QUALIFIED CERTIFICATION
SERVICES PROVIDER
Tel.: 0700 14 220
support@mail.stampit.org www.stampit.org

Provision of qualified certification services by

Information Services JSC

QUALIFIED CERTIFICATION SERVICES

PRACTICE STATEMENT

OF INFORMATION SERVICES JSC (eIDAS-CPS)

Version: 5.3

Publication date: 07.06.2017

Last revision date: 12.01.2022

Contents

TERMS AND ABBREVIATIONS

Regulation (EU) No 910/2014	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.
Directive 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Certification service	Electronic service provided by Information Service AD for pay, consisting of: a) creation and validation of electronic signatures, electronic seals and electronic timestamps as well as certificates related to such services; b) creation and validation of website authentication certificates.
Qualified certification service	Certification service that meets the applicable requirements laid down in Regulation (EC) No. 910/2014.
Signatory	A natural person who creates 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
Advanced electronic signature	Electronic signature which meets the following requirements: a) it is uniquely linked to the signatory; b) it is capable of identifying the signatory; c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
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.
Electronic signature creation data	Unique data which is used by the signatory to create an electronic signature.
Certificate for electronic signature	an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person,
Qualified certificate for electronic signature (QCES)	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I to Regulation (EU) No. 910/2014;
Electronic signature creation device	Configured software or hardware used to create an electronic signature
Advanced electronic signature creation device	Electronic signature creation device that meets the requirements laid down in Annex II to Regulation (EU) No. 910/2014
Creator of a seal	A legal person who creates 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;

Advanced electronic seal	Electronic seal which meets the following requirements: a) it is uniquely linked to the creator of the seal; b) it is capable of identifying the creator of the seal; c) 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 d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
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
Electronic seal creation data	Unique data, which is used by the creator of the electronic seal to create an electronic seal.
Certificate for electronic seal	an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person
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 to Regulation (EU) No. 910/2014;
Electronic seal creation device	Configured software or hardware used to create an electronic seal
Advanced electronic seal creation device	Electronic seal creation device that meets the requirements laid down in Annex II to Regulation (EU) No. 910/2014
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;
Qualified electronic time stamp	Electronic time stamp which meets the following requirements: a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; b) it is based on an accurate time source linked to Coordinated Universal Time; and c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.
Electronic document	Any content stored in electronic form, in particular text or sound, visual or audio-visual recording
Website authentication certificate	Certificate that allows certification of the website authentication that relates it to the natural person or the legal person to whom the certificate has been issued.
Qualified website authentication certificate	A website authentication certificate that is issued by a qualified certification services provider and meets the requirements laid down in Annex IV to Regulation (EU) No. 910/2014;
Relying party	A natural or legal person that relies upon an electronic identification or a trust service
National law	The valid Bulgarian law
Supervisory authority	Supervisory authority in the meaning of article 17 of Regulation (EU) **№** 910/2014
IO JSC/ Provider/ Qualified trust service provider	Information Service AD in the capacity of qualified trust service provider that is granted the qualified status by a supervisory body.
Practice	Practice for provision of qualified certification services

	(Certification Practice Statement - CPS)
Policy	POLICY for provision of qualified certificates for qualified electronic signature and qualified electronic seal (eIDAS-CP-QES) POLICY for provision of time-stamping services (eIDAS-CP-TS) POLICY for provision of qualified certificates for advanced electronic signature and advanced electronic seal (eIDAS-CP-AES) POLICY for provision of qualified website authentication certificates (eIDAS-CP-SSL)
RA	Registration authority
CA	Certification authority
RSA Rivers-Shamir-Adelman	Cryptographic algorithm (asymmetric)
SHA2 Secure Hash Algorithm	Hash function
SHA256/RSA Signature algorithm	Algorithm for creation of qualified electronic signature by IO AD
SSCD	Secure signature creation device
URL Uniform Resource Locator	Locator of resource/web address
QCP-l-qscd	**Policy for qualified certificates issued to legal persons when the private key of the related certificates is generated on QSCD**
QCP-n-qscd	**Policy for qualified certificates issued to natural persons when the private key of the related certificates is generated on QSCD**
QSCD	**Qualified signature creation device**
NCP+	**Extended normalized certificate policy, which includes additional requirements for qualified certificates in compliance with Regulation (EU) No. 910/2014**
Certification Authority (CA)	**Certification authority**
Common Name (CN)	**public name**
Certificate Policy (CP)	**Policy for provision of qualified certificates for qualified electronic signature and qualified electronic seal**
Certification Practice Statement (CPS)	**Practice for provision of certification services**
Certificate Revocation List (CRL)	**List of suspended and terminated certificates**
Distinguished Name (DN)	**Distinguished name of a subject entered in the certificate**
Enhanced key usage	**Enhanced goals for key usage**
Federal Information Processing Standard (FIPS)	**Federal information processing standard**
Hardware Security Module	**Hardware cryptographic module**
Object Identifier (OID)	**Object identifier**
Public Key Cryptography Standards (PKCS)	**Series of standards for public key cryptography**
Public Key Infrastructure (PKI)	**Public key infrastructure**
Registration Authority (RA)	**Registration authority**

1. Introduction

Information Services JSC is a legal entity that is a commercial company registered in accordance with the Bulgarian law. The company has been registered in the Commercial Register with the Registry Agency under company number (EIK) 831641791. The company seat and registered address are located in the city of Sofia, Oborishte region, 2, Panayot Volov Str., contact details: +359 2 9420340, fax +359 2 943 6607 Website: https://www.is-bg.net.

Information services JSC is a provider of qualified certification services, which meet the requirements specified in Regulation (EU) № 910/2014 and the valid national law. Information Services JSC has implemented and applies in its business Integrated Management System, which is certified under the standards ISO/IEC 9001:2013, ISO/IEC 27001:2013 and ISO/IEC 20000-1:2011. Information Services JSC as provider of certification services uses the reserved trademark StampIT.

1.1 Overview of the qualified certification services practice statement (eIDAS-CPS)

The Qualified Certification Services Practice Statement, hereinafter referred to as CPS is a public statement of the practices of StampIT and of the general requirements for provision of qualified certification services by Information Services JSC.

The document contains the terms and conditions for issuing, suspension, revocation and resumption of the validity of qualified certificates and for issuing qualified electronic time-stamps within the hierarchy of StampIT. It lists the documents required for the provision of qualified services and the conditions under which the collected information is stored by StampIT. It also describes the security measures applied by the Provider upon provision of qualified certification services. The document also settles the rights, the duties and the responsibilities of the staff of the Provider involved in the provision of qualified certification services and of all third persons authorized by the Provider to perform functions connected with the provision of these services. It describes the rights, the duties and the responsibilities of the signatory of QES/ the creator of QESL and of the subscriber upon using the qualified certification services provided by Information Services JSC.

The document contains description of the following services provided by Information Services JSC:

- Issuing and management of qualified electronic signature certificates (QES): qualified certificates for qualified electronic signatures – QES (qualified) and qualified certificates for advanced electronic signatures – QES (advanced);

- Issuing and management of qualified electronic seal certificates (QESL): qualified certificates for qualified electronic seals – QESL (qualified) and qualified certificates for advanced electronic seals – QESL (advanced);
- Issuing and management of qualified website authentication certificates (QWA): qualified website authentication certificates - QWA (domain) and qualified website authentication certificates - QWA (organisation);
- Qualified time stamping service - issuing qualified electronic time stamps (QETS).

This CPS has been developed in compliance with Regulation (EU) № 910/2014 and is based on the requirements of the generally accepted and recognized international standards, practices and specifications:

- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 3628 - Policy Requirements for Time-Stamping Authorities;
- RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
- ETSI EN 319 401 Electronic Signatures and Infrastructures(ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 412 Certificate Profiles;
- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 422 Time-stamping protocol and electronic time-stamp profiles;
- ETSI TS 102 176-1 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms;
- ETSI TS 102 176-2 - Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices.

1.2 Document name, identification and management

The full name of this document is ‘‘Qualified Certification Services Practice Statement’’ of Information Services JSC (eidas-cps).

This CPS is publicly accessible in electronic form on address:

http://www.stampit.org/repository/

CPS is provided to each person upon request sent to email: support@mail.stampit.org

This document may be amended by Information Services JSC at any time and each change shall be entered in the new updated version of the document, which enters into force after its publication on website: http://www.stampit.org/repository/.

In respect of the Subscribers and third parties will be valid only the version applicable as at the time of using the services of Information Services JSC.

The new versions are developed by employees of Information Services JSC and are published after approval by the executive director of Information Services JSC.

CPS is connected with the following policies:

- POLICY for provision of qualified certificates for qualified electronic signature and qualified electronic seal (eIDAS-CP-QES)
- POLICY for provision of time-stamping services (eIDAS-CP-TS)
- POLICY for provision of qualified certificates for advanced electronic signature and advanced electronic seal (eIDAS-CP-AES)
- POLICY for provision of qualified website authentication certificates (eIDAS-CP-SSL)

CPS shall meet the general requirements of the certification policies indicated in standard ETSI EN 319 411-1: NCP for QCP-l; NCP for QCP-l-qscd; NCP for QCP-n.

The qualified certificates issued by StampIT contain identifiers of the policies for their issuing, which may be verified in PolicyInformation and CertificatePolicies.

To each policy on which basis are issued the qualified certificates by StampIT is assigned object identifier (OID - Object Identifier), with value as follows:

Values of object identifiers

	Policy Identifier

Information Services Plc.	1.3.6.1.4.1.11290
StampIT	1.3.6.1.4.1.11290.1
StampIT Primary Root CA	1.3.6.1.4.1.11290.1.1
StampIT Qualified CA	1.3.6.1.4.1.11290.1.1.1
StampIT Time Stamping	1.3.6.1.4.1.11290.1.1.2
StampIT OCSP Validation	1.3.6.1.4.1.11290.1.1.3
StampIT DocPro Certificate	1.3.6.1.4.1.11290.1.1.1.1
StampIT Doc Certificate	1.3.6.1.4.1.11290.1.1.1.5
StampIT Global Root CA	1.3.6.1.4.1.11290.1.2
StampIT Global Qualified CA	1.3.6.1.4.1.11290.1.2.1
StampIT Global TSA	1.3.6.1.4.1.11290.1.2.1.1
StampIT DocPro Certificate	1.3.6.1.4.1.11290.1.2.1.2
StampIT Doc Certificate	1.3.6.1.4.1.11290.1.2.1.3
StampIT Seal Certificate	1.3.6.1.4.1.11290.1.2.1.4
StampIT Enterprise Certificate	1.3.6.1.4.1.11290.1.2.1.5
StampIT Enterprise Pro Certificate	1.3.6.1.4.1.11290.1.2.1.6
StampIT Enterprise Seal Certificate	1.3.6.1.4.1.11290.1.2.1.7
StampIT Server DVC	1.3.6.1.4.1.11290.1.2.1.8
StampIT Server OVC	1.3.6.1.4.1.11290.1.2.1.9
StampIT Global OCSP	1.3.6.1.4.1.11290.1.2.1.10
StampIT Global AES CA	1.3.6.1.4.1.11290.1.2.2

Information Services JSC may expand the supported Policies for issued certificates through operational certification authorities

1.3 Participants in the public key infrastructure maintained by Information Services JSC

Information services JSC is a trusted provider of qualified certification services, which meet the requirements specified in Regulation (EU) № 910/2014 and the valid national law.

Information services JSC provides qualified certification services through **certification authority** and a network of **registration authorities**.

The certification authority and the registration authorities perform their activities for provision of qualified certification services on behalf of and on the account of Information Services JSC.

The CPS contains rules and procedures which settle both the relations between the persons in the structure of the provider and the relations between the provider and the users of qualified certification services (relying parties and subscribers).

Information Services JSC provides qualified certification services to all natural and legal persons who agree with the rules of this document.

1.3.1 Certification authority

StampIT is the Certification authority of Information Services JSC which issues qualified certificates for electronic signature (QES) to natural persons, qualified certificates for electronic seal (QESL) to legal persons and qualified website authentication certificates (QWA)..

The certification authority carries out the activities, which include the issue, renewal, suspension, resumption and revocation of QES, QESL and QWA, keeping registers and providing access to them.

Profile of StampIT Root certificate of Information Services JSC

StampIT Global Root CA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Root CA	Name
	C	BG	State
	O	Information Services	Organization

		JSC	
	L	Sofia	
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Validity	20 years		
Subject	CN	StampIT Global Root CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	District
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Public Key	RSA 4096 bits		
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)		
Friendly Name	StampIT Global Root CA		
Basic constrains (Critical)	Subject Type=CA Path Length Constraint=None		
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.stampit.org/repository/		

Profile of StampIT Operational (subordinate) certificate of Information Services JSC

StampIT Global Qualified CA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Root CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Validity	20 years		
Subject	CN	StampIT Global Qualified CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	District
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Public Key	RSA 4096 bits		
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)		
Friendly Name	StampIT Global Qualified CA		
Basic constrains	Subject Type=CA		

(Critical)	Path Length Constraint=0
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.stampit.org/repository/stampit_global_root_ca.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/
CRL Distribution Point /Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.stampit.org/repository/

1.3.2 Registration authorities

The certification authority issues a qualified certificate (QES/ QESL/ QWA) after verification of the subscriber's identity.

In this regard Information Services JSC provides its services to the subscribers through a network of Registration authorities that have the following functions:

- to accept, verify, approve or reject requests for issuing qualified certificates;

- to register the submitted requests for qualified certification services of StampIT;
- to take part in all phases upon identification of the subscribers as specified by StampIT depending on the type of qualified certificate, which they issue;
- to refer to formal, notarized or other specified documents to verify the request submitted by the applicant;
- after approval of the request to notify StampIT in order to initiate the issue of a qualified certificate;
- to register the submitted requests for renewal, termination, suspension and resumption of the validity of a qualified certificate.

The registration authorities act with the approval and subject to the authorization by Information Services JSC in compliance with its practices and procedures.

1.3.3 Subscribers

Subscribers are natural and legal persons who have submitted request and after successful completion of the procedure have received a qualified certificate.

Before the verification and issue of a qualified certificate, the subscriber is only an applicant for the qualified services of StampIt.

The relations between Information Service JSC as provider of qualified certification services and the subscriber shall be settled by a contract in writing.

1.3.4 Relying parties

Relying parties are natural and legal persons who use the certification services with qualified certificates issued by StampIT and rely on these qualified certificates and/ or advanced/ qualified electronic signatures and/ or advanced/ qualified electronic seals, which may be verified through the public key entered in the qualified certificate of the subscriber.

To confirm the validity of the qualified certificate, which they get, the relying parties refer to the StampIT directory, which includes Certificate Revocation List every time before they decide whether to trust the information in them.

1.3.5 Other participants

1.3.5.1 Time-stamping authority

For the issuing of certificates for qualified electronic time stamps is used time-stamping authority StampIT Global TSA, signed with qualified electronic signature StampIT, in its role of qualified provider of qualified certification services.

Profile of StampIT certificate for issuing qualified time stamp of Information Services JSC

StampIT Global TSA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Qualified CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Validity	5 years		
Subject	CN	StampIT Global TSA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	District
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Public Key	RSA 2048 bits		

Key Usage (Critical)	Digital Signature
Friendly Name	StampIT Global TSA
Extended key usage (Critical)	Time Stamping (1.3.6.1.5.5.7.3.8)
Basic constrains (Critical)	End entity
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.stampit.org/repository/stampit_global_qualified.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/
CRL Distribution Point/Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global_qualified.crl
Certificate Policies (Non Critical)	Policy identifier = 1.3.6.1.4.1.11290.1.2.1.1 Repository = http://www.stampit.org/repository/

StampIT Global TSA accepts requests for time stamping of provided content of electronic document by the Subscriber or the Relying party; applies technology for binding the date and time with the data and thus to a great extent excludes the opportunity for unnoticed change of data; it is based on source of accurate time connected with the universal time coordinate; it is signed with qualified electronic signature of StampIT; it

provides opportunity to prove in a subsequent period of time (after expiration of the period of validity of QETS) of the fact of signing/ stamping an electronic document/ another object.

1.4 Types of qualified certificates. Usage.

1.4.1 Types of qualified certificates and applicability.

1.4.1.1 Qualified certificate for electronic signature (QES)

Qualified certificate for electronic signature allows a natural person who takes part in electronic transaction to identify itselff to the other participants in this transaction.

QES may be used for activities, which include identification, signing, authenticity and encrypting.

Types:

1) **Qualified certificates for qualified electronic signatures - QES (qualified)**
   - **Qualified certificate for qualified electronic signature StampIT Doc, which is issued to a natural person;**

StampIT Doc QES is issued to natural persons (signatories of electronic signature) and may be used for identification of the subscriber, protected and encrypted sending of electronic messages and protected and encrypted communications, access to information and online Internet transactions of any kind as for example Internet access subscription services.

StampIT Doc QES provide high level of identity and the requestor is required to prove their identity by appearing in person or through a representative duly authorized with notarized power of attorney to the Registration Authority. The validity of these QES may be 1 (one) or 3 (three) years effective from the date of issuing and is determined in the contract for qualified certification services.

   - **Qualified certificate for qualified electronic signature for a natural person associated with a legal persons StampIT DocPro**

StampIT DocPro QES is issued to natural persons (signatories of electronic signature), which are associated with legal persons. They may be used for identification of the subscriber, protected and encrypted sending of electronic messages and protected and encrypted communications, access to information and online Internet transactions.

StampIT DocPro QES provide high level of identity and the requestor is required to prove their identity by appearing in person or through a representative duly authorized with notarized power of attorney to the Registration Authority. The validity of these QES may be 1 (one) or 3 (three) years effective from the date of issuing and is determined in the contract for qualified certification services.

