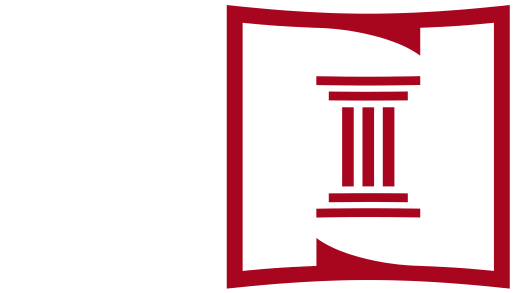

InfoNotary

POLICY FOR PROVIDING QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE

OF THE QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

VERSION 1.3

Entry into force 19.03.2021

CONTENT

1. INTRODUCTION

The current document POLICY FOR PROVIDING QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE 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 (EU) 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
  - 319 411-1 v1.1.1: General requirements;
  - 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 412 Certificate Profiles
  - 319 412-1 v1.1.1: Overview and common data structures;
  - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons;
  - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons;
  - 319 412-5 v2.1.1: QCStatements;
- COMMISSION IMPLEMENTING DECISION (EU) 2016/650 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- ETSI TS 119 431-1/2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers;
  - Part 1: TSP service components operating a remote QSCD /SCDev;
  - Part 2: TSP service components supporting AdES digital signature creation;
- ETSI TS 119 432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation;
- EN 419241-1:2018. Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements;

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework;
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificates Profile;
- RFC 3279: Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

The main purpose of the document POLICY FOR PROVIDING QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE is to make the qualified certification services public for the consumers through a detailed description of the rules and policies which INFONOTARY 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 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 Service 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 certificate services for qualified electronic signature, including:

- Acceptance and verification of applications for issuing qualified certificates;
- Creating Qualified Certificates Based on the established identity and valid data for Holder and Creator of a Seal;
- Signing qualified certificates;
- Issuance of qualified certificates.

Qualified certificate management services for qualified electronic signature:

- 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 certificate access services for qualified electronic signature:

- 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;

Validation Qualification Services for qualified electronic signature:

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

Cryptographic keys generation services:

- generation of a public and private key pair from an asymmetric cryptosystem via Qualified Signature Creation Device (QSCD) - Smart Card.

Secure cryptographic key generation and storage services for cloud qualified electronic signature/seal:

- generation and secure storage on assignment by the Holder/ Creator of a Seal of a pair of public and private key of an asymmetric cryptosystem through a remote device for creating a signature/seal - InfoNotary Remote Qualified Signature/Seal Creation Device (RQSCD);
- certified management and use of the hosted cryptographic keys, only under the sole control of the Holder/Signatory for creating an electronic signature or of the Creator of a seal for creating an electronic seal.

Remote signing or stamping services with a cloud qualified electronic signature/seal:

- certified management and use of hosted cryptographic keys, only under the sole control of the Holder/Signatory for creating an electronic signature or of the Creator of a seal for creating an electronic seal.

In carrying out the activities of issuance and managing Qualified Certificates for Qualified Electronic Signature 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 Qualified Electronic Signature"** (Policy), is named **"InfoNotary CP QESn"** and is identified by the following object identifier in the issued certificates:

Policy name	Identifier (OID)
InfoNotary Qualified Natural Person Signature CP	1.3.6.1.4.1.22144.3.1.1
InfoNotary Qualified Delegated Signature CP	1.3.6.1.4.1.22144.3.1.2

The policy includes:

- description of the terms and conditions that the Provider complies with and will follow when issuing Qualified Certificates for Qualified Electronic Signature, as well as the applicability of these certificates in view of the level of security and the limitations of their use;
- a set of specific procedures to be followed in the process of issuing and managing qualified certificates for Qualified Electronic Signature, the initial identification and authentication of the Holders of certificates, the conditions and the necessary security levels for creating the electronic signature and storing and saving the private key of the Holders.
- determines the feasibility and reliability of the information included in the Qualified Certificates for Qualified Electronic Signature.

1.3. PARTICIPANTS IN THE CERTIFICATION 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 Authorities

The Provider renders its services to end users through a network of specified Registration Authorities.

The Provider's Registration Authority perform activities of:

- carrying out verifications with eligible means and confirming the identity of a natural persons, the identity of legal entities and organizations and of natural persons representing legal entities regarding the provision of the trusted services by the Provider
- 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;
- generating key pair from an asymmetric cryptosystem on a cryptographic device at the request of the Holder;

- installing the certificate and transmitting the cryptographic device (QSCD) and the activation data (PIN and AIN) to the Holder or to persons authorized by them;
- signing agreements for the provision of qualified trusted services with clients on behalf of and at the expense of the Provider.

All or part of the registration activities can be performed by the Registration Authority of the Provider:

- in the office, in a personal presence of the natural person (applicant for a trusted service) in a personal capacity, as an authorized representative of another natural person, as an authorized representative of a legal entity or organization or as a legal representative of a legal entity or organization;
- trough an online information system or mobile application of the Provider/Registration Authority, which is accessible and used remotely by the natural person (applicant for a trusted service) in a personal capacity, as an authorized representative of another natural person, as an authorized representative of a legal entity or organization or as a legal representative of a legal entity or organization. The Registration Authority may remotely verify the identity of the natural person by means of secure video identification, means of electronic identification, qualified certificate for the qualified electronic signature and other legal means of secure remote identification.

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.

Current list of the Authorized Registration Authorities of the Provider has been published and is publicly available on the official website of the Provider at https://www.infonotary.com.

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.

1.3.4. 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.

1.3.5. Holder/Signer

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

The Holder keeps the private key for an electronic signature corresponding to the public key entered in the certificate and creates electronic signatures.

The QSCD device is under the Holder's sole control. He uses it to generate and store a public and private key pair from an asymmetric cryptosystem and the access data to the private key, which is corresponding to the public key included in the Qualified electronic signature Certificate.

The Holder could assign to the Provider the activities of generation and secure storage of a public and private key pair of an asymmetric cryptosystem through the InfoNotary's Remote Qualified Signature Device (RQSCD). The RQSCD is a separate part of the Provider's infrastructure and the access data to the private key, which is corresponding to the public key included in the Cloud qualified electronic signature certificate are solely under Holder's control.

1.3.6. Representatives

"A Representative" is a natural person duly empowered by the Holder

who performs on his/her behalf actions of certificate issuance and management before the Provider.

The Representative is a person, different from the Holder and is not entered in the certificate and cannot make electronic statements signed with the Holder's electronic signature and on behalf of the Holder.

1.3.7. Platform for cloud qualified certificates and remote signing and stamping of electronic documents

The INFONOTARY's platform for cloud qualified certificates and remote signing and stamping of electronic documents is a specialized part (hardware and software) of the certification infrastructure of the Provider and ensures the provision of:

Secure cryptographic key generation and storage services for cloud qualified electronic signature/seal:

- generation and secure storage on assignment by the Holder/Creator of a Seal of a pair of public and private key of an asymmetric cryptosystem through a remote device for creating a signature/seal - InfoNotary Remote Qualified Signature/Seal Creation Device (RQSCD);
- certified management and use of the hosted cryptographic keys in the RQSCD, under the sole control of the Holder/Signatory or of the Creator of a seal.

