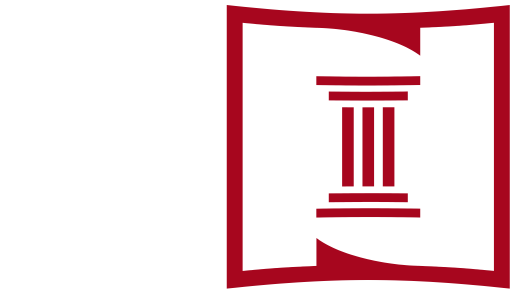

InfoNotary

POLICY FOR PROVIDING QUALIFIED TIME STAMP SERVICES

OF THE QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

VERSION 1.3

Entry into force 2.06.2023

CONTENT

1. INTRODUCTION

The current document POLICY FOR PROVIDING QUALIFIED TIME STAMP SERVICES 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;
- ETSI EN 319 421, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI TS 102 023 v.1.2.1 Policy Requirements for time-stamping authorities
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
    - 319 411-1 v1.1.1: General requiremenTS;
- IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)";
- IETF RFC 5816 ESSCertIDv2 Update for RFC 3161

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework.

The main purpose of the Policy is to make the qualified Time Stamp Services public for the consumers through a detailed description of the rules and policies which INFORNOTARY PLC has implemented and observes for the performance of its activity and providing funds to all interested parties for establishing the compliance of the Provider's activity the provisions and

requirements of Regulation (EU) 910/2014, the applicable legislation of the Republic of Bulgaria and the reliability and security of the certification activity.

The Policy is a public document developed in accordance with ETSI EN 319 421.

2. 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

3. 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
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 time stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
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**
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 provide	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 Electronic
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List - List of suspended and revoked certificates
DN	Distinguished Name - Unique name
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standard
IEC	International Electrotechnical Commission
ISO	International Standardization Organization
LDAP	Lightweight Directory Access Protocol - A protocol for simplified directory access
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
SHA	Secure Hash Algorithm – Hash Algorithm for hash identifier extraction
SSL	Secure Socket Layer – Secure data transmission channel
URL	Uniform Resource Locator

4. BASICS

4.1.1. 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 certification activities and provides qualified time stamping services through the Time Stamp Authority named InfoNotary Qualified TimeStamping Service.

The Time Stamp Authority of the Provider issues qualified time stamps through which users (Subscribers of the Provider and Relying parties) can certify the time for submitting an electronic document, signing a document or an electronic signature transaction, and so on.

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.

4.1.2. DENOMINATION AND IDENTIFICATION OF THE DOCUMENT

The **"Policy for Providing Qualified Time Stamp Services"** (Policy), is named **"InfoNotary Qualified TimeStamping Service CP"** and is identified by the following object identifier in the issued certificates:

Policy name	Identifier (OID)
InfoNotary Qualified TimeStamping Service CP	1.3.6.1.4.1.22144.3.4.1

The policy includes:

- description of the terms and conditions that the Provider complies with and will follow when provides qualified time stamps;
- common terms for providing qualified time stamps.

The issued certificates contain a policy identifier issued in accordance with IETF RFC 3647 [I.4], p.3.3, which can be used to identify them by the Relying party when using them.

The Qualified Electronic Time Stamp policy identifier specified in this document are as follows:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1) baseline-ts-policy (1)

The object identifier (OID) according to the type of the certification policy is:

	Name	InfoNotary Policy Identifier	ETSI Policy Identifier
Qualified Time Stamp	InfoNotary Qualified TimeStamping Service	1.3.6.1.4.1.22144.3.4.1	0.4.0.2023.1.1

4.2. PARTICIPANTS IN THE CERTIFICATION INFRASTRUCTURE

4.2.1. 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).

4.2.2. Operational Certification Authority for Qualified Time Stamps (InfoNotary Qualified TimeStamping Service CA)

The certificate for the public key of the Operational Certification Authority for Qualified Time Stamps (**InfoNotary Qualified TimeStamping Service CA**), **OID: 1.3.6.1.4.1.22144.3.4**, 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 qualified time stamps are signed with the private key of the Operational Certification Authority **InfoNotary Qualified TimeStamping Service CA**, according to the current policy and the CPS.

