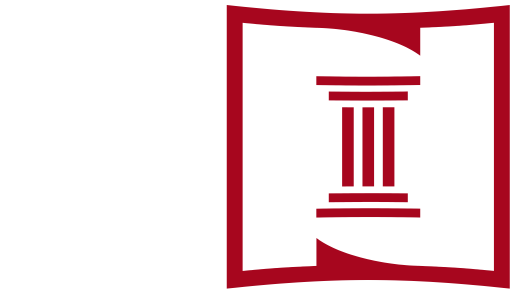

InfoNotary

POLICY FOR PROVIDING QUALIFIED SERVICES FOR WEBSITE AUTHENTICATION CERTIFICATE

OF THE QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

VERSION 2.1

Entry into force 14.10.2019

CONTENT

1. INTRODUCTION

The current document Policy for providing Qualified Certification Services for Website Authentication Certificate (The Policy) to the Trust Service Provider INFONOTARY PLC has been made in accordance with Regulation (EU) No 910/2014 of the European Parliament and the Council from 23 July 2014 on Electronic Identification and Certification Services for Electronic Transactions in the Internal Market and repealing Directive 1999/93/EC (Regulation (EC) 910/2014) and the applicable legislation of Republic of Bulgaria and refers to the objectives or some of the following generally accepted international standards and specifications:

- EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
- 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 412 Certificate Profiles
- 319 412-5 v2.1.1: QCStatements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- TS 119 495 v1.2.1: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.

The main purpose of the document Policy for providing Qualified Certification Services for Website Authentication Certificate is to make the qualified certification services public for the consumers through a detailed description of the rules and policies which INFORNOTARY PLC has implemented and observes for the performance of its activity and providing funds to all interested parties for establishing the compliance of the Provider's activity the provisions and requirements of Regulation (EU) 910/2014, the applicable legislation of the Republic of Bulgaria and the reliability and security of the certification activity, the requirements and guidelines defined by the CA/ Browser Forum (https://cabforum.org/) and the reliability and security of the certification activity.

The Policy is a public document developed in accordance with, and covering the formal requirements for content, structure and form of the internationally recognized International Engineering Task Force (IETF) RFC 3647: "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework.

The current policy can be amended as necessary in case of changing regulatory, technological and procedural requirements, and any changes

thereto are publicly available to all interested parties at: http://repository.infonotary.com and https://repository.infonotary.com.

1.1. BASICS

1.1.1. Trust Services Provider

INFONOTARY PLC is a Provider of Qualified Trust Services under Regulation (EU) No 910/2014 and has been granted qualified status by the Authority 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 UIC 131276827. The company has its registered office and address at 16, Ivan Vazov Str., Sofia, phone: +359 2 9210857, Internet address: http://www.infonotary.com. The company uses its registered trademark InfoNotary in its trade.

As a qualified provider INFONOTARY PLC performs the following activities and provides the following qualified certification services:

Qualified Website Authentication Certificate including:

- acceptance and verification of applications for issuing qualified certificates;
- creating qualified certificates based on the established identity and valid data for Holder;
- signing qualified certificates;
- issuing of qualified certificates.

Qualified Website Authentication Certificate management services including:

- reflecting changes in the validity status of an issued qualified certificate;
- suspension, resumption and termination of a qualified certificate;
- maintenance of a register of the issued qualified certificates;
- publishing of each issued Qualified Certificate in the Register;
- publishing in the Register of a list of suspended and terminated qualified certificates.

Qualified Website Authentication Certificate access services including:

- granting access to the registry with the issued certificates to relying parties;
- granting relying parties access to the lists of suspended and revoked certificates;

- providing services for restricting access to published certificates;

Qualified Website Authentication Certificate validation services, including:

- providing of services for on-line certificate status validation (OCSP).

In carrying out the activities of issuance and management of qualified website authentication certificates, INFONOTARY PLC applies the ISO/IEC 9001: 2008 certified Management System implemented in the company and ISO/IEC 27001: 2013 certified management system.

1.2. DENOMINATION AND IDENTIFICATION OF THE DOCUMENT

The **"Policy for providing Qualified Certification Services for Website Authentication Certificate"** (Policy) is named **"InfoNotary CP QWA"**and is identified by the following object identifier in the issued certificates:

Policy name	Identifier (OID)
InfoNotary Qualified Validated Domain CP	1.3.6.1.4.1.22144.3.3.1

The policy includes:

- description of the terms and conditions that the Provider complies with and will follow when issuing Qualified Website Authentication Certificates, as well as the applicability of these certificates in view of the level of security and limitations in their use;
- a set of specific procedures that are followed in the process of issuing and managing qualified website authentication certificates, the initial identification and authentication of the certificate Holders;
- determines the feasibility and reliability of the information included in the Qualified Website Authentication Certificate.

1.3. PARTICIPANTS IN THE CERTIFICATE INFRASTRUCTURE

1.3.1. Certification Authority

InfoNotary is the Certification Authority of the Trust Service Provider carrying out the following activities: issuance of electronic signature and electronic seal certificates, management of certificates, including suspension, resumption and termination of certificates, keeping a register of certificates issued and providing access and means of constraint access to certificates.

The Certification Authority (root CA) controls Provider's Certification Policies defining the information types contained in the different types of End User Certificates, identifying the Holder information, application restrictions, and responsibilities.

The Certification Authority issues different types of certificates, according to the certification policies through its differentiated **Operational Certification Authorities** (operational CAs).

1.3.2. Registration Authority

The Provider renders its services to end users through a network of specified Registration Authorities. The Provider's Registration Authority perform activities of:

- acceptance, checking, approval or rejection of certificate applications;
- registration of the applications submitted to the Certification Authority for certificate management certification services: suspension, resumption, termination and renewal;
- performing of check-ups of the application with permissible resources the identity data of applicants (Holders) and other data, depending on the certificate type and in accordance with the Certification Policies of the Provider;
- certificate issuance initiation after a positive examination and approval of the request and notification of the certification Authority.
-

The Provider may delegate rights and authorize third parties to act as a Registration Authority on behalf of INFONOTARY PLC. The Authorized Registration Authorities perform their activities in accordance with the InfoNotary Qualified CPS, Provider's Certification Policies and documented internal procedures and policies.

1.3.3. Subscribers

"A subscriber" is a natural or legal person who has a written agreement with the Qualified Trust Service Provider.

Where practicable, the Provider provides accessibility and usability for persons with disabilities when providing certification services and products related to the use of the services.

1.3.1. Relying parties

"Relying parties" means natural or legal persons who use trust services with qualified certificates issued by the provider and trust these qualified certificates and/or advanced/qualified electronic signatures/advanced/qualified electronic seals which can be verified through the public key embedded in the subscriber's qualified certificate.

Relying parties should have the ability to use electronic signature/seal and website authentication certificates and only trust the qualified certificates issued by the Provider after checking the status of the certificate in the List of Suspended and Revoked certificates or the automated information provided by the Provider via OCSP protocol.

Relying parties are required to verify the validity, suspension or termination of certificates from actual information about their status and to take into account and take action with any limitations on the use of the certificate included in the certificate itself or InfoNotary Qualified CPS and certification policies.

1.3.2. Holder

"Holder" is a natural person owning a qualified certificate issued by the Provider and is entered as such in the certificate.

1.3.3. Representatives

A "Representative "is duly empowered by the Subscriber, the Holder/Creator of the seal natural person who performs acts on his behalf for issuing and managing electronic signature/electronic seal certificates, certificates of website authenticity or for use of other trust services to the Provider.