Remote signing or stamping services with a cloud qualified electronic signature/seal:

- certified management and use of hosted cryptographic keys, only under the sole control of the Holder/Signatory for creating an electronic signature or of the Creator of a seal for creating an electronic seal to an electronic document presented in the Platform.

1.4. CERTIFICATES USAGE

1.4.1. Certificates of the Certification Authority

1.4.1.1. Basic 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.

1.4.2. Operational Certification Authority for Qualified Certificates for Electronic Signature of natural person (InfoNotary Qualified Personal Sign CA)

The certificate for the public key of the Operational Certification Authority for Qualified Electronic Signature Certificates of natural person (**InfoNotary Qualified Personal Sign CA**), **OID: 1.3.6.1.4.1.22144.3.1**, is signed with the private key of the base Certification Authority **InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3**.

End user's certificates for qualified electronic signature of natural person **InfoNotary Qualified Natural Person Signature**, according to the respective certification policy and InfoNotary Qualified CPS are signed with the private key of the operating authority **InfoNotary Qualified Personal Sign CA**.

The list of suspended and terminated end-users certificates (**qualified-natural-ca.crl**) is signed with the private key of the operating authority **InfoNotary Qualified Personal Sign CA**.

With the private key of the operating authority **InfoNotary Qualified Personal Sign CA** are signed certificates for qualified electronic signature of natural person with delegated rights: **InfoNotary Qualified Delegated Signature** to end users, according to the respective certification policy and InfoNotary Qualified CPS.

The list of suspended and terminated end-users certificates (**qualified-natural-ca.crl**) is signed with the private key of the operating authority **InfoNotary Qualified Personal Sign CA**.

1.4.3. Qualified certificates for qualified electronic signature of a natural person

INFONOTARY PLC issues qualified certificates for qualified electronic signature to individuals in full compliance with the provisions and requirements of Regulation (EU) 910/2014.

InfoNotary Qualified Natural Person Signature

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

The certificate is associated with a pair of cryptographic keys that are generated and stored only on a qualified electronic signature creation device (QSCD). The device, the access data to it (PIN, AIN) as well as the data for activation of the private key for creation of an electronic signature, are available and are only under the sole control of the Holder. The qualified certificate may be issued by the Provider as a Cloud Certificate for qualified electronic signature, when the Holder assigns the managment of the qualified electronic signature cration device to the Provider, who observs appropriate mechanisms and procedures to ensure, that only the Holder has sole control over the use of his electronic signature creation data.

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

InfoNotary Qualified Delegated Signature Certificate

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

The certificate is associated with a pair of cryptographic keys that are generated and stored only on a qualified electronic signature creation device (QSCD). The device, the access data to it (PIN, AIN) as well as the data for activation of the private key for creation of an electronic signature, are available and are only under the sole control of the Holder. The qualified certificate may be issued by the Provider as a Cloud Certificate for qualified electronic signature, when the Holder assigns the managment of the qualified electronic signature cration device to the Provider, who observs appropriate mechanisms and procedures to ensure, that only the Holder has sole control over the use of his electronic signature creation data.

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

1.4.1. 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.

1.4.2. Certificate activity limitations

Qualified certificates issued by the Provider, depending on their type and certification policy may be limited in terms of purpose - for electronic signature, for electronic printing or electronic identification and authentication and/or the deals value and financial interest.

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

The Provider shall not be liable for damages due to the use of the issued by him certificates, beyond their permitted use and application restrictions related to the purpose of use, the deals's valule and the financial interest. Such

use will void the guarantees that INFONOTARY EAD 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 electronic signature	Electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person
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
Electronic signature creation data	Unique data which is used by the signatory to create an electronic signature
Electronic signature creation device	Configured software or hardware used to create an electronic signature
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign
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 Electronic Signature Certificate
Qualified certificate for electronic signature	A certificate for electronic signatures, that is issued by a qualified trust service provider and

	meets the requirements laid down in Annex I, Regulation EU 910/2014
Qualified electronic signature creation device	An electronic signature creation device that meets the requirements laid down in Annex II, Regulation EU 910/2014
Remote Qualified electronic signature creation device (RQSCD)	An electronic signature creation device that meets the requirements set out in Annex II to Regulation (EU) № 910/2014, which is a separate part of the Provider's infrastructure.
Platform for cloud qualified certificates and remote signing and stamping of electronic documents	Dedicated part of the certification infrastructure of the Provider, which meets the requirements set out in Annex II to Regulation (EU) № 910/2014, and through which the data for creation of a cloud qualified electronic signature / seal by the Provider are generated, stored and managed, on assignment by the Holder of the electronic signature or the Creator of the electronic seal.
Qualified electronic signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures
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)
Signatory/ Holder	A natural person who creates an electronic signature

Trust service provider	A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider
Trust service	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
RA	Registration Authority
RSA	Rivest-Shamir-Adelman – Cryptographic algorithm for signature generation
SSCD	Secure Signature Creation Device
QSCD	Qualified Signature Creation Device
RQSCD	Remote Qualified electronic 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. PUBLICATION AND REPOSITORY RESPONSIBILITIES

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

2.1. Repositories

2.1.1. Public Documental Repository

All public information related to the Provider's activity is published and updated regularly in an electronic documental 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 documental 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 documental repository for the purpose of reading and retrieving them is unlimited and free.

2.1.2. 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 Electronic Signatures, Qualified Electronic Seal Certificates and Website Authentication Certificates.

2.2. Publishing certificate information

The issued Qualified Electronic Signature Certificates are published in the Certificate Register promptly after being signed by the relevant Certification Authority of the Provider - **Qualified Personal Sign 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.

2.3. 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 Documental directory are published immediately after they are accepted by the Board of Directors of INFONOTARY PLC.

2.4. 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 Regiser 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 Electronic Signature Certificates. 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 paragraph 3.3 of this document.

3.1. Initial identification and identity validation

For initial identification and authentication of the Holder of a Qualified Certificate requested, the Provider performs the following checks for:

- holding of the private key corresponding to the public key submitted to the Provider by natural person, indicated as Holder in the certificate or by a natural person representing the legal entity;
- verification and confirmation the identity of the natural person - Holder and Legal entity.

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

3.1.1. Method of verifying the holding of the private key

The holding of the Private Key corresponding to the public key submitted to the Provider for inclusion in a certificate is subject to verification by various

methods depending on the Certification policies for the type of certificates.

When a request for issuing a qualified electronic certificate is submitted, the verification of the possession of the private key is performed by the Registration Authority by check of the electronic signature with which with which the the request for issuance of a certificate in PKCS # 10 format has been signed.