2) Qualified certificates for advanced electronic signatures - QES (advanced)

- **Qualified certificate for advanced electronic signature StampIT Enterprise**

StampIT Enterprise QES is issued to natural persons (signatories of electronic signature) and may be used for identification of the subscriber, protected and encrypted sending of electronic messages and protected and encrypted communications, access to information and online Internet transactions of any kind as for example Internet access subscription services. They are applicable in all cases for which qualified electronic signature is not required.

StampIT Enterprise QES provide high level of identity and the requestor is required to prove their identity by appearing in person or through a representative duly authorized with notarized power of attorney to the Registration Authority. The validity of these QES may be 1 (one) or 3 (three) years effective from the date of issuing and is determined in the contract for qualified certification services.

- **Qualified certificate for advanced electronic signature StampIT EnterprisePro**

StampIT EnterprisePro is issued to natural persons (signatories of electronic signature), which are associated with legal persons. They may be used for identification of the subscriber, protected and encrypted sending of electronic messages and protected and encrypted communications, access to information and online Internet transactions. They are applicable in all cases for which qualified electronic signature is not required.

StampIT EnterprisePro provides high level of identity and the requestor is required to prove their identity by appearing in person or through a representative duly authorized with notarized power of attorney to the Registration Authority. The validity of these QES may be 1 (one) or 3 (three) years effective from the date of issuing and is determined in the contract for qualified certification services.

1.4.1.2 Qualified certificates for electronic seal (QESL)

Qualified electronic seal certificate allows a legal person participating in electronic transaction to prove its identity to other participants in this transaction by connecting data about the validity of the electronic seal with the legal person and confirms the name of that person.

QESL may be used to guarantee the origin and the integrity or data provided by the legal persons such as electronic documents, photos, drawing and software.

Types:

- **Qualified certificate for qualified electronic seal for a legal person StampIT eSeal - QESL (qualified)**

StampIT eSeal are issued to legal persons (creators of qualified electronic seal). They may be used for identification of the subscriber/ the creator of the qualified electronic seal, protected and encrypted sending of electronic messages and protected and encrypted communications, access to information and online Internet transactions.

StampIT eSeal provides high level of identity and the requestor (the legal representative of the subscriber/ the creator of the qualified electronic seal) is required to prove their identity by appearing in person or through a representative duly authorized with notarized power of attorney to the Registration Authority. The validity of these QES may be 1 (one) or 3 (three) years effective from the date of issuing and is determined in the contract for qualified certification services.

- **Qualified certificate for qualified electronic seal for a legal person StampIT EnterpriseSeal - QESL (advanced)**

StampIT EnterpriseSeal are issued to legal persons (creators of advanced electronic seal). They may be used for identification of the subscriber/ the creator of the qualified electronic seal, protected and encrypted sending of electronic messages and protected and encrypted communications, access to information and online Internet transactions. They are applicable in all cases for which qualified electronic seal is not required.

StampIT EnterpriseSeal provides high level of identity and the requestor (the legal representative of the subscriber/ the creator of the advanced electronic seal) is required to prove their identity by appearing in person or through a representative duly authorized with notarized power of attorney to the Registration Authority. The validity of these QES may be 1 (one) or 3 (three) years effective from the date of issuing and is determined in the contract for qualified certification services.

1.4.1.3 Qualified website authentication certificate (QWA)

The qualified certificate for website authentication allows to establish the website authenticity by linking it to the natural or person to which the qualified provider of certification services has issued the certificate in compliance with the requirements of Regulation (EU) № 910/2014.

Types:

StampIT Server DVC - qualified website authentication certificate, Domain Validation - used for certification of website authentication. The validity of these QWA may be 365 (three hundred sixty-five) or 825 (eight hundred twenty-five) days effective from the date of issuing and is determined in the contract for qualified certification services.

StampIT Server OVC - qualified website authentication certificate, Organization Validation - used for certification of website authentication and its link with specific natural person or legal person. The validity of these QWA may be 365 (three hundred sixty-five) or 825 (eight hundred twenty-five) days effective from the date of issuing and is determined in the contract for qualified certification services.

1.4.1.4 Qualified electronic time stamp (QETS)

A qualified electronic time stamp allows establishing that specific data have existed at specific time. The qualified electronic time stamp is presumed to show accurately the date and time and to ensure integrity of the data with which the date and time is bound.

Through the electronic time stamps the Subscribers and the Relying parties may certify the time for submission of electronic documents and electronic messages and is a proof that the signed data object existed as at the time of applying the time stamp.

A qualified electronic time stamp (QETS) is issued to natural and legal persons who are signatories or relying parties. A qualified electronic time stamp (QETS) has formal certification ability after it is entered in the register kept by StampIT accessible on https://tsa.stampit.org.

1.5 Usage. Availability of services.

StampIT renders assistance to its clients for the selection of appropriate qualified certification service.

Subscribers are required to determine carefully their requirements to the specific uses of the qualified certification services as well as the levels of security for protected and encrypted communications and etc. before submission of request for provision of the relevant type of qualified certification service.

Qualified certificates issued by StampIT may not be used in a manner, which is incompatible with the applicability announced for them as well as in applications, which do not meet the requirements of clause 1.4.

It is forbidden to use the qualified services for performance of activities that are restricted by the national law and the applicable regulations and directives of the European Union.

If practical, the provided qualified certification services and the products used upon their provision will be accessible for people with disabilities too.

2. Public registers and management

2.1 Maintained public registers

2.1.1 Register of issued certificates

StampIT publishes the issued qualified certificates in the register of issued certificates.

StampIT may publish qualified certificates in other registers, which are considered appropriate however it shall not be liable for the validity, accuracy and availability of directories maintained by third parties.

Subscribers on their hand may also publish qualified certificates issued by StampIT in other registers.

The subscriber may prevent the publication of the issued certificate in the maintained registers by explicit declaration of will upon conclusion of the contract for qualified certification services.

2.1.2 Register of suspended and revoked qualified certificates

StampIT shall maintain a register of suspended and revoked qualified certificates – CRL.

2.1.3 Checking the status of issued qualified certificates

StampIT shall maintain interface about the status of the issued qualified certificates – OCSP.

2.1.4 Checking the status of issued qualified certificates for electronic time stamp.

StampIT maintains a register of issued qualified certificates for electronic time stamp.

2.2 Other public information

Current and previous versions of all documents that are subject to publication including:

- Qualified certification services practice statement of Information Services JSC, Policies for provision of qualified certification services, Policy for provision of time stamping services, rules, procedures and documents, which are intended for the Subscribers and the Relying parties;
- Audit reports carried out by the compliance assessment authorities and the supervisory authorities;
- Additional information, which the provider has to publish.

2.3 Frequency of refreshing and publication

2.3.1 Frequency of refreshing the published qualified certificates is as follows:

Name	Address	Frequency for publishing
StampIT Global Root CA	http://www.stampit.org/crl/stampit_global.crl	365 days
StampIT Global Qualified CA	http://www.stampit.org/crl/stampit_global_qualified.crl	Maximum 3 hours or immediately in case of change
OCSP	http://ocsp.stampit.org	real time
Search in issued qualified certificates	https://stampit.org	real time

2.3.2 Qualified certification services practice statement of Information Services JSC, Policies for provision of qualified certification services, Policy for provision of time stamping services - immediately upon each update.

2.3.3 Audit reports that are subject to publication - immediately after receipt.

2.4 Access

StampIT shall provide HTTP/HTTPS(TLS) and OCSP based access to the maintained registers.

The access to the published data shall not be limited unless the Signatory/ the Creator requires so and only with regard to their own valid qualified certificate.

Information published in the registers and other public information shall be accessible 24 hours per day and 7 days per week except in case of events beyond the control of StampIT.

StampIT has taken the relevant measures for protection against unauthorized changes (including removal and adding) of information as well as for immediate recovery in case of identified breaches.

3. Identification and validation of identity data

The activities for identification and validation of identity data of the requestor, the signatory/ creator and the subscriber are carried out by the Registration authority upon receipt of request for issuing a qualified certifi-

cate. The registration authority shall collect and verify the data, which are included in the certificate as well as other identification and identity data, which StampIT has to collect, process and store according to Regulation (EU) № 910/2014 and the national law. StampIT guarantees that before issuing a qualified certificate natural and legal persons are correctly identified, their identity is validated and the requests for issuing are verified and approved.

When the information provided by the requestor is confirmed, the Registration authority sends the request to the Certification authority for the issue of the requested qualified certificate.

3.1 Name:

The issued qualified certificates shall contain the names of the Signatory/the Creator and the Subscriber (if other than the Signatory/Creator) according to the presented valid formal documents and other identifiers according to the type of certificate. Object identifiers in ASN.1 notation are also included.

Names in the certificates comply with the requirements of ETSI EN 319 412 and the recommendations of RFC 5280. DNS record in compliance with RFC 2247 is also allowed.

The field „Subject" contains the name of the Signatory/ the Creator. This information is provided by the requestor and shall be confirmed with the presented documents. The registration authority makes checks in the primary state registers (if applicable) and in other registers, if necessary.

For each certificate shall be entered Distinguished Name (DN), formed in compliance with the requirements of X.520.

Upon issuing a qualified certificate the Subscriber may request the entry of a pseudonym. Issuing a qualified certificate by using „pseudonym" is made only after the Registration authority collects the required identifying information as required by the national law.

The used structure of DN complies with the requirements of X.520 and consists of at least the following elements:

- C – two-letter abbreviation of the country's name according to ISO 3166-1 alpha2
- CN – full name of the natural person or the organisation
- GN – first name of the natural person
- SN – family name of the natural person
- O – name of the organisation represented by the person
- E – user's email address

- SerialNumber – unique identifier of the natural person
- Other fields, which are described in details in the policies for the relevant profiles of the qualified certificates.

Signatory/ Creator with unique DN may have more than one issued qualified certificate within StampIT but with different SerialNumber.

The combination „Issuer“ and "SerialNumber“ guarantee the uniqueness of the issued certificate in global aspect.

StampIT guarantees that it will not publish qualified certificates and other identification data unless the Subscriber gives its explicit consent.

When they provide and use domain and distinguished name as well as any other information upon submission of request for the issue od a qualified certificate) the Subscribers shall not violated any third-party rights with regard to their trademarks, trade names or other intellectual property rights. Subscribers of StampIT shall not use the domain and distinguished names for any illegal purpose, for disloyal competition and shall not provide information, which is misleading or confusing for a given person notwithstanding it is a natural person or legal person. StampIT shall not be liable for non-performance of these obligations on the part of the Subscribers.

If notified for any dispute concerning the use of names, StampIT may refuse issuing a qualified certificate or may terminate the contract for qualified certification service for any issued certificate unilaterally.

3.2 Initial registration upon issuing a qualified certificate

The initial registration shall be carried out according to a procedure, which purpose is to collect all required data for identification of the requestor and the Signatory/ the Creator/ the Subscriber before proceeding to the actual issue of a qualified certificate.

Identity and identification data are subject to confirmation with personal appearance to the Registration authority and in case the request is submitted through an attorney - personal appearance of the authorized to Notary public or to an official performing notary functions.

According to the type of the applicant the following verifications are made:

- or legal person, which is registered according to the national law - verification in the relevant registers based on submitted EIK, respectively BULSTAT;

- for authorized representative of a legal person - verification and certification "True copy" and signature on the required documents.
- for natural person - appearance in person with identity document
- In case the required documents are presented by an attorney - notarization of the authorization documents is required;
- Check of the validity of the presented identity document shall be carried out through the register of issued personal documents kept by the Ministry of the Interior (when personal documents are presented issued according to the national law).
- Verification of the representative authority of one natural person toward a legal person is carried out through verification in the Commercial Register/ BULSTAT Register with the Registry Agency (for legal persons registered according to the national law).

After verification of the submitted data and conclusion of a contract for qualified certification service, the person shall be included as Subscriber of the services of StampIT.

3.2.1 Verification for public key possession

Services may be provided through local or remote generation of the key pair in the presence of a specialist of StampIT.

For the issue or the extension of the qualified certificate it is necessary to generate electronic request in PKCS#10 format through the systems of StampIT, signed by the Signatory/ Creator holding the private key. In such case after successful verification of the validity of the electronic signature/ electronic seal of StampIT will assume that the requestor holds a private key, which complies with the technical requirements and corresponds to the public key, with which the request is signed. When a qualified certificate for qualified electronic signature/ qualified electronic seal is issued, the key pair for which the qualified certificate is issued must be generated in the device for electronic signature/ seal creation.

3.2.2 Verification of legal persons

A representative of the Registration authority shall carry out ex officio verification in the public registers of the legal persons - Commercial Register/ BULSTAT Register with the Registry Agency (if a legal person is registered under the national law).

In case that the verification is impossible, the following shall be presented to the Registration authority:

- Certificate of Good Standing of the legal person issued by a competent authority - original or notarized copy;
- Unique identifier representing the legal person to the state authorities.

3.2.3 Verification of the natural persons who represent a legal person

The verification of the identity of a legal person aims to prove that during the consideration of the request the legal person exists and that the authorized representative who has requested the issuance of a qualified certificate has the representative authority to request the issuing.

The following must be presented to the Registration authority:

- Identity document of the natural person who requested the issuance of the qualified certificate - original;
- Document/ power of attorney from which ensues the representative authority of the natural person for the legal person (if in the qualified certificate are entered the data of the legal person) - original and copy certified by the requestor. This document is required in case that the ground for the authorization is not included in the other documents about the status of the legal person.

3.2.4 Verification of natural persons

Verification of natural persons is carried out by the Registration authority by presenting the following documents:

- Identity document (identity card) of a natural person - original (if the applicant appears in person);
- Power of Attorney with notarization of signature (if applying through an attorney);
- Identity document (identity card) of the natural person authorized to represent the applicant - original.

3.2.5 Inclusion of non-confirmed information

Non-confirmed information is any information, which is requested before the issuance of the qualified certificate but is not subject to compulsory verification. Unconfirmed information may be included in the content of the issued qualified certificate and in such case StampIT is not liable for such information.

3.2.6 Verification and subsequent activities of the certification authority

After successful completion of the processes of identification and verification by the Registration authority of the persons and the conditions for issuance or management of a qualified certificate, the Registration authority confirms the data to the Certification authority. The certification authority shall publish immediately the issued qualified certificate in the Public register/ Repository of issued certificates accessible through OCSP or respectively in the List of suspended and revoked certificates - CRL.

3.2.7 Verification of the possession of a domain

When website authentication certificate is issued, the Registration authority shall perform the required checks to confirm the authenticity of the domains and/ or public IP addresses presented for certification. This is made by checks in the relevant databases maintained by third parties - who is records maintained by the relevant registrar managing the basic domain or RIPE for verification of the public IP addresses.

For Organization Validation qualified certificates in addition shall be carried out the required inspections for the organisation requesting the issue in the relevant registers - Commercial Register/ BULSTAT Register with the Registry Agency.

3.2.8 Compliance with Regulation (EU) No 910/2014

Qualified certificates issued by StampIT meet the requirements of Regulation (EU) № 910/2014 and are recognized in the European Union. For the purpose of guaranteeing the cross-border interoperability of the qualified electronic signatures and qualified electronic seals issued by StampIT, qualified certificates do not exceed the compulsory requirements laid down in Regulation (EU) № 910/2014. StampIT guarantees that to the extent the qualified certificates contain specific data included on national level, they do not prevent the trans-border interoperability and the recognition of the qualified certificates in the European Community.

3.3 Identification and verification of the identity information upon renewal of a qualified certificate

Renewal of a qualified certificate is admissible in the cases when the private key is generated in the electronic signature/ seal creation device and the certificate has not been terminated in the period of validity.

The period of validity of the qualified certificate is marked in the relevant field of the certificate. As the requirements for renewal may differ from those related to the initial issue, StampIT shall publish and update the conditions for renewal of qualified certificates issued by it.

Renewal) may be carried out only if the qualified certificate with validity term of 1 (one) year and all data in the certificate remain unchanged as stated in the initial request.

Renewal of a qualified certificate issued by StampIT is made in accordance with the terms and conditions valid as at the time of renewal and the valid regulatory requirements.

The subscriber shall constantly control the correctness and the accuracy of information published in the renewed qualified certificate. Request for renewal shall be received by StampIT before the date of expiry of the validity, entered in the certificate however not later than 30 days after that date. Submission of request for renewal may be carried out on-site at the Registration authority or remotely - by electronic request signed with qualified certificate. Upon submission of request for renewal to the Registration authority, identification and verification shall be carried out of the information about the identity of the requestor.

In case of remote submission of request for renewal additional identification and verification of identity documentation is not required.

When there are changes in the declared circumstances entered in the qualified certificate or the maximum term of validity of the qualified certificate has expired according to the relevant Policy, a new key pair (rekey) must be generated with a new term of validity. In such case the requestor shall appear in person to the Registration authority and to comply with the procedures for identification and verification of the identity information, whiich are applied upon issuing of a qualified certificate of the relevant type.

3.4 Identification and verification of the identity information upon suspension of a qualified certificate

Suspension of a qualified certificate aims that its use is temporarily stopped and for the period of suspension, the qualified certificates is considered invalid.

Suspension is carried out by StampIT immediately after receipt of request for suspension and for the acceptance and the performance of the request, identification and verification of identity information of the requestor is not required. The certificate shall be immediately included in the CRL list with the relevant reason (Reason) for suspension.

The validity of the qualified certificate shall be resumed upon expiration of the term of suspension, upon withdrawal of the ground for suspension or at the request of the Subscriber in accordance with the regulatory system.