1.4. USE OF CERTIFICATES

1.4.1. Certificates of the Certification Authority

1.4.1.1. Base certificate (Root)

The Root certificate for the Public Key of the Certification Authority of the Provider, named as: **InfoNotary TSP Root** is a self-issued and self-signed qualified electronic signature certificate, signed with the Provider's basic private key. The Basic Private Key of the Provider, certified by the certificate of its public key **InfoNotary TSP Root**, is used to sign the certificates of the Operational Certification Authority of the Provider and other data related to the management of the certificates issued by the Provider, including the List of Suspended and terminated certificates issued by it (root-ca.crl). The provider uses other basic private keys as well and issues other self-signed certificates for their public keys for its activities they perform and the services they provide to end users outside the scope of the regulated certification services in Regulation (EU) No 910/2014.

Certificates of the Operational Certification Authority (InfoNotary Operational CAs)

The Operational certification Authority of the Provider issue and sign end users certificates and data for the status of certificates issued by them. The Operational Certification Authorities of the Provider issue Qualified Certificates to consumers in accordance with the Practice and Policy for Providing Qualified Certification Services.

1.4.1.2. Operational Certification Authority for qualified website authentication certificates (InfoNotary Qualified Validated Domain CA)

The certificate for the public key of the Operational Certification Authority for website authentication **InfoNotary Qualified Validated Domain CA**, OID: 1.3.6.1.4.1.22144.3.3 is signed with the private key of the Basic Certification Authority InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3.

With the private key of the Operational Certification Authority **InfoNotary Qualified Validated Domain CA**, according to the respective Certification Policy and InfoNotary Qualified CPS are signed:

- End-user qualified certificates for website authentication InfoNotary Qualified Validated Domain;
- End-user qualified certificates for website authentication for organization InfoNotary Qualified Organization Validated Certificate;
- End-user qualified certificates for website authentication for PSD2 InfoNotary Qualified PSD2 WA Certificate

The list of suspended and revoked certificates of end-users (**qualified-domain-ca.crl**) is signed with the private key of **InfoNotary Qualified Validated Domain CA.**

1.4.1.3. InfoNotary Qualified Website Authentication Certificates

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.

1.4.2. Usage and accessibility of services

When 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.

1.4.3. Certificate activity limitations

Qualified Website Authentication Certificates issued by the Provider on the basis of this Policy may be limited in terms of goals and application. The Provider shall not be liable for damages incurred as a result of the use of the certificates issued by him outside their authorized use and according to the limitations of the application with regard to the purpose and will lead to the cancellation of the guarantees that INFONOTARY PLC gives to the Holder and the Relying parties.

1.5. Management of the Provider's Certification Policy

The Provider's certification policy is determined by the Board of Directors of INFONOTARY PLC.

All changes, modifications and additions to the Policy are accepted by the Board of Directors of INFONOTARY PLC.

New versions of the documents are published after their approval in the Documentary repository of the Provider and are publicly available at: http://repository.infonotary.com and https://repository.infonotary.com.

All comments, inquiries, and clarifications on the Practice for the provision of Qualified Certification Services and Certification Policies can be addressed at:

"INFONOTARY" PLC
1000 Sofia, Bulgaria
16 "Ivan Vazov" Str.
Tel:+359 2 9210857
e-mail: legal@infonotary.com
URL: www.infonotary.com

1.6. TERMS AND ABBREVIATIONS

Authentication	Electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed
Certificate for website authentication	Attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
Electronic document	Any content stored in electronic form, in particular text or sound, visual or audio-visual recording
Electronic identification	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service
Person identification data	Set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
PIN	Personal Identification Number
Practice	Certification Practice Statement is a document containing rules on the issuance, suspension, renewal and revocation of certificates, the conditions for certificates access **InfoNotary Qualified CPS**
Policy	Policy for Providing Qualified Certification Services for Qualified Website Authentication Certificate
PSD2 Directive	DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE

	COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
Qualified certificate for website authentication	A certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV, Regulation EU 910/2014
Qualified trust service provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body
Qualified trust service	A trust service that meets the applicable requirements in Regulation EU 910/2014
Relying party	A natural or legal person that relies upon an electronic identification or a trust service
Regulation	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
Regulation GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Trust service provide	A natural or a legal person who provides one or more trust services either as a qualified or

Trust service	as a non-qualified trust service provider Electronic services normally provided for remuneration by the Trust Service Provider which consists of: - the creation, verification, and validation of electronic signatures, electronic seals or electronic time-stamps, electronic registered delivery services and certificates related to those services, or - the creation, verification and validation of certificates for website authentication or - the preservation of electronic signatures, seals or certificates related to those services.
Validation	The process of verifying and confirming the validity of an electronic signature or seal
Validation data	Data that is used to validate an electronic signature or an electronic seal
Person identification data	A set of data to identify the identity of a natural or legal person or a natural person representing a legal person

ABBREVIATIONS

ASN.1	Abstract Syntax Notation One – Abstract object-description language for certificates
CA	Certification Authority
CC	Common Criteria
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CP	Certificate Policy
CPS	Certification Practice Statement
CRC	Communications Regulation Commission
CRL	Certificate Revocation List - List of suspended and revoked certificates
DN	Distinguished Name - Unique name
ETSI	European Telecommunications Standards Institute
EU	European Union
EBA	European Banking Authority
FIPS	Federal Information Processing Standard
IEC	International Electrotechnical Commission
ISO	International Standardization Organization
LDAP	Lightweight Directory Access Protocol - A protocol for simplified directory access
NCA	National Competent Authority
OID	Object Identifier

OCSP	On-line Certificate Status Protocol – Protocol for real-time checking of certificate status
PKCS	Public Key Cryptography Standards – Cryptographic standard for public key transfer
PKI	Public Key Infrastructure
PSD2	Payment Service Directive 2
PSP	Payment Service Provider
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider issuing Card-based payment instruments
PSP_AI	Payment Initiation Service Provider
RA	Registration Authority
RSA	Rivest-Shamir-Adelman – Cryptographic algorithm for signature generation
SSCD	Secure Signature Creation Device
QSCD	Qualified Signature Creation Device
SHA	Secure Hash Algorithm – Hash Algorithm for hash identifier extraction
SSL	Secure Socket Layer – Secure data transmission channel
URL	Uniform Resource Locator

2. OBLIGATIONS AND REPOSITORY RESPONSIBILITIES

The Provider publishes information about the Qualified Certification Services and the issued Certificates that it provides in a database and publicly available electronic registers.

2.1. Repositories

2.1.1. Public Document Repository

All public information related to the Provider's activity is published and updated regularly in an electronic document repository, publicly accessible at: http://repository.infonotary.com

The published versions and updated editions of at least the following documents of the Provider are maintained in the document repository:

- Certification Practice Statement for qualified certification services;
- Certification Policies for qualified services;
- Qualified certification services agreement;
- Tariff for providing qualified certification services;
- Other public documents and information.

The access to the documents published in the document repository for the purpose of reading and retrieving them is unlimited and free.

2.1.1. Certificate Register

The Provider keeps an electronic certificate register where it publishes all certificates issued by it. The electronic certificates register is a database that is updated upon issuance of a certificate.

The Provider maintains and publishes in the electronic register separate lists of suspended and terminated Qualified Website Authentication Certificates.