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

When issuing a qualified electronic signature certificate, the Registration Authority also checks the availability in the cryptographic device of the private key corresponding to the public key submitted to be included in the certificate and whether the device meets the requirements of Regulation (EU) 910/2014.

The Provider approves and defines in advance the devices for creating of the electronic signatures, which the users should used with issued by him qualified certificates for qualified electronic signatures, to meet the requirements of Regulation (EU) № 910/2014.

The Provider upon issuance of the cloud certificate for qualified electronic signature on assignment by the Holder provides a service for generation and secure storage of a pair of public and private key of an asymmetric cryptosystem by means of InfoNotary Remote Qualified Signature Creation Device (RQSCD). The Provider manages the RQSCD on assignment and behalf of the Holder. The data for access to the RQSCD and for remote activation of the private key for creating an electronic signature remotely are available and are only under the sole control of the Holder. Prior issuing the certificate, the Holder activates the private key in the RQSCD by using his personal data for remote activation (personal code), as performing this action verifies the possession of the private key.

3.1.2. Identifying a natural person – Holder or Authorized Representative

For identifying a natural person requesting the issuance/management of a certificate, certain procedures and rules are applied by the Provider according to the type of certificate requested and the conditions for its issuance/management. The Provider reserves the right to change his requirements regarding the information and documents necessary for the identity validation of a natural person – Holder, if this is required by the law or

in accordance with his certification policies.

When a qualified electronic certificate is issued, the information check and verification is performed by the Registration Authority in accordance with the rules and procedures of the Provider and in full compliance with the CPS and other internal regulations.

The Registration Authority checks and verifies the following information identifying the natural person – Holder or an authorized representative:

- first name, middle name, surname;
- date of birth;
- place of birth;
- nationality;
- gender;
- address, city, country, postal code;
- Personal Identification Number;
- identity card number: ID card, passport;
- issuer, date of issue and validity of the identification document;
- representative power of the Holder/Authorized Representative;
- contact and billing information.

The Holder or Authorized Representative of the legal entity shall submit to the Registration Authority in person the following documents:

- a valid identity card: ID card or passport;
- notarized power of attorney for empowerment of the Holder/ Representative of a legal entity or an authorized representative;
- document proving the representative power of the legal representative of a legal person - court resolution, current status certificate, notarized power of attorney or other empowerment act.

3.1.3. Identity validation of a Legal entity

In order to identify and verify the identity of a legal entity applying for a certificate, certain procedures and rules are applied, according to the type of the requested certificate and the conditions for its issuance. The Provider reserves the right to alter the requirements regarding the information and documents needed for the identity validation of the Holder-Legal entity, if necessary in view of its certification policy or the provisions and requirements of applicable law.

When a qualified electronic signature certificate is issued, the Registration Authority checks and verifies the information in accordance with the rules and procedures established by the Provider and in full compliance with the CPS and other interior regulations and documents.

The Registration Authority checks and verifies the following information identifying a Legal entity:

- name of the legal entity/person;
- address, city, country, postal code;
- number of the national tax register and/or
- UIC number;
- BULSTAT number;
- Domain name;
- legal and current status;
- right to brand name, trademark, domain etc.;
- contact and billing information.

The procedure for verification and confirmation of the identification data of the legal entity can be performed remotely, in case of a possibility for automated download of the necessary information from the corresponding State registers, maintained by a primary data administrators.

The legal representative of the legal entity, respectively an authorized representative of the legal entity submits personally to the Registration Authority the following documents:

- certificate for entry in Commercial Register, registration or act of origin;
- current status certificate issued not earlier than 1 month from the date of submission;
- BULSTAT registration document;
- document proving the right to use, name, etc.
- power of attorney for the representative of the legal person.

3.1.4. Unverified Information

In some cases, the Provider may include in the issued certificates and unconfirmed information for the Holder, such as e-mail, etc. Unconfirmed information is information which is outside the range of mandatory details, included in the content of the certificate in accordance with Regulation (EU) 910/2014 and cannot be verified by the Provider on the basis of official documents or in another way provided by the law. The Provider shall not be held responsible for any unconfirmed information included in the certificate.

3.2. Identity validation and authentication of a certificate revocation request

Termination of a certificate shall be made by the Certification Authority of the Provider after the Registration Authority initiates the termination in accordance with the provisions of the CPS. The Registration Authority requests

termination from the Provider upon receiving a certificate revocation request by the Holder and the performance of actions to verify the identity and identity of the applicants and their confirmation at the Registration Authority's office or remotely by electronical means.

The Holder or the authorized representative of the Holder who made a request for termination shall submit in person to the Registration Authority the following documents:

- a valid identity card: ID card or passport;
- notarized power of attorney for empowering the Representative to represent the Holder in front of the Provider for issuance and management of certificates;
- a document proving the representative power of the legal representative of a legal person - court resolution, current status certificate, notarized power of attorney or other empowerment act;
- signed certificate revocation request.

3.3. Identity validation and authentication of a certificate suspension request

An application for suspension of a certificate may be made to the Provider under the terms and conditions described in the CPS. A valid certificate is suspended by the Certification Authority of the Provider for the term needed according to the circumstances but not for more than 48 hours.

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

- 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;
- upon order by the Supervisory Authority when there is a risk for the interests of third parties or when there is sufficient evidence of violation of the law.

The resumption of the certificate is performed by the Certification Authority of the Provider under the terms and conditions described in the CPS and after a resumption initiation by the Registration Authority.

The Registration Authority performs identity validation and authentication of the Holder when he has submitted in person or through an authorized representative a signed request for resumption of a certificate.

The Holder or his authorized representative requesting the resumption of a certificate personally presents to the Registration Authority the following

documents:

- a valid identification card: ID card or passport;
- notarized power of attorney for authorizing the Representative to represent the Holder in front of the Provider;
- signed Request for the resumption of a certificate containing a statement that the Holder is aware of the reason and grounds for the suspension of the certificate and the request for resumption is submitted as a result of this.

4. EFFECTIVE CONDITIONS

Holders of qualified certificates for electronic signature shall notify the Provider immediately if there are any changes regarding the information contained in and concerning the certificate issued, during the term of its validity and until it is revoked.

The Certification Authority of the Provider issues, suspends and terminates the validity of the certificates after a verified and duly signed request for this by its Registration Authority.

4.1. Request for issuance of a certificate

The Provider's Registration Authorities accept and service all certificate requests and are required to provide the Certifying Authority with correct and validated information regarding end-user endorsements.

4.1.1. Applicants

Request for issuance of a certificate can be submitted to the Provider by every person who:

- fills in an application form for the issuance of a certificate;
- generate a pair of cryptographic keys on their own or through the Provider;
- provide the Certification Authority of the Provider, the public key corresponding to the private key;
- accept the terms of the Qualified Certification Services Agreement and the Practice for Providing Qualified Certification Services.

The request for issuance of a certificate to the Provider can be submitted personally by the Holder or by his authorized representative.