End user's qualified time stamps, according to the respective certification policy and InfoNotary Qualified CPS are signed with the private key of the operating authority **InfoNotary Qualified TimeStamping Service CA.**

The certificate of the Operational Certification Authority **InfoNotary Qualified TimeStamping Service CA** contains the following basic information:

InfoNotary Qualified TimeStamping Service CA	
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 + 19 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 Qualified TimeStamping Service CA
Domain Component	DC	qualified-timestamp-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 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=1.3.6.1.4.1.22144.3.4 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified TimeStamping Service CA	
Subject Key Identifier	SubjectKeyIdentifier	
Authority Key Identifier	AuthorityKeyIdentifier	

4.2.3. 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.

4.2.4. Relying Parties

„Relying parties" means natural or legal persons who rely on a trust service and who are addressees of electronically stamped electronic time stamp documents. The relying parties should have the skills to use the validation of electronic time stamp and to trust the electronic time stamps issued by the provider only after verifying the status of the authority's certificate in the list of suspended and terminated Certificates (CRL) or the automatic information provided by the provider via the OCSP protocol.

4.3. Applicability of electronic time stamps

The current policy is aimed to meet the requirements for qualified time stamps in compliance with the provisions of Regulation (EU) No 910/2014 and ETSI EN 319 122.

The policy does not include any limitations of the application of the time stamp issued by the Provider and in accordance with it.

The policy can be applied to verify the time of creating an electronic signature/seal without any limitations.

5. OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES

The obligations, responsibilities and warranties of the Provider, Holders, Creators 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 current policy and the Qualified Certification Services Agreement.

5.1. Provider's Obligations

The Provider undertakes to:

- complies with its internal rules and procedures, practice for providing qualified certification services and policies;
- complies with Regulation (EU) No 910/2014 and the provisions of national law;
- provide uninterrupted access to the Qualified Time Stamp Service, except for planned prevention and force majeure situations;
- provides and uses reliable technological equipment in the provision of the certification service;
- provide services in compience with the requirements of generally accepted international standards and recommendations.

5.2. Guarantees and responsibilities of the Provider

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 the current policy.

The activities of providing qualified time stamping services are subject

of verification by an independent conformity assessment body and the national supervisory authority.

The Provider is responsible to the Subscribers and the Relying parties for damages caused by:

- failure to comply with the Provider's obligations under Regulation (EU) 910/2014 and national law governing issuing, management and the content of the qualified time stamp;
- from false or missing data in the qualified electronic time stamp at the time of issuance.

5.3. Responsibility of the Subscribers

The Subscribers of the qualified Time Stamp service are required:

- when submitting requests for electronic time stamp to comply with the requirements of the Provider on the form and the way of requesting;
- upon receiving the issued time stamp to verify the validity of the Time Stamping Authority's electronic signature by CRL and OCSP verification;
- to comply with the obligations described in the CPS for Qualified Certification Services.

5.4. 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 Time Stamps issued by the Provider by means of the published status data of the Certificates from the Provider - Certificate Revocation List;
- trust the qualified Time Stamps issued by the Provider only if the result of validity checks that are made are correct and up-to-date;
- perform validations on the applicability of the cryptographic algorithms used to create the time stamp.

5.5. Responsibility Disclaimer

The Provider does not respond in cases where the damages are due to negligence, lack of care or basic knowledge of usage of qualified time stamps by the Subscribers 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 Subscribers or Relying party.

5.6. Provider's Liability Limitation

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

5.7. Compensation for the Provider

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

6. REQUIREMENTS TO THE TIME STAMPING AUTHORITY

The Provider ensures that it provides mechanisms for control over the activity of the Time Stamp Authority, which allows the provision of the qualified service in accordance with the provisions of this policy.

All events in the TimeStamp system are recorded as system journals that are archived and stored securely. Access to the journals has only authorized employees.

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.

7. PRACTICES AND PROCEDURES OF TIME STAMP AUTHORITY

Procedures and control mechanisms for the provision of the Qualified Time Stamp Service are described in the CPS of InofNotary PLC.

The management, maintenance and improvement of the services provided by the Ttime Stamping Authority are carried out in accordance with the requirements of the ISO 27001: 2013 Information Security System, implemented by InfoNotary PLC.

7.1. Accessibility of the service

The basic practices for providing Qualified Time Stamp services are described in the CPS of InofNotary PLC.