3.5 Identification and verification of the identity information upon revocation of a qualified certificate

Revocation of a qualified certificate stops permanently the validity of the certificate and from the moment of termination, the qualified certificate loses its validity and it may not be restored under any circumstances.

StampIT shall terminate the validity of a qualified certificate under the following circumstances:

- existence of reasonable data and circumstances from which it is evident that there is loss, theft, change, unauthorized disclosure or other compromising of the private key;
- The Signatory/ the Creator of a seal, respectively the Subscriber is in breach of its obligations under the relevant policy and this practice of StampIT;
- The Signatory/ the Creator of a seal, respectively the subscriber is in breach of its obligations under the contract fot provision of qualified certification services;
- the performance of any obligation under the relevant policy and this practice of StampIT has been delayed or has not been performed due to natural disaster, failure of computers or communications or any other reason, which is beyond the human control and in result the information of the other person is threatened or compromised;
- there is change in the information, which is contained in the qualified certificate of the Subscriber;
- termination of the contract for qualified certification services

The termination is carried out at the request of the Signatory/ the Creator of a seal or the Subscriber and at the request of the authorities indicated in a statutory instrument, after identification and verification of the identity information of the person who requested the termination and specification of the reason for termination. The certificate shall be immediately included in the CRL list with the relevant reason (Reason) for revocation.

StampIT shall reliably store the information concerning the revocation of the validity of the qualified certificates and shall provide it to each relying party.

StampIT does now allow renewal or resumption of a qualified certificate after its revocation.

4. Life-cycle of qualified certificates. Operational requirements.

The life-cycle of qualified certificates issued by StampIT based on contract for qualified certification services include the following operating procedures for issuing and management:

- submission of a request for issuing a qualified certificate;

- processing of a request for issuing a qualified certificate;
- issuing a qualified certificate;
- delivery of a qualified certificate;
- Use of a qualified certificate and a key pair;
- Renewal of a qualified certificate (renewal);
- Renewal of a qualified certificate (rekey);
- Suspension/ resumption of the validity of a qualified certificate;
- Revocation of a qualified certificate;
- Services for verification of the status of a qualified certificate

The contract for qualified certification services may be terminated by the Signatory/ the Creator of a seal as well as by the Subscriber.

The time in the systems connected with suspension and revocation of certificates is synchronized toward UTC at least every 24 hours.

4.1 Submission of a request for issuing a qualified certificate

The submission of request for issuing a qualified certificate is operational procedure by which the subscriber refers the Registration authority with the request for issuing qualified certificates consistent with the policy for issuing the requested certificate.

4.1.1 Persons who may submit request for the issuing of a qualified certificate

The qualified certificates are issued at the request of the signatory/ the creator of a seal or the subscriber (if it does not coincide with the signatory/ the creator of a seal) or to duly authorized person in compliance with the relevant Policy. Request for issuing may be also submitted by an employee of the Provider authorized with functions by the Certification authority.

If it is requested that a legal person is entered in QES with which the signatory is associated, the request must originate from the legal person or its duly authorized representative.

Before or during the process of requesting qualified certification services before the Registration authority, the requestors shall follow the steps below:

- submit request for issuing and accept the terms and conditions of the contract for qualified certification services, the relevant policy of the trusted provider of qualification services as well as this CPS.

- present evidence for their identity (as required according to the standard procedures of StampIT pursuant to item 3) consistent with the type of the requested qualified certificate.

4.1.2 Content of the request for issuing a qualified certificate

The request for issuing includes the following elements for identification and the relevant documents in compliance with the type of the qualified certificate and the terms and conditions for its issuance:

4.1.2.1 For issuing qualified certificate for electronic signature (QES)

- name of the requestor;
- post address of the requestor
- pseudonym of the requestor (if a pseudonym is requested)
- personal number/ personal identification number/ uniform identification code (if ay);
- name of the legal/ authorized representative and the number of the authorization document;
- name of the natural person linked to the legal person - requestor;
- pseudonym of the natural person linked to the legal person - requestor (if an entry of a pseudonym is requested);
- city, country;
- proof of payment;
- identity document of the requestor (if applicable)
- identity document of the legal/ authorized representative (if applicable)
- certificate of good standing of the requestor (if applicable)
- authorization document (if applicable)
- submitted request for issuing a qualified certificate with specified type of requested certificate;
- signed contract for qualified certification services;
- public key (in the cases when the key pair is generated with the Signatory)

4.1.2.2 For issuing qualified certificate for electronic seal (QESL)

- name of the requestor;
- post address of the requestor;
- uniform identification code (if any);
- name of the legal/ authorized representative and the number of the authorization document;
- city, country;

- proof of payment;
- certificate of good standing (if applicable)
- authorization document (if applicable)
- identity document of the legal/ authorized representative;
- submitted request for issuing a qualified certificate with specified type of requested certificate;
- signed contract for qualified certification services.
- public key (in the cases when the key pair is generated with the creator)

4.1.2.3 For issuing qualified website authentication certificate (QWA)

- name of the requestor;
- post address of the requestor;
- personal number/ personal identification number/ uniform identification code (if any);
- name of the legal/ authorized representative and the number of the authorization document;
- city, country;
- name of the domain/ name of the domains supported by the requestor for which the issuance of a qualified certificate is requested;
- proof of payment;
- certificate of good standing (if applicable)
- authorization document (if applicable)
- identity document of the legal/ authorized representative (if applicable)
- submitted request for issuing a qualified certificate with specified type of requested certificate;
- signed contract for qualified certification services.
- public key (in the cases when the key pair is generated with the subscriber)
- StampIT may modify the requirements to the information concerning the requests of persons in order to meet its requirements, the business context of the use of the qualified certificates upon observance of the recommendations of Regulation (EU) № 910/2014 and the national law.

4.1.3 Processing of the request for issuing a qualified certificate

4.1.3.1 Issuing user certificates

Processing the request shall be carried out after verification of the request for issuing and conclusion of contract for qualified certification services and includes the following steps:

- **registration of the request for issue**. Registration includes the whole information, which is contained in the request for issue including unconfirmed information under item 3.2.5;
- **key pair generation**. Registration authorities of StampIT are entirely liable for the safe generation of a key pair of the subscriber. When a key pair is generated for qualified certificates for qualified electronic signature/ qualified electronic seal, in all cases the device for secure creation of an electronic signature/ electronic seal with the relevant required security level according to Regulation (EU) № 910/2014; If the key pair is generated with the Signatory/ the Creator of a seal or the Subscriber, the Registration authority shall verify the requirements for the level of security of the device for creation of an electronic signature/ seal and verification for compliance with the cryptographic requirements.
- **generation of request for issuance signed with the private key of the generated/ provided key pair;**
- **sending the request to the Certification authority;**
- **issuing a qualified certificate by the Certification authority by signing the request for issuance with the private key of the Certification authority. Immediate publication of the issued certificate in the Register of issued certificates**
- **recording the certificate and the key pair in the device for secure electronic signature/ seal creation..**
- **submission of the qualified certificate by the Registration authority to the Subscriber/ the authorized representative together with access code for the private key.**
- **acceptance of the qualified certificate of the Subscriber.**

4.1.3.2 Issuing certificates to the Certification authority and to Registration authority

Keys and certificates of the Certification authority of StampIT may be generated only upon performance of the ceremony for key generation in which take part only persons explicitly authorized by StampIT.

Certificates of external Registration authorities may be issued only after conclusion of contract with StampIT, which stipulates the order for determination of the persons who will perform functions of Registration

authorities and requirement for confirmation of their consent to represent the two parties upon contract performance.

4.1.4 Renewal and change of a qualified certificate

The Signatory/ the Creator of a seal or the Subscriber may request renewal of a qualified certificate issued by StampIT upon observance of the relevant Policy and this Practice and consistent with the terms and conditions and the regulatory requirements valid as at the time of renewal.

Renewal of a qualified certificate is admissible in the cases when the private key is generated in the electronic signature/ seal creation device and the certificate has not been terminated in the period of validity.

The period of validity of the qualified certificate is marked in the relevant field of the certificate. As the requirements for renewal may differ from those related to the initial issue, StampIT shall publish and update the conditions for renewal of qualified certificates issued by it.

4.1.4.1 Renewal

Renewal may be carried out only if the qualified certificate with validity term of 1 (one) year and all data in the certificate remain unchanged as stated in the initial request. The qualified certificate may be renewed until the maximum term of validity of 3 (three) years is reached.

The subscriber shall constantly control the correctness and the accuracy of information published in the renewed qualified certificate.

For renewal it is necessary to submit Request for renewal, which shall be received by StampIT before the date of expiry of the validity, entered in the certificate. Submission of request for renewal may be carried out on-site at the Registration authority or remotely - by electronic request signed with qualified certificate.

Request for renewal may be submitted not later than 30 (thirty) days after the date of expiry of the validity, entered in the certificate. In such case request for renewal may be submitted only on-site with the Registration authority.

4.1.4.2 Renewal (rekey)

Rekey is carried out only if there are changes in the stated circumstances entered in the qualified certificate or the maximum term of validity of the qualified certificate has expired according to the relevant Policy. In such case a new key pair (rekey) with a new term of validity shall be generated.

For renewal it is necessary to submit Request for renewal, which shall be received by StampIT before the date of expiry of the validity, entered in the certificate however not later than 30 (thirty) days after the expiration of the term of validity entered in the certificate.

Submission of request for renewal (rekey) may be submitted only on-site with the Registration authority.

4.1.4.3 Information and documents for renewal of a qualified certificate.

- name of the requestor;
- personal number/ personal identification number/ uniform identification code (if any);
- name of the legal/ authorized representative and the number of the authorization document;
- name of the natural person linked to the legal person - requestor;
- proof of payment;
- identity document of the requestor (if applicable)
- identity document of the legal/ authorized representative (if applicable)
- certificate of good standing of the requestor (if applicable)
- authorization document (if applicable)
- signed request for renewal of a qualified certificate with specified type of requested certificate;
- qualified certificate which renewal is requested - upon renewal;
- a new key pair - in the cases when renewal (rekey) is requested and the key pair is generated with the Signatory/ the Creator of a seal or the Subscriber;

4.1.4.4 Change in the content of a qualified certificate issued by StampIT

StampIT does not allow other changes in the content of the qualified certificates unless extension of the term of validity upon renewal.

4.1.5 Submission of request for suspension, resumption and revocation of a qualified certificate

Suspension of a qualified certificate aims that its use is temporarily stopped and for the period of suspension, the qualified certificates is considered invalid.

Suspension is carried out by StampIT immediately after receipt of request for suspension and for the acceptance and the performance of the request, identification and verification of identity information of the requestor is not required.

Request for suspension may be submitted by the Signatory/ the Creator of a seal. the Subscriber of a qualified certificate on-site with the Registration authority by electronic means or by phone.

The certificate shall be immediately included in the CRL list with the relevant reason (Reason) for suspension.

The validity of the qualified certificate shall be resumed upon expiration of the term of suspension, upon withdrawal of the ground for suspension or at the request of the Subscriber in accordance with the regulatory system.

StampIT shall terminate the validity of a qualified certificate under the following circumstances:

- existence of reasonable data and circumstances from which it is evident that there is loss, theft, change, unauthorized disclosure or other compromising of the private key;
- The Signatory/the Creator of a seal, respectively the Subscriber is in breach of its obligations under the relevant policy and this practice of StampIT;
- The Signatory/ the Creator of a seal, respectively the subscriber is in breach of its obligations under the contract for provision of qualified certification services;
- the performance of any obligation under the relevant policy and this practice of StampIT has been delayed or has not been performed due to natural disaster, failure of computers or communications or any other reason, which is beyond the human control and in result the information of the other person is threatened or compromised;
- there is change in the information, which is contained in the qualified certificate of the Subscriber;
- In case of death or putting under judicial disability of the Signatory/ the Subscriber (if the subscriber is a natural person);
- termination of the representative authority of the Signatory toward the Subscriber

The revocation is carried out at the request of the Signatory/ the Creator of a seal or the Subscriber and at the request of the authorities indicated in a statutory instrument, after identification and verification of the identity information of the person who requested the revocation and specification of the reason for revocation. The certificate shall be immediately included in the CRL list with the relevant reason (Reason) for revocation.

StampIT shall reliably store the information concerning the revocation of the validity of the qualified certificates and shall provide it to each relying party.

StampIT does now allow renewal or resumption of a qualified certificate after its revocation.

StampIT will revoke any issued qualified certificates if it terminates its business without transferring it to another provider. In such case StampIT will notify the subscribers, the signatories/ the creators and will revoke the certificates with one-month advance notice. Within one-month after notification, StampIT will refund to the subscribers the amount paid by them in a size calculated in accordance with the residual term of the contract for qualified certification service.

StampIT will suspend or revoke the certificate of the Certification authority from the infrastructure in case of reasonable data and circumstances from which it is evident that the private key of that availability has been compromised. Upon revocation of a certificate of the operational certification authority for issue and management of qualified certificates, all valid certificates issued by it shall be revoked.

If the revocation of a qualified certificate is due to error of the staff of StampIT, the Provider will issue to the Subscriber equivalent qualified certificates on its own account upon observance of the rules and procedures for issuing the relevant type of certificate.

Services for suspension, resumption and revocation are accessible 7 days per week and in case of failure of the systems, the supplier shall restore the services not later than 3 hours.

4.2 Processing of requests

Requests for issuing and managing qualified certificates shall be submitted on-site with the Registration authority. Requests for renewal may be submitted remotely - with electronic request signed with valid qualified certificate.

4.2.1 Identification and validation of identity data

The activities for identification and verification of the identity documentation of the Signatory/ the Creator/ the Subscriber and of the authorized representatives are settled in details in section 3.

4.2.2 Processing of request by the Registration authority

Each submitted request in the Registration authority shall pass the following processing:

- receipt of the request;

- -verification of data contained in the request; verification for possession of private key (if applicable), verification of other required data (if applicable);
- -verification of information for payment of the price of the requested qualified certification service (if payment is due before service provision)
- in case of positive result from verification - the Registration authority confirms the requests, generates key pair and sends the request to the Certification authority.
- in case of negative result from the verification - the Registration authority rejects the request or corrects it.

The Registration authority may reject the request:

- When the requestor is not able to prove its rights on the stated DN;
- when the provided information and/ or documents contain incorrect data or there is any doubt that they contain incorrect data;
- If the price is not paid (in the cases when it is due before service provision).

In case of rejection of the request, the requestor may submit a new request.

4.2.3 Term for consideration of the request

Request for issuance shall be verified by the Registration authority immediately after its receipt.

The certification authority shall issue qualified certificate immediately after receipt of request by the Registration authority.

The term for consideration of the request for performance of the statutory allowed verifications in publicly accessible electronic registers and for issuing a qualified certificate by StampIT may not be longer than 3 (three) days after submission of the request.

4.3 Issuing a qualified certificate

4.3.1 Processing of request by the Certification authority

After performance of the activities for processing the request, the Registration authority shall send request for issuance to the Certification authority.

The certification authority shall immediately (in real time) issue the requested qualified certificates, sign it with the private key of StampIT and publishes it immediately in the List of issued qualified certificates.

The certification authority shall sent the certificate to the Registration authority to deliver it to the Signatory/ the Creator, the Subscriber or its authorized representative.

4.3.2 Provision of a qualified certificate

The registration authority shall record the certificate on the electronic signature/seal creation device on which is generated the key pair for the said certificate and delivers it to the Signatory/ Creator/Subscriber or its authorized representative.

4.4 Acceptance of the issued qualified certificate by the Subscriber.

4.4.1 Confirmation for acceptance

The obligation of the Signatory/ the Creator/ the Subscriber is to verify the content of the issued qualified certificates both with regard to the entered data and for the availability of a public key corresponding to the possessed private key.

If the issued qualified certificate contains gaps or errors, the signatory/ the creator respectively the subscriber may object within 3 days after its publication in the register of the issued certificates. They are eliminated immediately by the provider by issuing a new qualified certificate without payment of any fee unless this is due to provision of incorrect data.

It is assumed that the qualified certificate is accepted if within 3 days after its publication the signatory/the creator respectively the subscriber have not objected that it contains gaps or errors.

The acceptance of the qualified certificate is considered confirmation that the signatory/ he creator, respectively the subscriber has become aware of the procedures for the issuance of certificate and accepts the Practice and the relevant Policy.

4.4.2 Publication of a qualified certificate

The issued qualified certificate is published immediately in the register of issued certificates and is valid from the moment of its publication. From this moment on the certificate is publicly accessible, including for all stakeholders.

4.4.3 Information for the relying parties

The public key in the qualified certificate corresponding to the private key held by the Signatory/ the Creator/ the Subscriber is accessible for all relying parties in the Public register of the issued qualified certificates. Each relying party shall use the public key and the certificate of the Signatory/ the Creator/ the Subscriber in compliance with the requirements of the policy mentioned in the qualified certificate.

The relying parties must use the public key only after verifications of: the status of the qualified certificate and the electronic signature of the Provider.

4.5 Use of a qualified certificate and a key pair

4.5.1 Usage by the Signatories/ the Creators

When using the qualified certificates and the private keys, the Signatories/ the Creators must:

- use them in compliance with their designation determined in this Policy and in compliance with the restrictions and the goals entered in the application and as agreed with the Provider;
- use them only in the period of their validity;
- not use suspended certificate for the creation of an electronic signature/ seal;
- not disclose the private key to any third person and must not provide the qualified electronic signature/ the qualified electronic seal creation device and the method of identification (PIN code).
- take the required measures to prevent compromising, loss, disclosure, modification or other unauthorized use of their private key through reliable protection of their personal identification code (PIN) for work with the key pair and/ or physical access to the qualified electronic signature/ qualified electronic seal creation device storing the key pair.