4.1.2. Process of applying a certificate issuance

The request for a certificate must contain the following data:

- information individualizing the Holder and the empowering legal entity if such information is to be provided;
- the public key corresponding to the private key from the pair of cryptographic keys generated by the Holder;
- the type of the selected certificate.

The request for issuance of a certificate is an electronic document in PKCS#10 format, signed with the private key corresponding to the public included in the document.

Additional information may be required in the Certificate Request.

The issuance request is submitted personally by the Applicant or by a person authorized by him at the Provider's Registration Authority office or electronically or trough online information system or mobile application of the Provider / Registration Authority, which is accessible and used remotely by the natural person (applicant for a trusted service) in a personal capacity or as an authorized representative of a legal entity or as a legal representative of a legal entity or organization.

The Provider's/Registration Authority's online information system or mobile application requires pre-registration and remote identification of the Applicant. The Applicant can use them to submit data and select services, as well as to create request and apply for issuing a certificate together with the public key from the pair of cryptographic keys, which are generated by the Applicant itself on a device for creating a qualified electronic signature/seal (QSCD) or through software.

When an application for issuing a cloud electronic signature certificate is submited, the Provider, on assignment by the Holder, must generated the key pair on HSM in RQSCD with the required security level (CC EAL 4+ and higher).The private key is accessible remotely and the Holder of the seal is activated it, by using a personal access code (PIN), password or key solely under his control. The request for issuance of a cloud certificate and generation of the cryptographic key pair from the Provider on HSM in RQSCD can be submitted at the Registration Authority's office or through the Provider's/Registration Authority's online information system or mobile application.

The Provider's Registration Authority provides a service to all individuals for: generation a pair of cryptographic keys, the creation of a request for the issuance of a certificate with a public key included, the creation of a request for

the issuance of a cloud certificate and generation the cryptographic key pair from the Provider on HSM in RQSCD and submitting the requests to the Provider, if technically possible.

When the Provider's Registration Authority, by the request of the Holder, generates a pair of cryptographic keys, uses a secure signature/seal cration device (QSCD) and provides them to the Holder or authorized by him representative.

The rights to access the private key - PIN code or password, are submitted by the Registration Authority to the Holder or a authorized by him representative in a protected form.

After the submission by the Registration Authority of the secure signature/seal cration device on which the private key and access rights are stored, the Holder bears full responsibility for preventing the compromise, loss, disclosure, modification or other unauthorized use of the private key (the means of creating an electronic signature).

4.2. Procedure for requesting a certificate

The functions of identification and authentication of the applicants for issuance of a qualified electronic signature certificate are performed by an authorized Registration Authority of the Provider. In observance of the procedures approved by the Provider and according to the CPS, based on the received request for issuance of the certificate and the submitted documents and in the personal presence of the Applicant - the Holder or a person authorized by him, the Registration Authority verifies and confirms to the Certification Authority:

- the Holder's identity and the identity of the authorized by him representative, if any;
- the representative authority of the Holder and of a representative authorized by him.

When the request for issuance of a cloud certificate is submitted remotely, the checks are performed (automatically or by an operator of the Registration Authority) within the session for registration and remote identification of the Applicant.

Before confirming the application for a certificate, the Registration Authority of the Provider carries out the necessary checks according to the requirements described in the CPS:

- verifies and confirms the identity of the Applicant, the Holder or his representative on the basis of documents provided by them;

- verifies and confirms the representative power of the Holder and of a representative authorized by him;
- verifies and confirms the possession of the private key corresponding to the public key included in the request at the time of its generating;
- verifies and confirms the additional information requested to be included in the certificate, with the exception of unconfirmed information;
- verifies the accuracy of a received, or made signed electronic request (in PKCS10 format) for issuance of a certificate;
- confirms the Holder's acceptance of the conditions of the CPS, this document and the signed Qualified Certification Services Agreement.
- provides to the Holder for adoption, the information that has been collected and will be included in the issued certificate;
- confirms the Holder's acceptance of the conditions of this CPS and the signing of a Qualified Certification Services Agreement;
- collects dated and signed by the Applicant by hand copies of the documents, based on which the Holder's identity and empowerment and representative authority of the autoriezed representative has been checked.

If the verification process of the certificate application is completed successfully, the Registration Authority confirms the electronic request for issuance of a certificate to the Provider's Certification Authority and affirms that:

- the issuance request originates from the Holder or from a person duly empowered by him;
- the information regarding the Holder submitted for inclusion in the certificate is correct and complete;
- the private key is technically appropriate to be used for the generation of an improved electronic signature and corresponds to the public key, so that it is possible, through the public key, to verify the fact that a certain electronic signature is generated with the private key;
- the private key is in the possession of the Holder;
- the Holder has the following means under his control for personal remote access to the private key stored in the Provider's RQSCD - a mobile application of the Provider, personal registration in the Provider's information system or other registered means of access to the key.

If the verification process of the certificate application is unsuccessful, the Registration Authority rejects the request for issuance the certificate. The Registration Authority immediately notifies the Applicant and states the reason for the denial. Applicants whose application for a certificate has been rejected may apply again for a certificate.

The Registration Authority completes and stores the documents provided by the Holder and by the Authorized Representative on paper, as well as records and stores the information, data and digital copies of the documents provided by the Applicant during the remote identification process.

The Provider controls the accuracy of the information included in the certificates provided by the Holder of a Seal and confirmed by the Registration Authority at the time of issue of the certificate.

In all cases and for all types of certificates issued by the Provider, the Holder has the permanent obligation to observe the accuracy of the information provided and to inform the Provider of any changes that occur after the issuance of the certificate.

The verification and confirmation of the information in the requests for issuance of certificates shall be processed within a reasonable time and within 5 working days from the date of acceptance of the issuance request and submission of the necessary data and documents by the Applicant. The Provider shall issue the certificate immediately after confirmation of the issuance request by the Registration Authority.

4.3. Issuance of a certificate

4.3.1. Actions of the Certification Authority when issuing a Certificate

The Provider's Certification Authority issues the certificate on the basis of a issuance request received by the Registration Authority. The Registration Authority's issuance request of a certificate guarantees the validity of the application made by the Applicant and the validity of the data contained therein. The request is signed by an operator of the Registration Authority who performed the inspections. The Certification Authority of the Provider verifies the identity of the Registration Authority and the identity of the operator of the Registration Authority on the basis of a credentials (special administrative certificate of a operator of a Registration Authority).

The Provider promptly notifies the Holder of the issued Qualified Certificate by sending an email to him. After issuing the certificate, the Provider delivers it to the Holder:

- by publishing a link for downloading the certificate in the sent email;
- through the Provider's/Registration Authority's online information system where the registered Holder or the person authorized by him has personal access;

- through the Registration Authority by storing the issued certificate on QSCD under the control of the Holder or the person authorized by him.

The cloud qualified certificate is not provided to the Holder. It's stored in the Provider's RQSCD on assignment by the Holder.

