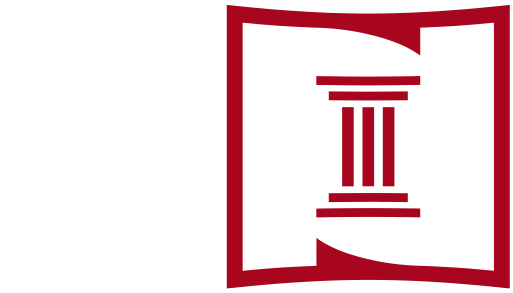


InfoNotary

CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES

PROVIDED BY

QUALIFIED TRUST SERVICE PROVIDER

INFONOTARY PLC

Version 2.3

Entry into force 01.07.2021

CONTENT

1. INTRODUCTION 7

1.1. GENERAL TERMS AND CONDITOIN 9
1.1.1. Trust Service Provider 9
1.2. DENOMINATION AND IDENTIFICATION OF THE DOCUMENT 11
1.3. PARTICIPANTS IN THE CERTIFICATE INFRASTRUCTURE 13
1.3.1. Certification Authority 13
1.3.2. Registration Authority 16
1.3.3. Subscribers 17
1.3.4. Relying Parties 17
1.3.5. Holder/Signer 18
1.3.6. Creator of a Seal 18
1.3.7. Representatives 18
1.3.8. Platform for cloud qualified certificates and remote signing and stamping of electronic documents 19
1.4. CERTIFICATES USAGE 19
1.4.1. Certificates types and usage 19
1.4.2. Usage and accessibility of services 43
1.4.3. Certificate activity limitations 43
1.5. POLICY ADMINISTRATION 44
1.6. TERMS AND ABBREVIATIONS 45

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 52

2.1. REPOSITORIES 52
2.1.1. Public Documental Repository 52
2.1.2. Certificate Register 52
2.2. PUBLISHING CERTIFICATE INFORMATION 52
2.3. FREQUENCY OF PUBLICATIONS 53
2.4. ACCESS TO THE CERTIFICATE REGISTER 53
2.4.1. Public access to the register 53
2.4.2. Access control in keeping the directory 54

3. IDENTIFICATION AND AUTHENTICATION 54

3.1. NAMING 54
3.1.1. Name types 55
3.1.2. Pseudonyms 55
3.1.3. Rules for interpreting different forms of names 55
3.1.4. Uniqueness of the names 56
3.1.5. Recognition, authenticity and role of trademarks 56
3.2. INITIAL IDENTIFICATION AND IDENTITY VALIDATION 57
3.2.1. Method of verifying the holding of the Private key 57
3.2.2. Identity validation of a Legal Entity 58
3.2.3. Identifying a natural person - Holder or Authorized Representative 59
3.2.4. Unconfirmed information 61
3.3. IDENTITY VALIDATION AND AUTHENTICATION IN REQUEST FOR REPLACEMENT OF KEYS IN A CERTIFICATE 61
3.4. IDENTITY VALIDATION AND AUTHENTIFICATION OF A CERTIFICATE REVOCATION REQUEST 61
3.5. IDENTITY VALIDATION AND AUTHENTIFICATION OF A CERTIFICATE SUSPENSION REQUEST 62

4. EFFECTIVE CONDITIONS 63

4.1. REQUEST FOR ISSUANCE OF A CERTIFICATE 63
4.1.1. Applicants 63
4.1.2. Process of applying a certificate issuance 63
4.2. PROCEDURE FOR SUBMITTING A REQUEST A CERTIFICATE 65
4.2.1. Performing the functions of identifinaction and authentification 65
4.2.2. Granting or denying certificate applications 65
4.2.3. Term for processing certificate applications 67
4.3. ISSUANCE OF A CERTIFICATE 67
4.3.1. Actions of the Certification Authority when issuing a Certificate 67
4.3.2. Notifying the Holder/Creator of the seal by the Certification Authority of issuance and delivery of the certificate 68
4.4. ACCEPTING AND PUBLISHING THE CERTIFICATE 68
4.4.1. Accepting the Certificate 68
4.4.2. Publishing the certificate by the Certification Authority 69
4.5. DATA SECRECY OF QUALIFIED TRUST SERVICES AND CERTIFICATES USAGE 69
4.5.1. Data secrecy 69
4.5.2. Usage of validation data from Relying parties and certificate usage 69
4.6. CERTIFICATE RENEWAL 70
4.6.1. Conditions for certificate renewal 70
4.6.2. Who can apply for renewal request 70
4.6.3. Procedure for submitting a renewal request 70
4.6.4. Notifying the Holder by the Certification Authority of issuance and delivery of the new certificate 72
4.6.5. Acceptance of the renewed certificate 72
4.6.6. Issuance and publishing the renewed certificate by the Certification Authority 73
4.7. KEY REPLACEMENT IN CERTIFICATE 73
4.8. MODIFICATION OF A CERTIFICATE 73
4.9. TERMINATING A CERTIFICATE 73
4.9.1. Conditions for terminating a certificate 73
4.9.2. Who can ask a certificate termination 74
4.9.3. Termination request procedure 74
4.9.4. Grace period for serving the termination request 75
4.9.5. Verification requirements for termination of a certificate to the Relying parties 75
4.9.6. Frequency of updating the Certificate Revocation List 75
4.9.7. Maximum delay of publishing the Certificate Revocation List 76
4.9.8. Option for certificate status check in real time (OCSP) 76
4.9.9. Requirements for using OCSP 76
4.10. SUSPENSION OF A CERTIFICATE 76
4.10.1. Conditions for suspending a certificate 76
4.10.2. Who can request suspension 76
4.10.3. Suspension request procedure 77
4.10.4. Limitation of the certificate suspension term 77
4.10.5. Resuming a suspended certificate 77
4.11. CERTIFICATE RESUMPTION PROCEDURE 78
4.11.1. Resumption upon the request of the Holder/Creator 78
4.11.2. Resumption by order of the Supervisory Authority 78
4.11.3. Resumption after the end of the suspension term 78
4.12. TERMINATION OF THE AGREEMENT FOR QUALIFIED TRUST SERVICES 79
4.13. KEY RECOVERY AND KEY ESCROW 79

5. EQUIPMENT, PROCEDURE AND MANAGEMENT CONTROL 79

5.1. PHYSICAL CONTROL 79

5.1.1. Layout and design of the premises ... *79*
5.1.2. Physical access ... *79*
5.1.3. Power supply and ambient conditions ... *80*
5.1.4. Floods ... *80*
5.1.5. Fire alarm and protection ... *80*
5.1.6. Data storage devices ... *80*
5.1.7. Taking a technical components out of use and operation ... *80*
5.1.8. Duplicate components ... *81*
5.2. PROCEDURAL CONTROL ... 81
5.2.1. Positions and functions ... *81*
5.2.2. Number of employees involved in a certain task ... *81*
5.2.3. Identification and authentication of each position ... *81*
5.2.4. Requirements for division of responsibilities for separate functions ... *82*
5.3. STAFF CONTROL, QUALIFICATION AND TRAINING ... 82
5.3.1. Requirements to independent suppliers ... *82*
5.3.2. Documentation provided to the staff ... *82*
5.4. PROCEDURES FOR THE PREPARING AND MAINTENANCE OF INSPECTION DATA JOURNAL ... 83
5.4.1. Frequency of generating records ... *84*
5.4.2. Record storage period ... *84*
5.4.3. Record security and protection ... *84*
5.4.4. Procedure for generating back-up copies of the records ... *84*
5.5. ARCHIVING ... 84
5.5.1. Types of archives ... *85*
5.5.2. Storage period ... *85*
5.5.3. Archive protection and security ... *85*
5.5.4. Archive restoring procedures ... *85*
5.5.5. Requirements for verifying the date and time of records ... *86*
5.5.6. Archive storage ... *86*
5.5.7. Procedures for acquiring and verifying information from an archive ... *86*
5.6. MODIFICATION OF A CERTIFICATE KEY ... 86
5.7. KEY COMPROMISE AND DISASTER OR UNEXPECTED CASES RECOVERY ... 86
5.7.1. Action in case of disasters and accidents ... *87*
5.7.2. Incidents related to hardware, software, and/or data failures ... *88*
5.8. PROCEDURES FOR TERMINATING THE ACTIVITY OF THE PROVIDER ... 88
5.8.1. Termination of activity ... *88*
5.8.2. Transfering the activity of another qualified provider of qualified trust services ... *89*
5.8.3. Withdrawal of the qualified status of the Provider ... *90*

6. TECHNICAL SECURITY CONTROL ... 90

6.1. GENERATING AND INSTALLING KEY PAIR ... 90
6.1.1. Generating key pair ... *91*
6.1.2. Private key delivery ... *93*
6.1.3. Delivery of the Public Key to the issuer of the Certificate ... *93*
6.1.4. Delivery of the Public Key of the Certification Authority to the Relying Parties ... *93*
6.1.5. Key length ... *93*
6.2. PRIVATE KEY PROTECTION AND TECHNICAL CONTROL OF THE CRYPTOGRAPHIC MODULE ... 94
6.2.1. Cryptographic Module Standards ... *94*
6.2.2. Storage and usage of a private key control ... *94*
6.2.3. Storage of Private keys ... *95*
6.2.4. Private keys archiving ... *95*
6.2.5. Private keys Transfer in and out of the cryptographic module ... *95*
6.2.6. Activation and Deactivation of Private Keys ... *96*

6.2.7. Private Keys Destruction ... 96
6.3. OTHER ASPECTS OF MANAGING THE KEY PAIR ... 96
6.3.1. Public key archival ... 96
6.3.2. Validity period of the certificate and period of use of the key pair ... 97
6.4. ACTIVATION DATA ... 97
6.4.1. Generation and installing activation data ... 97
6.4.2. Activation data protection ... 98
6.5. COMPUTER SECURITY CONTROL ... 98
6.5.1. Specific requirements for computer security ... 98
6.5.2. Computer security rating ... 98
6.6. TECHNICAL LIFE CYCLE CONTROL ... 98
6.7. NETWORK SECURITY CONTROL ... 99
6.8. TIME STAMPING SERVICE ... 99
6.8.1. Time Stamping procedure ... 99
6.8.2. Independent source for accurate time ... 100
6.9. QUALIFIED VALIDATION SERVICE ... 101
6.9.1. Provision of the Qualified Validation Service ... 102