4.5.2 Usage by the relying parties

Upon use of the public keys and their certificates, the relying parties must:

- use them according to their designation and the entered restrictions for use, consistent with that Practice and taking into account the attributes of the certificate;
- use then only after verification of their status and verification of the electronic signature of the Certification authority that issued the qualified certificate.

- use them only when they are valid (must no use suspended or revoked certificates as well as invalid keys).

4.6 Renewal of a qualified certificate (renewal);

Renewal may be carried out only if the qualified certificate with validity term of 1 (one) year and all data in the certificate remain unchanged as stated in the initial request.

The qualified certificate may be renewed until the maximum term of validity of 3 (three) years is reached.

The subscriber shall constantly control the correctness and the accuracy of information published in the qualified certificate.

4.6.1 Circumstances which require renewal

StampIT will perform any request for renewal under the following conditions:

- request is submitted by the same Subscriber;
- the qualified certificate is not suspended;
- it is submitted within the term of validity of the qualified certificate or not later than 30 (thirty) days after the date of expiry of the validity, entered in the certificate.
- the qualified certificate is not renewed more than once.

4.6.2 Persons who are allowed to submit request for renewal

The request for renewal of a qualified certificate may be submitted only by the signatory/ the creator of the electronic signature/ the electronic seal or by the subscriber of the qualified website authentication certificate. Submission of request for renewal may be carried out on-site at the Registration authority or remotely - by electronic request signed with qualified certificate.

If the request for renewal is submitted after expiration of the term of validity, entered in the certificate, renewal is possible only on-site with the Registration authority.

4.6.3 Processing of the request for renewal of a qualified certificate with generation of a new key pair

Request for renewal of a qualified certificate shall be received by StampIT before the date of expiry of the validity, entered in the certificate however not later than 30 (thirty) days after expiry of the validity.

Submission of request for renewal may be carried out on-site at the Registration authority or remotely - by electronic request signed with qualified certificate.

After successful identification and verification of the conditions for renewal of a qualified certificate, the Registration authority shall confirm its request and shall send an order to the Certification authority that performs the request.

After unsuccessful identification and verification of the conditions for renewal of a qualified certificate, the Registration authority shall reject the request and shall inform the requestor for the reason. The rejection of the request does not prevent submission of a new request for renewal.

The certification authority shall immediately (in real time) extend the validity of the requested qualified certificate, sign it with the private key of StampIT and publish it immediately in the List of issued qualified certificates.

The certification authority shall send the renewed certificate to the Registration authority to deliver it to the Signatory/the Creator, the Subscriber or its authorized representative.

4.6.4 Provision of the renewed qualified certificate

The registration authority shall record the certificate on the electronic signature/ seal creation device on which is generated the key pair for the said certificate and delivers it to the Signatory/ Creator/ Subscriber or its authorized representative.

4.6.5 Confirmation of the acceptance of the renewed qualified certificate

The requirements of item 4.4.1 shall apply.

4.6.6 Publication of renewed qualified certificate

The renewed qualified certificate is published immediately in the register of issued certificates and is valid from the moment of its publication. From this moment on the certificate is publicly accessible, including for all stakeholders.

4.7 Issuing of a qualified certificate by generating a new key pair (rekey)

Generating a new key pair with a new validity term shall be carried out always when the issuance of a qualified certificate is requested by a new subscriber or renewal (rekey) by already registered subscriber.

Renewal (rekey) is carried out only if there are changes in the stated circumstances entered in the qualified certificate or the maximum term of validity of the qualified certificate has expired according to the relevant Policy.

The procedure for observance of a qualified certificate is observed and the generation of a new key pair is not connected with other certificates.

When the request is for renewal (rekey) of a valid certificate, the content of the new certificate differs by the serial number, the public key, the term of validity and the electronic signature/ electronic seal.

StampIT shall inform the Subscribers about the expiration of the term of validity of the qualified certificates issued by its at least 30 days before the expiry date by sending a notice to the email address specified by the subscriber.

The procedure for the issuance of a qualified certificate with generation of a new key pair (rekey) applies also with regard to qualified certificates of the Certification authority and the Registration authority.

4.7.1 Circumstances in which applies the issuance of a qualified certificate with generation of a new key pair (rekey)

StampIT will perform a request for renewal (rekey) under the following conditions:

- request is submitted by the same Subscriber;
- the qualified certificate is not suspended;
- it may be submitted within the term of validity of the qualified certificate as well as up to 30 days after expiration of that term;
- if the request for issuing is for the same type of qualified certificate or for qualified certificate under the same Policy under which the valid qualified certificate was issued.

4.7.2 Persons who are allowed to submit request for updating a key pair

The request for renewal of a qualified certificate by generating of a new key pair (rekey) may be submitted only by the signatory/ the creator of the electronic signature/ the electronic seal or by the subscriber of the qualified website authentication certificate.

4.7.3 Processing of the request for renewal of a qualified certificate with generation of a new key pair (rekey)

The request for renewal of a qualified certificate with generation of a new key pair (rekey) shall be received by StampIT before the date of expiry of the validity, entered in the certificate however not later than 30 (thirty) days after expiry of the validity.

Submission of request for renewal may be carried out on-site at the Registration authority or remotely - by electronic request signed with qualified certificate.

After successful identification and verification of the conditions for renewal of a qualified certificate with generation of a new key pair (rekey), the Registration authority shall confirm its request and shall send an order to the Certification authority that performs the request.

After unsuccessful identification and verification of the conditions for renewal of a qualified certificate with generation of a new key pair (rekey), the Registration authority shall reject the request and shall inform the requestor for the reason. The rejection of the request does not prevent submission of a new request for issuing a qualified certificate.

The certification authority shall immediately (in real time) issue the requested qualified certificates, sign it with the private key of StampIT and publishes it immediately in the List of issued qualified certificates.

The certification authority shall sent the certificate to the Registration authority to deliver it to the Signatory/ the Creator, the Subscriber or its authorized representative.

In the event of a remote renewal the Certification authority shall send the certificate to the Signatory/ the Creator/ the Subscriber who shall record it on the electronic signature/ seal creation device on which the key pair for that certificate is generated.

4.7.4 Provision of a new qualified certificate

The registration authority shall record the certificate on the electronic signature/ seal creation device on which is generated the key pair for the said certificate and delivers it to the Signatory/ Creator/ Subscriber or its authorized representative.

4.7.5 Confirmation of the acceptance of a new qualified certificate

The requirements of item 4.4.1 shall apply.

4.7.6 Publication of a new qualified certificate

The issued new qualified certificate is published immediately in the register of issued certificates and is valid from the moment of its publication. From this moment on the certificate is publicly accessible, including for all stakeholders.

4.7.7 Information for the relying parties

The public key in the qualified certificate corresponding to the private key held by the Signatory/ the Creator/ the Subscriber is accessible for all relying parties in the Public register of the issued qualified certificates. Each relying party shall use the public key and the certificate of the Signatory/the Creator/the Subscriber in compliance with the requirements of the policy mentioned in the qualified certificate.

The relying parties must use the public key only after verifications of: the status of the qualified certificate and the electronic signature of the Provider.

4.8 Change of a qualified certificates

4.8.1 Circumstances which require change in a qualified certificate

Change in a qualified certificate is required in case of change of data, which are entered in already issued and published qualified certificate. In such case a new key pair is generated and a new qualified certificate is issued. In case of change the procedure for issuing a new qualified certificate is issued.

4.8.2 Persons who may submit request for change of a qualified certificate

The request for change of a qualified certificate may be submitted only by the signatory/ the creator of the electronic signature/ the electronic seal or by the subscriber of the qualified website authentication certificate.

4.8.3 Processing of the request for change of a qualified certificate

Request for change of a qualified certificate shall be received by StampIT before the date of expiry of the validity, entered in the certificate however not later than 30 (thirty) days after expiry of the validity.

Submission of request for change may be carried out on-site at the Registration authority or remotely - by electronic request signed with qualified certificate.

After successful identification and verification of the conditions for change of a qualified certificate, the Registration authority shall confirm its request and shall send an order to the Certification authority that performs the request.

After unsuccessful identification and verification of the conditions for change of a qualified certificate, the Registration authority shall reject the request and shall inform the requestor for the reason. The rejection of the request does not prevent submission of a new request for issuing a qualified certificate.

The certification authority shall immediately (in real time) issue the requested qualified certificates, sign it with the private key of StampIT and publishes it immediately in the List of issued qualified certificates.

The certification authority shall send the certificate to the Registration authority to deliver it to the Signatory/the Creator. the Subscriber or its authorized representative.

4.8.4 Confirmation of the acceptance of a new qualified certificate

The requirements of item 4.4.1 shall apply.

4.8.5 Publication of a new qualified certificate

The issued new qualified certificate is published immediately in the register of issued certificates and is valid from the moment of its publication. From this moment on the certificate is publicly accessible, including for all stakeholders.

4.8.6 Information for the relying parties

The public key in the qualified certificate corresponding to the private key held by the Signatory/ the Creator/ the Subscriber is accessible for all relying parties in the Public register of the issued qualified certificates. Each relying party shall use the public key and the certificate of the Signatory/ the Creator/the Subscriber in compliance with the requirements of the policy mentioned in the qualified certificate.

The relying parties must use the public key only after verifications of: the status of the qualified certificate and the electronic signature of the Provider.

It is of great significance that the relying parties do not use the public key after the certificate is revoked or when it is suspended.

4.9 Suspension and revocation of a qualified certificate

Suspension and revocation of a qualified certificate is subject to established operational practices of StampIT.

Suspension and revocation of a qualified certificate represent actions of StampIT, which may be performed within the period of validity of the certificate.

Suspension of a qualified certificate aims that its use is temporarily stopped and for the period of suspension, the qualified certificates is considered invalid.

Revocation of a qualified certificate stops permanently the validity of the certificate and from the moment of termination, the qualified certificate loses its validity and it may not be restored under any circumstances. StampIT does now allow renewal or resumption of a qualified certificate after its revocation.

Upon suspension or revocation, the certificate shall be included immediately, however not later than 3 (three) hours after receipt of the request, in the CRL list with the relevant reason for the suspension. The validity of the certificate shall be suspended from the date and time of publication in the CRL list.

Upon revocation of the certificate of the Certification authority by which the qualified certificates for electronic signature/ electronic seal/ website authentication are signed, all certificates issued by it shall become invalid.

Suspension and revocation may be carried out only by the Certification authority having issued the qualified certificate.

StampIT shall reliably store the information concerning the revocation of the validity of the qualified certificates and shall provide it to each relying party without restrictions. This information is accessible in the course of validity of the revoked qualified certificate and upon expiration of that term.

StampIT will revoke any issued qualified certificates if it terminates its business without transferring it to another provider. In such case StampIT will notify the subscribers, the signatories/ the creators and will revoke the certificates with one-month advance notice. Within one-month after notification, StampIT will refund to the subscribers the amount paid by them in a size calculated in accordance with the residual term of the contract for qualified certification service.

If the revocation of a qualified certificate is due to error of the staff of StampIT, the Provider will issue to the Subscriber equivalent qualified certificates on its own account upon observance of the rules and procedures for issuing the relevant type of certificate.

Services for suspension, resumption and revocation are accessible 7 days per week and in case of failure of the systems, the supplier shall restore the services not later than 3 (three) hours.

The time in the systems connected with suspension and revocation of certificates is synchronized toward UTC at least every 24 hours.

4.9.1 Grounds for revocation of a qualified certificate

StampIT shall terminate the validity of a qualified certificate issued by it under the following circumstances:

- existence of reasonable data and circumstances from which it is evident that there is loss, theft, change, unauthorized disclosure or other compromising of the private key;
- The Signatory/ the Creator of a seal, respectively the Subscriber is in breach of its obligations under the relevant policy and this practice of StampIT;
- The Signatory/ the Creator of a seal, respectively the subscriber is in breach of its obligations under the contract fot provision of qualified certification services;
- the performance of any obligation under the relevant policy and this practice of StampIT has been delayed or has not been performed due to natural disaster, failure of computers or communications or any other reason, which is beyond the human control and in result the information of the other person is threatened or compromised;
- there is change in the information, which is contained in the qualified certificate of the Subscriber;
- In case of death or putting under judicial disability of the Signatory/ the Subscriber (if the subscriber is a natural person);
- termination of the representative authority of the Signatory toward the Subscriber
- termination of the contract for qualified certification service;
- termination of the activity of the certification authority;

A qualified certificate that belongs to the Certification authority may be revoked by its issuing authority subject the existence of the following circumstances:

- when the Certification authority has grounds to consider that the information in the issued certificate is untrue;
- when the private key of the Certification authority or its information system are compromised in a manner affecting the reliance on the certificates issued by that authority;

- when the Certification authority has materially breached any obligation ensuing from this Qualified Certification Services Practice Statement.

4.9.2 Persons who may submit request for revocation of a qualified certificate Grace period.

Revocation shall be carried out at the request of:

- the Signatory/ the Creator or the Subscriber;
- an authorized representative of the Certification authority (in case that the authorized person is security administrator of StampIT).

Persons entitled to request revocation of a qualified certificate must submit request for revocation as soon as possible after becoming aware that there are grounds for revocation.

Revocation shall be carried after identification and verification of the information about the identity of the person who requested revocation and specification of the reason for revocation.

Request for revocation of a qualified certificate may be submitted:

- on-site with the Registration authority;
- remotely - with submitted by electronic way request for revocation of a qualified certificate, when it is signed with the qualified certificate which revocation is requested or with qualified certificate for qualified electronic signature issued by the same Signatory/ Creator or Subscriber.

4.9.3 Procedure for revocation of a qualified certificate

4.9.3.1 Procedure for revocation of a qualified certificate of an end user

Following submission of a request for termination of a qualified certificate to the Registration authority, the request shall be registered and verified by the Registration authority.

Verification covers identification and verification of the information about the identity of the person who requested revocation and specification of the reason for revocation.

In case of positive result from the verification of the request, the Registration authority shall send request for revocation to the Certification authority, which shall revoke the qualified certificate.

The certificate shall be immediately included in the CRL list with the relevant reason (Reason) for revocation.

After unsuccessful identification and verification of the identity of the requestor and/or conditions for revocation, the Registration authority shall reject the request and shall inform the requestor for the reasons. The requestor may submit a new request for revocation of the qualified certificate by eliminating the reasons for the refusal.

4.9.3.2 Procedure for revocation of a qualified certificate of Certification authority or Registration authority

Qualified certificate issued to Certification authority or to Registration authority may be revoked by the authority having issued it.

Revocation is carried out after submission of request for revocation by authorized representative of the Certification authority (in case that the authorized person is security administrator of StampIT) to StampIT. The certification authority shall immediately revoke the qualified certificate.

The certificate shall be immediately included in the CRL list with the relevant reason (Reason) for revocation.

4.9.4 Term for processing the request for revocation

StampIT shall process the request for revocation without unreasonable delay by terminating the qualified certificate and publishing it in the CRL list not later than 60 minutes after confirmation of the request for termination.

4.9.5 Verification in the Certificate Revocation List (CRL) Frequency of publishing.

Each Relying party shall, upon receipt of an electronic document, signed with qualified electronic signature/qualified electronic seal by the Signatory/Creator, verify the status of the qualified certificate in the updated Certificates Revocation List (CRL).

Certificates Revocation Lise (CRL) maintained by StampIT are accessible on the following addresses:

Issuer	Address	Frequency for publishing
StampIT Global Root CA	http://www.stampit.org/crl/stampit_global.crl	Immediately after change, however not more than 365 days

StampIT Global Qualified CA	http://www.stampit.org/crl/stampit_global_qualified.crl	Immediately after change, however not more than 3 hours
StampIT Global AES CA	http://www.stampit.org/crl/stampit_global_aes.crl	Immediately after change, however not more than 3 hours

Information Services JSC shall not be liable for any harms caused to the relying parties from non-performance of their duty for verification of the status of the qualified certificate.

4.9.6 Real-time verification of the status of a qualified certificate

Each person (signatory/ creator/ subscriber, relying party and etc.) may carry out real time verification of the current status of any qualified certificate issued by Information Services JSC through the interface provided by StampIT for verification of the status of the issued qualified certificates - OCSP.

The OCSP service generates response based on database. The OCSP response is valid for 7 days. To maintain the correct system performance, the responses of OCSP are cashed for predetermined time (usually not more than a few hours).

The certificate status verification service is publicly accessible on website: http://ocsp.stampit.org.

Each Relying party shall, upon receipt of an electronic document, signed with qualified electronic signature. qualified electronic seal by the Signatory/ Creator, verify the status of the qualified certificate.

Information Services JSC shall not be liable for any harms caused to the relying parties from non-performance of their duty for verification of the status of the qualified certificate.

4.9.7 Notification for breach of the security of the private key of the Certification authority

In case of breach of the integrity/ disclosure of the private key of the Certification authority, StampIT shall immediately inform the relying parties.

4.9.8 Grounds for suspension of a qualified certificate

Suspension of a qualified certificate aims that its use is temporarily stopped and for the period of suspension, the qualified certificates is considered invalid.

StampIT shall suspend a valid qualified certificate issued by it upon existence of conditions for suspension.

The activities for suspension shall be undertaken immediately after receipt of request for suspension.