2.1. Publish certificate information

The issued certificates shall be published in the Register of Certificates promptly after being signed by the relevant Certification Authority of the Provider - InfoNotary Qualified Validated Domain CA. In the event of suspension or revocation of a certificate, the change shall be entered into the Provider's database and such certificates shall be published on the Certificate

Revocation List by the respective Certification Authority of the Provider in a timely manner after their suspension or revocation but no later than 24 hours of their being suspended or revoked. Resumed certificates are removed from the List of Suspended or Revoked Certificates

2.1. Frequency of publications

The certificate database is updating automatically, immediately when a newly issued certificate is published and when the status of a certificate is changed. The lists of the suspended or revoked certificates are updated automatically in a timely manner after inclusion in the list of suspended certificate, revoked certificate and withdrawal from the list of resumed certificate. The lists of suspended and revoked certificates are as well updated within 3 hours of the last publishing if they have not been updated. The term of validity of a published list of suspended or revoked certificates is 3 hours. 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.

Any changes to documents published in the Document repository are published immediately after they are accepted by the Board of Directors of INFONOTARY PLC.

2.1. Access to the certificate register

Provider's certificates are publicly available through HTTP/HTTPS access at www.infonotary.com and LDAP based access at:

ldap://ldap.infonotary.com/dc=infonotary,dc=com

Any interested party may initiate a search in the Certificates Register according to certain criteria and may read or retrieve/download published certificates from:

http://www.infonotary.com/site/?p=search

The Provider does not limit in any way and in any form the access to the Certificates Directory. The Directory is constantly accessible, except in cases of force majeure or events beyond the Provider's control. Upon explicit request of the Holder, the Provider may restrict the access for reading and downloading his qualified certificate but information about the issued certificate and its status is always presented.

The Provider ensures complete physical, technological and procedure

control in keeping the register ensuring that:

- only duly Authorized personnel may enter data into the register;
- changes to the data in the register are not possible;
- the possibility of unauthorized interference is minimized.

3. IDENTIFICATION AND AUTHENTICATION

The Provider maintains Registration Authorities that verify and confirm the identity and/or other data included in Qualified Website Authentication Certificate. Before the issuance of a certificate by the Certification Authority of the Provider to be confirmed, the Registration Authority confirms the Holder's identity. The Provider's Registration Authorities observe specific procedures for checking the names, including the protected data in some names. Registration Authorities authenticate requests for terminating the validity of certificates in accordance with the provisions of the InfoNotary CPS.

3.1. Naming

The qualified certificates have a format in conformity to X.509 standard. The Registration Authorities shall verify and ensure that the names in the request for certificate issuance comply with the X.509 standard.

The "Subject" field on the certificate contains the name of the Holder.

The name and other distinguishing signs of the Holder in the corresponding fields for each type of certificate are in accordance with the DN (Distinguished Name) formed according to X.500 and X.520 standard.

3.1.1. Name types

When identifying the Holder in the certificates, the Provider uses different name types for the name and individualized data such as X.500 unique names and RFC-822 names.

In a certificate issued by the Provider the names assigned to the Holder are unique and are always used in combination with a unique certificate number.

The names included in the Distinguished Name (DN) of the Holder have their meaning in Bulgarian or in another foreign language. The DN structure depends on the type of certificate and Holder. DN consists of the following areas (the descriptions are in conformity with RFC 3280 and X.520):

- C – international abbreviation of the name of the country name (BG for Bulgaria),
- CN – domain name (DNS name) or public IP address;
- the full name of the natural person or the legal entity,
- GN – given name of the natural person,
- SN – surname of the natural person,
- O – name of the legal person,
- Organization Identifier
- E – e-mail address,
- Serial Number – the natural person unique identifier,
- Other fields that are detailed in the policies for the relevant qualified certificates profiles.

3.1.2. Pseudonyms

The Provider does not issue Qualified Certificates based on the use of a pseudonym as a means of naming the Holder.

3.1.3. Alternative name (Subject Alt Name)

Contains at least the CN records, with additional domains/public IP addresses under the control of the Holder of the certificate.

3.1.4. Rules for interpreting different forms of names

Only the information contained in the request and duly supported by documentation, identifying the Holder, is included in the qualified certificate issued by the Provider.

For the identification of the Holder - Individual, the certificate shall include the following data in GN - the personal name of the individual and the SN - surname of the individual.

The information for identification of a Legal Person other than the Holder is entered into the OrganizationName field and includes:

- Organization name of legal person - the full name of the organization as it appears on its registration document

In Qualified Website Authentication Certificates, the unique name (DN) necessarily contains the name of the domain that is owned by the legal entity - Holder.

3.1.5. Uniqueness of the names

The Provider issues certificates with a unique number in his register.

The combination of the Holder's name, together with the type of certificate is unique for valid certificates.

3.1.6. Recognition, authenticity and role of trademarks

The Provider complies with verification procedures when issuing certificates with regard to the right of the Holders over reserved trademarks, brand names, domains, etc., requested to be included in a certificate.

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.

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

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

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

3.1. Initial identification and identity verification

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

3.1.1. Method for verifying the holding of the private key

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

3.1.2. Identity validation of a Legal entity

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

3.1.3. Identifying a natural person

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

3.1.4. Authentication of domain name (website)

Before issuing the Qualified Website Authentication Certificate, the Provider verifies the domain name and/or IP address requested for registration. The verification includes verification of ownership of the domain by the person requesting the certificate, and whether the domain and IP address are operational and under its control.

3.1.5. Unconfirmed information

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

3.2. Identity validation and authentication of a certificate revocation request

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

3.3. Identity validation and authentication of a certificate suspension request

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4. EFFECTIVE CONDITIONS

4.1. Request for issuance of a certificate

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.2. Procedure for requesting a certificate

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.3. Issuance of a certificate

4.3.1. Action of the Certification Authority when issuing a Certificate

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.4. Data secrecy of qualified trust services and certificates usage

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.5. Certificate renewal

4.5.1. Conditions for certificate renewal

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.5.2. Renewal request procedure

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.6. Termination of a certificate

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

4.6.1. Conditions for terminating a certificate

The validity of valid certificates issued by the Provider is automatically terminated:

- when the certificate validity date expires;
- when the Provider's legal entity revokes the trust services without transferring the activity of another qualified provider of qualified certification services.

The Trust Service Provider revokes the certificate validity in case of:

- termination of the legal person - Holder;
- finding out that the certificate was issued on the basis of false information.

The Provider takes immediate actions on the termination of the certificate validity when there is justification for doing so. The Certification Authority of the Provider revokes the validity of certificates issued by him. The Provider immediately notifies the Holder of the circumstances regarding the validity or reliability of the certificate issued.

The Trust Service Provider is obliged to terminate the validity of a certificate when the Holder asks for it after checking the identity and the legal entity of the Holder.

4.6.2. Termination request procedure

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.6.3. Verification requirements for termination of a certificate to the Relying parties

The Relying Parties shall rely on qualified certificates issued by the Provider only after checking their status in the Certificate Revocation List or through the automatic information provided by the Provider through an OCSP

protocol.

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

4.6.4. Frequency of updating the Certificate Revocation List

The Certificate revocation list is updated automatically after a certificate is listed therein. The term of validity of the Certificate revocation list is 3 astronomic hours.

The Certificate revocation list is updated automatically no later than 3 hours of publishing the last CRL.

The Provider offers the service of checking the status of certificates issued by him in real time through an OCSP protocol. The Relying Parties may use the information provided by the automated system to verify the status of a certificate using an OCSP protocol in accordance with the provisions of this document.

4.7. Suspension of a certificate

4.7.1. Conditions for certificate suspension

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. The Provider takes immediate actions regarding the suspension of a certificate if the circumstances for that are established. The Provider immediately notifies the Holder of circumstances concerning the validity or trustworthiness of the certificate issued to him. For the period of suspension the certificate is deemed invalid.