7. PROFILES ... 103

7.1. QUALIFIED CERTIFICATE PROFILE ... 103
7.1.1. Version number ... 103
7.1.2. Certificate Extensions ... 103
7.1.3. Electronic signature algorithm identifiers ... 106
7.1.4. Naming forms ... 106
7.1.5. Name limitations ... 106
7.2. PROFILE OF THE LIST OF SUSPENDED AND REVOKED CERTIFICATES (CRL) ... 106
7.2.1. Version number ... 106
7.2.2. Attributes of the list and its certificates ... 107
7.3. OCSP PROFILE ... 108
7.3.1. OCSP Request Profile ... 108
7.3.2. Profile of OCSP Response ... 109
7.3.3. OCSP Data Response ... 110
7.3.4. Individual OCSP responses ... 110
7.4. TIMESTAMP PROFILE ... 110
7.4.1. TimeStamp Request Profile ... 110
7.4.2. TimeStamp Response Profile ... 110
7.5. VALIDATION REPORT ... 111

8. AUDITING AND CONTROL OF THE ACTIVITY ... 112

8.1. REGULAR OR CIRCUMSTANTIAL AUDITS ... 112
8.2. QUALIFICATION OF THE AUDITORS ... 113
8.3. RELATION BETWEEN THE AUDITOR AND THE AUDITED ORGANIZATION ... 113
8.4. VERIFICATION SCOPE ... 113
8.5. MEASURES FOR CORRECTING ESTABLISHED DEFECTS ... 114
8.6. ANNOUNCING THE RESULTS ... 114

9. OTHER BUSINESS AND LEGAL CONDITIONS ... 115

9.1. PRICES AND FEES ... 115
9.1.1. Remuneration under Qualified Certification Services Agreement ... 115
9.1.2. Billing ... 116
9.1.3. Certificate reclamation and payment refunding policy ... 116
9.2. FINANCIAL RESPONSIBILITIES ... 116

9.2.1. Financial responsibility 116
9.2.2. Insurance of the Provider's activity 116
9.3. INFORMATION CONFIDENTIALITY 117
9.3.1. Scope of confidential information 117
9.3.2. Information beyond the scope of the confidential information 118
9.3.3. Obligation for confidential information protection 118
9.4. PERSONAL DATA CONFIDENTIALITY 119
9.5. INTELLECTUAL PROPERTY RIGHTS 120
9.6. OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES 120
9.6.1. Provider's Obligations, Responsibilities and Warranties 121
9.6.2. Guarantees and responsibilities of the Registration Authority 121
9.6.3. Responsibility of the Holder/Creator of the seal to relying parties 122
9.6.4. Relying parties care 122
9.7. RESPONSIBILITY DISCLAIMER 123
9.8. PROVIDER'S LIABILITY LIMITATION 123
9.9. COMPENSATION FOR THE PROVIDER 124
9.10. TERM AND TERMINATION 124
9.10.1. Term 124
9.10.2. Termination and invalidity 124
9.10.3. Termination Effect 125
9.11. INDIVIDUAL NOTIFICATION AND COMMUNICATION BETWEEN PARTICIPANTS 125
9.12. CHANGES IN CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES 125
9.13. CONFLICT MANAGEMENT AND JURISDICTION 125
9.14. APPLICABLE LAW 126
9.15. COMPLIANCE WITH THE APPLICABLE LAW 126
9.16. OTHER PROVISIONS 126

1. INTRODUCTION

The current document **CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES** provided by 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), Electronic document and electronic trust services act 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 v2.2.1 General Policy Requirements for Trust Service Providers
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
- EN 319 411-1 v1.2.2: General requirements;
- EN 319 411-2 v2.2.2: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- 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;
- 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organizations;
- 319 412-5 v2.2.1: QCStatements;
- EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles;
- 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 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP;
- RFC 3279: Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- TS 119 495 v1.2.1: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366;
- ETSI TS 119 441 Policy Requirement for TSP providing signature validation services.
- ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol for TSPs providing signature validation services"
- ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".
- ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part1: Creation and Validation.
- ETSI TS 119 102-2: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report;
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

All international standards and specifications are used in actual and valid versions.

The main purpose of the document CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES also known as (Practice or InfoNotary Qualified CPS), to make the Qualified Trust Services public for the consumers through a detailed description of the rules and policies which INFORNOTARY 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.

InfoNotary Qualified CPS describes the technical and procedural practices for all services, connected with providing of certification services for the issuance and management of qualified electronic signature certificates, qualified electronic seals and qualified electronic time stamps, as well as the related policy for the provision of qualified certification services.

InfoNotary Qualified CPS 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 .

InfoNotary Qualified CPS 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 и https://repository.infonotary.com.

1.1. GENERAL TERMS AND CONDITOIN

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 issuance services:

- Acceptance and verification of applications for issuance 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:

- 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:

- granting access to the registry with the issued certificates to relying parties;
- granting relying parties access to the lists of suspended and revoked certificates;
- providing services for restricting access to published certificates.

Qualified validation service of qualified certificates, qualified electronic signature and qualified electronic seal:

- providing of services for on-line certificate status validation (OCSP) for Qualified certificates issued by InfoNotary;
- providing of services for on-line validation of a qualified certificate, qualified electronic signature and qualified electronic seal (InfoNotary Qualified Validation Service - IQVS).

Time verification services of a signed document:

- issuing a qualified time stamp to certify the date and time of the submission of an electronic signature created for a specific electronic document;
- providing services for verification of a qualified time stamp issued by the Provider for the date and time of an electronic document.

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 its activity 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 **"Certification practice statement for qualified certification services to INFONOTARY PLC"** document (Practice), is named **"InfoNotary Qualified CPS"** and is identified by the following object identifier in the issued certificates: OID:1.3.6.1.4.1.22144.3

An object identifier (OID) is a string of decimal numbers, that uniquely identifies an object.

INFONOTARY's OID that designate the organization uniquely, is registered as a Private Enterprise Number (PEN) in IANA (http://www.iana.org/assignments/enterprise-numbers)
iso. org.dod.internet.private.enterprise (1.3.6.1.4.1)

PEN of INFONOTARY PLC: 22144

The OID structure that INFONOTARY PLC use is the following:

InfoNotary Plc	InfoNotary CSP	InfoNotary TTP	InfoNotary TSP	Roots	CAs	End Entity
1.3.6.1.4.1.22144	1	2	3	1	1	1

Practice relates to Certification Policies for providing Qualified Certificates for Qualified Electronic Signature, Qualified Certificates for Qualified Electronic Seal, Qualified Certificates for Advanced Electronic Signature, Qualified Certificates for Advanced Electronic Seal, Qualified Website Authentication Certificates, Q and Other Certification Services.

The practice includes:

- description of the conditions that the Provider complies with and will follow when issuing Qualified Certificates, 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, the initial identification and authentication of the Holder of certificates, the conditions and the necessary security levels for creating the electronic signature and storing and saving the private key of the Holders and Creators of seals.
- determines the feasibility and reliability of the information included in the Qualified Certificates.

The certification policies which are applicable to the different types of qualified certificates and are issued by the Provider to end-users are identified by the following object identifiers in the certificates:

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

InfoNotary Qualified TimeStamping Service CP	1.3.6.1.4.1.22144.3.4.1
InfoNotary Qualified OCSP CP	1.3.6.1.4.1.22144.3.5.1
InfoNotary Qualified Validation Service CP	1.3.6.1.4.1.22144.3.5.2
InfoNotary Qualified Certificate for Natural Person AESignature CP	1.3.6.1.4.1.22144.3.6.1
InfoNotary Qualified Certificate for Delegated AESignature CP	1.3.6.1.4.1.22144.3.6.2
InfoNotary Qualified Certificate for Legal Person AESeal CP	1.3.6.1.4.1.22144.3.7.1
InfoNotary Qualified Certificate for PSD2 AESeal CP	1.3.6.1.4.1.22144.3.7.2

1.3. PARTICIPANTS IN THE CERTIFICATE INFRASTRUCTURE

1.3.1. Certification Authority

InfoNotary is the Certification Authority of the Trust Service Provider carrying out the following activities: electronic signature and electronic seal certificates issuance, certificates management, 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/Creator information, application restrictions, and responsibilities.

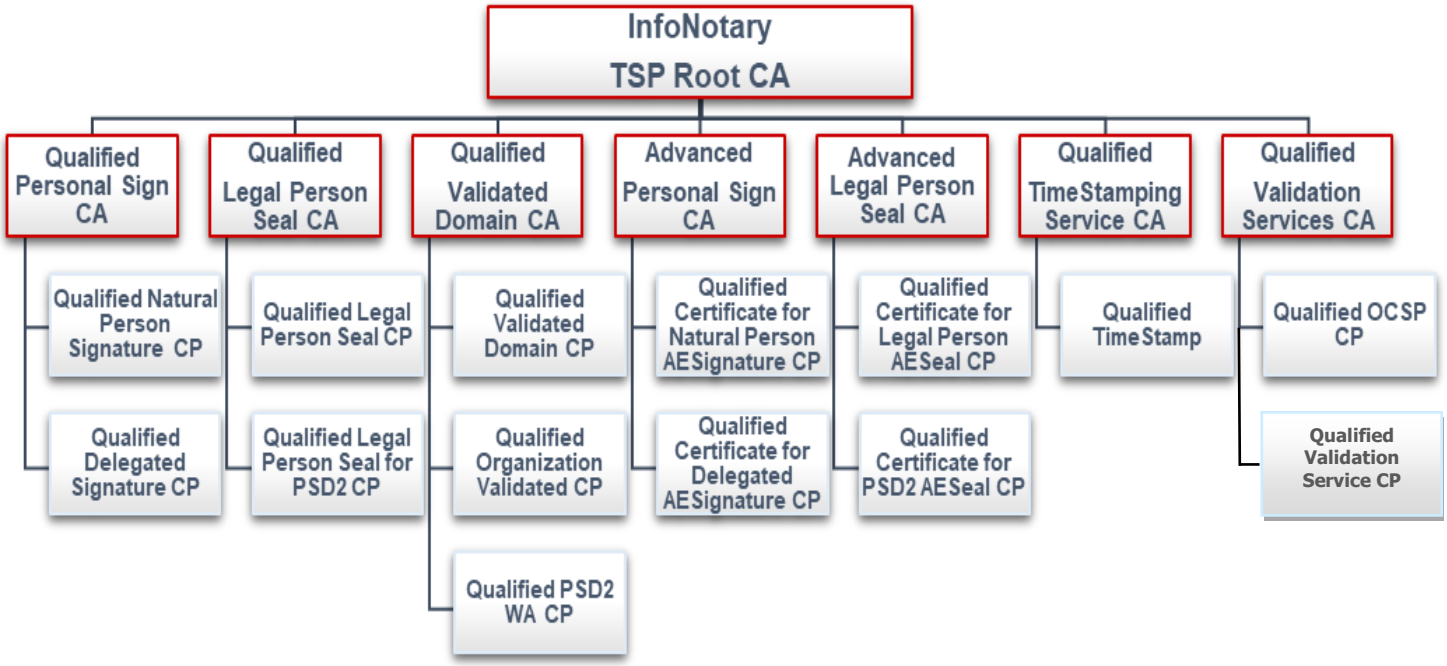
The Certification Authority issues different types of certificates, according to the certification policies through its differentiated **Operational Certification Authorities** (operational CAs).