The Provider issues the certificate in accordance with the consent of the Holder.

The Holder or a person authorized by him accepts the content of the issued qualified certificate by signing a Protocol for acceptance of a certificate or by using the confirmation features of the Provider's/Registration Authority's online information system or mobile application. The Provider considers, that the certificate has been accepted by the Holder without signing a protocol or doing an electronic confirmation, if the Holder within 3 days from the date of issuance of the certificate and its publication in the Public Register does not object to the Provider, that the data in the certificate are incorrect or incomplete.

The Provider publishes the issued qualified certificate on its Certificate Register immediately.

4.4. Data secrecy of qualified trust services and certificates usage

4.4.1. Data secrecy

No one apart from the Holder has the right to access the data for creating an electronic signature, electronic seal, electronic time stamp and website authentication data.

The Holder has full responsibility for the storage and usage of the private key and for preventing the compromise, loss, disclosure, modification or other unauthorized use of a private key (the data for creating an electronic signature, electronic seal, electronic time stamp and website authentication data.

The Holder bears full responsibility for actions or omissions by persons authorized by him when he has given them access to generate, keep, store or destroy their private keys.

The Holder shall use the certificate and the key pair only according to the permitted use specified in the certification policy and the type of the certificate, as well as with the permitted use stated in the certificate itself and only during its validity period.

4.4.2. Usage of validation data from Relying parties and certificate usage

Relying parties use the validation data included in a Qualified Certificate issued by the Provider to check the validity of the electronic signature or electronic seal.

4.5. Certificate Renewal

4.5.1. Conditions for renewing a certificate

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

A certificate issued by the Provider may be renewed only if all data contained in the certificate is unchanged and the content of the certificate is identical with the valid certificate, and the new term of validity is entered in the new certificate. A valid, not suspended, qualified certificate may be renewed once only for another term of validity.

Renewal of the certificate shall be requested by the Holder, entered in the valid certificate, at least 10 (ten) days before the expiration of the period of validity of the certificate.

Cloud qualified certificates are not renewable. The Provider issues a new cloud certificate at the request of the Applicant, performing the initial procedure for identification and identification.

Renewal of a issued certificate is provided by Provider only if: the certification policy under which it is issued allows that; all data in the certificate and the respective key pair are unchanged; the content of the new certificate is identical to the valid certificate, except for the validity period. The new validity period is entered in the new certificate.

A valid, not suspended, qualified certificate may be renewed once only for another term of validity, but up to a total of 3 years of validity period.

4.5.2. Renewal claim procedure

The Holder or by a authorized by him person submits the renewal request personally at the Provider's Registration Authority office or electronically or trough an online information system or mobile application of the Provider/Registration Authority, which is accessible and used remotely by the

natural person (applicant for a trusted service) in a personal capacity or as an authorized representative of a legal entity or as a legal representative of a legal entity or organization, at least 10 (ten) days before the expiration of the period of validity of the certificate.

The electronic application has to be signed by the Holder with the valid certificate for which renewal is requested.

The Registration Authority of the Provider may request from the Applicant up-to-date documents proving the accuracy and correctness of the information included in the certificate at the time of submitting the request for renewal.

The Applicant declares that the data provided at the time of initial issue and those entered on the certificate are correct, accurate and unchanged at the time of submitting the request for renewal.

The Provider's Registration Authority shall carry out the necessary inspections in accordance with the CPS before confirming the application for renewal of a certificate.

If the verification process of the certificate renewal request completed successfully, the Registration Authority confirms the electronic request for certificate renewal to the Provider's Certification Authority and affirms that:

- the renewal request originates from the Holder or a person duly empowered by him;
- the Holder's information included in the certificate is accurate, true and up to date;
- the private key is in the possession of the Holder;
- the certificate whose renewal is requested is valid.

If the verification process of the certificate renewal request is unsuccessful, the Registration Authority rejects the request for renewal. The Registration Authority immediately notifies the Applicant and states the reason for the denial. Applicants whose application for a certificate renewal has been rejected may apply for a new certificate.

The Registration Authority completes and stores the documents provided by the Holder and by the Authorized Representative on paper, as well as records and stores the information, data and digital copies of the documents provided by the Applicant during the remote identification process.

The verification and confirmation of the information in the renewal request of a certificate shall be processed within a reasonable time and the Provider shall issue the certificate within 5 working days from the date of acceptance of the request and the documents.

The Provider's Certification Authority issues the new certificate on the basis of an electronic request for renewal received from the Registration Authority.

The Provider notifies the Holder of the new certificate issued immediately by sending an e-mail.

After issuing the certificate, the Provider delivers it to the Holder:

- by publishing a link for downloading the certificate in the sent email;
- through the Provider's/Registration Authority's online information system where the registered Holder or the person authorized by him has personal access;
- through the Registration Authority by storing the issued certificate on QSCD under the control of the Holder or the person authorized by him.

The Provider issues the certificate in accordance with the consent of the Holder.

The Holder or a person authorized by him accepts the content of the issued qualified certificate by signing a Protocol for acceptance of a certificate or by using the confirmation features of the Provider's/Registration Authority's online information system or mobile application. The Provider considers, that the certificate has been accepted by the Holder without signing a protocol or doing an electronic confirmation, if the Holder within 3 days from the date of issuance of the certificate and its publication in the Public Register does not object to the Provider, that the data in the certificate are incorrect or incomplete.

The provider publishes the certificate issued in the Register of Certificates immediately.

4.6. Termination of a certificate

Upon termination of the Root or Operating Certificates of the Provider's Certification Autority due to the compromise of their private keys, all valid certificates signed by the Provider with these keys are terminated.

4.6.1. Conditions for termination of a certificate

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

- upon the expiration of the validity of the certificate;

- upon termination of the legal entity of the Provider of Qualified Trust Services without transferring the activity of another qualified provider of qualified trust services.

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

- death or imprisonment of the Holder;
- termination of the legal entity when the certificate is issued with an entry of a Holder-legal entity;
- termination of the representative power of the Holder in respect of a legal person when the certificate is issued with the entry of the data for the legal entity;
- finding out that the certificate was issued on the basis of incorrect data.

The Provider takes immediate actions in respect of the termination of the Certificate when establishing the relevant grounds.

The Certification Authority of the Provider terminates the validity of certificates issued by the Provider.

The Provider shall immediately notify the Holder for 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, after having ascertained the identity and representative power of the Holder.

4.6.2. Termination request procedure

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

- the Holder or a person authorized by him to submit a written request for termination of the certificate to the Provider;
- the Provider's Registration Autority to verify the identity of the Holder or a person authorized by him.

The termination request is submitted personally by the Holder or or by a authorized by him person at the Provider's Registration Authority office or electronically or trough an online information system or mobile application of the Provider/Registration Authority, which is accessible and used remotely by the natural person (applicant for a trusted service) in a personal capacity or as an authorized representative of a legal entity or as a legal representative of a legal entity or organization.