The Provider shall suspend the certificate without carrying out identification and authentication of the applicant under the following conditions:

- by request of the Holder;
- by request of a person for whom it is apparent from the circumstances that he or she may be aware of security breaches of the private key or other circumstances;
- by order of the Supervisory authority - in case of imminent danger to the interests of third parties or in case of sufficient evidence of violation of the law.

4.7.2. Suspension request procedure

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

4.7.3. Resuming a suspended certificate

The Provider resumes the suspended certificate at:

- expiration of the suspension period (48 hours);
- grounds of suspension removal;
- upon request of the Holder, once the Provider or the Supervisory Authority is certain that he/she has learned of the reason for the suspension and that the request for resumption is made as a result of this information.

Once the certificate has been resumed by the Certification Body of the Provider, it is considered valid.

4.7.4. Resuming a suspended certificate procedure

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

5. EQUIPMENT, PROCEDURE AND MANAGEMENT CONTROL

5.1. Physical control

The Provider ensures physical protection and access control to all critical parts of its infrastructure that are located in its own, rented or leased by the Provider.

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 premises

The premises 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

The provider ensures strict control of access to all its premises and information resources by means 24-hour physical security, electronic access control systems, video surveillance systems and alarm systems, etc.

Access control procedures, as well as physical access control systems - monitoring, access and signaling, are subject of scheduled and incidental audit and control.

Only the authorized members of the Provider's personnel, who strictly adhere to and follow the established internal procedures for identification, verification and documenting access, have access to certain premises and information resources of the Provider.

5.1.3. Power supply and ambient conditions

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.

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.

The antenna systems used by the Provider are equipped and protected with an overload protection system.

5.1.4. Floods

The Provider ensures a system for monitoring and notification in case of flooding in the premises.

5.1.5. Fire alarm and protection

The provider ensures fire alarm devices and fire protection system in case of fire on its premises.

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 components out of use and operation

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

5.1.8. Duplicate components

The Provider duplicates all critical components of the Certification Authority's infrastructure, as well as monitoring tools and automatically replaces critical components, if necessary.

5.2. Procedural control

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 the competence to perform the activity of Qualified Provider of Certification Services in accordance with the requirements of Regulation (EU) 910/2014 and the applicable Bulgarian

legislation.

The procedures described in the InfoNotary Qualified CPS related to the activity of the Certification Authority of the Provider are implemented in accordance with the established internal rules and regulations of the Provider.

All persons from the Provider's staff sign a declaration of absence of conflict of interest, confidentiality of information and protection of personal data.

The Provider provides double control over all critical functions of the Certification Authority.

For certain activities, the Provider may also use outsiders.

5.2.1. Positions and functions

The Provider has at his disposal the requisite number of qualified personnel who, at any time of the execution of his activity, shall ensure the fulfillment 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 staff members.

5.2.3. Identification and authentication of each position

The provider has developed job descriptions for each of the positions of his staff.

5.2.4. Requirements for division of responsibilities for separate functions

The positions under cl. 5.2.1 are performed by different members from the Provider's staff.

5.3. Staff control, qualification and training

The technical staff of the Provider is carefully selected and possesses professional knowledge in the following areas:

- security technologies, cryptography, public key infrastructure (PKI);

- technical standards for security assessment;
- information systems;
- large databases administration;
- network security;
- audit, etc.

The Provider checks his future employees on the basis of references issued by competent authorities, relying parties and on the basis of statements.

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

The provider organizes regular refreshing training to ensure continuity and timeliness of staff knowledge and procedures.

The Provider imposes sanctions on the staff for unauthorized actions, malpractice and unauthorized use of Provider's systems.

5.3.1. Requirements to independent suppliers

Independent suppliers used by the Provider comply with the same policies and procedures, including information privacy and personal data protections as well as the Provider's staff.

5.3.2. Documentation provided to the staff

The Provider provides documentation - procedures and rules to the Certification Authority and the Registration Authority staff for initial training, qualification improvement, etc.

5.4. Procedures for the preparation and maintenance of inspection data journal

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

The Provider records all events related to the activities of the Certification Authority, including but not limited to:

- issuing a certificate;
- signing a certificate;
- termination of a certificate;
- suspension of a certificate;

- publication of a certificate;
- publication of a list of suspended and revoked certificates.

The records contain the following information:

- identification of the operation;
- date and time of the operation;
- identification of the certificate involved in the operation;
- identification of the person who performed the operation;
- a reference to the request for the operation.

The Provider records all events related to the operation 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 access to the software PKI components of the systems;
- in cases software and hardware system failures, etc.;
- in cases of managing and using the hardware cryptomodules.

Records of actions performed by the Registration Authority in the process of registering Subscribers, identifying Holders and Creators, etc., are also stored.

Recorded generated by the communication devices of the Provider are also stored.

Back-up copies of the records and logs are generated at discreet intervals of several hours up to 24 hours for the different modules. The back-up copies are saved on physical carriers and stored in a room with a high level of protection, security and access control.

Records and logs are kept for 10 (ten) years.

All records and logs generated by the components of the certification infrastructure are stored electronically. Only qualified authorized members of the Provider's staff have the right to access and work with these records and logs.

Back-up copies of the records and logs are generated at discreet

intervals of several hours up to 24 hours for the different modules. The back-up copies are saved on physical carriers and stored in a room with a high level of protection, security and access control.

5.5. Archive

The Provider stores as internal repository the following documents:

- all certificates issued for a period of at least 10 (ten) years after expiry of the term of validity of a certificate;
- all records and logs related to the issuance of a certificate for a period of at least 10 (ten) years after the issuance of a certificate;
- all records and logs relating to the termination of a certificate for a period of at least 10 (ten) years after the termination of the certificate;
- lists of suspended and revoked certificates for a period of at least 10 (ten) years after termination or expiry of the term of validity of the certificate;
- all documents related to the issuance and management of certificates (requests, identification and authentication documents, agreements, etc.) for a period of at least of 10 (ten) years after expiry of the term of validity of the certificate.

The Provider stores the records in a recoverable format. The Provider ensures the integrity of the physical carriers and implements a copying mechanism to prevent data loss. The repository is accessible only to authorized personnel of the Provider and the Registration Authority, if necessary.

The Provider keeps a repository of the certificates, inspection data, information related to the request for issuance and management of certificates, logs, records and facilitating documentation of the certification services.

The Provider keeps the archive for a period of 10 (ten) years. Upon expiration of this period, the archived data may be destroyed.

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

- only staff authorized to keep the archive has access to it;
- protection of the archive from modifications by recording the data on single-entry devices;
- protection from archive erasing;
- Protection ensuring the destruction of carriers on which the archives has been stored, after the regular transfer of data to a new carrier.

The time of creation of separate records and documents from the

Provider's systems is verified by certifying the date and time of their creation and signing through the TimeStamp Server of the Provider.

Archival information is stored in rooms with a high level of physical protection and in conditions allowing the safe and long-term storage of paper, magnetic, optical and other carriers. Archive information that is public is published and is available in the Public Registry of the Provider in a readable form.

5.6. Key compromise and disaster and unexpected cases recovery

In order to maintain the continuity and integrity of its services, the Provider implement, document and periodically test appropriate contingency plans and procedures for disaster and unexpected cases recovery.

The Provider make every endeavor to ensure full and automatic recovery of its services in the event of a disaster, computer resources failures, software or information corruption.

With a priority the Provider ensures the recovery of maintenance and the public access to the Certificate Register and the list of suspended and revoked certificates.

In case of compromising the private key of the Certification Authority of the Provider, the following actions are taken:

- the Provider's electronic signature certificate is terminated immediately;
- the Supervisory Authority is notified of the termination of the Provider's certificate;
- the customers of the certification services of the Provider are informed by publishing information on the public site and by e-mail;
- 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 reissued.