The Provider's certification Authority employs one- or two-level certification architecture for differentiation electronic signature and seal certificate issuance and management activities, depending on the certification policy for the different certificate types, as shown in the table below:

Name	Type	OID
InfoNotary TSP Root CA	Root CA	1.3.6.1.4.1.22144.3

Name	Type	OID
InfoNotary Qualified Personal Sign CA	Operational CA	1.3.6.1.4.1.22144.3.1
InfoNotary Qualified Legal Person Seal CA	Operational CA	1.3.6.1.4.1.22144.3.2
InfoNotary Qualified Validated Domain CA	Operational CA	1.3.6.1.4.1.22144.3.3
InfoNotary Qualified TimeStamping Service CA	Operational CA	1.3.6.1.4.1.22144.3.4
InfoNotary Qualified Validation Services CA	Operational CA	1.3.6.1.4.1.22144.3.5
InfoNotary Advanced Personal Sign CA	Operational CA	1.3.6.1.4.1.22144.3.6
InfoNotary Advanced Legal Person Seal CA	Operational CA	1.3.6.1.4.1.22144.3.7

In performing its activities, the Provider's certification Authority uses the following certification infrastructure model:



1.3.2. Registration Authority

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

The Provider's Registration Authority perform activities of:

- 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 applications for certificate issuance;
- 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 (Holder and Creator of a Seal) 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/Creator of a seal;
- installing the certificate and transmitting the cryptographic device (QSCD) and the activation data (PIN and AIN) to the Holder/Creator 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 Provider assigns the performance of the activities of Registration Authority on the basis of a bilateral written contract.

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.

Part of the Registration Authority's functions can be performed by Local Registration Offices, acting under the supervision of the Registration Authorities.

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, corresponding to the public key, entered into the issued certificate and creates electronic signatures.

The Holder is also the owner of the cryptographic device – smartcard or token (Qualified Signature Creation Device), used for generation and storage of cryptographic keys, qualified certificates for electronic signature/seal and electronic signature/seal creation data.

1.3.6. Creator of a Seal

The Creator of a Seal is a legal entity that creates electronic seals and is entered as such in the electronic seal certificate.

Only the Creator has the right to access the private key for creating sealed electronic statements.

1.3.7. Representatives

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

The Representative is a person, different from the Subscriber/Holder/Creator of the seal; it is not entered in the certificate and cannot make electronic statements signed with the Holder's electronic signature or seals with the electronic seal of the Creator of a Seal and on behalf of the Holder/Creator.

1.3.8. 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 types and usage

1.4.1.1. Certificates of the Certification Authority

1.4.1.1.1. Basic certificate (Root)

The Root certificate for the public key of the Certification Authority of the Provider, named **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 and for the services provided to end users outside the scope of the regulated certification services in Regulation (EU) No 910/2014.

The base **InfoNotary TSP Root** certificate contains the following basic information:

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

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

1.4.1.1.2. 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 issues Qualified Certificates to consumers in accordance with the Practice and Policy for Providing Qualified Certification Services.

1.4.1.1.2.1. Operational Certification Authority for Qualified Certificates for Qualified 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**, and end user's certificates for qualified certificates for delegated electronic signature of natural persons **InfoNotary Qualified Delegated 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.**

The Certificate of the Operational Certification Authority **InfoNotary Qualified Personal Sign CA** contains the following basic information:

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
Algorithm of the electronic signature		SHA256/RSA
Attributes of the Issuer:		
Attribute		**Value**
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC

Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of 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=keyid,issuer

1.4.1.1.2.2. Operational Certification Authority for Qualified Certificates for Qualified Electronic Seal of legal persons (InfoNotary Qualified Legal Person Seal CA)

Certificate for the public key of the Operational certification Authority **InfoNotary Qualified Legal Person Seal** for qualified electronic seal, OID: 1.3.6.1.4.1.22144.3.2, is signed with the private key of the **InfoNotary Root Certification Authority**, OID: 1.3.6.1.4.1.22144.3.

End user's qualified certificates for qualified seal **InfoNotary Qualified Legal Person Seal and InfoNotary Qualified Legal Person Seal for PSD2** according to the respective certification policy and InfoNotary Qualified CPS, are signed with the private key of the **InfoNotary Qualified Legal Person Seal CA.**

The list of suspended and revoked certificates of end-users (**InfoNotary Qualified Legal Person Seal CA**) is signed by the private key of the Operating Authority (**qualified-legal-ca.crl**).

The Certificate of the Operational Certification Authority **InfoNotary Qualified Legal Person Seal CA** contains the following information:

InfoNotary Qualified Legal Person Seal 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
Algorithm of the electronic signature		SHA256/RSA
Attributes of the Issuer:		
Attribute		**Value**
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attribute of the Holder (x509 Subject DN):		
Attribute		**Value**
Common Name	CN	InfoNotary Qualified Legal Person Seal CA
Domain Component	DC	qualified-legal-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=1.3.6.1.4.1.22144.3.2 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Legal Person Seal CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

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

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

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

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

- End-user qualified certificates for website authentication for PSD2 InfoNotary Qualified PSD2 WA Certificate

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

The Certificate of Operational Certification Authority **InfoNotary Qualified Validated Domain CA** contains the following basic information:

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

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

1.4.1.1.2.4. Operational Certification Authority for Issuance of Qualified Time Stamp (InfoNotary Qualified TimeStamping Service CA)

Certificate for the public key of the Operational Certification Authority for the issuance of Qualified Electronic Time Stamps **InfoNotary Qualified TimeStamping Service CA**, **OID: 1.3.6.1.4.1.22144.3.4**, is issued and signed with the private key of the InfoNotary TSP Root CA, OID: 1.3.6.1.4.1.22144.3.

The electronic time stamps for end-users are signed with the private key of the Operational Certification Authority **InfoNotary Qualified TimeStamping Service CA** in accordance with the appropriate certification policy and InfoNotary Qualified CPS.

The Certificate of 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
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 Issuer:		
Attribute		Value
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia

Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of Holder (x509 Subject DN):		
Attribute		Value
Common Name	CN	InfoNotary Qualified 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

1.4.1.1.2.5. Operational Certification Authority for Validation Services (InfoNotary Qualified Validation Services CA)

The Certificate for the Public Key of the Operational Certification Authority for the provision of electronic signature or seal validation services **InfoNotary Qualified Validation Services CA**, OID: 1.3.6.1.4.1.22144.3.5, is issued and signed with the private key of the InfoNotary TSP Root CA, OID: 1.3.6.1.4.1.22144.3.

Qualified OCSP status checks responses for end-users are signed with the private key of the Operating Authority **InfoNotary Qualified Validation Services CA**, according to the respective certification policy and InfoNotary Qualified CPS.

The private key of the Operational Authority (InfoNotary Qualified Validation Services CA) signs the qualified certificate supporting advanced electronic seal, which stamps the respons to a requests for validation and validation reports of a qualified certificates, qualified electronic signature and qualified electronic stamps according to Certification policy (OID: 1.3.6.1.4.1.22144.3.5.1; OID: 1.3.6.1.4.1.22144.3.5.2) and InfoNotary Qualified CPS.

The Certificate of Operational Certification Authority **InfoNotary Qualified Validation Services CA** contains the following basic information:

InfoNotary Qualified Validation Services 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
An electronic signature algorithm		SHA256/RSA
Attributes of the Issuer:		
Attribute		**Value**
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of Holder (x509 Subject DN):		
Attribute		Value
Common Name	CN	InfoNotary Qualified Validation Services CA
Domain Component	DC	qualified-validation-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=1.3.6.1.4.1.22144.3.5 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Validation Services CA
Subject Key Identifier	SubjectKeyIdentifier
Authority Key Identifier	AuthorityKeyIdentifier

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

The Certificate for the public key of the Operational Certification Authority for Qualified Certificates for Advanced Electronic Signature of natural person (**InfoNotary Advanced Personal Sign CA**), **OID: 1.3.6.1.4.1.22144.3.6**, 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 certificates for advanced electronic signature of natural person **InfoNotary Qualified Certificate for Natural Person AESignature**, and end user's qualified certificates for delegated advanced electronic signature of natural persons **InfoNotary Qualified Certificate for Delegated AESignature** 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-aes-ca.crl**) is signed with the private key of the operating authority **InfoNotary Advanced Personal Sign CA.**

The Certificate of the Operational Certification Authority **InfoNotary Advanced Personal Sign CA** contains the following basic information:

InfoNotary Advanced 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
Algorithm of the electronic signature		SHA256/RSA
Attributes of the Issuer:		
Attribute		**Value**
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		**Value**
Common Name	CN	InfoNotary Advanced Personal Sign CA
Domain Component	DC	qualified-natural-aes-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=1.3.6.1.4.1.22144.3.6 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Advanced Personal Sign CA	
Subject Key Identifier	subjectKeyIdentifier	
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer	

1.4.1.1.2.7. Operational Certification Authority for Qualified Certificates for Advanced Electronic Seal of legal persons (InfoNotary Advanced Legal Person Seal CA)

Qualified Certificate for the public key of the Operational certification Authority **InfoNotary Advanced Legal Person Seal CA** for advanced electronic seal, OID: 1.3.6.1.4.1.22144.3.7, is signed with the private key of the **InfoNotary Root Certification Authority**, OID: 1.3.6.1.4.1.22144.3.