The identification and authentication of the applicants who have requested for a certificate termination are performed by the Registration

Authority of the Provider in accordance with the CPS.

The Certification Authority of the Provider revokes the certificate on the basis of a request for termination received from the Registration Authority.

The certificate termination request from the Registration Authority guarantees the validity of the application made by the Applicant, the validity of the information contained therein. The request is signed by the administrator of the Registration Authority performing the checks and validations.

The Certification Authority of the Provider verifies the identity of the Registration Authority and the identity of the administrator of the Registration Authority on the basis of a credentials (special administrative certificate of the administrator of the Registration Authority).

After terminating the certificate the Provider includes it in the Certificate revocation list and update the publicly available electronic register of certificates.

After terminating the certificate, the Provider notifies the Holder directly or through the Registration Authority of the actions taken, as well as by e-mail or via the Provider's / Registration Authority's online information system or mobile application, if the request has made through these systems.

Certificates terminated by the Provider cannot be resumed.

The check and validation of the information provided in the certificate requests for termination are processed within a reasonable time and the Provider revokes the certificates within 24 hours of receiving the documents.

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 suspending a certificate

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:

- upon request of the Holder person authorized by him,;
- upon request of a person for whom, according to the circumstances, it is obvious that he might be aware about the security of the private key-word as a representative, partner, employee, member of the family, etc.;
- upon request of the Supervisory authority in case the presence of an immediate danger for the interests of third persons or in the presence of enough information for violation of the law.

4.7.2. Suspension request procedure

To act on suspension of a certificate the Certification Authority of the Provider it is necessary to obtain/receive:

- a request for suspension of a certificate by the Holder to the Provider;

- a request for suspension by a person such as a representative, partner, employee, family member, etc. who according to the circumstances may know about security violations of the private key;
- written order of suspending a certificate issued by a Supervisory Authority if there is reasonable doubt that the certificate should be terminated and
- an order for suspension by a Supervisory Authority in the immediate risk of the interests of third parties or if there is sufficient evidence of a violation of the law.

The Holder or person duly authorized by him makes the request for suspension through:

- the Provider's online information system or mobile application, if the Applicant is a registered user and has the appropriate access rights;;
- by telephone, fax, e-mail or
- personally at the Provider's Registration Authority.

No prior identification and authentication of the applicants requesting suspension of a certificate and their representative power is required.

The Certification Authority suspends the validity of the certificate within a reasonable term, according to the circumstances, of receiving the request, and publishes it on the Certificates Revocation List.

The Provider shall suspend the validity of a certificate, issued by him, within a reasonable term, according to the circumstances, but no longer than 48 hours of receiving the request for suspension.

4.7.3. Resuming a suspended certificate

The Provider resumes the suspended certificate at:

- the expiration of the term of suspension (48 hours);
- upon dropping the grounds for suspension;
- upon request of the Holder or authorized by him person, after the Provider, respectively the Supervisory authority, assure themselves that he has learned about the reason of the suspension, as well as that the request for renewal has been made as a result of the learning;

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

4.7.4. Certificate resumption procedure

When the resumption is made upon the request of the Holder,

verification of the request and identification of the Holder shall be made by the Registration Authority of the Provider in accordance with the CPS. Upon receiving a confirmation of a verified request for resuming by the Registration Authority and its verification, the Certification Authority of the Provider removes the suspended certificate from the Certificate Revokation List and publishes it.

The Certification Authority of the Provider resumes the validity of the certificate and removes it from the Certificate Revokation List upon receiving:

- written order to resume the certificate issued by the Supervisory Authority if there was reasonable motive for that
- an order from the Supervisory Authority if it was suspended due to imminent danger to the interests of third parties or due to the existence of sufficient evidence of a violation of the law.

Upon expiration of the suspension period (48 hours from the moment of suspension of the certificate) the Certification Authority of the Provider automatically resumes the validity of the certificate and removes it from the List of Suspended and Revoked Certificates, except in the cases described in the CPS.

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.

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.

5.1.6. Taking a technical components out of use and operation

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

5.1.7. 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 for 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 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 as a paper and/or electronic archive.

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 or 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 case 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

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;
- by the Provider, when generating cryptographic keys for issuing a qualified electronic signature cloud certificate. The keys are generated in HSM in RQSCD with the required level of security (CC EAL 4+ and higher).

When generating the key pair for Qualified certificate is performed by the Provider or by the User himself, a Qualified Signature Creation Device (smart cards, HSM and other cryptographic devices) - 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 must be used.

On the basis of contractual relations, the Provider may grant to the Holder 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 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 of

cryptographic keys for Qualified Certificates issued by the Provider, the use of licensed software by a particular software by 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 generation, installation and storage of the root key pair of the Provider's Root Certification Authority and the operational key pairs of the Operational Certification Authority is is performed by authorized employees of the Provider and in the presence of a member of the Board of Directors of " INFONOTARY "EAD according to a documented rocedure.

The secret parts of the root private key, as well as of all operational private keys of the Certification Authority shall be distributed, stored and provided for use, if necessary, by persons authorized by the Provider.

The compromising and unauthorized use of the Provider 's Certification Authority private keys is additionally protected by the implemented policy of access control to:

- the hardware module management by means of secret data accessible only to authorized persons and divided between at least two of these authorized persons;
- management and use of the parts of the Certification Authority's root and operational keys by means of separate secret data, accessible only to authorized persons and divided between at least two of these authorized persons.

6.1.1.2. Generating key pair for Subscriber

The provider offers a service for secure generation and storage of a key pair per subscriber, on the electronic signature creation device (QSCD), smart card and other cryptographic device, with a security profile defined in accordance with the "General Criteria", security level EAL 4 + or higher and in accordance with a secure profile for a qualified electronic signature in accordance with Regulation (EU) № 910/2014.

The Private Key of the Holder, is generated/recorded on a technical tool - smart card or other cryptographic device, and is automatically and irreversibly erased from the Provider's resources if such are used in generation.

The Provider is generated the key pair for a cloud qualified electronic signature certificate on HSM in RQSCD with the security level (CC EAL 4+ and higher) and the security profiles SAD / SAP / SAM in the RQSCD in compliance to ETSI EN 419 241- 2/3. The key pair is stored by the Provider following the approved internal rules and security procedures.

The private key is accessible remotely and is activated by the Holder via a personal access code (PIN), password or key solely under his control.

6.1.2. Private key delivery

When the Provider generates the key pairs of the Holder, the private key of that pair is:

- generated and 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 device is handed over to the Holder a person authorized by him, together with the access rights (PIN, AIN);
- generated and stored in encrypted form on HSM in RQSCD of the Provider and accessed by a personal access code (PIN), password or key solely under control of the Holder.

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

This procedure is performed only by the Holder 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 may provide the electronic request:

- personally in the Registration Authority or
- by electronic means via the online information system of the Provider /Registration Authority.