In the event of the Holder’s private key being compromised, the latter shall immediately notify the Provider of the initiation of the procedure for termination of an existing certificate.

5.6.1. Action in case of disasters and accidents

Archival data containing information on requests for issuance, management and termination of certificates as well as records of all certificates issued in the database are stored in a safe and reliable place and are accessible by authorized employees of the Provider in the event of a disaster or accident. For emergency actions, the Provider has developed a "Contingency plan", which is checked once a year.

The provider must be able to detect any possible incident. After analyzing what has happened, the aim is to prevent future incidents based on system errors or failures of service and technologies. The Provider monitors all systems and services without interruption (24/7) and has an information and help phone where users can report incidents or faulty services.

The plan identifies the approximate time to detect any kind of incidents. The provider ensures that any potential incident can be detected. The provider is able to distinguish between real incidents and false alarms. Serious accidents are reported to the management. The plan identifies the approximate time for notification and confirmation. It defines roles and responsibilities and evaluates the type of incident, the right response time and further actions. The events are recorded. The causes for the accident and the way it has affected the work efficiency are documented. The measures presented (response time and recovery time of the service or system, etc.) are recorded. All data is analyzed and the Provider's actions are subject to change and improvements if necessary. The plan provides the type of archiving and provisioning that is used, at what intervals the archiving takes place, where to store the information and the structure, etc.

5.7. Termination procedures of the provider's activity

The activity of the Provider is terminated in accordance with the applicable national legislation. Upon termination of its activities, the Provider shall notify the Supervisory Authority of its intentions not later than 4 months before the date of termination and whether it will transfer its activity to another Provider. The Provider notifies the Supervisory Authority 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 procedure. The Provider shall make every effort and care to continue the validity of the certificates he has issued by transferring it to an operative qualified certification services provider.

The Provider shall notify the Supervisory Authority and the consumer in written form that the Provider's activities are undertaken by another qualified

provider no later than the time of termination. A written notice is also published on the Provider's web site and also contains information on the name and contact details of the provider-successor. The Provider notifies its users about the conditions of maintenance of the transferred certificates to the provider-successor. The Provider duly transfers all documentation related to its activities to the provider-successor together with all repositories and all certificates issued (valid, terminated and suspended). In case that the Provider fails to transfer his activity to another qualified provider, he shall suspend the validity of all certifying authorities, all issued end user certificates by him and and stores all documentation relating to the activity all records and all issued certificates (valid, terminated and suspended) for a period of 10 years.

If the qualified status of the Provider has been removed, the information must be transmitted electronically or in written form to holders of valid qualified certificates, relying parties and to entities that have concluded contracts directly related to the provision of qualified certification services. This information will be published at the webpage of the Provider: www.infonotary.com and will be displayed prominently in all registration offices or will be published in other ways as specified in the applicable national legislation. The information will also include a statement declaring that qualified certificates issued by the Provider can no longer be used in accordance with applicable law.

6. TECHNICAL SECURITY CONTROL

6.1. Generating and installing key pair

The Provider protects its own private keys according to the provisions of current practice.

The Provider uses the Intermediate and Operating Private Keys for signing the Certification Authority only to sign certificates and certificate revocation lists in accordance with the permitted use of these Keys in this document.

The Provider will refrain from using the private keys used by the Certification Authority for use beyond the limits of the Certification Authority.

Users of the certification services of the Provider generate their pair of cryptographic keys - private and public, for Qualified Certificates for Electronic Signature, Electronic Seal and Website Authenticity:

- alone, at the Holder - with hardware and software under their control,
- at the Provider or an Authorized Registration Authority with its hardware and software, part of the Provider's infrastructure.

When generating the key pair for Qualified certificate is performed by the Provider, a Qualified Signature Creation Device (QSCD) with a Common Criteria defined security layer (EAC) 4 + or higher according to ISO 15408 or other specification defining equivalent security levels and compliance with the provisions of Regulation (EU) 910/2014 is used.

On the basis of contractual relations, the Provider may grant to the Holder/Creator technical devices (software, smart cards and other cryptographic devices) that comply with the level of security requirements and regulations, approved under Regulation (EC) 910/2014 and national legislation of Regulation (EU) 910/2014.

The Holder or the Creator may also use other cryptographic devices and software complying with the requirements of Regulation (EU) 910/2014 other than those provided by the Provider if they are approved for use under Regulation (EU) 910/2014 and national legislation.

In the case of self-generation and installation by the Holder or Creator of cryptographic keys for Qualified Certificates issued by the Provider, the use of licensed software by a particular manufacturer is mandatory.

6.1.1. Generating key pair

6.1.1.1. Generating a private key of the Certification Authority of the Provider

For generating and installing the private keys of the Certification Authority, the Provider uses the highest reliability and security system following a documented internal procedure.

For generating and usage of the private key of the Certification Authotiry, hardware security modules FIPS 140-2 Level 3 or higher level are used.

The documented procedure for generating and installing the root pair of keys of the Certification Authority of the Provider is carried out by an authorized employee of the Provider and in the presence of the members of "INFONOTARY" PLC Board of Directors.

The secret portions of the base private key and all operational private keys of the Certification Authority are distributed, stored and presented as necessary for use by persons authorized by the Provider.

The additional protection against compromise and unauthorized use of the private keys of the Certification Authority of the Provider is guaranteed by the additional access control policy implemented by the Provider:

- the management of the hardware module through secret data accessible only to authorized persons;
- control of access to management and use of the private operating keys of the Certification Authority through separate secret data accessible only to authorized persons.

6.1.1.2. Generating key pair for Subscriber

The Provider offers a subscriber key pair generation service which uses a security mechanism for creating a qualified signature ("Qualified Signature Creation Device" – QSCD) with a security profile defined in accordance with the general requirements ("Common Criteria") level of security EAL 4+ or higher in accordance with a security profile under Regulation (EU) No 910/2014 on technical means for securely generating and storing key pair- cryptographic smart cards and other cryptographic devices.

The Private Key of the Holder, respectively the Creator, is generated/recorded on a technical tool - smart card, token, etc., and is

automatically and irreversibly erased from the Provider's resources if such are used in generation.

6.1.2. Private key delivery

When the Provider generates the pair of keys of the Holder or the Creator respectively, the private key of that pair is recorded on a smart card or other technical means in accordance with the requirements of Regulation (EU) No 910/2014 and accessed by a PIN or password.

The technical means are passed on to the Holder, respectively the Creator, together with access rights (PIN, AIN)

6.1.3. Delivery of the Public Key to the issuer of the Certificate

This procedure is performed only by the Holder, respectively the Creator, who generates the key pair and delivers the public key to the Provider for the purposes of the certification process.

The electronic certificate issuance request through which the public key is delivered to the Provider should be in the PKCS#10 file and in DER format.

The Holder/The Creator may provide the electronic request:

- personally in the Registration Authority or
- by electronic means and at address http://www.infonotary.com.

6.1.4. Delivery of the Public Key of the Certification Authority to the Relying Parties

The public keys of the Certification Authority of the Provider are publicly available on the Provider's Internet portal at: http://www.infonotary.com.

6.1.5. Key length

The length of the private key of the certification authority's underlying certificate – InfoNotary TSP Root CA e RSA is 4096 bits.

The length of the private key of the RSA Operational Certificates is 3072 bits.

For the issuance of a Qualified Electronic Signature Certificate, Qualified Electronic Seal and Website Authenticity, the Private Key of the Holder or Creator respectively must be at least 2048 bits long for the RSA algorithms.