End user's qualified certificates for advanced seal **InfoNotary Advanced Legal Person Seal CA and InfoNotary Qualified Certificate for PSD2 AESeal** according to the respective certification policy and InfoNotary Qualified CPS, are signed with the private key of the **InfoNotary Advanced Legal Person Seal CA.**

The list of suspended and revoked certificates of end-users (**InfoNotary Advanced Legal Person Seal CA**) is signed by the private key of the Operating Authority (**qualified-legal-aes-a.crl**).

The Certificate of the Operational Certification Authority **InfoNotary Advanced Legal Person Seal CA** contains the following information:

InfoNotary Advanced Legal Person Seal 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
Algorithm of the electronic signature		SHA256/RSA
Attributes of the Issuer:		
Attribute		**Value**
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG

Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		**Value**
Common Name	CN	InfoNotary Advanced Legal Person Seal CA
Domain Component	DC	qualified-legal-aes-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=1.3.6.1.4.1.22144.3.7 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Advanced Legal Person Seal CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

1.4.1.2. End-User Certificates

The Qualified Certificates issued by the Provider to end-users may have a different purpose, according to the Policies for these Certificates.

The Qualified Certificates issued by the Provider contain the extensions defined by the X.509 v.3 standard, as well as additional constrains and extensions as defined by the International Organization for Standardization (ISO).

The Qualified Certificates contain the extension "Key Usage" defining certificate application constraints. The attribute is of category of "critical".

Certificates issued by the Provider according to their Certification Policy can be used for the following purposes:

- authentication – assurance of identity;
- confidentiality – encryption and decryption of data;
- integrity – ensuring the integrity and immutability of the signed data;
- non-repudiation – impossibility for signing rejection.

The Qualified Certificates contain the extension "Extended Key Usage", which details the certificate application with view to its designation. This attribute belongs to the category of "non critical".

1.4.1.2.1. Types of Qualified Certificates

INFONOTARY PLC, as a Qualified Trust Service Provider, issues Qualified Certificates for Qualified Electronic Signatures, Qualified Electronic Seals, Advanced Electronic Signatures and Advanced Electronic Seals, Qualified Electronic Time Stamps, Qualified Website Authentication Certificates and

performs validation services for electronic signatures and seals in full compliance with the provisions and the requirements of the Regulation (EU) 910/2014.

InfoNotary Qualified Natural Person Signature

Qualified certificate for qualified electronic signature of a natural person

The certificate is issued to a natural person (Holder) and can be used for personal identification to Internet applications, financial transactions, secured and encrypted communication, electronic correspondence, electronic document signing and making statements, authentication and data encryption activities. The certificate is associated with a pair of cryptographic keys that are generated and stored only on a qualified electronic signature creation device (QSCD). The device, the 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 Certificate for Qualified Delegated Signature

Qualified certificate for qualified electronic signature of a natural person with delegated authority

The certificate is issued to a natural person (Holder) and contains information about a legal entity that has delegated authority to the Holder and can be used for for personal identification to Internet applications, financial transactions, secured and encrypted communication, electronic correspondence, electronic document signing and making statements, authentication and data encryption activities. The certificate is associated with a pair of cryptographic keys that are generated and stored only on a qualified electronic signature creation device (QSCD). The device, the 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 Certificate for Qualified Legal Person Seal

Qualified certificate for qualified electronic seal of a legal entity

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

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

InfoNotary Qualified Certificate for Legal Person Seal for PSD2

Qualified certificate for qualified electronic seal of PSD2 legal entity

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

InfoNotary Qualified Validated Domain Certificate

Qualified Certificate for website authenticity with validated domain

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

InfoNotary Qualified Organization Validated Certificate

Qualified Certificate for website authenticity with validated organization

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

InfoNotary Qualified PSD2 WA Certificate

Qualified Certificate of Authenticity of the PSD2 organization website

The certificate is issued to a legal person/organization (Holder) – Payment Service Provider PSP – PSD2 Directive and may be used to certify the authenticity of a website that is entered in the certificate. The certificate is issued in accordance with the requirements of Regulation (EU) 910/2014 and

PSD2 Directive and is used to create assurance in the visitors, that the website stakeholder is real and legitimate subject. The Qualified Certificate contains specific attributes that provide the necessary information to identify the PSD2 Payment Service Provider.

InfoNotary Qualified TimeStamp Certificate

Qualified Electronic time stamp

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

InfoNotary Qualified Certificate for Natural Person AESignature

Qualified certificate for an advanced electronic signature of an natural person

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

InfoNotary Qualified Certificate for Advanced Delegated Signature

Qualified certificate for an advanced electronic signature of a natural person with delegated authority

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

InfoNotary Qualified Certificate for Advanced Legal Person Seal

Qualified certificate for Advanced electronic Seal of a legal entity

The certificate is issued to a Legal Person (Creator of a Seal) as a means

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

InfoNotary Qualified Certificate for PSD2 AESeal

Qualified certificate for Advanced electronic seal of PSD2 legal entity

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

1.4.2. Usage and accessibility of services

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

1.4.3. Certificate activity limitations

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

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

The Provider is not responsible for damages resulting from the use of the certificates issued by him beyond their authorized use and according to the limitations of the application regarding the purpose and the value of the transactions and financial interest and will lead to the cancellation of the guarantees, which INFONOTARY PLC gives the Holder/ Creator of the seal and the Relying Parties.

1.5. POLICY ADMINISTRATION

The certification policy and the Provider's practice are determined by the Board of Directors of INFONOTARY PLC.

Any and all amendments, modifications and additions to the qualified certification services provision practice and certification policies for the different qualified certificate types shall be adopted by the Board of Directors of INFONOTARY PLC.

The new versions of the documents shall be published in the Provider's Documentary repository immediately after their approval by the Board of Directors and shall be publicly accessible at: http://repository.infonotary.com and https://repository.infonotary.com.

Any and all comments, inquiries for information and clarifications of the qualified certification services provision practice and certification policies may be addressed to:

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

Advanced electronic seal	An electronic seal, which meets the requirements: - it is uniquely linked to the creator of the seal; - it is capable of identifying the creator of the seal; - it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and - it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
Advanced electronic signature	An electronic signature which meets the requirements: - it is uniquely linked to the holder; - it is capable of identifying the holder; - it is created using electronic signature creation data that the holder can, with a high level of confidence, use under his sole control; and - it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable
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 seal	Electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person
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;

Certificate for website authentication	Attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
Creator of a seal	Legal person who creates an electronic seal
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 seal creation data	Unique data, which is used by the creator of the electronic seal to create an electronic seal
Electronic seal creation device	Configured software or hardware used to create an electronic seal
Electronic seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity
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;
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**
Policy	Policy for Providing Qualified Certification Services for Qualified Electronic Signature Certificate; Policy for Providing Qualified Certification

	Services for Qualified Electronic Seal Certificate; Policy for Providing Qualified Certification Services for Qualified Website Authentication Certificate; Policy for Providing Qualified Time Stamp Services. Policy for Providing Qualified Certification Services for Advanced Electronic Signature Certificate; Policy for Providing Qualified Certification Services for Advanced Electronic Seal Certificate;
PSD2 Directive	DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
Qualified certificate for electronic seal	A certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III, Regulation EU 910/2014
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 certificate for website authentication	A certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV, Regulation EU 910/2014
Qualified electronic seal creation device	An electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II, Regulation EU 910/2014
Qualified electronic seal	An advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal
Qualified electronic signature creation device (QSCD)	An electronic signature creation device that meets the requirements laid down in Annex II, Regulation EU 910/2014
Qulified validation service	The validation service is provided by a qualified certification service provider, in accordance with Regulation 910/2014 (Articles

	32, 33 and 40)
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
PSD2	Payment Service Directive 2
PSP	Payment Service Provider
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider issuing Card-based payment instruments
PSP_AI	Payment Initiation Service Provider
RA	Registration Authority

RSA	Rivest-Shamir-Adelman – Cryptographic algorithm for signature generation
SSCD	Secure Signature Creation Device
RQSCD	Remote Qualified Electronic Signature Creation Device
QSCD	Qualified Signature Creation Device
SHA	Secure Hash Algorithm – Hash Algorithm for hash identifier extraction
SSL	Secure Socket Layer – Secure data transmission channel
URL	Uniform Resource Locator

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

The published versions and updated editions of 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;
- Price-list/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 also keeps and publishes in the electronic register a separate list of suspended or terminated Qualified Electronic Signatures, Qualified Electronic Seal Certificates and Website Authentication Certificates.

2.2. Publishing certificate information

The issued certificates are published in the Certificate Register promptly after being signed by the Certification Authority of the Provider.

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

2.4.1. Public access to the register

Proveder’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.

2.4.2. Access control in keeping the directory

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 Signatures, Qualified Electronic Seals and Website 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. Naming

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

The "Subject" field on the certificate contains the name of the Holder/Creator of a Seal.

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

3.1.1. Name types

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

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

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

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

3.1.2. Pseudonyms

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

3.1.3. Rules for interpreting different forms of names

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

For identification of the Holder – a natural person, the following data is included in the name attribute on the certificate (CommonName) of (x509 Subject DN):

- First name, middle name and surname of natural person

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

- Organization name of legal person

The full name of the organization as it appears on its registration document

In Qualified Certificates of legal entities, the unique name (DN) necessarily contains information about the Legal Person Holder/Creator of a Seal.

3.1.4. Uniqueness of the names

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

The uniqueness of the issued certificates is ensured by combinations of the name of the Holder / Creator, the type of the certificate, the issuer, the unique number in the Provider's register and the period of validity. The Holder/Creator may have more than one valid certificate issued.

3.1.5. Recognition, authenticity and role of trademarks

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

Holders of rights to such names or marks, etc., prove such rights in the registration procedure by presenting the relevant official documents to the Registration Authority of the Provider.

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

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

The Provider shall not include any graphic reserved symbols, logos or

other graphic materials subject to copyright in the certificates issued by the Provider.

3.2. Initial identification and identity validation

For initial identification and authentication of the Holder/Creator of the Seal of a qualified certificate requested to be issued, the Provider performs the following checks for:

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

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

3.2.1. 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 Authentication Policies for a certain type of certificate.