4.9.9 Persons who may submit request for suspension of a qualified certificate

Suspension of a qualified certificate is carried out at the request of:

- the Signatory/ the Creator or the Subscriber;
- A person who, based on the circumstances, obviously might be aware of the breach of the private key security;
- Supervisory authority

Request for suspension of a qualified certificate may be submitted:

- by phone;
- on-site with the Registration authority;
- remotely - with request submitted electronically.

4.9.10 Procedure for suspension of a qualified certificate. Period of suspension.

Following submission of a request for suspension of a qualified certificate to the Registration authority, the request shall be registered.

The Registration authority may not reject a request for suspension.

The Registration authority shall send request for suspension to the Certification authority, which shall suspend the qualified certificate.

The certificate shall be immediately included in the CRL list with the relevant reason (Reason) for suspension and the term for suspension.

After suspension of the certificate, the Provider shall immediately notify the Signatory/ the Creator/ the Subscriber of the suspended qualified certificate.

StampIT shall suspend a valid qualified certificate for a period until clarification of the reasons for suspension however for not more than 48 (forty-eight) hours.

4.9.11 Resumption of the validity of suspended qualified certificate

StampIT shall resume the validity of a qualified certificate under the following conditions:

- If the reason for the suspension is cancelled before expiration of the period for suspension;
- At the request of the Signatory/ the Creator or the Subscriber, after clarification of the reasons for which the suspension has been requested.
- After resumption, the qualified certificate shall be considered valid.

4.9.12 Procedure for resumption of a suspended qualified certificate

Following submission of a request for resumption of a qualified certificate to the Registration authority, the request shall be registered and verified by the Registration authority.

The verification shall include identification and verification of the identity information of the person who requested the resumption.

In case of positive result from the verification of the request, the Registration authority shall send request for resumption to the Certification authority, which shall remove the qualified certificate from the current CRL.

Following expiry of the term for suspension, the Certification authority shall resume immediately the validity of the suspended certificate.

In any cases, the procedure for resumption shall remove the suspended certificate from the current CRL list and shall publish a new list.

4.10 Verification of the status of qualified certificates

Directly or through the services of third parties, StampIT shall provide public access and shall manage directories with issued, suspended and revoked qualified certificates in order to increase the level of confidence in its services. User and relying parties are notified that they shall always check the directories with issued and revoked qualified certificates before deciding whether to trust the information entered in a qualified certificate.

StampIT shall update the Certificates Revocation List as specified in clause 4.9.5.

StampIT shall publish and provide access to repositories containing data and documents referring to certification services including this CPS and any other information, which is considered important for the provided services.

The status verification service for a qualified certificate issued by StampIt is publicly accessible on website: http://ocsp.stampit.org.

Services for verification of the qualified certificates status are accessible 24 hours per day, 7 days per week.

4.11 Termination of the contract for qualified certification services by a subscriber

The contract for qualified certification services shall be terminated:

- upon expiration of the validity of the certificate;
- upon termination of the validity of the certificate subject to the relevant grounds;
- if it is established that the certificate is issued on the basis of incorrect data provided by the **Subscriber** respectively on the basis of concealed data;
- upon termination of the legal persons of the **Provider** without transfer of the activity to another provider of certification services;
- in case of death or putting under judicial disability of the **Subscriber** – natural person or upon termination of the legal person of the **Subscriber** or deletion of the **Subscriber** – sole trader from the Commercial Register;
- in case that any contracting party becomes subject to insolvency or liquidation proceedings;
- upon occurrence of force majeure circumstances provided that the parties duly notify each other for such circumstance;
- upon non-performance of the duties of the **Subscriber**, indicated in the contract, the Practice for provision of qualified certification services by Information Services JSC, the relevant policy for provision of qualified certificates, and General Terms and Conditions for provision of qualified certification services issued by Information Services JSC.
- upon non-performance of the duty of the **Subscriber** for payment of the price in the agreed term.

4.12 Trusted storage of private key (escrow)

Information Services JSC does not provide services for trusted storage of private key (escrow).

5. Physical and organizational security control

In this part of the Qualified Certification Services Practice Statement are described the general requirements that are met by StampIT with regard to the control of the physical and organizational security as well as with regard to the activity of the employees.

5.1 Physical security control

The measures taken with regard to the physical protection of StampIT are part of the Integrated Management System developed and implemented in Information Services JSC corresponding to the requirements of the international standards ISO/IEC 9001:2008, ISO/IEC 27001:2013 and ISO/IEC 20000-1:2011.

The measures relating to the physical protection of information data, technology systems, premises and the related support systems are designed to prevent:

- unauthorized access, damages and interference in the working conditions;
- loss, damage or compromise of resources;
- compromise or theft of information or information processing means.

Information Services JSC provides physical protection and access control to premises where there are critical components installed in the infrastructure:

- Qualified Root Certification Authority - StampIT Global Root CA;
- Qualified Operational Certification Authority - StampIT Global Qualified CA;
- Qualified Time Certification Authority - StampIT Global TSA;
- Qualified Certification Authority for Certificates Status Validation - StampIT Global OCSP;
- Registers and repositories;
- Registration authorities.

Physical access to the protected part of the systems of StampIT shall be limited and is provided only for duly authorized employees depending on their functional duties. Measures are taken for protection from emergencies or compromising of assets that lead to termination of business activities as well as for detection and prevention of attempts for compromising data or theft of data and data processing devices.

5.1.1 Premises and structure of the premises

StampIT uses for its activity two centres for data processing (basic and stand-by) accommodated in specially designed and equipped premises in buildings property of Information Services JSC. The premises have the highest degree of control of the physical access, protection from fire, flood and earthquake as well as sensors for unauthorized entry detection. In the data processing centres of Information Services JSC are arranged stations (individual cabinet with equipment), which accommodate the Certification authority of the Provider and all central components of the infrastructure.

5.1.2 Physical access

The physical security of the certificates issuance and management systems complies with the requirements of international standards and recommendations. Physical integrity is ensured for the equipment of StampIT, as well as two-factor control of access and 24-hour security guarding is established. Access to the equipment cabinet is not allowed unless at least 2 (two) authorized technical persons of StampIT are present and each access to the critical infrastructure premises is documented in special journals and in the electronic access control system of Information Services JSC.

There is video surveillance system, signal security systems and access control system in the premises of StampIT. All systems are regularly inspected toward the requirements of the integrated management system and the applicable national law. The authorized persons of the staff of StampIT strictly observe the developed internal procedures for access to the different zones with restricted physical access.

In the offices of Information Services JSC, the Registration authorities and separated from the other premises and are equipped with the equipment that is necessary for the safe storage of data and documents. The access to these zones is control and restricted only to authorized persons connected with the activity of the Registration authority (operators of the registration authority, system administrators) and their clients.

5.1.3 Power supply and air-conditioning systems

The equipment serving StampIT is supplied by redundant UPS system. In the data processing centres is installed air-conditioning system, which maintains constant temperature and humidity (according to the parameters recommended by the manufacturer). In the two centres is maintained additional external power supply from a diesel generator, which is switched on when necessary. In case of failure of the main power supply, the system shifts to the emergency power supply source (UPS and/ or diesel generator).

5.1.4 Flood

To monitor the humidity in the data processing centres sensors have been installed to report the humidity level. These sensors are integrated into the security systems of the buildings of Information Services JSC. The guards and employees of StampIT are instructed and required in case of possible hazards to immediately inform the relevant services, the security administrator and the system administrator.

5.1.5 Fire protection

StampIT complies with all standards for fire safety by conducting its business in accordance with all regulatory requirements and good practices for fire protection.

The protected premises with critical infrastructure (data processing centres) are located in buildings in which have been installed: a sound and light fire alarm system and active fire extinguishing system with gas. In case of fire, it is provided that the supply of electricity to the devices is switched off and the fire is extinguished by gas if local (manual) extinguishing is impossible.

5.1.6 Data media storage

All media containing software, data archives or audit information are stored in a fireproof safe in a special archive room with access control. StampIT manages data storage as specified in the relevant applicable standards and according to the policies and procedures of the Integrated Management System of Information Services JSC.

5.1.7 Data media destruction

StampIT observes the rules for reliable destruction of data media - soft copies and/ or hard copies - in accordance with the Integrated management system of Information Services JSC, which include:

- use of means for secure destruction of data on electronic media;
- cutting printed materials and tapes

Hard copies and electronic media that contain potentially material information about the security of StampIT after expiration of the period of retention according to the internal rules, are destructed in special shredders.

The data carriers for cryptographic keys and PIN/ PUC numbers used for their storage are crushed with appropriate devices. This refers to carriers, which do not allow final deletion of the stored data and their reuse.

5.1.8 Lifetime of technical components

The lifetime of physical elements in the composition of all critical infrastructure components of StampIT is observed according to the operational requirements prescribed by the manufacturer. Upon expiration of the lifetime prescribed by the manufacturer, these are decommissioned.

Regular preventive maintenance of all critical devices is carried out at intervals not longer than 6 (six) months.

5.2 Organizational control

This part of the Qualified Certification Services Practice Statement presents a list of roles assigned to the employees of the Information Services JSC who are responsible for the operation of StampIT and describes the responsibilities and obligations associated with each particular role.
All procedures related to the security of the issuance, management and use of qualified electronic signature certificates/seals, are performed by the trusted staff of StampIT. The provider maintains a sufficient number of qualified employees who, at any moment of its activities' performance, ensure compliance with applicable laws and the company's internal rules and regulations.

5.2.1 Trusted roles

A detailed allocation of the functions and responsibilities of the personnel is stipulated in the internal documents of IO JSC: job and staff list and the relevant internal operating procedures. The functions allocation is implemented in such a way as to minimize the risk of compromising, confidential information leakage and/ or the emergence of a conflict of interests.

5.2.1.1 Trusted roles in Information Services JSC

Information Services JSC keeps qualified employees at positions ensuring the fulfilment of its obligations at any time during its activities of issuing, maintenance and management of qualified certificates in accordance with the regulations. The provider performs its activities with its own staff. Job descriptions have been developed and approved for each trusted role of the personnel, as follows:

- Security Administrator – overall responsibility for the management and implementation of systems security procedures: develops the security policy; takes measures for technical protection of data and systems; defines the operational security measures; exercises direct control over the compliance with the information systems' security requirements, monitoring the compliance with security procedures for installation, configuration, maintenance and changes in the information systems or the network.
- system administrator – responsible for the installation, configuration and maintenance of reliable systems for the services management: system recovery if necessary; reconfiguration of devices and systems in connection with the implementation of new services or solutions; monitoring of the technical and software status of the servers and alarms for incidents;
- System Operator – directly responsible for the operation of the reliable technological systems of StampIT and for the system backup: creation and management of certificates for qualified electronic signature/seal, including the creation of key pairs – private and public for a qualified electronic signature/seal; use of efficient technologies to ensure the daily operation of the system; testing and inspections for the reliable system operation and security; compliance with the technical requirements for the devices operation and in case of technical failure notifying the relevant officials;
- System Auditor – in charge of data storage, backup and management of event logs (especially for their integrity verification) in carrying out internal audits, as well as the compliance of the activity with Regulation (EU) № 910/2014. The system auditor supervises the activities of all registration authorities operating as assigned by StampIT.

5.2.2 Requirements for the division of responsibilities

The trusted roles of the staff of StampIT must be performed by different employees of Information Services JSC.

5.2.3 Identification and verification of the identity for each role

The staff of StampIT is subject to identification and verification of personality in the following situations:

- when they are included in a list of persons with a limited access to buildings/ premises of StampIT;
- when they are included in a list of persons with physical access to the technological system and network resources of StampIT;

- when they are authorized to perform a specific assigned role;
- creation and assignment of an account and a password in the information system of
- StampIT;
- Any authorization for the performance of a certain role requires:
- The role to be unique and directly related to a specific person;
- not to be shared with another person;
- it should be limited to the function resulting from the role and to be performed by a specific person.

For the performance of each role Information Services JSC provides to the employee software, technological system and access to the operational systems of StampIT.

5.3 Control over the staff

The staff of Information Services JSC consists of a sufficient number of highly qualified employees. The persons performing trusted roles have the necessary professional training and experience, which ensures thecompliance with security requirements and technical standards for security assessment. The professional knowledge in the field of information systems, cryptography and infrastructure of public keys enables the employees with trusted roles to perform their official duties in high quality. The employees of IO JSC pass periodic courses for additional training to meet the current requirements in the area of provision of services connected with qualified electronic signature as well as the related services.

5.3.1 Staff qualification

IO JSC makes sure that the person performing a trusted role of the Certification authority or in the Registration Authority system meets at least the following requirements for the position:

- has graduated at least high education;
- Has signed a freelance or employment contract describing his/her role in the system and the corresponding responsibilities;
- Has undergone the necessary training related to the scope of duties and the tasks of his/her position;
  Has been trained in the field of personal data protection;
- Has signed an agreement containing a clause on the protection of sensitive information and the user data confidentiality;

- Does not perform tasks that may lead to a conflict of interest with the activity of StampIT.

5.3.2 Staff testing procedures

Each new employee of Information Services JSC, performing a trusted role is tested:

- to confirm previous employment and professional experience;
- for recommendations (including verification of recommendations);
- to confirm the educational degree;
- to verify the certificate of no conviction;
- to verify his/ her medical fitness;
- to verify his/ her identity.
- IO JSC may reject the application related to the implementation of the trusted role or take action against a person who is already employed and performs a trusted role if it is established that:
- It was misled by an applicant or employee with respect to the above required data;
- receives highly unfavourable or not very reliable recommendations from previous employers;
- obtains information about any criminal record of the applicant or its employee has been sentenced by an enforced and valid judgement of court.

In the presence of any of these hypotheses, the further steps are carried out in accordance with the applicable law.

5.3.3 Requirements to staff training

The personnel performing the duties and tasks arising from his/her employment in StampIT or the employment in the Registration Authority (in case of an external Registration Authority), must go through the following trainings:

- POLICY for provision of qualified certificates for qualified electronic signature and qualified electronic seal (eIDAS-CP-QES)
- POLICY for provision of time-stamping services (eIDAS-CP-TS)
- POLICY for provision of qualified certificates for advanced electronic signature and advanced electronic seal (eIDAS-CP-AES)
- POLICY for provision of qualified website authentication certificates (eIDAS-CP-SSL)

- Qualified certification services practice statement of Information Services JSC (eIDAS - CPS)
- regulations, procedures and documentation related to the occupied position;
- Security technologies and procedures related to security used by the Certification Authority and the Registration Authority;
- system software of the Certification Authority and the Registration Authority;
- Responsibilities arising from the roles performed in the system;
- Procedures performed upon system failure or suspension of the activities of the Certification authority.

5.3.4 Frequency of training and requirements for qualification improvement of the employees

Trainings described above are carried out at regular intervals - at least once every 12 (twelve) months.

In case of any changes in the regulations and/ or the documentation and the activity of StampIT, trainings shall be carried out promptly and always before the entry into force of the relevant change.

5.3.5 Change of job

Information Services JSC has no requirements in this area.

5.3.6 Sanctions for unauthorized activities

In case of detection or suspicion of unauthorized access, the system administrator, together with the security administrator (employees of the Provider) or only the system administrator (employee of the Registration Authority, in the presence of an external Registration Authority) may terminate the access of the perpetrator to the system of the Registration Authority. The further disciplinary actions are consulted with the management of Information Services JSC.

5.3.7 Contract with the staff

Except employees working under employment contract, Information Services JSC may hire external persons under freelance contract for performance of trusted roles in StampIT. In such cases, they meet the same requirements applicable to the persons employed at Information Services JSC.

The same requirements apply with regard to consultants of Information Services JSC when subject of consultations are the activities performed by individuals with trusted roles in StampIt. Service providers and consultants pass through the same procedure for verification as the employees of Information Services JSC.

5.3.8 Documentation made available to the staff

The management of Information Services JSC and of the management of Registration Authority (in the case of an external Registration Authority) must provide their employees with access to the following documents:

- POLICY for provision of qualified certificates for qualified electronic signature and qualified electronic seal (eIDAS-CP-QES)
- POLICY for provision of time-stamping services (eIDAS-CP-TS)
- POLICY for provision of qualified certificates for advanced electronic signature and advanced electronic seal (eIDAS-CP-AES)
- POLICY for provision of qualified website authentication certificates (eIDAS-CP-SSL)
- Qualified certification services practice statement of Information Services JSC (eIDAS - CPS)
- regulations, procedures and documentation related to the occupied position;
- Security technologies and procedures related to security used by the Certification Authority and the Registration Authority;
- system software of the Certification Authority and the Registration Authority;
- Responsibilities arising from the roles performed in the system;
- Procedures performed upon system failure or suspension of the activities of the Certification authority.
- Templates of requests, applications and declarations;
- Excerpts from documents corresponding to the performed role including all urgent procedures;
- Responsibilities and duties connected with the performed role in the system of the Provider.

5.4 Event records and logs maintenance

Management of events recording the activities of users, exceptions, errors and events related to data security shall be carried out on the basis of the developed policies and procedures for events management. Registered events may be used for the future analyses and monitoring of the access control mechanisms.

The audit team of Information Services JSC shall perform on regular basis inspections for the observance of the implemented mechanisms, controls and procedures according to the Practice for provision of qualified certification services, Regulation (EU) № 910/2014 and the valid national law. The audit team shall assess the efficiency of the existing security procedures.

5.4.1 Types of records

StampIT creates records for each activity within the infrastructure managing the provision of qualified certification services and related services.