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

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

Each Relying Party may install in the systems under its control the service certificates of the Provider.

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 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 Certificates, the qualified electronic signaturel creation device (smart cards, HSM and other cryptographic devices) in which the Holder private key is generated and stored to be with a security profile determined in accordance with the general requirements ("Common Criteria"), security level EAL 4+ or higher in accordance with a secure profile for a qualified electronic signature in

accordance with Regulation (EU) № 910/2014.

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 to the Certification Authority's root private key, as well as to all operational private keys are stored divided on smart cards, protected with PIN. The provision of the divided parts to the persons authorized for their storage and presentation shall be documented in writing.

The Holder Private Key is only used in an electronic signature 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 Holder's private key of the cloud qualified certificate is used only in the HSM of the RQSCD in the Provider 's Cloud Electronic Signature Platform and is accessible through a secure profile of the platform through approved security mechanisms for personal control in accordance with SAD / SAP / SAM (Signature Activation Data/Signature Activation Protocol/Signature Activation Module) and is activated by a personal access code (PIN), password or key under the sole control of the Holder.

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'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.

The Holder's private key of the Cloud Electronic Signature is generated and stored in encrypted form of the RQSCD in the Provider 's Cloud Electronic Signature Platform, in accordance with the requirements of Regulation (EU) № 910/2014.

The Provider's procedure for storing the cutomer's private keys on RQSCD in the Provider's cloud electronic signature platform includes the procedure for restoring the private keys for work in a backup technical center, using a backup HSM of the RQSCD. The Provider stored in encrypted form a copy of the customers's private keys, only for the purposes of systems recovery, if necessary, and for management period of Provider's the backup.

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's private keys that are generated on a qualified signature creation device - QSCD.

In case the Holder damages, loses or destroys the QSCD, the Provider shall terminate the issued certificate related to the keys generated trough this device.

In case of a defect, loss or destruction of the HSM in RQSCD in the Provider's cloud electronic signature platform, the cloud electronic signature Holder's private keys generated in this HSM shall be restored to a new device from the backup copies of the encrypted keys. The personal control over the key from the Holder is guaranteed.

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'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).

The cloud electronic signature Holder's private keys may be transferred

to another HSM in encrypted form in the following cases:

- in case of recovery after failure of the hardware cryptographic module on which it was created;
- upgrading the technological infrastructure of the Provider.

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 is deactivated by deleting the containers where the private key is stored on the signature creation device or by physically destroying the device itself.

The private key of the cloud electronic signature Holder is activated by entering the access user code to the RQSCD (the remote qualified electronic signature creation device) and the protected user profile in the HSM to perform a specific cryptographic operation.

The private key of the cloud electronic signature Holder is deactivated automatically after performing the cryptographic operation for which it was activated and by terminating the logical access to the protected user profile in the RQSCD of the cloud signature platform.

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

The private key of the cloud electronic signature Holder is destroyed by deleting it from the protected user profile in the RQSCD of the cloud signature platform.

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 on secure media and archives with a high level of protection the activation data related to the private keys and activities of the Certification Authority.

The Holder is obliged to store and protect from compromising the personal data that he uses to activate his private key.

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

If the Provider generates a key pair for the Holder, the activation data is provided personally to the Holder or to a person authorized by him along with the generated key pair.

The generation of the key pair of the cloud signature Holder is performed in the secure HSM user profile in the Provider's RQSCD, ensuring personal control to the private key, through private key activation data that is under the Holder's sole control.

6.4.2. Activation data protection

The Holder is required to store and protect against compromise the access codes for the qualified signature creation device (QSCD and RQSCD for cloud signatures).

In case of a certain number of failed attempts to use the correct access code to the QSCD and RQSCD, the device is blocked and can be unblocked by the Holder with owned by him AIN (administrative access code).

The Provider does't store a copy of the generated access codes and cannot restore the Holder's personal access to the device after its blocking.

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 Certificate InfoNotary TSP Root Profile

InfoNotary TSP Root	
Basic x509 Attributes:	
Attribute	Value
Version	3 (0x02)
Serial number	Unique to 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

7.2. Operational Certificate InfoNotary Qualified Personal Sign CA Profile

InfoNotary Qualified Personal Sign 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
Electronic signature algorithm		SHA256/RSA
Attributes of the Publisher:		
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 Qualified Personal Sign CA
Domain Component	DC	qualified-natural-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=1.3.6.1.4.1.22144.3.1 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Personal Sign CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier

7.3. Profile of a Qualified Electronic Signature Certificate - InfoNotary Qualified Natural Person Signature CP

InfoNotary Qualified Natural Person Signature Certificate	
Basic x509 attributes:	
Attribute	Value
Version	3 (0x02)

Serial number			Unique to 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, 2 or 3 years
Electronic signature algorithm			SHA256/RSA
Attributes of the Issuer:			
Attribute			Value
Domain Component	DC	qualified-natural-ca	
Common Name	CN	InfoNotary Qualified Personal Sign 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
Domain Component	DC	qualified-natural-ca	
Common Name	CN	Full name	
Given Name	G	First name according to identity document (Latin)	
Sur Name	Sn	Surname by identity card (Latin)	
Email	E		
Country Name	C		
Locality Name	L		
Serial Number	2.5.4.5	PNOBG-XXXXXXXXXX (identification number PIN) PASBG-XXXXXXXXXX (passport number IDCBG- XXXXXXXXXX (ID card number) TINBG-XXXXXXXXXX (Tax identification number)	

		PNOYY-XXXXXXXXXX (National Personal Number) PASYY-XXXXXXXXXX (Passport Number) IDCYY- XXXXXXXXXX (National ID card Number) YY – Country code
Additional attributes of x509 extensions (x509v3 extensions):		
Attribute		Value
Basic Constraints (Critical)	End entity	
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data 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-natural-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-natural-ca.crl	
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.1.1 [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 Natural Person Certificate [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [3]Certificate Policy: Policy Identifier=0.4.0.1456.1.1	

Qualified Certificate Statement (Non Critical)	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-qcs-QcSSCD (oid=0.4.0.1862.1.4) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcRetentionPeriod (oid=0.4.0.1862.1.3) id-etsi- qcs-QcLimitValue (oid=0.4.0.1862.1.2) 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)	Email protection Client Authentication

7.4. Profile of the Qualified Electronic Signature Certificate of an individual with delegated powers InfoNotary Qualified Delegated Signature

InfoNotary Qualified Delegated Signature Certificate			
Basic x509 attributes:			
Attribute			Value
Version			3 (0x02)
Serial number			Unique to 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, 2 or 3 years
Electronic signature algorithm			SHA256/RSA
Attributes of the Issuer:			
Attribute			Value
Domain Component	DC	qualified-natural-ca	
Common Name	CN	InfoNotary Qualified Personal Sign 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
Domain Component	DC	qualified-natural-ca	
Common Name	CN	Full name	
Given Name	G	First name according to identity document (Latin)	