When a request for issuing a qualified electronic certificate is submitted, the verification/check of the holding/possession of the private key is performed by the Registration Authority by means of a check of the electronic signature with which the request for the issuance of a certificate in the PKCS#10 format is 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/Creator of a Seal 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 (smart card) of the private key corresponding to the public key submitted to be included in the certificate.

The Provider, on assignment by the Holder/Creator along with issuance ot the Cloud certificate for a qualified electronic signature/seal provides him with a service for generation and secure storage of a public and private key pair from asymmetric cryptosystems through the InfoNotary's Remote Qualified Signal Device (RQSCD). The RQSCD is managed by the Provider on behalf of the Holder/Creator of a seal. The data for access to the RQSCD and for remote activation of the private key for creating a remote electronic signature/seal are solely under the control of the Holder/Creator of a seal. Prior to issuance of the certificate, the Holder/Creator activates the private key in the RQSCD device by means of his personal data for remote activation (personal code), which checks the holding of the private key.

3.2.2. 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 verification policy or the provisions and requirements of applicable laws.

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 Person:

- 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 a brand name, trademark, domain etc.;
- contact and billing information.

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

For legal entity, which is PSD payment service provider, the following specific information is verified:

- role/roles of the Payment Service Provider (PSP);
- authorization number of PSP issued by National Competent Authority;
- name of National Competent Authority authorized the PSP.

The legal representative of the legal person, respectively the authorized representative of the Seal Creator, personally presents 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.

3.2.3. 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 or Creator, 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/Creator, 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/Creator or the authorized representative;
- contact and billing information.

The Holder/Creator or authorized representative of the Holder/Creator personally submits to the Registration Authority the following documents:

- a valid identification card: ID card or passport;
- notarized power of attorney for empowerment of the Holder/Representative of a Legal Person or an authorized representative;
- 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.

The procedure for verification and confirmation the natural person's identity is carried out at a Registration Authority's office in a personal presence of the natural person.

The Registration Authority may remotely verify the identity of the natural person through secure video identification, electronic identification, a qualified certificate of qualified electronic signature and other legal means of secure remote identification, where the data provided by individuals can be further verified using special methods of comparison and confirmation, with the same data downloaded from the corresponding State registers, maintained by a primary data administrators.

The person who is legal representative of a legal entity, respectively its authorized representative when requesting the issuance of a qualified electronic signature may use the procedure for remote verification of the identity of the natural person.

3.2.4. Unconfirmed information

In some cases the Provider may include in the issued certificate unconfirmed information about the Holder/Creator of a Seal, 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.

3.3. Identity validation and authentication in request for replacement of keys in a certificate

Not supported by the Provider.

3.4. Identity validation and authentification of a certificate revocation request

The validity of a certificate is revoked by the Certification Authority of the Provider after the Registration Authority initiates the termination in accordance with the provisions of paragraph 4.9.3 of this document.

The Registration Authority requests termination to the Provider after receiving a request for termination by the Holder/Creator of a Seal and performing identity validation and authentication of the applicants and their confirmation at the Registration Authority's office or remotely electronically.

The Holder/Creator or the authorized representative of the Holder, who has submitted a request for terminating a certificate, personally presents to the Registration Authority the following documents:

- a valid identification card: ID card or passport;
- notarized power of attorney for empowering the Representative to represent the Holder/Creator of a Seal 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.

3.5. Identity validation and authentification of a certificate suspension request

An application for suspension of a certificate may be submitted to the Provider in accordance with the conditions and order provided in 4.9.12 of this document.

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/Creator of the seal;
- 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 in the order of cl. 4.11 and after a resumption initiation by the Registration Authority.

The Registration Authority performs identity validation and authentication of the Holder/Creator of the seal when he has submitted in person or through an authorized representative a signed request for resumption of a certificate at the registration authority's office or remotely electronically.

The Holder/Creator 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/Creator of a Seal 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

Holder/Creator, Registration Authority and other participants in the certification infrastructure of the Provider shall inform him 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 for the issuance of a certificate and are required to provide to the Certification Authority 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 CPS of the Provider.

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

4.1.2. Process of applying a certificate issuance

The request for the issuance of a certificate has to contain the following data:

- information individualizing the Holder and the empowering legal entity if such information is to be provided;

- information individualizing the Creator of a Seal;
- the public key corresponding to the private key from the pair of cryptographic keys;
- 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 one included in the document.

Depending on the certification policy of the different types of certificates issued by the Provider, it may be necessary to include additional information in the application for a Certificate.

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 applying for issuing a Cloud electronic signature/seal certificate the Provider, on assignment by the Holder/Creator, 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 is activated by the Holder / Creator of the seal by 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 Registration Authority of the Provider 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 Applicant, generates a cryptographic key pair, uses a secure signature/seal cration device (QSCD) and provides them to the Holder/Creator of a seal 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 / Creator of the seal 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 /Creator of a seal 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 submitting a request a certificate

4.2.1. Performing the functions of identifinaction and authentification

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 paragraph 3.2 of this document, based on the received application for issuance of the certificate and the presented documents and in the personal presence of the Applicant - the Holder or the Creator of the seal or a person authorized by him, the Registration Authority verifies and confirms to the Certification Authority:

- the identity of the Holder/Creator of the seal or his authorized representative;
- the representative power of the Holder and the Representative Authorized by the Holder.

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.

4.2.2. Granting or denying certificate applications

Before confirming the application for a certificate, the Registration

Authority of the Provider carries out the necessary checks according to the requirements of item 3.2 of this document:

- verifies and confirms the identity of the Applicant, the Holder/Creator or the person representing it on the basis of documents provided by them;
- verifies and confirms the representative power of the Holder and the person authorized by the Holder to represent 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 correctness of the received or generated signed electronic application (in PKCS#10 format) for issuance of a certificate;
- provides the Holder/Creator of a seal with the information that is confirmed and will be included in the issued certificate for approval of its content;
- confirms the Holder's/Creator's of a seal acceptance of the conditions of this CPS and the signing of a Qualified Certification Services Agreement.
- collects by hand a certified copy dated and signed by the Applicant of the documents on the basis of which the identity of the Holder/Creator of a Seal and the authorization of the Holder and the power of the Representative.

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 request for issuance originates from the Holder/Creator of the seal or from a person duly empowered by him;
- the information regarding the Holder and the Signatory/Creator, provided to be included 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, and
- the private key is in the possession of the Holder.
- the Holder/Creator of the seal 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 delays the application for issuance of a certificate.

The Registration Authority immediately notifies the Applicant and indicates the reason for the denial.

Applicants whose application for issuance of a certificate has been denied may apply for the issuance of a certificate again.

The Registration Authority completes and stores the documents provided by the Holder/Creator and 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/Creator 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/Creator of a Seal have the permanent obligation to observe the correctness of the presented information and to inform the Provider of any changes that have become effective after the issuance of the certificate.

4.2.3. Term for processing certificate applications

The verification and confirmation of the information provided in the application for the issuance of a certificate are processed within a reasonable period of time, and within of 5 working days from the date of acceptance of the application and receiving the necessary documents by the Applicant. The Provider issues the certificates immediately after confirmation of the request for issuance by the Registration Authority.

4.3. Issuance of a certificate

4.3.1. Actions of the Certification Authority when issuing a Certificate

The Certification Authority of the Provider issues the certificate on the basis of a request for issuance received by the Registration Authority.

The request for issuance of a certificate by the Registration Authority

guarantees the confirmation of the validity of the Applicant's application, the validity of the data contained therein and is signed by an operator of the Registration Authority who performed the cheks.

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).

4.3.2. Notifying the Holder/Creator of the seal by the Certification Authority of issuance and delivery of the certificate

The Provider promptly notifies the Holder/Creator of a Seal of the Qualified Certificate of the issuance of a qualified certificate by sending an email to the Holder/Creator of a Seal.

After issuing the certificate, the Provider delivers it to the Holder/Creator of a Seal:

- 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 / Creator of the seal 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 / Creator of the seal or the person authorized by him.

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

It is stored by the Provider on assignment by the Holder/Creator in the Infonotary's RQSCD.

4.4. Accepting and publishing the Certificate

4.4.1. Accepting the Certificate

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

The Holder/Creator of the seal 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/Creator without signing a protocol or doing an electronic confirmation, if the Holder/Creator 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.

4.4.2. Publishing the certificate by the Certification Authority

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

4.5. Data secrecy of qualified trust services and certificates usage

4.5.1. Data secrecy

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

The Holder/Creator 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/Creator 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 / Creator of the seal 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.

4.5.2. 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.

4.6. Certificate Renewal

4.6.1. Conditions for certificate renewal

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

Certificate renewal – the issuance of a certificate with a renewed term of validity without any change to the data included in it and to the respective pair of keys, is a service supported by the Provider on conditions and requirements depending on the type of the certificate and its application.

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.

A certificate issued by the Provider may be renewed only if the certification policy under which it is issued allows it and 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, but up to a total of 3 years validity period.

4.6.2. Who can apply for renewal request

The Holder or the Signatory/Creator or authorized by him person entered in the valid certificate may submit a request for renewal at least 10 (ten) days prior to the expiry of the term of validity of the certificate.

4.6.3. Procedure for submitting a renewal request

The Holder/Creator 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.

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

The Registration Authority of the Provider may require that the Applicant provide updated documents evidencing the truthfulness and correctness of the information included in the certificate as of the time of submitting the request for renewal.

The Applicant declares that the information provided at the initial issuance and the information included in the certificate is true, correct and unchanged to date.

Before granting the submitted certificate renewal request, the Registration Authority of the Provider carries out the necessary checks and validations in compliance with cl. 3.2. and 4.2.

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/Creator or a person duly empowered by him/her;
- the information concerning the Holder and the Signatory/Creator included in the certificate is correct, true and updated;
- the private key is in the possession of the Holder;
- the certificate whose renewal is requested is valid.

If the process of confirming the certificate renewal request is completed unsuccessfully, the Registration Authority delays the certificate renewal request.

The Registration Authority immediately notifies the Applicant and indicate the reason for the denial.

Applicants whose application for issuance of a certificate has been denied may apply for the issuance of a certificate again.

The Registration Authority completes and stores the documents provided by the Holder/Creator and 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 requests for renewal of the certificates are processed within a reasonable time and the Provider issues the certificates within 5 working days from the date of

acceptance of the documents.

The Certification Authority of the Provider issues the new certificate on the basis of a request for renewal received from the Registration Authority.