These records are divided in three separate categories:

- System records
  - when new or additional software is installed;
  - upon startup of systems and applications thereto;
  - in successful attempts to launch and access to hardware and software PKI-components (Public Key Infrastructure of the systems);
  - generation and management of the key pairs and certificates for the certification authorities and the infrastructure components of StampIT;
  - management of crypto-modules;
  - generation and management of key pairs and User certificates; launch of the systems and applications therein;
  - while trying to launch and access the hardware and software PKI-components of the systems;
  - generation of Certificate Revocation List (CRL);
  - publication of issued valid certificates in the Public Register;
  - configuration of profiles of certificates;
  - Real-time status of a certificate;
  - time stamping for submitted content.
- Errors
  - the records contain information about errors at the level of network protocols;
  - upon a failure of the systems and the applications thereof;

- upon unsuccessful attempts to start and access the hardware and software PKI-components of the systems;
- upon system software and hardware systems failures and other anomalies in the platforms;

- audits – the records contain information relating to the qualified certification services, for example:
  - received registration documents – for the purpose of identity check and identity verification;
  - requests for issuance, renewal, suspension/resumption and termination of certificates; internal procedures for the identification and registration;
  - release of a Certificates Revocation List (CRL);
  - Other
- The event records include the following but not limited to:
  - data about identification of users;
  - date, time and details for important events, for example login and logout;
  - records of successful attempts for system log;
  - records of successful attempts for access to data and other resources;
  - use of privileges;
  - accessed files and type of access;
  - alarms evoked by the access control system;

Logs of the information systems are adjusted to register errors and exceptions while working with the operational systems and the applied programmes. Logs are regularly reviewed by the authorized persons. Recorded errors are analysed and if necessary actions are taken to remedy the causes of them.

5.4.2 Frequency of records creating

The information on the electronic logs is automatically generated.

In order to detect possible illegal activities, the security administrator, the system administrators and the auditor analyse the information at least once within one working day.

The security administrator is obliged to review and assess the accuracy and completeness of registered events and to verify the compliance with the security procedures of Information Services JSC.

The records in the events register are reviewed in detail at least once a month. Each event is subject to explanation and is described in the log of the system administrator.

5.4.3 Period of records retention

Registered events record logs are stored in files on the system drive for at least six (6) months. After that period, records are stored in the archives.

Archived logs are retained for at least 10 (ten) years.

5.4.4 Protection of records

Rules have been introduced for monitoring and use of the information processing means, documented in the rules and procedures for events management and the results thereof are reviewed at regular intervals by authorized employees.

Monitoring of the systems include regular review of the granted access rights as described in PIS 06 Access control and network security.

The events record may be reconsidered only by the security administrator, the system administrator or the auditor. Access to the events record is configured in such a way that:

- only authorized representatives are entitled to read the records in the register;
- only the security administrator may archive or delete filed (after being archived) containing the registered events;
- it is possible to identify any breach of integrity.

5.4.5 Keeping backup copies of events records

Backup copies of the records in the logs of the system are kept, which are reliably stored based on the procedure for creation of backup copies, which is a part of the IMS of Information Services JSC.

5.4.6 Notification system after records analysis

Frequency of review of the monitoring results depends on the included risks determined by the performed risk assessment.

The risk factors include:

- criticality of the processes of the programme;
- the value, the sensitivity and the criticality of the involved information;
- the experience gained from previous penetration and incorrect use of the system and frequency of used vulnerabilities;
- degree of binding the system (especially with public networks);
- deactivation of recording devices.

The policies for monitoring and use of the system ensure that the users perform only activities for which they are explicitly authorized.

5.4.7 Vulnerability and assessment

Information Services JSC classifies and maintains registers of all assets in compliance with the requirements of ISO/IEC 27001:2013. According to the developed and implemented IMS of Information Services JSC analysis is carried out for assessment of the vulnerability under all internal procedures, applications and information systems. The requirements for analysis also may be determined by external institution authorized to carry out audit of Information Services JSC by a second party.

Risk analysis is carried out at least once a year. The decision to proceed to analysis is made by the Management Board.

The security administrator shall be responsible for the internal audits in the part referring to the provision of qualified certification services. It shall control the protection of the security records in the journals, the correct archiving of the backup copies, the activities in case of threats and the compliance with this Practice.

5.5 Archiving

The information about significant events is archived in electronic form at regular intervals based on preliminary approved Backup Plan.

Information Services JSC shall archive all data and files connected with:

- information upon registration;
- the system security;
- all requests submitted by subscribers;

- the whole information about subscribers;
- all keys used by the Certification authorities and by the Registration authority
- the whole correspondence between StampIT and the subscribers
- all documents and data used in the process of identity verification.

The company shall store the archives in a format allowing reproduction and retrieval

5.5.1 Types of archives

StampIT manages two types of archives: paper-based and electronic.

5.5.2 Period of archives retention

StampIT stores reliably its archives for a period not shorter than 10 (ten) years. The retention period starts on the date the information is received. Such archives may be stored as soft copies or hard copies or any other appropriate format.

5.5.3 Protection of archival information

StampIT stores archived records in a way excluding unauthorized and untrusted individual sharing access thereto. The information archived electronically is protected against unauthorized viewing, modification, deletion or falsification through the implementation of an Access control system (via accounts and passwords). For the purposes of archiving reliable electronic media are used that cannot be easily destroyed or erased during the period of retention. For the purposes of the safe storage of archive files in electronic form, they contain an electronic signature.

5.5.4 Retrieval of archived data

The possibility to fully retrieve the backups is essential for the proper functioning of StampIT. Policies and procedures for retrieval are described in PIS 09 Information security.

5.5.5 Requirements for the archiving time recording

Archive records are secured by authentication of the exact time of their signing.

5.5.6 Archive storage

The archive data collecting system is an internal system of StampIT.

Archival information (on paper and electronic media) is properly stored in a special safe, in a room with a high degree of physical protection.

5.5.7 Archival information access and verification procedures

Access to the archive is only available to authorized employees of StampIT after a successful authentication and confirmation of access rights.

The data are checked periodically and compared against the original data to verify the integrity of archived information. This activity is supervised by the security administrator by keeping records for each stage of the procedure. The verification results are recorded in the respective registers of events.

If damages or modifications to the original data are identified, the damages are removed as quickly as possible, in accordance with the internal procedures and rules of StampIT.

5.6 Change of the Provider's key

The provider can change the key corresponding to an issued certificate only issuing a new certificate or renewing the current one by "Re-Key".

The private key of a Certification Authority can be changed in case of:

- expiration of the validity of the accompanying certificate;
- introduction of new services by StampIT, entailing changes in the private key characteristics (for example, changes relating to the security and a requirement for new applicable cryptographic combinations).

In case of a change in the private key of the Certification Authority of StampIT the following rules are observed:

- the Certification authority, with whose key user certificates are signed, and whose key will be modified, suspends the issuing of certificates sixty (60) days prior to the moment when the remaining period of validity of the private key equals with the validity period of the last issued certificate;

- the Certification authority, whose private key signs the Certificates Revocation List (CRL) and whose private key will be changed, continues to publish lists signed with old private key until the moment when the last published certificate validity expires.

5.7 Compromising keys and recovery after accidents

This part of the ‘‘Qualified Certification Services Practice Statement’’ describes the procedures performed by StampIT in case of accidents (including natural disasters) to restore the service to the users as described in PIS 14-03 Disaster Recovery Plan.

Upon a possible threat of occurrence of accidents, analysis is made of the availability of critical resources needed to restore the system. Current recovery cost estimates are made as well. The Provider has procedures for assurance processes continuity connected both with the information technologies and the business processes.

The disaster recovery plan is tested annually and is subject to training by the employees of StampIT. The main goals of the Plan are:

- To recover as soon as possible and in an efficient manner the usual work of the structural units of the Provider in case of extraordinary circumstances or disaster.
- To develop, test and document well structured and understandable Disaster Recovery Plan, which may help the organization recover as soon as possible and in an efficient manner from unforeseen disaster or extraordinary situation, which interrupts the information systems and the work operations.

5.7.1 Actions in case of accidents

In case of a crisis or occurrence of any incident, crisis, disaster, accident, high risk or intensive situation, the Executive Director of Information Services JSC announces disaster situation and determines which scenarios will be applied for the particular situation in order to limit the impact on the staff, the resources and the assets of the organization. At the time when the incident is counteracted and the disaster is under control, transition is made to OD PIS 14-01 Business Continuity Plan.

Archival data containing information on requests for issuance, management and revocation of certificates, as well as the records of all issued certificates in the database are stored in a safe and reliable place and are available in case of an accident.

For prompt detection of possible disasters and accidents, Information Services JSC monitors all systems and services on 24x7 basis and has all-day centre for services management through which users may notify about incidents or non-functioning services.

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

The whole information in case of theft of hardware, software and/or data is transmitted to the security administrator who acts in accordance with the internal procedures developed by IO JSC.

These procedures are associated with analysis of the situation, investigation of the incident, measures to minimize the consequences and to prevent similar incidents in the future.

In the event of failures in the hardware, software or data, the Provider notifies the users, recovers the components of the infrastructure and resumes in priority the access to the Public register and the Certificates Revocation List (CRL).

For the achievement of the above, Information Services JSC has developed Policy for management of information security incidents. The Provider has a plan for management of all incidents that affect the normal operation of the public key infrastructure. This plan corresponds to the Continuity plan and the Disaster recovery plan.

5.7.3 Compromised or compromise-suspected private key infrastructure of the Certification authority of StampIT

The provider takes the due care to maintain the continuity and integrity of the qualified certification services related to the certificates issued, maintained and managed.

The provider takes its best care, within its capacities and resources, to minimize the risk of compromising the keys of its Certification authorities due to natural disasters or accidents.

In case of compromising or suspected compromising of the private key infrastructure of the Certification authority of StampIT, the following actions are taken:

- the operating authority's license is immediately terminated;
- the Certification Authority generates a new key pair and a new license;
- all license users are immediately informed about what happened, using the mass media (information on the website of StampIT) and by e-mail;
- all trusting parties are informed;

- the certificate, corresponding to the compromised key is entered in the Certificates Revocation List (CRL), together with the appropriate reason for termination;
- all user licenses, issued by the certificate corresponding to the compromised private key are terminated and entered in the Certificates Revocation List, indicating an adequate reason for their termination;
- new certificates are issued to affected subscribers;
- the new certificates of subscribers are issued at the expense of StampIT (subscribers are not charged with the price for the certificates);
- an instant analysis is made and a report is prepared on the cause of compromising.
- These operations are carried out according to the plan developed by StampIT for security incidents. This plan is developed by a team of StampIT under the leadership of the security administrator and is approved by the Board of Directors.

5.7.4 Business continuity and disaster recovery

Information Services JSC has developed and implemented PIS ‘‘Business continuity plan’’ for the cases of accidents occurrence, such as large system or network interruptions. This document governs the preparation and processes to ensure the preservation of the activity of StampIT. The purpose of the Policy is to ensure continuous operation and bringing to the minimum the negative effects such as interruption of the service of the clients and harming the public prestige of Information Services JSC.

Within this general goal, the particular task is to ensure successful resumption of the communications and the operation of the information systems upon occurrence of emergency or breakthrough in the information security through a combination of preventive actions and mechanisms for control and recovery. The policy is consistent with the requirements for services management.

The procedures for system recovery after accident are tested on each component of the technological system of StampIT at least once a year. These tests are a part of the internal audit.

Software updating is possible only after performance of intensive tests in a test environment and actions in strict compliance with the described procedures of StampIT. Each change in the system requires the consent and the approval of the security administrator.

Upon each system recovery after disaster, the security administrator or the system administrator will perform the following:

- change all previously used passwords;
- remove all access rights to the system resources;

- change all codes and PIN numbers associated with the physical access to the facilities and system components;
- Review analysis of the disasters causes.

5.8 Termination of the activity of StampIT

The obligations described below are designed to minimize disruptions to the subscribers' and relying parties' activities arising from the decision of StampIT to cease operations.

5.8.1 Requirements relating to the transition to the cessation of the provider

Before the certification authority terminates its services, it is obliged to:

- inform the Supervisory authority of its intention to terminate its services, in the event of a claim for declaring the company bankrupt, declaring the company insolvent or another request for termination or commencement of liquidation proceedings. The notification shall be made four (4) months prior to the agreed date of termination;
- notify (at least 4 months in advance) its subscribers of the decision to terminate its services; terminate the contracts with organizations, which are external Registration authorities;
- change the status of its certificates;
- terminate all certificates of subscribers within the period stated for the termination of its activities;
- inform all its subscribers on the services termination and transfer of the information support to another trusted persons;
- make the reasonable commercial efforts to minimize the violation of interests of the subscribers;
- perform the required activities for transfer of the support of the whole relevant information related to data issued and received in the capacity of qualified provider of qualified certification services and particularly with a view to provision of proof upon legal disputes and ensuring succession upon service provision to another reliable person for sufficiently long period. That information includes: data provided upon issuance, suspension and revocation, archives of logs of events for the relevant period determined by the subscriber and the relying parties. Information includes the Certificates Revocation List for certificates with unexpired validity term.
- to pay compensations to the subscribers proportional to the remaining period of validity of the certificates.

If Registration authority as an external organisation has made decision to terminate its representation for StampIT for the provided certification services, it shall:

- notify StampIT of its intent to terminate the activity. The notification shall be made four (4) months prior to the agreed date of termination;
- submit to StampIT the whole documentation connected with the service of the subscribers including the archives and the audit data.

5.8.2 Transfer of activities to another provider of qualified certification services

To ensure the continuity of providing qualified certification services to the users, StampIT can sign an agreement with another qualified provider of certification services.

In such case StampIT shall carry out the following:

- inform the Supervisory authority of its intention, but not later than 4 months before the date of termination and transfer of activities;
- make all efforts and care to extend the issued subscribers' certificates;
- notify the Supervisory authority and the subscribers in writing that its activities are taken over by another registered provider, as well as of its name. The notification shall be published on the website of StampIT;
- inform the Subscribers about the maintenance terms of the certificates transferred to the receiving Provider;
- change the status of operational certificates and duly transmit to the receiving provider the whole documentation related to the activities, along with all archives and all issued certificates (valid, revoked and suspended);
- perform the necessary actions to transfer the information maintenance obligations to the receiving Provider;
- transfer the management of the already issued end-user certificates to the receiving Provider;

The receiving provider shall assume the rights and obligations of StampIT with its discontinued operations, and continue to manage the active certificates until the expiry of their validity.

The archive of StampIT with terminated status must be transferred to the Provider which received the activity.

5.8.3 Withdrawal of the qualified status of StampIT or the qualified status of a particular service

Upon the revocation of the Qualified status of StampIT or of any certification service provided thereby, it shall perform the following:

- Inform its subscribers about its changed status, or that of its services;
- change the status of its certificates;
- terminate all qualified certificates of its subscribers at the moment of the changed status entry into force and notify them about the transfer of the maintenance of information to another trusted person;
- make the reasonable commercial efforts to minimize the violation of interests of the users;
- perform the required activities for transfer of the support of the whole relevant information related to data issued and received in the capacity of qualified provider of qualified certification services and particularly with a view to provision of proof upon legal disputes and ensuring succession upon service provision to another reliable person for sufficiently long period. That information includes: data provided upon issuance, suspension and revocation, archives of logs of events for the relevant period determined by the subscriber and the relying parties. Information includes the Certificates Revocation List (CRL) for certificates with unexpired validity term.
- to pay compensations to the subscribers proportional to the remaining period of validity of the certificates.

6. Technical security control and management

This part of the Qualified Certification Services Practice Statement describes the procedures for generation and management of cryptographic keys and the related technical requirements.

6.1 Key pair generation and installation

Cryptographic key pairs for the operational certificates of StampIT are generated and installed according to the instructions and procedures in this document. T The generation is performed by authorized persons at StampIT. To create a signature a protective mechanism is used, with a safety profile established in accordance with the technical specifications defining the security levels.

The provider uses its private keys only for the purposes of its activities, as follows:

- to sign the issued operating certificates of the Certification Authorities in its infrastructure;
- to sign the issued and published Certificate Revocation List (CRL);
- to sign all issued and published certificates of electronic signature/seal of the Subscribers.

The cryptographic key pair (private and public) of the electronic signature/seal certificates issuedin the infrastructure of StampIT is generated by an operator of the Registration authority of StampIT, with hardware and software, which is under the control of StampIT:

For the generation of a key pair of a qualified electronic signature/seal certificate, a device for electronic signature creation/sealing is always used, with a protective profile according to Regulation (EU) № 910/2014.

Only electronic signatures/seals, created by the private key of a key pair generated in a device for the creation of qualified electronic signature/seal have the character of a qualified electronic signature/seal.

The Signatory/ the Creator/ the Subscriber shall use licensed software for work with electronic signature/ seal creation device.

6.1.1 Generation of a key pair to Certification authority

The provider generates pairs of cryptographic (RSA) keys to the basic and the operating Certification Authorities using a hardware cryptographic system (HSM/Hardware Security Module) with security level FIPS 140-2 Level 3 or higher, respectively CC EAL 4+ or higher.

Authorized persons from the staff of StampIT perform the steps of the generation, installation and storage of the key pairs of basic and operational Certification Authorities, respectively ‘‘StampIT Global Root CA’’ and ‘‘StampIT Global Qualifie CA’’, in accordance with a documented internal procedure agreed and approved by the management of Information Services JSC.

The procedure is performed in the presence of the Executive Director of the Information Services JSC and a representative of the Legal Department.

Prior to the generation of a base key pair of StampIT, procedure is performed to access the installed crypto module (HSM/Hardware Security Module), by generating separately and independently from each other symmetric keys, stored on tokens, protected by a Personal Identification Number (PIN) for access. Each of the administrator's smart cards contain a part of the access keys and encryption of the asymmetric keys of the provided in the crypto-module (HSM). For management and restoration of the private keys of StampIT

stored in the crypto-module are required three of the total of five smart cards generated upon initialization of the crypto module (HSM) and the relevant PIN codes for access.