To ensure a quality and accessibility service, all system components and communication connectivity are at least doubly reserved. Uninterruptible power supply infrastructures based on uninterruptible power supplies (UPS) and diesel power generators.

7.2. Managing the life cycle of the Time Stamp key pair

7.2.1. Generating and installing a key pair

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

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 the CPS.

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

7.2.2. 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, CC EAL 4+ or higher level are used.

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

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

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

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

7.2.3. Delivery of the Public key of the Certifying 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.

7.2.4. Key length

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

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

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

7.3.1. Cryptographic Modul Standarts

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.

7.3.2. Storage and usage of 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.

Secret access parts to the base private key, as well as all operational private keys of the Certification Authority, are shared separately on smart card, protected with PIN.

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

7.3.3. 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.

7.3.4. 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.

7.3.5. 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.

7.3.6. 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.

7.3.7. 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.

7.4. Other aspects of managing the key pair

7.4.1. 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.

7.4.2. 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.

7.5. Activation data

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

7.6. Computer security control

7.6.1. 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.

The computer system management operated by all critical components of the infrastructure of the Provider in the operational and backup center is provided to protect the access to the software and the data is implemented in accordance with the Provider's information security policy.

The Provider has implemented an information security management system ISO/IEC 27001: 2013 and manages the security of the used technical and technological equipment in its infrastructure in accordance with the standard.

7.6.2. 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 and in accordance with the Provider's information security policy.

7.7. 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.

7.8. Network security control

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

8. QUALIFIED TIME STAMPING SERVICE

The Provider provides to Subscribers the time stamping service by issuing qualified electronic time stamps.

Electronic time stamps are data in electronic form that connect other data in electronic form with a particular point in time and represent evidence that the latest data existed at that time.

The electronic time stamp issued by the Provider certifies the date and time of submission of an electronic document signed with a private key

corresponding to the public key and included in a qualified electronic signature certificate issued by the Provider. Qualified electronic time stamp is issued to physical and legal persons who are holders or are a trusting party.

Timing activities and providing an independent source of time are performed solely by the Provider.

The Provider's Time Stamp Authority system - InfoNotary Qualified TimeStamping Service is developed and offers services according to (EU) № 910/2014 Regulation and in complete accordance with ETSI EN 319 422, ETSI TS 119 421, IETF RFC 3161 and IETF RFC 5816 and ETSI TS 102 023 v.1.2.1 (2003-01) Policy Requirements for time-stamping authorities.

8.1.1. Time Stamping procedure

The Provider's Time Stamp Authority system - InfoNotary Qualified TimeStamping Service accepts request and returns responses in a format defined by RFC 3161 - „Internet X.509 Public Key Infrastructure - Time-Stamp Protocol".

The issued qualified electronic time stamps are compatible with RFC 3161. The service issues RSA 2048 bit-encrypted SHA-256 time certificates.

The request must contain a hash of the electronic signature of the document whose signature time is authenticated as well as version of the request.

Optionally, it may also contains an inclusion request in the reply of the signing certificate along with the Certification Authority's chain.

The time stamp request can be generated through a specialized client

software of INFONOTARY PLC.

Qualified electronic time stamp (token) issued by the Provider validates the exact date and time at which the client electronic document is registered at the Provider's TimeStamp server. The issued time stamps are recorded in the Provider's register.

The accuracy used by the Provider for issuing electronic time stamp is +/- 500ms (half second) or better than UTC.

The Qualified electronic time stamp issued by the Provider contains the following elements:

- status - an integer indicating whether the signature was successful;
- time certificate version (version 1);
- the hash of the signature that was contained in the request;
- unique subsequent serial number;
- UTC signing time;
- Timestamp authority identification – the Provider.

Time stamp certificates are signed with a private key of the Provider intended only for this activity by the operating authority InfoNotary Qualified TimeStamping Service CA.

Time stamp certificate signing operation is performed by hardware security module with a high level of reliability and security.

The Provider's Time Stamp Authority system is under high physical and technological control mode access and is stored in a specialized room with access control for authorized employees.

The service for issuing qualified electronic time stamps is available at http://ts.infonotary.com/tsa

8.1.2. Independent source for accurate time

The Provider operates its own system for independent source for accurate time (Time Sinhronizator), which supports the following protocols:

- NTPv4 (RFC 5905)
- SNMPv1 (RFC 1157), SNMPv3 (RFC 3411-3415)

The system is synchronized via GPS, synchronization from other NTP servers.