The request for renewal of a certificate by the Registration Authority guarantees the validity of the request submitted by the Applicant, the validity of the information contained in it and has been 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).

4.6.4. Notifying the Holder by the Certification Authority of issuance and delivery of the new certificate

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

After the certificate is issued, the Provider delivers it to the Holder and the Creator respectively:

- 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 / Creator of the seal 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 / Creator of the seal or the person authorized by him.

4.6.5. Acceptance of the renewed certificate

The Provider shall issue the certificate in accordance with the consent of the Holder/Creator of the seal.

The Holder/Creator of the seal 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/Creator 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.

4.6.6. Issuance and publishing the renewed certificate by the Certification Authority

The provider publishes the renewed certificate in the Certificates Register immediately.

4.7. Key replacement in certificate

Not supported by the Provider.

4.8. Modification of a certificate

Not supported by the Provider.

4.9. Terminating a certificate

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

4.9.1. Conditions for terminating a certificate

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

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

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

- death or when the Holder is under judicial disability;
- termination of the legal entity when the certificate is issued with an entry of a Holder-Legal Person;
- 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 Person;
- finding out that the certificate was issued on the basis of false information.

The Provider takes immediate actions on the termination of the certificate validity when there is justification for doing so.

The Certification Authority of the Provider revokes the validity of certificates issued by him.

The Provider immediately notifies the Holder/Creator of the circumstances regarding the validity or reliability of the certificate issued.

4.9.2. Who can ask a certificate termination

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

4.9.3. Termination request procedure

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

- a written request for termination of a certificate by the Holder, respectively the Creator or autorized by him person to the Provider to be made;
- the Registration Authority to verify the identity and the representative power of the Holder, respectively the Creator or autorized by him person.

The termination request is submitted personally by the Holder/Creator 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 p3.4.

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

The certificate termination request from the Registration Authority guarantees the validity confirmation of the application made by the Applicant, the validity of the information contained therein and it 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 List of the suspended and revoked certificates and updates publicly the available electronic certificate directory.

After terminating the certificate, the Provider notifies the Holder/Creator 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.

4.9.4. Grace period for serving the termination request

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.

4.9.5. 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 ckeck of the status of a certificate, the Provider shall not be held responsible for any ensuing damage to the Relying Party.

4.9.6. 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.

4.9.7. Maximum delay of publishing the Certificate Revocation List

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

4.9.8. Option for certificate status check in real time (OCSP)

The Provider offers the service of checking the status of certificates issued by him in real time through an OCSP protocol.

4.9.9. Requirements for using OCSP

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.

4.10. Suspension of a Certificate

4.10.1. 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/Creator of circumstances concerning the validity or trustworthiness of the certificate issued to him.

For the period of suspension the certificate is deemed invalid.

4.10.2. Who can request suspension

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

- by request of the Holder/Creator or person authorized by him;
- by request of a person for whom it is apparent from the circumstances that he or she may be aware of security violation of the private key or other circumstances;

- by order of the Supervisory authority in case of immediate risk of the interests of third parties or in case of sufficient evidence of violation of the law.

4.10.3. 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, respectively the Creator or authorized by him person 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, Creator or person duly authorized by them 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.

4.10.4. Limitation of the certificate suspension term

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.

4.10.5. Resuming a suspended certificate

The Provider resumes the validity of a suspended certificate:

- when the term for suspension expires (48 hours);
- when the grounds and circumstances for the suspension no longer exist;
- upon the request of the Holder/Creator or authorized by him person , once the Provider or the Supervisory Authority is certain that he/she has found out the reason for the suspension and that the request for resumption is made as a result of this finding.

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

4.11. Certificate Resumption Procedure

4.11.1. Resumption upon the request of the Holder/Creator

When the resumption is made upon the request of the Holder/Creator, the Registration Authority of the Provider shall verify the request and validate the identity of the Holder in accordance with cl.3.2. After receiving a confirmation of a verified request for resuming and of an identity validation from the Registration Authority of the Provider, the Certification Authority shall remove the suspended certificate from the List of suspended and revoked certificates, and publishes it.

4.11.2. Resumption by order of the Supervisory Authority

The Certification Authority of the Provider resumes the validity of the certificate and removes it from the Certificate Revocation 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 for resuming a certificate which has been suspended, on account of an immediate threat to the interests of third parties or sufficient evidence of violation of the law.

4.11.3. Resumption after the end of the suspension term

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 Certificate Revocation List, unless the Holder/Creator and/or the Supervisory

Authority do not request an extension of the suspension term.

4.12. Termination of the agreement for qualified trust services

The Provider's Qualified Trust Services agreement with the Subscriber is terminated if the certificates issued on it are terminated, expired and on other grounds specified in the agreement.

4.13. Key recovery and Key escrow

Not supported by the Provider.

5. EQUIPMENT, PROCEDURE AND MANAGEMENT CONTROL

5.1. Physical control

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

The infrastructure of the Certification Authority of the Provider is logically and physically separated and is not used by any other departments or organizations of the Provider.

5.1.1. Layout and design of the premises

The premises in which the critical components of the system are located are specially designed, constructed and equipped to store objects and information in conditions of strict admission and access control.

5.1.2. Physical access

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

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

Only the authorized members of the Provider's personnel, who strictly

adhere to and follow the established internal procedures for identification, verification and documenting access, have access to certain premises and information resources of the Provider.

5.1.3. Power supply and ambient conditions

The Provider makes sure that the power supply for the whole equipment of the infrastructure of the Provider is protected from power cuts by additional/emergency power supply provided by backed-up sources.

The Provider adheres to all the requirements of the manufacturers of his technical equipment regarding the conditions for its storage and operation and provides means of monitoring and maintaining the necessary ambient conditions.

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

5.1.4. Floods

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

5.1.5. Fire alarm and protection

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

5.1.6. Data storage devices

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

5.1.7. Taking a technical components out of use and operation

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

5.1.8. Duplicate components

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

5.2. Procedural control

The Provider pursues in his activity such a policy of management and human resource management as to guarantee reliability and trustworthiness in fulfilling all obligations assumed by him as well as the competence to perform the activity of Qualified Provider of Certification Services in accordance with the requirements of Regulation (EU) 910/2014 and the applicable Bulgarian legislation.

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

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

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

For certain activities, the Provider may also use outsiders.

5.2.1. Positions and functions

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

5.2.2. Number of employees involved in a certain task

The assigned tasks connected with the functioning of the Certification Authority of the Provider are performed by at least two staff members.

5.2.3. Identification and authentication of each position

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

5.2.4. Requirements for division of responsibilities for separate functions

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

5.3. Staff control, qualification and training

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

- security technologies, cryptography, public key infrastructure (PKI);
- technical standards for security assessment;
- information systems;
- large databases administration;
- network security;
- 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.

5.3.1. Requirements to independent suppliers

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

5.3.2. Documentation provided to the staff

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

5.4. Procedures for the 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.

5.4.1. Frequency of generating records

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.

5.4.2. Record storage period

The records and logs are stored for a period of 10 (ten) years.

5.4.3. Record security and protection

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.

5.4.4. Procedure for generating back-up copies of the records

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. 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.

5.5.1. Types of archives

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 electronic archive.

5.5.2. Storage period

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

5.5.3. Archive protection and security

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.

5.5.4. Archive restoring procedures

The Provider restores data from the maintained archive, if necessary.

5.5.5. Requirements for verifying the date and time of records

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.

5.5.6. Archive storage

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.

5.5.7. Procedures for acquiring and verifying information from an archive

Archive information that is public is published and is available in the Public Registry of the Provider in a readable form.

5.6. Modification of a certificate key

Not supported by the Provider.

5.7. 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.

5.7.1. 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.

5.7.2. Incidents related to hardware, software, and/or data failures

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.

5.8. Procedures for terminating the activity of the Provider

5.8.1. Termination of activity

The activity of the Provider is terminated in accordance with the applicable national legislation.

Upon termination of its activities, the Provider shall notify the Supervisory Authority of its intentions not later than 4 months before the date of termination and whether it will transfer its activity to another Provider.

The Provider notifies the Supervisory Authority if there is a claim for declaring the company insolvent, for declaring the company inoperative, or there is some other claim for dissolving or starting liquidation procedure.

The Provider shall make every effort and care to continue the validity of the certificates he has issued by transferring it to an operative qualified certification services provider.

The Provider shall notify the Supervisory Authority and the consumer in written form that the Provider's activities are undertaken by another qualified provider no later than the time of termination.

A written notice is also published on the Provider's web site and also

contains information on the name and contact details of the provider-successor.

The Provider notifies its users about the conditions of maintenance of the transferred certificates to the provider-successor.

The Provider duly transfers all documentation related to its activities to the provider-successor together with all repositories and all certificates issued (valid, terminated and suspended).

In case that the Provider fails to transfer his activity to another qualified provider, he shall suspend the validity of all certifying authorities, all issued end user certificates by him and and stores all documentation relating to the activity all records and all issued certificates (valid, suspended) for a period of 10 years.

If a Registration Authority, as an external organization of the Provider, decides to discontinue the representation of the Provider in relation to the provided certification services, it is obliged to:

- inform the Provider of its intention to terminate the activity. The notification shall be made within 3 months before the agreed date of termination;
- transfer all documentation related to customer service, including archive and audit data to the Provider.

5.8.2. Transfering the activity of another qualified provider of qualified trust services

To ensure continuity of providing qualified trust services to consumers, the Provider may transfer the activities to another qualified trust service provider. In such case, the Provider is obliged to:

- notify the Supervisory Authority of its intention, but no later than 4 months before the date of termination and transfer of activities;
- make all efforts and care to maintain the issued certificates;
- notify the Supervisory Authority and users in written form that its activity has been taken over by another qualified service provider;
- inform the users about the conditions for the maintenance of certificates transferred to the receiving provider;
- change the status of the operational certificates of the Certification Authority and duly transmit to the receiving provider all documentation related to the activities together with all the archives and all issued certificates (valid, suspended and terminated);
- perform the necessary actions to transfer the information maintenance obligations to the receiving provider;

- transfer the management of end-user certificates already issued to the receiving provider;
- the receiving provider assumes the rights and obligations of the Provider with suspended activities and continues to manage the active certificates until their expiration.