The smart cards for access, encryption and restoration of the private keys in the crypto-module (HSM) are stored shared in protected premises of StampIT with compulsory access by two or more persons together, strictly determined by order of the management of Information Services JSC. The shared smart cards with the stored keys required for restoration of the private keys of StampIT and the multiple access control to them ensures that these keys may not be compromised and/ or unlawfully recovered outside the security zones of StampIT.

6.1.2 Generation of a key pair of the signatory/ creator.

The key pair of the Signatory/ the Creator of qualified certificate for electronic signature/ seal shall be generated only in approved by StampIT electronic signature/ seal device (external) verified for security level and for successful work in the infrastructure of StampIT for the issue and management of qualified certificates for electronic signature/ seal. The private key of the generated key pair may not be extracted from the device. The private key is controlled by access code (PIN). The signatory shall use PIN for access to the device in order to carry out access to the private key for qualified electronic signature/ seal creation.

6.1.3 Delivery of the private key to the user

The signatory/ the creator of a seal or their authorized representative shall receive the private key and the issued qualified certificate on electronic signature/ seal creation device in the Registration authority of the provider. Upon initial issuing of certificate on electronic signature/ seal creation device, after generation of a key pair, the device is initialized and the following access codes are created: User code (User) and Administrator code ("SO"). The user's access code:

- is generated by the Signatory/ Creator of a seal in the Registration office of StampIT;
- provide initially randomly generated PIN code of the Signatory/ Creator of a seal or its authorized representative in a sealed, non-transparent envelope. The signatory/ creator of a seal shall change its initial User's access code to the device via the software, which is provided with it. StampIT recommends to the Signatory/ Creator of a seal to change regularly its User's PIN code for access.

In case of specified number unsuccessful attempts for entering correct access code to the private key of the Signatory/ Creator of a sea, the access to it shall be blocked. In such case the signatory/ the creator of a seal or its duly authorized attorney shall visit the Registration office of StampIT and shall present identity

document and electronic signature/ seal creation device. Operator of StampIT provides opportunity for new generation of PIN code on the part of the signatory/ the creator of a seal or provides a new randomly generated PIN code.

At the request of the signatory/ creator of a seal, StampIT may provide Administrator's access code (SO) for unblocking the blocked electronic signature/ seal creation device.

6.1.4 Delivery of provider's public key to the relying parties

The public keys of published in the certificates of the Certification authority to Administrative ("SO") in the format X.509 v.3/X.520.

Certificates are published and accessible in the repository of StampIT on address:https://www.stampit.org/bg/page/814.

Each relying party establishes its confidence to StampIT by adopting and installing the operating certificates of StampIT in the systems under its control.

6.1.5 Length of keys

The length of the base key of StampIT ‘‘StampIT Global RSA Root CA’’ is 4096 bits, with an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA.

The length of the key pair of the operative Certification authority ‘‘StampIT Global Qualified CA’’ is 4096 bits, with an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA .

The length of the key pair of the operative authorities ‘‘StampIT Global TSA’’ is 2048 bits, with an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA.

The length of the key pair for the electronic signature/seal of the Signatory/Creator, generated by the infrastructure of StampIT is 2048 bits, with an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA.

6.1.6 Private key parameters

The Signatory/the Creator of a key pair are responsible for verification of the quality of the parameters of the generated private key. He is obliged to check the ability of the keys to create electronic signature.

The qualified electronic signature/ seal creation devices provided by StampIT and the secured environment for generation and storing the keys of the Signatory. the Creator have security level CC EAL 4+ , respectively FIPS 140-2 Level 3.

6.1.7 Key usage

The parameters of the key pair usage, in particular that of the private key, are contained in the certificate, issued by StampIT through the attributes ‘‘Key Usage’’ and ‘‘Extended Key Usage’’, meeting the standard X.509 v3.

6.2 Private key protection and control of cryptographic module

Any user and operator of Registration Authority create and store private keys using a reliable system for its safety. The Registration Authority generates a key pair by using the device for secure creation and storage of keys (sscd) and delivers them in protected form to the user.

6.2.1 Cryptographic modules standards

The main components of the infrastructure of StampIT use a reliable cryptographic system (Hardware Security Module/HSM), certified for security level FIPS 140-2 Level 3, which meets the statutory requirements.

The qualified electronic signature creation devices in which is generated and stored the private key of the Signatory/ the Creator shall have security level CC EAL 4+ , respectively FIPS 140-2 Level 3 or higher.

6.2.2 Control over the utilization and storage of private key

The private keys of the Certification Authorities of StampIT are stored and used only in the cryptosystem (HSM/Hardware Security Module) and are accessible for restoration and use only by authorized systems, which use them for signing the end clients' certificates and Certificates Revocation Lists (CRL). The basic certification authority of StampIT is in ‘‘Offline’’ mode.

For the management of the private keys of StampIT stored in the crypto module, three of five generated smart cards are required and respectively personal identification numbers (PIN) for access.

Initial keys archive is made – after the creation of all keys, and subsequently – after the regeneration of some of them. The private keys located in the cryptosystem (HSM) with security level FIPS 140-2 Level 3 are stored and archived in encrypted form and for their recovery are required three of the five generated smart cards upon the initial initialization of the crypto-module (HSM). After creation of the archiver (Backup), it is stored in a remote location with the required security measures.

The private key of the Signatory/Creator is used only in the device for electronic signature/seal creation device or on a device with an equivalent security level (as required by Regulation (EU) № 910/2014) and is accessible via a personal access code. Along with the generation of a key pair for the Signatory/Creator, storage of the private key is made on an electronic signature/seal creation device.

The Provider does not in any way store or archive the private key of a Signatory/Creator for electronic signature/seal creation.

6.2.3 Trusted storage of private key (escrow)

StampIT does not provide trusted storage of private key.

6.2.4 Private key storage

The private keys of the Certification authorities of StampIT are stored in encrypted form and for their decryption three of five generated smart cards are required and respectively personal identification numbers (PIN) for access.

The separate storage of the keys on several smart cards required for decrypting the private keys of the Certification authority and the controlled access to these devices prevents the keys from being compromised or being subjected to unauthorized reproduction outside StampIT.

The reproduction/ restoration of the private keys of StampIT on a reserve crypto module after a defect on the operational one is made only according to strictly controlled procedure, by order of the management of Information Services JSC and in the presence of at least two authorized persons each controlling the access to different smart cards.

StampIT does not store copies of the private keys of the operators of the Registration authority.

The Provider does not create copies of the private keys of the users. The private key of the Signatory/ the Creator shall be stored only on the qualified electronic signature/ seal creation device (QSCD) and may not be reproduced on another device.

In case of fault of a user's device for qualified electronic signature/ stamp, the Subscriber must replace it and request the issuance of a new qualified certificate.

6.2.5 Private key backup

The private key of the Certification authority, used for the creation of qualified electronic signatures/seals will be archived for at least 10 years after the expiry of its validity or after its termination. The same requirement applies also for the public key certificate corresponding to the private key after its expiration or after its revocation.

The expired or revoked certificates of StampIT shall be accessible on the official website of the Provider for at least10 years.

StampIT does not create backup copies of the private keys of the operators of the Registration Authority and the private keys of the end users.

6.2.6 Transfer of private key in a cryptographic module

Transfer of a private key in a cryptographic module is carried out in the following cases:

- In case of creation of mirror crypto-modules working in a cluster for the purpose of load balancing and high availability.
- In case of defective crypto module and the need to replace it with another.

The transfer of a private key in a crypto module is a specific operation. Such an operation requires appropriate measures and procedures to prevent the disclosure of the private key or its alteration and falsification during the operation execution.

The transfer of a private key in a cryptographic module requires a recovery of the key with a quorum three of five smart cards, which are generated upon the first initialization of the cryptographic module. The activities are performed according to strictly controlled procedure, by order of the Executive Director of Information Services JSC and in the presence of at least two authorized persons each controlling the access to different smart cards.

6.2.7 Storage of a private key in a cryptographic module

Depending on the cryptographic module used, the private keys of the Certification authority of StampIT are stored in encrypted form. Regardless of the private key storage form, it is not accessible to unauthorized persons outside the cryptographic module.

6.2.8 Private key activation method

Private keys of the Provider are activated via the individual parts of the keys, which are recorded on three of the five generated smart cards upon initialization of the cryptographic module (HSM). The protection of the private keys and their usage is carried out from the cryptographic module and the access to them is possible only after adding authorized clients via the administrative interface of the cryptographic module. Activation of the certification authorities /Root CA and SubCAs/, which use the relevant private keys of StampIT shall be carried out through the administrative interface of the system for certificates issue and management.

6.2.9 Private key deactivation method

A private key of the Certification Authority of StampIT, located in a cryptographic module (HSM) is deactivated by the suspension of the logical access to that key. The deactivation requires cleaning of the environment in which the key is stored and encrypted. This terminates the possibility for access and use of the private key. Each deactivation of private key of the Certification authority of StampIT is carried out by order of the Executive Director of Information Services JSC based on procedure with defined roles and responsibilities.

A private key of a Signatory/Creator is deactivated by deletion of the containers containing the private key of the device for creation of qualified electronic signature or through its physical destruction on the device. This terminates ultimately the possibility for access and use of the private key.

6.2.10 Evaluation of the cryptographic module

StampIT uses reliable cryptographic devices (Hardware Security Module/HSM), certified for security level FIPS 140-2 Level 3

6.3 Other aspects of the key pair management

The requirements described in this part of the Qualified Certification Services Practice Statement are applied to the procedures for public keys archiving and the procedures describing the validity terms of the user keys and the certification authority keys.

6.3.1 Public key archiving

The public keys of the Certification authorities are contained in the issued operating certificates of StampIT and are stored in an internal register. The public keys are accessible for the relying parties and the users by publishing the certificates in a repository accessible on the website of StampIT.

The public keys of the Certification authorities are archived and stored for a period of at least 10 years after expiration of the period of validity or termination of the relevant certificates.

The public keys of the Signatories/ Creators are contained in the certificates issued for them, which are published in the Public register on the website of StampIT.

The public keys of the Signatories/ Creators are stored and regularly archived.

6.3.2 Period of validity of qualified certificates and use of keys

Period of use of the public keys is determined by the values of the fields in its certificate describing the public key validity. The validity of the certificates and their relevant private keys may be shorted in case of revocation of the certificates.

Maximum periods of use of qualified certificates:

StampIT Global Root CA	20 (twenty) years
StampIT Global Qualified CA	20 (twenty) years
StampIT Global AES CA	20 (twenty) years
StampIT Global TSA	5 (five) years
StampIT Global OCSP	5 (five) years
Signatory/ Creator	up to 3 (three) years

When a signing key is used after its certificate's expiration, the signature is invalid.

Twelve months before the expiry of a Certification Authority's qualified certificate, the Provider shall issue a new qualified certificate and generate a new key pair. The certificate shall be made public in accordance with the procedures described in this document.

6.4 Activation data

The operations for private key activation of the Signatory/ Creator/ Subscriber are carried out by the Registration authority. The users use the access control to their private key by means of user's PIN.

6.4.1 Generation and installation of activation data

Activation data are used in the initial issuance of a certificate, on a signature/seal creation device, after a key pair generation. In such case the device is initialized and access codes are created: User code (User) and Administrator code ("SO"). These codes allow personal access and use of the private key generated and stored in the device and if necessary to unblock it.

The codes for access for qualified electronic signature/seal creation device are generated by the Signatory/Creator or a person authorized thereby or are provided randomly generated by the Registration authority codes in a sealed, opaque paper envelope.

In case that randomly generated personal access codes are provided in a sealed opaque envelope, the signatory shall change the initial user's access code through the software, which is provided together with the device.

The Provider recommends that the Signatory/ the Creator changes periodically its user's access code to the qualified electronic signature/ qualified electronic seal creation device.

The Provider shall use Administrative code /SO PIN/ for unblocking a blocked device.

6.4.2 Activation data protection

The signatory/ creator shall store and protect from compromising the access codes to the qualified electronic signature/ qualified electronic seal creation device.

Users must know that in case of a few unsuccessful attempts to access the device, it is blocked (locked). In such case the signatory/ the creator of a seal or its duly authorized attorney shall visit the Registration office of StampIT and shall present identity document and electronic signature/ electronic seal creation device. Operator of StampIT provides opportunity for new generation of PIN code on the part of the signatory/ the creator of a seal or provides a new randomly generated PIN code.

At the request of the signatory/ creator of a seal, StampIT may provide Administrator's access code (SO) for unblocking the blocked electronic signature/ electronic seal creation device.

The provider recommends that data for device activation are never stored together with the device itself.

6.4.3 Other aspects of activation data

Activation data must always be kept in a single copy. The personal identification number (PIN) for the access must be periodically changed. Activation data can be archived.

6.5 Computer systems security

StampIT uses only reliable and secure hardware.

The computer systems on which all critical components of the infrastructure of StampIT operate, are equipped and configured by means of local protection of the access to the software and computer data.

StampIT uses information security management procedures for its entire infrastructure in accordance with standards generally accepted in the international practice.

For higher reliability and security of the systems, the technical and cryptographic security of the processes performed by them, StampIT performs a number of tests and inspections of the equipment and technologies used.

Tests and inspections of computer systems are made in accordance with a methodology for security assessment (regarding: processors status – consumption, load, use, storage status; core memory state, padding in-out; status of storage, number of running processes; load balancing). They are made both periodically and upon any change affecting the infrastructure security.

For the computer systems' security management, StampIT takes into account the requirements of ISO/IEC 27001:2015.

Information Services JSC has valid Council of the integrated system for the management of quality, information security and services, which is the controlling authority on information security. The Board participates in the analysis of information risks and is convened to discuss any issues or incidents related to information security.

6.5.1 Degree of computer security

The degree of security of the systems used in the infrastructure of StampIT meets the legal requirements for the implementation of the activities of StampIT and is determined by the document Policy for information security of Information Services JSC.

6.6 Technological system life cycle security

6.6.1 Controls on the technological system development

The software applications used in the technological system of StampIT have been developed and implemented by highly qualified specialists. Before the introduction of new applications, they pass through the test period. The tests are made on separate systems, independent of those in regular operation in a specially developed test environment.

All hardware changes are monitored and recorded. Upon the purchase of a new technical equipment, it is supplied with the necessary operating procedures and instructions for use.

The technological security of the system is guaranteed as follows:

- technological equipment is delivered in a manner allowing its tracking.
- supply and replacement of technological equipment is made only with original hardware. The change is carried out by trusted and trained personnel.

6.6.2 Controls on the technological system security management

The purpose of security management control is to supervise the functionality of the technological system and to ensure that it functions properly and in accordance with the supplied production configuration.

The current configuration of the technological system of StampIT, as well as any amendments and updates to the system are recorded and performed under control. The controls allow continuous checks of the technological system integrity, timely updating, and troubleshooting.

6.6.3 Technological system life cycle security assessment

The Qualified Certification Services Practice Statement does not contain any requirements in this area.

6.7 Network security

The infrastructure of StampIT uses modern technical means of information exchange and protection to ensure the network security of the systems against external interventions and threats.

Servers and critical technological system of StampIT are separated in a protected internal local network.

The remote access to the Registration authority from the network of the infrastructure (PKI) of StampIT is performed by two-level protection of access with authentication and authorization. For that purpose is used specially installed and configured VPN server which accepts authentication through a user name and password, managed by the active directory of Information Services JSC or user name and password, which are issued/ respectively generated only for that purpose to authorized persons /external registration authority/ involved in the issuance of electronic signature/seal and infrastructure administration (Public Key infrastructure/PKI).

Subsequent authorization in the system for issuance and management of certificates is carried out through personal certificates issued on smart cards (HSM, tokens) from internal certification authority and with strictly defined roles. Activation/ deactivation of users in the system is carried out by security administrator, after approved by the information security managed (ISM) request for provision/ withdrawal of the access and order of the executive director of Information Services JSC for determination of the authorized persons..

The computer system of StampIT is protected against services failure in case of attacks. The security control was developed based on firewall and routers and proxy services traffic filtering. Attempts for intrusion in the system are monitored by the implemented IDS/IPS system. All alarms activated upon intrusion or potential intrusion, as well as attacks of the ‘‘Access denial’’ type are sent to the system administrators for analysis. Attempts for unauthorized access to the system are documented by the Intrusion Prevention System (IPS).

A detailed description of the network configuration of StampIT and the protection means of StampIT are presented in the technical documentation of the infrastructure. Documentation is accessible only by authorized persons.

6.8 Time stamping

StampIT issues time-stamp certificates in accordance with Regulation (EU) № 910/2014 and in full compliance with ETSI EN 319 422, ETSI TS 119 421, IETF RFC 3161 и IETF RFC 5816.

The qualified electronic time stamps issuance authority ‘‘StampIT Global TSA’’ is a separate and indivisible unit to the Certification Authority of StampIT in the structure of Information Services JSC.

„StampIT Global SA‘‘ (Time-stamping service) issued time stamp certificates in compliance with ETSI EN 319 422. By incorporating an object identifier: 1.3.6.1.4.1.11290.1.2.1.1 in the issued certificates for time stamping, StampIT confirms the compliance with the Policy for provision of time-stamping services (eIDAS-CP-TS). The object identifier is in compliance with ETSI BTSP (best practices policy for time-stamp) OID = 0.4.0.2023.1.1, according to ETSI EN 319 422.