6.2. Private key protection and Technical Control of the Cryptographic Module

6.2.1. Cryptographic Module Standards

The Certification Authority of the Provider uses secure and reliable hardware cryptographic modules covering all regulatory requirements.

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 FIPS 140-2, Level 3, FIPS 140-1 Level 2, CC EAL 4+ or higher.

The Provider accepts upon issuance of a Qualified Signature/Seal Certificates, the qualified electronic signature/seal creation device in which the Holder/Creator's private key is generated and stored to be a security level CC EAL 4+/FIPS 140-2 Level 3 or higher.

6.2.2. Storage and usage of a private key control

A procedure for the storage of the private keys and their archiving is simultaneously performed with the process of generating and installing the keys of the Certification Authority of the Provider.

The secret parts for access the base private key, as well as all operational private keys of the Certification Authority, are stored, shared on smart cards protected by PIN.

Providing the shared parts to the persons authorized for their preservation and presentation shall be documented in writing.

The Holder/Creator’s Private Key is only used in an electronic signature /seal creation device or in a device with an equivalent level of security (as required by Regulation (EU) No 910/2014) and is accessible via PIN.

The Provider does not in any way store or archive a Holder/Creator’s private key to create an electronic signature/seal.

6.2.3. Storage of Private keys

The private keys of the Certification Authorities of the Provider are stored

in encrypted form in the Hardware Security Module (HSM); the decryption requires secret parts to access keys that are shared and used only by authorized persons, provided that a required quorum of at least 2 out of 4 persons. The private key storage procedure also includes the procedure for recovering the private keys for work in a backup technical center by means of a backup HSM subject to the same requirements for shared use of the secret parts for access the keys by authorized persons and in quorum 2 out of 4.

The Holder/Creator's private key is generated and stored on signature/seal creation device as required by Regulation (EU) No 910/2014 and is accessible via PIN and cannot be stored on another device or outside it.

6.2.4. Private keys archiving

The Provider archives all of its private keys of the Certification Authorities and stores them for a period of 10 years after their expiration term or after their termination.

Keys archiving is performed by authorized employees of the Provider.

The Provider does not make copies and does not archive the Holder/ Creator's private keys that are generated on a qualified signature/seal creation device. In the event of a defect, loss or destruction of the qualified electronic signature/seal creation device, the Provider shall terminate the certificate issued in connection with the keys generated by this device.

6.2.5. Private keys Transfer in and out of the cryptographic module

The Provider generates and stores all its private keys to the Certification Authorities in hardware cryptographic module (HSM) in encrypted form, and can only be transferred to another cryptographic device in encrypted form, subject to a special procedure for this purpose, by authorized for that purpose Provider’s employees and shared access rights to secret data.

Transfer of Provider’s private keys can be made upon a recovery after HSM defect or upgrade of the Provider's technological infrastructure.

The Holder/Creator’s Private Key cannot be transferred from/to the qualified signature/seal creation device which it was generated as required by Regulation (EU) No 910/2014).

6.2.6. Activation and Deactivation of Private Keys

Provider's private keys are activated depending on the type of service they use.

The Private Key of the Base Certificate Authority (root CA) is stored disabled in offline mode on a separate HSM cryptographic device and is activated via special procedure by authorized persons holding shared access rights to secret units and in quorum 2 of 4 persons. All actions are documented and kept in the Provider's records. The Root CA private key is enabled to execute the signing of newly issued Operational Certification Authorities and to manage already issued, including the signing of CRL, terminated and suspended certificates.

The private keys of the Operational Certification Authorities are stored and used activated in a cryptographic device HSM; upon their activation and deactivation, a special procedure is followed by authorized persons holding shared access rights to secret units and in quorum 2 out of 4 persons and all actions are documented and kept in the Provider's records.

Private key of the Holder/Creator is deactivated by deleting the containers where the private key is stored on the signature/seal creation device or by physically destroying the device itself.

6.2.7. Private Keys Destruction

Provider's private keys are destroyed in accordance with the procedure of destruction of the private keys of the Certification Authority of the Provider upon expiration of their validity term by authorized employees.

The procedure guarantees their final destruction and the impossibility of their recovery and use. The process of destroying the keys is documented and the related records are stored in the Provider's archive.

Private keys of the Holder/Creator's are destroyed by deleting the container of the qualified signature/seal creation device or by physical destruction of the device itself.

6.3. Other aspects of managing the key pair

6.3.1. Public key archival

The Provider archives all of its public keys and stores them for a period of 10 years after their expiration or termination.

6.3.2. Validity period of the certificate and period of use of the key pair

The Provider issues Qualified Electronic Signatures, Qualified Electronic Seal Certificates, Qualified website authentication certificates to end users with a validity period that is entered in the content of the Certificate.

Certificates issued by the Certification Authority of the Provider for the basic public key and the operational public keys are issued with a specified validity period that is entered in the content of the certificate.

The validity period of the certificate is also a validity period for usage of the key pair connected with it.

Creating signatures by using a private key of an expired certificate is invalid.

6.4. Activation data

The Provider stores the activation data related to the private keys of the Certification Authority and activities on secure media and high-level protection archives.

The Holder using a smart card to store his private key is required to store and protect the personal data for activation of his smart card or token - a PIN or password against compromising.

6.4.1. Generation and installing activation data

Activation data is generated when the device initiates a qualified electronic signature/seal initialization.

If the device is provided by the Provider it is initialized in the presence of the Holder/Creator and access codes are generated: User (PIN) - access to the device and keys and Administrative (AIN) - for unblocking the PIN and

initialization.

The access codes are randomly generated by the Registration Authority and are provided personally to the Holder/Creator or to a person authorized by him. The codes are given to the Holder/Creator in a sealed, opaque envelope. The Holder/Creator is required to change the original PIN and AIN to access by using the software provided with the device.

6.4.2. Activation data protection

The Holder/Creator is required to store and protect against compromise access codes for the qualified signature/seal creation device.

The Provider does not store any copies of the initial randomly generated access codes and cannot restore access to the device after it has been blocked.

6.5. Computer security control

6.5.1. Specific requirements for computer security

The Provider shall provide and use procedures and methods for managing the security of the technical and technological equipment used in its infrastructure in accordance with generally accepted international standards for information security management. The Provider shall also provide tests and inspections of the technical equipment and technologies using a security assessment methodology based on the common security assessment methodology developed for the ISO 15408 Standard.

6.5.2. Computer security rating

The degree of reliability of the technical equipment, technologies and systems used by the Provider meets the statutory requirements for performing the activity as a Trust Service Provider.

6.6. Technical life cycle control

The Provider provides full technical control over the life-cycle of the systems through which Certification Services are provided by the Provider.

At all stages of the construction and operation of the systems, the

procedures and rules described in internal documents of the Provider are strictly observed.

Test results are documented and stored in the Provider's archive.

6.7. Network security control

The Provider maintains a high level of network security and means of reporting unauthorized access.