Sur Name	Sn	Surname by identity card (Latin)
Email	E	
Country Name	C	
Locality Name	L	
Serial Number	2.5.4.5	PNOBG-XXXXXXXXXX (identification number PIN) PASBG-XXXXXXXXXX (passport number IDCBG- XXXXXXXXXX (ID card number) TINBG-XXXXXXXXXX (Tax identification number)
		PNOYY-XXXXXXXXXX (National Personal Number) PASYY-XXXXXXXXXX (Passport Number) IDCYY- XXXXXXXXXX (National ID card Number) YY – Country code
Organization	O	
Organizational Unit	OU	
Organization Identifier	2.5.4.97	NTRYY-XXXXXXXXXX (National identification code) VATYY-XXXXXXXXXX (VAT number) TINBG-XXXXXXXXXX (Tax identification number) YY – код на държавата

Additional attributes of x509 extensions (x509v3 extensions):	
Attribute	Value
Basic Constraints (Critical)	End entity
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data 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-natural-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-natural-ca.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.1.2 [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 Certificate Of Delegated Authority [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [3]Certificate Policy: Policy Identifier=0.4.0.1456.1.1
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcRetentionPeriod (oid=0.4.0.1862.1.3) id-etsi- qcs-QcLimitValue (oid=0.4.0.1862.1.2) 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)	Email protection Client 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

The scope of the performed audits depends on the type of exercised control and the audited authority.

All activities, documents and circumstances concerning the functioning of the Provider are within the scope of the audit. The may include, but not be

limited to:

- the compliance of the Provider's operating procedures and principles of work with the procedures and policies defined in the CPS when providing Qualified Certification Services;
- Infrastructure management included in the certification services service.

The inspection by the Supervisory Authority covers the legal requirements for the Provider's activity under applicable legislation in the field of qualified certification services.

The audit by the conformity assessment body covers the entire operation of the Provider for the provision of Qualified Trust Services and the application of all standards and standardization documents related to Regulation (EU) 910/2014: Documentation; Archives; Information relating to the issue and management of qualified certificates; Physical and information security and reliability of the technological system and management; Certification Authorities.

The scope of the internal audits includes:

Verification of the provider's activity and its compliance with the CPS; comparison of the practices and procedures described in this document with their practical realization in the performance of the Provider's activities; verification of the activity of the Registration Authority; other circumstances, facts and activities related to the infrastructure, at the discretion of the management of INFONOTARY 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

The value of the Qualified Certification Services Agreement, which the Subscriber concludes with the Provider, is formed by the fees due by the Subscriber for services and goods requested for use by the Subscriber on the basis of the Tariff for Providing Qualified Certification Services.

Advance paid or subscription charges are not subject to return of the Subscriber if they are not consumed within the period for which they are paid.

In case of early termination of a qualified certificate issued and accepted by the Holder and/or the Qualified Certification Services Agreement for reasons the Provider is not liable for, the Subscriber shall not be required to return the remainder of the value paid for the remainder of the terminated qualified certificate.

All amounts due under the agreement are paid by the Subscriber by bank transfer, through the system of EASYPAY or ePay.bg. The transfer is deemed effected upon receiving a bank statement certifying that the whole amount due has been transferred into the specified account of the Provider. The value of the goods and services does not include the cost of payment of

the remuneration due to the agreement which the Subscriber owes to the payment service providers.

9.1.2. Billing

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

9.1.3. Certificate reclamation and payment refunding policy

In case of objections raised by the Holder of the seal of a qualified certificate within 3 days of its publication in the Register of certificates of incompleteness or inaccuracies contained therein, the Provider shall terminate the registered certificate and issue a new one free of charge or refund the payment made for issuing the complaint certificate.

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.

9.2.2. 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.

Upon occurrence of an event that could lead to a claim covered by the insurance, the injured party shall be obliged immediately, not later than 7 days after the event has become known, to notify in writing the Provider and the Insurer of the Provider.

Subscribers are required to promptly notify the Provider of any occurred damages and assist the Provider of their Insurer in establishing the facts confirming the claim.

9.2.2.1. Insurance coverage for end users

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

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

In the relations of the Provider with the Subscribers and all relying parties, these limits of compensation and conditions are in force from the date of the occurrence of the damage.

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

- failure to comply with the obligations of Qualified Certificates Holders, Creators of a Seal and Subscribers in accordance with the Certification Practice Statement for Qualified Certification Services, the respective Certification Policy for qualified certification type and the Qualified Certification Services Agreement;
- compromise or loss of a private key of the Holder due to the failure to exercise the due care for its conservation or use;
- non-compliance with the requirements of due diligence to verify the validity of the electronic signature certificate, the electronic seal certificate and the qualified electronic time stamp of the Relying Parties;
- force majeure, accidents and other events that are beyond the control of the Provider.

9.3. Information confidentiality

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

9.3.1. Scope of the confidential information

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

- any information regarding the Holder and Subscriber beyond the published in the certificate;

- the reason for suspending or terminating the validity of certificates, beyond the published status information of the certificate;
- correspondence related to the Provider's activity;
- the Provider's private keys;
- the Holder's private key, when stored by the Provider on assignment by Holder;
- the Agreement for Qualified Certification Services;
- archives of requests for issuance, suspension, resumption and termination of certificates;
- transaction archives;
- records of external and internal audits and reports;
- disaster and unforeseen cases recovery plans.
- reports of the: conformity assessment bodies; of the another external auditors and of the Supervisory Authority.

The following objects and information are not treated as confidential:

- the certificates published in the Provider's register;
- the data included in the certificates;
- the certificates status data, published in the Certificate revocation list.
- all public documents published in the Provider's document repository.

The Provider does not disclose and should not be demanded to disclose or to provide to third parties any confidential information, except when he is obliged by special law or at the request of a competent authority.

Registration Authorities, Subscribers, Holders, Creators of a Seal or their authorized persons may not distribute or allow the dissemination of information in connection with the performance of their obligations under the Contracts with the Provider without the prior express written permission of the other Party.

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/Authorized Representative is for the sole purpose of issuing and maintaining Qualified Certificates or providing another qualified certification service.

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

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

The information collected by the Holder/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/Authorized Representative and Subscriber of Qualified Certification Services of the types of information it collects for them, how it is provided and stored and accessed to third parties.

The Holder, when signing the Agreement for qualified certification services and accepting the terms and conditions of the Certification policy and the Certification practice statement for qualified certification services, agrees the personal data identifying him to be included in the qualified certificate and to be avaiable to the third parties from the Register of issued certificates.

9.5. Intellectual Property Rights

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

The Provider allows the certificates issued by him and without any limitation of access to them by the Holder to be reproduced and distributed,

provided that they are entirely reproduced and distributed.

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

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

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

9.6. Obligations, Responsibilities and Warranties

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

9.6.1. 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 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.

9.6.2. 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.

9.6.3. 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.

9.6.4. 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 of usage with 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 for Damage 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.