5.8.3. Withdrawal of the qualified status of the Provider

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) 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/Creator technical devices (software, smart cards and other cryptographic devices) that comply with the level of security requirements and regulations, approved under Regulation (EC) 910/2014 and national legislation of Regulation (EU) 910/2014.

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

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

6.1.1. Generating key pair

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

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

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

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

"INFONOTARY" PLC Board of Directors.

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

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

- the management of the hardware module through secret data accessible only to authorized persons and the division of this data between at least two of these 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 and the division of this data between at least two of these authorized persons;

6.1.1.2. Generating key pair for Subscriber

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

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

The Provider is generated the key pair for a cloud qualified electronic signature / seal 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 pair of keys of the Holder or the Creator respectively, 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/Creator or 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/Creator of the seal.

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

This procedure is performed only by the Holder, respectively the Creator, who generates the key pair and delivers the public key to the Provider for the purposes of the certification process.
The electronic certificate issuance request through which the public key is delivered to the Provider should be in the PKCS#10 file and in DER format.
The Holder/The Creator may provide the electronic request:

- personally in the Registration Authority or
- by electronic means and 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 or Creator respectively must be at least 2048 bits long for the RSA algorithms.

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

6.2.1. Cryptographic Module Standards

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

The hardware cryptographic modules used by the Provider for storing the private keys of the Certification Authority are certified for a high level of security and reliability FIPS 140-2, Level 3, FIPS 140-1 Level 2, CC EAL 4+ or higher.

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

6.2.2. Storage and usage of a private key control

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

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

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

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

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

6.2.3. Storage of Private keys

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

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

6.2.4. Private keys archiving

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

Keys archiving is performed by authorized employees of the Provider.

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

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

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

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

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

6.2.6. Activation and Deactivation of Private Keys

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

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

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

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

6.2.7. Private Keys Destruction

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

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

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

6.3. Other aspects of managing the key pair

6.3.1. Public key archival

The Provider archives all of its public keys and stores them for a period

of 10 years after their expiration or termination.

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

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

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

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

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

6.4. Activation data

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

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

6.4.1. Generation and installing activation data

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

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

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

using the software provided with the device.

6.4.2. Activation data protection

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

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

6.5. Computer security control

6.5.1. Specific requirements for computer security

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

6.5.2. Computer security rating

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

6.6. Technical life cycle control

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

At all stages of the construction and operation of the systems, the procedures and rules described in internal documents of the Provider are strictly observed.

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

6.7. Network security control

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

6.8. 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.

6.8.1. 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

6.8.2. Independent source for accurate time

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

- NTPv2 (RFC 1119)
- NTPv3 (RFC 1305)
- NTPv4 (IETF Draft Standard)

- SNTP (RFC 2030)
- Daytime Protocol (RFC876)
- Time Protocol (RFC 868)
- SNMPv1 (RFC 1157), SNMPv3 (RFC 3411-3415)

The system is synchronized via GPS, synchronization from other NTP servers or Dial-up connections.

All data for accurate time transmitted from TimeSinhronisator to TimeStamp server are encrypted by the synchronizer itself and protected from modification and compromise.

6.9. Qualified Validation Service

InfoNotary provides a qualified validation service of a qualified certificate, a qualified electronic signature and a validated electronic seal - InfoNotary Qualofied Validation Service.

The qualified validation service of a qualified electronic signature / seal allows for a reliable verification of its validity, as well as the validity of the issued certificates, including confirmation of their qualified status.

The Qualified Validation Service allows you to validate the following signature formats and profiles:

Format/Profile	BASELINE_B	BASELINE_T	BASELINE_LT	BASELINE_LTA
CAdES	√	√	√	√
XAdES	√	√	√	√
PAdES	√	√	√	√
ASiCS/ ASiCE	√	√	√	√

All certificates and related certification chains are validated against the European Trust List(EU MS TSL- https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home).

The validation results presented in a report that contains the status - VALID (TOTAL-PASSED), INVALID (TDOTAL-FAILED) or UNDEFINED (INDETERMINATE). The report is stamped with a advanced seal supported by qualified certificate of Infonotary, which guarantees the integrity and accuracy of the data in the report.

The Provider's validation system providing the service is developed and the validation of qualified electronic signatures / seals and certificates is carried

out in accordance with eIDAS Regulation and ETSI standards - ETSI TS 119 441; ETSI TS 119 442; ETSI TS 119 101; ETSI EN 319 102-1; ETSI TS 119 102; ETSI TS 319 172-1.

The Provider's validation system providing the validation service is under a regime of high control of physical and technological access by authorized employees.

6.9.1. Provision of the Qualified Validation Service

The validation service is available at https://www.infonotary.com/validate.

The Provider provides the service through a web client (Signature Validation Application - SVA), which uses a web browser and a secure communication channel / secure session (via HTTPS protocol/ web site authentication certificate) to connect to the validation server. After accessing the service, the User (the relaying party) uploads an electronically signed / sealed file or certificate that he wishes to verify, selects the parameters of the request and sends the request to the validation server.

The service can also be used in automatic mode, as the conditions are settled in a contract between the Provider and the Relying Party.

The validation process goes through the following steps according to ETSI TS 319 172-1:

Step 1: The SVA / web client generates and sends a validation request that contains the signed / sealed document or sends a document and signature;

Step 2: The validation server validates the electronic signature / seal using the Provider's internal services (CRL, OCSP, TSA) or external services of other providers or external sources of certificates (European Trusted List).

Step 3: The validation server generates and sends a validation report. The report is sealed with a advanced seal supported by qualified certificate of Infonotary.

Step 4: The web client visualizes the validation report in pdf format and it can be saved, locally on the user's computer, or printed.

Electronic signature / seal validation requests and the responses to these requests use client-server communication. The validation protocol is in accordance with ETSI EN 119 442.

7. Profiles

7.1. Qualified certificate profile

Qualified certificates issued by the Provider in line with the certification policies and current practice comply with the requirements of Regulation (EU) 910/2014.

The following standards are implemented and used in qualified electronic signature certificates issued by the Provider:

- qualified end-user certificates profiles and List of suspended and revoked certificates (CRL) correspond to the format included in ITU-T X.509 v.3 standard.
- OCSP profile complies with RFC 6960, and
- the qualified electronic TimeStamp profile complies with RFC 3161.

7.1.1. Version number

The Provider issues certificates in X.509 v.3 format.

The certificate version number is entered in the certificate itself.

7.1.2. Certificate Extensions

7.1.2.1. Mandatory Extensions

"Basic Constrains" Attribute

The attribute specifies the type of certificate holder - Certification Authority or end user. The attribute is "Critical".

"Key Usage" Attribute

It defines the constraints in certificate usage according to the key use designation. The attribute is "Critical".

The attribute is used to limit the key use according to the following possible usage:

- Digital Signature – for authentification;

- Non-repudiation – to prove the electronic signature use;
- Key encipherment – for key encipherment;
- Data encipherment – for data encipherment;
- Certificate Signing – used only by the Certification Authority of the Provider;
- CRL Signing – for signing CRLs, used only by the Certification Authority.

"Extended Key Usage" Attribute

The attribute is used to specify the applications in which the key may be used – protection of electronic correspondence, electronic authentication etc.

"Authority Key Identifier" Attribute

The Attribute contains SHA1 of the DER-encrypted Issuer's public key.

"Subject Key Identifier" Attribute

The Attribute contains SHA1 of the DER-encrypted public key.

"CRL Distribution Points" Attribute

The Attribute contains a link to the List of Suspended and Revoked Certificates maintained by the Provider.

"Authority Info Access" Attribute

The Attribute contains a link to the OCSP service maintained by the Provider and submitting certificate status information through OCSP protocol.

"Qualified Certificate Statement" Attribute

The attribute is mandatory for Qualified Electronic Signature Certificates, Qualified Electronic Seal and Website Authenticity that the Provider issues, and contains information whether the certificate was issued as qualified and whether the private key was generated and stored on qualified signature creation device (QSCD).

"Certificate Policy" Attribute

The attribute specifies the certificate issuance policies of the Provider. The attribute contains identifier (OID) of the respective certification policy according to the qualified certificate type.

Name	InfoNotary Policy Identifier	ETSI Policy Identifier
InfoNotary Qualified Natural Person Signature CP	1.3.6.1.4.1.22144.3.1.1	0.4.0.194112.1.2 (QCP-n-qscd)
InfoNotary Qualified Delegated Signature CP	1.3.6.1.4.1.22144.3.1.2	0.4.0.194112.1.2 (QCP-n-qscd)
InfoNotary Qualified Legal Person Seal CP	1.3.6.1.4.1.22144.3.2.1	0.4.0.194112.1.3 (QCP-l-qscd)
InfoNotary Qualified Validated Domain CP	1.3.6.1.4.1.22144.3.3.1	0.4.0.194112.1.4 (QCP-w)
InfoNotary Qualified Organization Validated CP	1.3.6.1.4.1.22144.3.3.2	0.4.0.194112.1.4 (QCP-w)
InfoNotary Qualified PSD2 WA CP	1.3.6.1.4.1.22144.3.3.3	0.4.0.194112.1.4 (QCP-w)
InfoNotary Qualified Certificate for Natural Person AESignature CP	1.3.6.1.4.1.22144.3.6.1	0.4.0.194112.1.0 (QCP-n)
InfoNotary Qualified Certificate for Delegated AESignature CP	1.3.6.1.4.1.22144.3.6.2	0.4.0.194112.1.0 (QCP-n)
InfoNotary Qualified Certificate for Legal Person AESeal CP	1.3.6.1.4.1.22144.3.7.1	0.4.0.194112.1.1 (QCP-l)
InfoNotary Qualified Certificate for PSD2 AESeal CP	1.3.6.1.4.1.22144.3.7.2	0.4.0.194112.1.1 (QCP-l)

Qualified certificate policy identifiers included in qualified certificate profiles are:

Qualified policies

- QCP-n-qscd: Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2);
- QCP-l-qscd: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3);
- QCP-n: Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0);
- QCP-l: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal(1);

- QCP-w: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web(4);
- Natural Person Semantics: itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121) id-etsi-qcs-semantics-identifiers(1) id-etsi-qcs-semanticsId-Natural(1);
- Legal Person Semantics: itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121) id-etsi-qcs-semantics-identifiers(1) id-etsi-qcs-SemanticsId-Legal(2);
- QcCompliance: itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1);
- Secure Signature Creation Device (SSCD): itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) 4;
- id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
- id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
- id-etsi-qct-web (oid=0.4.0.1862.1.6.3)
- id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)
- id-etsi-psd2-qsStatement (oid=0.4.0.19495.2)
- id-etsi-sars-SigType 5

7.1.3. Electronic signature algorithm identifiers

The electronic signature algorithm identifier idenifies:

- Hash-function: sha256-with-RSA;
- Encryption algorithm: RSA.