7. CERTIFICATE PROFILES

7.1. Base InfoNotary TSP Root Certificate Profile

InfoNotary TSP Root		
Basic x509 attributes:		
Attribute		Value
Version		3 (0x02)
Serial number		Unique for the Provider's register; 16-byte number
Valid from		Date and time of signing
Valid to		Date and time of signing + 20 years
Signature Algorithm		SHA256/RSA
Issuer:		
Attribute		Value
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		Value
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG

Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	InfoNotary TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Additional attributes of x509 extensions (x509v3 extensions):		
Attribute		Value
Basic Constraints (Critical)	Subject Type=CA	
Key Usage (Critical)	Certificate Signing, CRL Signing	
Public Key	RSA 4096 bits	
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html	
Subject Key Identifier	SubjectKeyIdentifier	

7.1. Operational Certificate InfoNotary Qualified Validated Domain CA Profile

InfoNotary Qualified Validated Domain CA		
Basic x509 attributes:		
Attribute		**Value**
Version		3 (0x02)
Serial number		Unique to the Provider's Register; 16-byte number
Start of validity period		Date and time of signing
End of validity period		Date and time of signing + 19 years
Attributes of the Issuer:		
Attribute		**Value**
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of Holder (x509 Subject DN):		
Attribute		**Value**
Common Name	CN	InfoNotary Qualified Validated Domain CA
Domain Component	DC	qualified-domain-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC

Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Additional attributes of x509 extensions (x509v3 extensions):		
Attribute		**Value**
Basic Constraints (Critical)	Subject Type=CA	
Key Usage (Critical)	Certificate Signing, CRL Signing	
Public Key	RSA 3072 bits	
Authority information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.infonotary.com/qualified	
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-root-ca.crl	
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice:InfoNotary Qualified Validated Domain CA	
Subject Key Identifier	subjectKeyIdentifier	
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer	

7.2. Certificate profile InfoNotary Qualified Validated Domain CP

InfoNotary Qualified Validated Domain Certificate		
Basic x509 attributes:		
Attribute		Value
Version		3 (0x02)
Serial number		Unique for the Provider's register; From 8-byte number to 16-byte number
Start of validity period		Date and time of signing
End of validity period		Date and time of signing + 1 or 2 years
Electronic signature algorithm		SHA256/RSA
Attributes of the Publisher:		
Attribute		Value
Domain Component	DC	qualified-domain-ca
Common Name	CN	InfoNotary Qualified Validated Domain CA
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		Value
Common Name	CN	Domain name, IP
Domain Component	DC	qualified-domain-ca

Country Name	C	
Locality Name	L	
Email	E	
Organization	O	
Organization Identifier	2.5.4.97	NTRYY-XXXXXXXXXX (National identification code) VATYY-XXXXXXXXXX (Tax registry number) TINBG-XXXXXXXXXX (VAT identification number) YY – country code
Given Name	G	
Sur Name	Sn	
Serial Number	2.5.4.5	PNOYY-XXXXXXXXXX (National Personal Number) PASYY-XXXXXXXXXX (Passport Number) IDCYY- XXXXXXXXXX (National ID card Number) TINBG-XXXXXXXXXX (VAT identification number) YY – Country code
Additional attributes of x509 extensions(x509v3 extensions):		
Attribute		Value
Basic Constraints (Critical)	End entity	
Key Usage (Critical)	Digital Signature, Key Encipherment	
Public Key	RSA 2048 bits	
Authority Key Identifier	AuthorityKeyIdentifier	
Subject Key Identifier	SubjectKeyIdentifier	

Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://repository.infonotary.com/qualified-domain-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-domain-ca.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=InfoNotary Qualified Domain Certificate [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3]Certificate Policy: Policy Identifier=0.4.0.2042.1.6
Subject Alternative Name	DNS name [Domain name or IP]

Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsld-Legal (oid=0.4.0.194121.1.2) id-etsi-qcs-semanticsld-Natural (oid=0.4.0.194121.1.1)* id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-web (oid=0.4.0.1862.1.6.3) id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	Client Authentication Server Authentication

7.3. Certificate profile InfoNotary Qualified Organization Validated Certificate

InfoNotary Qualified Organization Validated Certificate	
Basic x509 attributes:	
Attribute	Value
Version	3 (0x02)
Serial number	Unique for the Provider's register; From 8-byte number to 16-byte number
Start of validity period	Date and time of signing
End of validity period	Date and time of signing + 1 or 2 years
Electronic signature algorithm	SHA256/RSA
Attributes of the Publisher:	
Attribute	Value

Domain Component	DC	qualified-domain-ca
Common Name	CN	InfoNotary Qualified Validated Domain CA
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		Value
Common Name	CN	Domain name, IP
Domain Component	DC	qualified-domain-ca
Country Name	C	
Locality Name	L	
Email	E	
Organization	O	
Organization Identifier	2.5.4.97	NTRYY-XXXXXXXXX (National identification code) VATYY-XXXXXXXXX (Tax registry number) TINBG-XXXXXXXXX (VAT identification number) YY – country code
Additional attributes of x509 extensions(x509v3 extensions):		
Attribute		Value
Basic Constraints (Critical)	End entity	
Key Usage (Critical)	Digital Signature, Key Encipherment	
Public Key	RSA 2048 bits	
Authority Key Identifier	AuthorityKeyIdentifier	

Subject Key Identifier	SubjectKeyIdentifier
Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://repository.infonotary.com/qualified-domain-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-domain-ca.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= InfoNotary Qualified Organization Validated Certificate [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3]Certificate Policy: Policy Identifier=0.4.0.2042.1.7
Subject Alternative Name	DNS name [Domain name or IP]

Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsld-Legal (oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-web (oid=0.4.0.1862.1.6.3) id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	Client Authentication Server Authentication

7.4. Certificate profile InfoNotary Qualified PSD2 WA Certificate

InfoNotary Qualified PSD2 WA Certificate		
Basic x509 attributes:		
Attribute		Value
Version		3 (0x02)
Serial number		Unique for the Provider's register; From 8-byte number to 16-byte number
Start of validity period		Date and time of signing
End of validity period		Date and time of signing + 1 or 2 years
Electronic signature algorithm		SHA256/RSA
Attributes of the Publisher:		
Attribute		Value
Domain Component	DC	qualified-domain-ca
Common Name	CN	InfoNotary Qualified Validated Domain CA

Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		Value
Common Name	CN	Domain name, IP
Domain Component	DC	qualified-domain-ca
Country Name	C	
Locality Name	L	
Email	E	
Organization	O	
Organization Identifier	2.5.4.97	PSDYY-Z-XXXXXXXXXX YY – country code Z – 2 to 8 character of National Competent Authority (NCA) identifier X - PSP identifier
Additional attributes of x509 extensions(x509v3 extensions):		
Attribute		Value
Basic Constraints (Critical)	End entity	
Key Usage (Critical)	Digital Signature, Key Encipherment	
Public Key	RSA 2048 bits	
Authority Key Identifier	AuthorityKeyIdentifier	
Subject Key Identifier	SubjectKeyIdentifier	

Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://repository.infonotary.com/qualified-domain-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-domain-ca.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= InfoNotary Qualified PSD2 WA Certificate [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3]Certificate Policy: Policy Identifier=0.4.0.2042.1.7
Subject Alternative Name	DNS name [Domain name or IP]

Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Legal (oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-web (oid=0.4.0.1862.1.6.3) id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en id-etsi-psd2- qsStatement (oid=0.4.0.19495.2) RolesOfPSP (oid=0.4.0.19495.2) –one or more roles: roleOfPspName =PSP_AS roleOfPspOid (oid=0.4.0.19495.1.1), roleOfPspName =PSP_PI roleOfPspOid (oid=0.4.0.19495.1.2), roleOfPspName =PSP_AI roleOfPspOid (oid=0.4.0.19495.1.3) roleOfPspName =PSP_IC roleOfPspOid (oid=0.4.0.19495.1.4) nCAName = (name of National Competent Authority) nCAId = (Abbreviation of NCA identifier – YY-Z) YY – country code Z – 2 to 8 character of National Competent Authority (NCA) identifier
Extended Key Usage (Non Critical)	Client Authentication Server Authentication

8. AUDITING AND CONTROL OF THE ACTIVITY

The audits carried out on the Provider concern the processing of information data and the management of key procedures. Their purpose is also to control the CPS to what extent it is compatible with the integrated management system that includes the requirements of IEC 27001: 2013, by Regulation (EU) 910/2014 and internal management decisions and measures. The audits performed by the Provider relate to all Certification Authorities belonging to the basic Certification Authority, the Registration Authority and other elements of the Provider's certification infrastructure.