9. TimeStamp Profile

9.1.1. TimeStamp Request profile

Attribute	Value
HTTP Content-Type	application/timestamp-query
Version	1 (0x01)
Requested policy	Empty or 1.3.6.1.4.1.22144.3.4.1

9.1.2. TimeStamp Response profile

Attribute	Value	
HTTP Content-Type	application/timestamp-reply	
Status:	granted	according RFC 3161;

	grantedWithMods	according RFC 3161, not used;
	rejection	according RFC 3161;
	waiting	according RFC 3161, not used;
	revocationWarning	according RFC 3161, not used;
Errors:	BadAlgIdentifier; badRequest; badDataFormat timeNotAvailable unacceptedPolicy unacceptedExtension addInfoNotAvailable systemFailure	according RFC 3161;
Policy	1.3.6.1.4.1.22144.3.4.1	
Time marker	UTC, GPS current time	
Accuracy	0,5 seconds	
List of Issuer's Certificates	Contains the issuer's chain of the TSA certificate	

10. EQUIPMENT, PROCEDURE AND MANAGEMENT CONTROL

10.1. 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.

10.1.1. 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.

10.1.2. 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.

10.1.3. 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.

10.1.4. Floods

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

10.1.5. Fire alarm and protection

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

10.1.6. Data storage devices

The Provider uses reliable means and devices for the physical storage of data and confidential information, such as safes and metal cases with different degree of protection.

10.1.7. Taking a technical components out of use and operation

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

10.1.8. Duplicate components

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

10.2. 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.

10.2.1. 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.

10.2.2. 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.

10.2.3. Identification and authentication of each position

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

10.2.4. 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.

10.3. 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;
- auditing, 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.

10.3.1. Requirements to independent suppliers

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

10.3.2. 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.

10.4. Procedures for the preparing and maintenance of inspection data journal

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

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

- issuing a certificate;

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

The records contain the following information:

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

The Provider records all events related to the operation of the hardware and software platforms as follows:

- in cases of installing a new and/or additional software;
- in cases of shutting down or launching the systems and their applications;
- in cases of successful or unsuccessful attempts to launch or access to the software PKI components of the systems;
- in cases software and hardware system failures, etc.;
- in cases of managing and using the hardware cryptomodules.

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

are also stored.

Records are generated automatically and stored at discrete intervals for the different modules. Authorized personnel of the Provider checks the records and logs at regular intervals and establishes and reports irregularities.

The records and logs are stored for a period of 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.

10.5. Archiving

The Provider stores as internal repository the following documents:

- all certificates issued for a period of at least 10 (ten) years after expiry of the term of validity of a certificate;
- all records and logs related to the issuance of a certificate for a period of at least 10 (ten) years after the issuance of a certificate;
- all records and logs relating to the termination of a certificate for a period of at least 10 (ten) years after the termination of the certificate;

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

The Provider stores the records in a recoverable format.

The Provider ensures the integrity of the physical carriers and implements a copying mechanism to prevent data loss.

The repository is accessible only to authorized personnel of the Provider and the Registration Authority, if necessary.

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

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

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

- only staff authorized to keep the archive has access to it;
- protection of the archive from modifications by recording the data on single-entry devices;
- protection from archive erasing;

- Protection ensuring the destruction of carriers on which the archives has been stored, after the regular transfer of data to a new carrier.

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

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

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

10.6.1. 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.

All information in case of hardware, software and/or data corruption or theft is transmitted to the security administrator acting in accordance with internal procedures. These procedures are related to situation analysis, incident investigation, measures to minimize the consequences and to prevent such incidents in the future. In case of a hardware, software or data failure, the Provider notifies users, recovers infrastructure components and resumes in priority the access to the public register and the Certificate Revocation List (CRL). For such cases, the Provider has developed an "Incident Management

Plan". The Provider has a plan to manage all incidents that affect the proper functioning of the certification infrastructure. This plan is in line with the Business Continuity Plan and the Disaster Recovery Plan.

10.7. Procedures for terminating the activity 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.

11. OTHER BUSINESS AND LEGAL CONDITIONS

11.1. 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.