for the lawful processing of the personal data provided in connection with the qualified certification services in accordance with Directive 95/46/EC and the national law.

The Provider stores and processes the personal data provided to him as Qualified Provider of Qualified Certification Services in accordance with the Personal Data Protection Act.

The type and amount of personal data collected is proportionate to the purposes and 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 for the sole purpose of issuing and maintaining Qualified Certificates or providing another qualified certification service.

The information included in Qualified Certificates and Certificate Status Information may contain personal details of the Holder/Creator of a seal within the meaning of the Personal Data Protection Act. This data is stored and processed in the Provider's database and is available to third parties to the public.

The information collected by the Holder/Creator of a Seal/Authorized Representative and Subscriber and not included in the Qualified Certificates and in the information on their status and constituting personal data within the meaning of the Personal Data Protection Act 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.

By signing the Qualified Certification Services Agreement and the adoption of the provisions of the Certification Practice Statement for Qualified Certification Services and Certification Policies, the Holder/Creator of a Seal agrees that their personal data gathered by the Provider should be included in a Qualified Certificate and be publicly accessible to all interested persons by the Register of Certificates and the Certificate Revocation List.

11. INTELLECTUAL PROPERTY RIGHTS

The Provider owns and reserves all intellectual property rights to databases, websites, 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.