The activity of the Provider is subject to constant internal control exercised by the Board of Directors of INFONOTARY PLC.

The Provider is subject to an audit at least once every 24 months by a conformity assessment body. The purpose of the audit is to confirm that INFONOTARY PLC, as a Qualified Trust Service Provider and the Qualified Trust Services it provides, meets the requirements set out in Regulation (EU) 910/2014. The Provider shall submit the relevant conformity assessment report to the Supervisory Authority within three working days of receipt. The Supervisory Authority may at any time carry out an audit or request a Conformity Assessment Body to assess the Provider's compliance.

An external audit to assess the compliance of the Provider's activities with the provisions of Regulation (EU) 910/2014 is performed by an accredited and independent conformity assessment body and is regulated by a standard ISO/IEC 17065: 2012: Conformity assessment - Requirements for bodies certifying products, processes and services. External inspection by a Supervisory Authority is carried out at any time by authorized employees of the Supervisory Authority.

The internal audit is performed by the employees of the Provider with the necessary experience and qualifications. The activity of the Registration Authority is audited by employees of the Provider specifically authorized by the Provider’s Board of Directors or by external auditors.

8.1. Verification scope

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

8.2. Measures for correcting established defects

The Board of Directors of INFONOTARY PLC determines the measures necessary to be taken for the correction of the registered defects and the terms for their elimination.

The results from the audits are stored under the conditions and in order provided in this document.

Complete reports received from the Conformity Assessment Body must be submitted to the Supervisory Authority within 3 days of receipt.

9. OTHER BUSINESS AND LEGAL CONDITIONS

9.1. Prices and fees

The Provider determines prices and subscription fees for using the qualified trust services and the prices of goods related to these services (smart cards, readers, tokens, etc.) and publishes them in the Tariff for Providing Qualified Certification Services (Tariff, the Tariff), publicly available at: http://www.infonotary.com/.

The Provider reserves the right to unilaterally change the Tariff at any time during the term of the agreement. The changes are approved by the Board of Directors of INFONOTARY PLC and are published and available at URL address: http://www.infonotary.com/.

The Provider notifies the Subscribers about the changes individually or by publishing therein. The changes become effective and have effect on the Subscriber from the day following the notification or publication.

Changes have do not affect previously paid one-time or post-paid fees prior to the entry into force of the change.

9.1.1. Remuneration under Qualified Certification Services Agreement

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

9.1.2. Billing

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

9.1.3. Certificate reclamation and payment refunding policy

This procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

9.2. Financial responsibilities

9.2.1. Financial responsibility

INFONOTARY PLC is responsible for the provision of Qualified Certification Services to the Holder, the Subscriber and all relying parties who trust the Qualified Certificates issued by the Provider.

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

9.2.1. 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.

The procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

9.2.2. Insurance coverage for end users

- The procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

9.3. Information confidentiality

The procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

9.4. 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 Regulation (EU) 2016/679 (GDPR) 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 and Regulation (EU) 2016/679 (GDPR).

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 and Regulation (EU) 2016/679 (GDPR). 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 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.

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.

9.5. Intellectual property rights

The procedure is described in Certification Practice Statement for Qualified Certification Services of INOFONOTARY PLC.

9.6. Provider's Obligations, Responsibilities and Warranties

The Provider ensures that he is in compliance with all the provisions of Regulation (EU) 910/2014, the national legislation and current Certification Practice Statement for Qualified Certification Services, 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 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.

9.6.1. Guarantees and responsibilities of the Registration Authority

Registration authorities are required to perform their functions and duties in accordance with the current Practice when providing qualified certification services, strictly enforcing the procedures and following the policies set out in the Certification Policies for the different types of Qualified Certificates in their issue and management and internal documents of the Provider.

The Registration Authority undertakes to ensure the protection of personal data in accordance with the Personal Data Protection Act, Regulation (EU) 2016/679 (GDPR) and relevant legislation, to ensure protection of the private keys of the operators and their use only for the fulfillment of the registration activities for which they are authorized.

9.6.2. Responsibility of the Holder to relying parties

The Holder 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;
- when does not strictly meet the security requirements specified by the Provider;
- do 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 who has accepted the certificate at issue is responsible for the third party and the Provider if he/she has not been authorized to request the issuance of the certificate.

The Holder 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, resulting from the Certification Practice Statement for Qualified Certification Services, the Provider will hold responsibility for damages of the Holder.

9.6.3. 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;
- are 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 this document;

- validate Qualified Certificates issued by the Provider by means of the published status data of the Certificates from the Provider - Certificate Revocation List;
- use of 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 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.

9.7. Responsibility disclaimer

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

9.8. Provider's Liability Limitation

The maximum limit of compensation within which the Provider is responsible for damages for using a qualified certificate issued by him is up to the maximum limit set in accordance with national law.

9.9. Compensation for the Provider

In all cases of non-fulfillment of the Obligations by the Holder, respectively the Creator of the Printing, resulting from the Certification Practice Statement for Qualified Certification Services and/or the Qualified Certification Services Agreement, the Provider will consider the Holder, respectively the Creator's responsible.

9.10. Term and termination

9.10.1. Term

The policy becomes effective as soon as it is approved by the Board of Directors of INFONOTARY PLC and its publication at: http://repository.infonotary.com.

The policy is valid until a change or publication in the Document Repository and the Provider's Internet Portal of invalidity information occurs.

9.10.2. Termination and invalidity

The effect of the Policy shall be terminated upon termination of the Provider's activity.

In case any of the provisions of the current policy proves to be invalid, this will not entail any other clauses or parts of the policy, neither will result in the invalidity of the entire Agreement with the Subscriber. The invalid clause will be replaced by the mandatory rules of the law.

9.10.3. Termination effect

Upon termination of the policy, the provisions for the obligations of the Provider to maintain the archive of the documents and certificates in the volume and for the period remain in force for the consumer.

9.11. Individual notification and communication between participants

All interested parties can make announcements to the Provider about the provisions of the current policy and the agreement by means of signed electronic communications with qualified electronic signature, letters of return receipt or letters delivered by courier to the Provider.

Individual notification to the Provider can be made at the e-mail address: legal@infonotary.com or to the address: 1000, 16 Ivan Vazov Str., Sofia.

To contact its subscribers, the Provider uses e-mails signed with qualified electronic signature, e-mails, letters delivered by a courier, letters with acknowledgment of receipt.

9.12. Changes in the Policy for Providing Qualified Website Authentication Certificate

The Policy for providing Qualified Certification Services for Website Authentication Certificate can be change at any time, and any changes shall be subject to approval by the Board of Directors of INFONOTARY PLC and shall be publicly available to all interested parties at: http://www.infonotary.com.

Any person may make suggestions for changes (structural and meaningful) and notes for observed errors in the e-mail and e-mail addresses specified in this document for contact with the Provider.

9.13. Conflict management and jurisdiction

Any disputes arising between the parties in connection with the current policy shall be settled by agreement between the parties through understanding and a spirit of goodwill, and if not achieved, 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 Sofia, 16 Ivan Vazov Str., or electronically signed at the e-mail address: 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.

9.14. Applicable law

For all matters concerning the providing of qualified certification services and not covered by this Practice, the provisions of national law shall apply.

9.15. Compliance with the applicable law

This current Policy has been developed in accordance with the requirements of Regulation (EU) 910/2014 and the national legislation.

9.16. Other provisions

The current document does not contain any other provisions.