7.1.4. Naming forms

See p. 3.1.3 from the document.

7.1.5. Name limitations

See p. 3.1.4 from the document.

7.2. Profile of the List of Suspended and Revoked Certificates (CRL)

7.2.1. Version number

Lists of suspended and revoked certificates that the Provider maintains in the Public Directory of Certificates are in the format X.509 v.2.

7.2.2. Attributes of the list and its certificates

7.2.2.1. Attributes of the list

7.2.2.1.1. Base x509 CRL attributes

Attribute	Value
Version	2 (0x01)
Publication date	Date and time of signing the CRL
Subsequent publication date	Date and time of signing the CRL+ 24 hours
Electronic signature algorithm on CRL	rsaWithSHA256
CRL issuer attributes *(x509 CRL Issuer DN)*	The CRL Issuer attributes match the attributes of the Holder of the signing certificate.

7.2.2.1.2. Additional attributed of the List:

Attribute	**OID**	**Value**
/AuthorityKeyIdentifier	2.5.29.35	"subjectKeyIdentifier" of the issuer's signing certificate
/cRLNumber	2.5.29.20	Number of the CRL published in the Public Directory of Provider; 20-byte number

7.2.2.1.3. Attributes of the Certificates included in the list:

Attribute	**Value**
Serial number	The unique certificate number in the Provider's register
Date of suspension/termination	Date, hour and minute of suspension/termination of the certificate

Reason for suspension/termination	keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, unspecified

Meaning of the codes for indicating the reason for suspemcion and termination a certificate:

- Key Compromise – a compromised private key corresponding to the public key included in the content of the Qualified Certificate;
- CA Compromise – a compromised private key of the Certification Authority;
- Affiliation Changed – changed status of the Holder - change in the legal person or change in the representative power, withdrawal of the representative power with respect to the legal person;
- Superseded – a certificate is replaced by another certificate;
- Cessation of Operation – expired validity;
- Certificate Hold – the validity of a certificate is suspended;
- Unspecified – no reason listed for terminating the certificate

7.3. OCSP Profile

7.3.1. OCSP Request Profile

7.3.1.1. Request Attributes

Attribute	Value
Version	1 (0x00)
Applicant	Ignored
Certificate Identifier List	According to RFC 6960 (see 1.2)
Request extensions	Ignored

7.3.1.2. Certificate Identifier

Attribute	Value
Cryptographic checksum (CCS) algorithm	SHA-1
Issuer	SHA-1 from the Issuer's DER-encoded DN
CCS of the Issuer's key	SHA-1 from the Issuer's DER-encoded subjectPublcKeyInfo (excluding T and L)
Serial number	Unique in the Provider's register; 8-byte number

7.3.2. Profile of OCSP Response

7.3.2.1. Common attributes

Attribute	Value
Status	successfull – according to RFC 6960 malformedRequest – according to RFC 6960 internalError – *not used* tryLater – *not used* sigRequired – *not used* unauthorized – *not used*
Response type	id-pkix-ocsp-basic (1.3.6.1.5.5.7.48.1.1)
Response (see 2.2)	According to RFC 6960

7.3.2.2. Response attributes according to id-pkix-ocsp-basic (1.3.6.1.5.5.7.48.1.1)

Attribute	Value
Response data (see 7.3.3)	According to RFC 6960
An electronic signature algorithm on the answer	FIPS-186 DSS;
Electronic signature	Accoding to RFC 6960
List of Issuer's certificates	does not apply

7.3.3. OCSP Data Response

Attribute	Value
Version	1 (0x00)
OCSP Responder Identificator	DN of the signing certificate
Date of publishing	Date hour and minute of signing the response
Individual responses (see 2.4)	According to RFC 6960
Extensions	Does not apply

7.3.4. Individual OCSP responses

Attribute	Value
Certificate identifier	According to RFC 6960 (see 7.3.1.1.1)
Status	good – according to RFC 6960 revoked – according to RFC 6960 unknown – according to RFC 6960
Date of publishing	Date hour and minute of signing the CRL
Date of next publication	Date and hour of signing the CRL+ 24 hours
Extensions	Does not apply

7.4. TimeStamp Profile

7.4.1. 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

7.4.2. TimeStamp Response Profile

Attribute	Value

HTTP Content-Type	application/timestamp-reply	
Status:	granted	According to RFC 3161;
	grantedWithMods	According to RFC 3161 not used;
	rejection	According to RFC 3161;
	waiting	According to RFC 3161 not used;
	revocationWarning	According to RFC 3161 not used;
Errors:	BadAlgIdentifier; badRequest; badDataFormat timeNotAvailable unacceptedPolicy unacceptedExtension addInfoNotAvailable systemFailure	According to 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	

7.5. Validation Report

The results of the validation process are presented in a basic and detailed report in accordance with ETSI TS 119 102-1.

The basic report contains:

- Validation Policy;
- Status-indicators;
- Date and time of creation of the signature / seal;
- The format/ profile of the validated signature / seal;
- Name of the Holder / Creator of the signature / seal;
- Information about the signed / stamped document (name, number of signatures).

The validation status-idicators that SVA provides after validation of the specific format / profile of the signature / seal according to the Validation Policy is:

- TOTAL-PASSED - the checks of all cryptographic characteristics / parameters of the signature / seal are successful, as well as those in accordance with the Validation Policy;
- TOTAL-FAILED - the checks of all cryptographic characteristics / parameters of the signature / seal are unsuccessful, or the signature / seal is created after cancellation / termination of the qualified certificate or the format does not correspond to some basic formats;
- INDETERMINATE - the results of the individual / single checks do not allow the signature / seal to be assessed as TOTAL-PASSED or TOTAL-FAILED.

The detailed report includes complete information for cheks of all limitations, possible values and additional reporting data related to these values, according to the Validation Policy.

8. AUDITING AND CONTROL OF THE ACTIVITY

8.1. Regular or circumstantial audits

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.

For internal control purposes, the Board of Directors of INFONOTARY PLC appoints scheduled (routine) or unscheduled audits in the order and range according to the internal regulations of the Provider.

The Provider has constant control over the activities of the Registration Authorities and their local registration offices.

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.

8.2. Qualification of the auditors

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.

8.3. Relation between the auditor and the audited organization

The auditors must be independent, unrelated, directly or indirectly, and have no conflicting interests with the Provider.

The relations between the external auditors and the Provider are regulated by a written agreement (contract).

8.4. 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.

8.5. 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.

8.6. Announcing the results

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/Creator 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/Creator of a Seal, 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/Creator of the seal 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, respectively Creator, 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 confidential information

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

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

9.3.2. Information beyond the scope of the confidential information

The following objects and information are not treated as confidential:

- certificates published in the Provider's register;
- the data contained in the certificates;
- data on the status of the certificates published in the List of suspended and revoked certificates.
- all public documents published in the Provider's Documentary repository.

9.3.3. Obligation for confidential information protection

The Provider does not disclose and may not be required to disclose or disclose to relying parties any confidential information except when required under a special law to disclose such information 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/Creator of a Seal/Authorized Representative and Subscriber is for the sole purpose of issuing and maintaining Qualified Certificates or providing another qualified certification service.

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

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

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

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

The Provider shall inform in advance the Holder/Creator of a Seal/Authorized Representative and Subscriber of Qualified Certification

Services of the types of information it collects for them, how it is provided and stored and accessed to third parties.

The Holder/Creator of the seal, when signing the Agreement for qualified certification services and accepting the terms and conditions of the „Practice in providing qualified certification services" and of the Certification policies, agrees that the qualified certificate shall contain personal data that identifies him and which are avaiable to the third parties from the Register of the issued certificates. The Holder/Creator of the seal may restrict the public access to his certificate, published in 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/Creator and to any third party for damages caused by:

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

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/Creator of the seal to relying parties

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

- when creating the pair (public and private keys) the algorithm and devices for creation of electronic signature/seal does not meet the requirements of Regulation (EU) 910/2014;
- Does not strictly meet the security requirements specified by the Provider;
- 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/Creator 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/Creator of a Seal is responsible before the Provider if it has provided false data, or has skipped data relevant to the content or issuance of the certificate, and when it did not hold the private key corresponding to the public key specified in the certificate.

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

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 usage of Qualified Certificates by the Holder, Creator or Relying party.

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

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

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

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

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

The Provider is not responsible for the security, integrity and use of software products and hardware 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 responsible.

9.10. Term and Termination

9.10.1. Term

The Certification practice statement for qualified certification services 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 Practice is valid until a change or publication in the Document Repository and the Provider's Internet Portal of invalidity information occurs.

The term of a Qualified Certification Services Agreement is 1 year or another term agreed between the parties.

9.10.2. Termination and invalidity

The effect of the Certification Practice Statement for Qualified Certification Services shall be terminated upon termination of the Provider's activity.

In case any of the provisions of this Certification Practice Statement for Qualified Certification Services proves to be invalid, this will not entail any other clauses or parts of the Practice, 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.

The Certification Services Agreement shall terminate upon the termination of all Qualified Certificates issued on the basis of it, or in the presence of any other grounds for termination specified in the Certification Practice Statement for Qualified Certification Services.

9.10.3. Termination Effect

Upon termination of the Certification Practice Statement for Qualified Certification Services to the consumer, the provisions for the obligations of the Provider to maintain an archive of the documents and certificates in the volume and for the period described in the Practice.

9.11. Individual notification and communication between participants

All interested parties can make announcements to the Provider about the provisions of the Certification Practice Statement for Qualified Certification Services 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 Certification practice statement for qualified certification services

The Certification practice statement for qualified certification services can be changed 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 and и http://repository.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 regarding the Qualified Certification Services Agreement shall be settled by agreement between the parties through understanding and a spirit of goodwill, and if not possible otherwise, shall be settled by the competent Bulgarian court.

All complaints or claims by Subscribers must be addressed to the Provider in writing and sent to: 1000, 16 Ivan Vazov Str., or electronically signed at 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 Certification Practice Statement for Qualified Certification Services 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.