The issued qualified electronic time-stamps (time-stamp tokens) are compatible with RFC 3161. The service issues RSA 2048 bit encryption time certificates with algorithm SHA256.

The qualified electronic time-stamps issuance authority ‘‘StampIT Global TSA’’ accepts requests for the issuance of qualified electronic time-stamps of a content of an electronic document presented by the Signatory or a Relying party. It prepares a qualified electronic time-stamp of the submitted hash value of an electronic document and allows for a further (after the period of validity of the qualified certificate of electronic signature/seal) demonstration against the recipient party of the fact of signing a statement or an electronic document

Qualified electronic time-stamps can be integrated into the process of creating or adopting a qualified electronic signature/seal, of electronically signed documents and electronic transactions, at electronic data backup, electronic notaries, etc. .

For the performance of its service „StampIT Global TSA‘‘ uses a private key stored in cryptographic module HSM with FIPS 140-2 Level 3, used for signing of requests and issuing time stamps. For the service may be used also more than one key pair for the purpose of increasing the service productivity.

The policy for provision of time stamp certificates (eIDAS-CP-TS) of the time stamping services „StampIT Global TSA‘‘ refers to ETSI EN 319 401 concerning the general requirements ordinary for each service of

StampIT. The policy is directed at meeting the requirements for time stamping with a long validity period (ETSI EN 319 122), but is applicable to any use with equivalent quality requirements.

The generating algorithm, the length of the signature key and the signing algorithm used for signing time-stamp certificates are in accordance with ETSI TS 119 312.

TSA certificate is issued by the operational certification authority of StampIT - StampIT Global Qualified CA corresponding to ETSI EN 319 411-1.

The time-stamp service uses a set of Stratum -1 NTP servers (Network Time Protocol/a protocol for computer systems' clocks synchronizing) as an independent source of accurate time. Through this configuration, TSS achieves accuracy of the time within +/- 500ms (half a second) or better of UTC. StampIT Global TSA guarantees the integrity and the authentication of TSU public key through TSU public keys, which are accessible for the relying parties in TSU certificates on the website of StampIT on: https://www.stampit.org. The certificates of time are recorded in a register which is published in the repository of StampIT and is accessible on the official website of the Provider. Link for access to the Time-Stamp service: http://tsa.stampit.org

7. Profiles for qualified certificates, CRL and OCSP

The profiles of the user qualified certificates and of the Certificates Revocation List (CRL) correspond to the format described in the ITU-T X.509 v.3.

A certificate of the X.509 v.3 type is a set of data which unequivocally certifies the public key belonging to the Signatory/ the Creator of the qualified electronic signature/ qualified electronic seal. The profile of OCSP complies with the requirements of RFC 2560, and the profile of the qualified time stamp certificate meets RFC 3161.

7.1 Profile of qualified certificates

In accordance with the X.509 v.3 standard, the electronic certificate is a sequence of the following fields:

- Version: version of the certificate (X.509 v.3);
- SerialNumber: unique identification code of the certificate;
- SignatureAlgorithm: identifier of the algorithm for the electronic signature creation;
- Issuer: distinguished name of the certificate issuer (DN);

- Validity: validity period, described by the date and time of the certificate issuance (notBefore) to the date and time of certificate's expiry (notBefore) (universal coordinated time, presented in Zulu format);
- Subject: distinguished name (DN) of the Signatory/Creator, subject to entry in the certificate;
- SubjectPublicKeyInfo: key identifier
- Signature: identifier of the algorithm for the electronic signature/seal creation, in accordance with RFC 5280.

7.1.1 Version

All certificates issued by StampIT are in accordance with Version 3 (X.509 v.3)

7.1.2 Eligible extensions in the format of a qualified certificate

The values of the extensions are created in accordance with the RFC 5280 recommendation. The function of each extension is determined by the standard value of the respective object identifier (IDENTIFIER):

- Subject Key Identifier - formed by the public key, verified in the certificate as a hash value of the public key;
- Authority Key Identifier - formed as a hash value of the public key of the operational Certification Authority of StampIT;
- Issuer Alternative Name - includes a URL-string as an alternative name of StampIT;
- Basic Constrains - determines the certificate type and has a value of ‘‘End entity’’ in the User authentication;
- Certificate Policy - determines the identifier of the Policy on qualified certificates of qualified electronic signature/seal;
- Key Usage - an attribute setting the restrictions on the certificate usage;
- Extended Key Usage - adds to the meaning of the ‘‘Key Usage’’ attribute and indicates additional and specific applications of the certificate;
- CRL Distribution Point - contains a link to the current CRL of the operational Certification Authority of StampIT;
- Authority Information Access - contains the URL-address of the OCSP server of the certificate;
- Qualified Statements - the attribute contains an instruction that the certificate is qualified and indicates whether the private key is generated and stored on electronic signature creation devices (QSCD).

7.1.3 Identifiers of electronic signature/seal algorithms

The attribute ‘‘Signature algorithm’’ identifies the algorithms (cryptographic mechanisms) used.

StampIT uses an applicable combination of asymmetrical and hash algorithms:

- sha256-with-RSA и sha384-with-RSA.

7.1.4 Naming forms

The naming forms are described in the ‘‘Types of names’’ part of this document.

7.1.5 Restrictions on names

The types of restrictions on the names are described in the ‘‘Types of names’’ part of this document.

7.1.6 Policy identifier

A qualified certificate issued in accordance with the Policy of StampIT, which fits into the attribute ‘‘Certificate Policy’’ of the certificate.

7.1.7 Extension identifier

This identifier (‘‘Extensions’’) provides specific information related to the service. For its use at this stage the Practice sets no restrictions.

7.1.8 Designation of the qualified certificate

StampIT, in the qualified certificate with profile under the X.509 v.3 standard, uses the ‘‘Qualified Statements’’ attribute with identifier: „esi4-qcStatement-1“ (OID=0.4.0.1862.1.1).

StampIT, in the qualified certificate for qualified electronic signature with profile under the X.509 v.3 standard, uses the ‘‘Qualified Statements’’ attribute with identifiers: „esi4-qcStatement-1“ (OID=0.4.0.1862.1.1) и „esi4-qcStatement-4“ (OID=0.4.0.1862.1.4).

StampIT, in the qualified certificate with profile under the X.509 v.3 standard, uses the ‘‘Certificate Policy’’ to which the identifier (OID) is assigned with a meaning, as follows:

	Name	Policy Identifier
Qualified certificate for signing client's time certificates	StampIT Global TSA	1.3.6.1.4.1.11290.1.2.1.1
Qualified certificate for qualified electronic signature for a natural person associated with a legal person	StampIT DocPro Certificate	1.3.6.1.4.1.11290.1.2.1.2
Qualified certificate for qualified electronic signature for a natural person	StampIT Doc Certificate	1.3.6.1.4.1.11290.1.2.1.3
Qualified certificate for qualified electronic seal	StampIT Seal Certificate	1.3.6.1.4.1.11290.1.2.1.4
Qualified certificate for advanced electronic signature for a natural person	StampIT Enterprise	1.3.6.1.4.1.11290.1.2.1.5
Qualified certificate for advanced electronic signature for a natural person associated with a legal person	StampIT Enterprise Pro	1.3.6.1.4.1.11290.1.2.1.6
Qualified certificate for advanced electronic seal	StampIT Enterprise Seal	1.3.6.1.4.1.11290.1.2.1.7
Qualified certificate for website authentication /domain validation/	StampIT Server DVC	1.3.6.1.4.1.11290.1.2.1.8
Qualified certificate for website authentication /organization validation/	StampIT Server OVC	1.3.6.1.4.1.11290.1.2.1.9
Qualified certificate for OCSP service	StampIT Global OCSP	1.3.6.1.4.1.11290.1.2.1.10

Other identifiers (OID), entered in the ‘‘Certificate Policy’’ attribute of the qualified certificates	Name	Policy Identifier
Certification policy for qualified certificates, issued for	qcp-public-with-sscd	OID=0.4.0.1456.1.1

public services, requiring the use of a secure signature-creation device (SSCD)		
Certification policy for qualified certificates, issued for public services	qcp-public	OID=0.4.0.1456.1.2
QCP-n: Certification policy of the European union (EU) for Qualified certificates, issued to natural persons	qcp-natural	OID=0.4.0.194112.1.0
QCP-l: Certification policy of the European union (EU) for Qualified certificates, issued to legal persons/organizations	qcp-legal	OID=0.4.0.194112.1.1
QCP-n-qscd: Certification policy of the European union (EU) for Qualified certificates, issued to natural persons with a private key,related to the certified public key, located at the QSCD	qcp-natural-qscd	OID=0.4.0.194112.1.2
QCP-l-qscd: Certification policy of the European union (EU) for Qualified certificates, issued to legal persons/organizations with a private key, related to the certified public key, located at the QSCD	qcp-legal-qscd	OID=0.4.0.194112.1.3
QCP-w: Certification policy of the European union (EU) for website authentication certificate	qcp-web	OID=0.4.0.194112.1.4
DVCP (Domain Validated Certificate Policy) according to ETSI TS 102 042	dvcp	OID=0.4.0.2042.1.6
OVCP (Organizational Validation Certificate Policy) according to ETSI TS 102 042)	ovcp	OID=0.4.0.2042.1.7

7.1.9 Using an identifier for an extension of the “critical” key

In the Practice there are no requirements for the use of „CRITICAL CERTIFICATE EXTENSIONS“.

7.2 Profile of the Certificate Revocation List (CRL)

CRL profile of StampIT:

StampIT Global CRL, StampIT Global Qualified CRL, StampIT Global AES CRL		
Version	Version 2	
Issuer Name	CN	
	C	
	L	
	O	
	2.5.4.97 /OrganizationIdentifier/	
Effective date	[Date of CRL issuance]	
Next Update	[Next update]	
Signature algorithm	Sha256/RSA	
CRL Number	[CRL number]	
Authority key identifier	[Issuing Authority Key ID]	
Revocation List	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]
	Reason code	[Revocation reason code] (optional)

7.2.1 Version

StampIT, through its Certification Authority issues, publishes and maintains Certificates Revocation List (CRL) in the X.509 v.2 format. The version is entered in the issued CRL.

7.2.2 Format

StampIT issues, publishes and maintains Certificates Revocation List (CRL), whose format is consistent with the requirements of the international recommendation RFC 5280.

SrampIt does not issue and support a scheme of ‘‘partial’’ (delta) Certificates Revocation List (CRL), but reserves the right, if necessary, to introduce such a scheme.

7.2.3 Basic attributes of the Certificates Revocation List (CRL)

- Version - version of the List;
- Issuer Name – Name of the List issuer (Certification authority);
- Effective Date/This update – date and time of the List (CRL) issuance;
- Next Update - time of the CRL validity. After that time, the Certification authority shall immediately issue a new list. During the period of validity, in the event of cancellation/revocation of a certificate, the Certification authority automatically issues a new CRL;
- Signature algorithm – identifier of the algorithm for creation of an electronic signature of the CRL;
- Signature hash algorithm – algorithm for the creation of an electronic signature.

7.2.4 Additional attributes of the Certificates Revocation List (CRL)

‘‘Authority Key Identifier’’ – identifier of the Certifying authority, issuing and signing Certificates Revocation List (CRL), contains the meaning of ‘‘subjectKeyIdentifier’’ from the certificate of the Certification authority.

7.2.5 Format of an element in the Certificate Revocation List (CRL)

The Certificates Revocation List (CRL) of the Certification authority contains elements of all revoked certificates. These elements are constant in the List.

The Certificates Revocation List (CRL) of the Certification authority contains elements of all each suspended certificate by the Certification Authority. This element is temporary in the list until the certificate resumption.

7.2.5.1 Attributes of an element in the Certificate Revocation List (CRL)

- Serial number - - serial number of a suspended certificate;
- Revocation date - time of the certificate suspension/ revocation;
- CRL Reason Code - code identifying the reason for suspension/revocation.

7.2.5.2 Indications of the reason for suspension/ revocation of a certificate

- **Key Compromise** – compromised is the private key corresponding to the public key included in the content of the qualified certificate, therefore there are no grounds to rely on this certificate.
- **CA Compromise** – compromised is the private key of the Certification authority, which is used for signing the qualified certificates of the subscribers;
- **Affiliation Changed** – changes in the legal person - the subject entered in the qualified certificate has already changed its status with regard to the legal person;
- **Superseded** – the qualified certificate has been superseded by another qualified certificate.
- **Cessation of Operation** – the activities, connected with the initial issue of a qualified certificate are terminated.
- **Certificate Hold** – the activity of the qualified certificate is suspended (certificate is invalid at present).
- **Unspecified** – the qualified certificate is revoked with specifying the reason when there is valid request for termination.

7.3 Profile of a response for online verification of a certificate status (OCSP/Online Certificate Status Protocol)

The Certification authority for validation ‘‘StampIT Global OCSP’’ of the operational certification authority StampIT Global Qualified CA of StampIT work and provide the qualified service ‘‘online real-time check of certificate status’’ in accordance with the internationally approved recommendation IETF RFC 6960.

The OCSP user sends a request to check the status of a signature/seal to the OCSP server and receives a response – a certificate of status, signed by the Validation authority. The reply contains information on the status of the inspected electronic signature/seal certificate, the validity period of the reply and has a testimonial character. The OCSP server which issues confirmations about the state of the qualified certificates has a specially generated key pair, issued especially for that purpose.

7.3.1 Version

StampIT, through its Certification authorities for validation, issues status certificates for the issued qualified certificates in a format, specified in the international recommendation RFC 6960. The version is entered in the issued status certificates.

7.3.2 Format

StampIT issues status certificates whose format is consistent with the requirements in the international recommendation RFC 6960.

7.3.3 Basic attributes of the status certificates

- Version - version of the status certificate;
- Response Type – type of the response on status;
- OCSP Response Status – status of the response;
- Responder Id - Identifier of the service for validation
- Produced At - date and time of issuing the status certificate;
- Responses – information, uniquely identifying the qualified certificate, for which the request was sent and for which the validation authority issues this status certificate;
- Cert Status – status of the qualified certificate for which the request was sent;
- This Update - time of an issued CRL, on the basis of which the status certificate was issued;
- This Update - – validity time of the CRL, on the basis of which the status certificate was issued;
- Response Extensions – additional extensions included in the response;
- OCSP Nonce - – contains the same information, submitted at the request in the Nonce field;
- Signature Algorithm - algorithm used for the electronic signing of the status certificate;
- Certificate –Contains the qualified certificate of the validation authority of StampIT.

The contents of the status certificate of StampIT are:

StampIT Global OCSP	
Signature Algorithm	SHA256/RSA

Issuer	CN	StampIT Global Qualified CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Validity	5 Years		
Subject	CN	StampIT Global OCSP	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	District
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature		
Friendly Name	StampIT Global OCSP		
Extended key usage (Critical)	OCSP Signing (1.3.6.1.5.5.7.3.9)		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global_qualified.crl		

Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.11290.1.2.1.10 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.stampit.org/repository/

7.4 Other profiles

7.4.1 Profile of the qualified electronic time-stamp

The certification authority for qualified electronic time-stamps ‘‘StampIT Global TSA‘‘ issues qualified electronic time-stamps (Time-Stamp Tokens/TST) with one or more private keys, reserved only for that purpose. According to the recommendation RFC 3280 the certificates for qualified electronic time-stamps, in their attributes extensions, contain a field for their usage limitation (Extended Key Usage), marked as critical. This means that the certificate may be used by ‘‘StampIT Global TSA’’ only for the purposes of signing the qualified electronic time-stamps, issued by this authority.

7.5 Basic fields in the profile of the qualified electronic time-stamps:

- Version – version (Version 3);
- Serial Number – – unique identification code of the time-stamp;
- Signature hash algorithm – algorithm for the electronic signature creation (sha256WithRSAEncryption)
- Issuer (Distinguished Name) – – name of the time-stamp issuer (StampIT TSA);
- Not before (validity period/beginning date) – issuance date and time (universal coordinated time, represented in Zulu);
- Not after (validity period ending/date) – validity term expiration date and time;
- Subject (Distinguished Name) – name of the Signatory/ the Creator;
- Subject Public Key Info - Encoded field in accordance with RFC 3280, containing information about the RSA public key (key identifier and public key value);

- Signature - electronic signature, generated and encoded in accordance with the requirements, described in RFC 3280;
- Basic Constraints – basic constraints of the time-stamp;
- Key Usage – usage of the time stamp;
- Extended Key Usage - Time Stamping Authority (TSA);
- Certificate Policies – policy on the basis of which the time-stamp was issued;
- Authority Key Identifier – – identifier of the Certification authority key ((SHA1 hash of the public key).

The Certification authority ‘‘StampIT Global TSA‘‘ accepts requests for time certification to meet the specifications of IETF RFC 3161 and ETSI EN 319 422:

- The request for a qualified electronic time-stamp must contain the algorithm of the SHA256 hash function;
- The request for a qualified electronic time-stamp points the identifier of the policy of StampIT Global TSA Policy OID.

The qualified electronic time-stamp, issued by ‘‘StampIT Global TSA’’ contains information about the stamp(TSTinfo structure), situated in the SignedData structure (see RFC 2630), signed by StampIT TSA andimplied in the ContentInfo structure (see RFC 2630).

8. Audit

Audit is systematic, independent and documented process to obtain audit evidence and their objective assessment to determine the extent to which the audit criteria are met; Audit criteria are a totality of policies, procedures or requirements used as a basis for comparison toward which are compared the evidence from the audit.

In Information Services JSC are carried out internal audits to determine whether the Integrated quality management system, the information security and services (ISS), the purpose of the control, the mechanisms for control, the processes, documents and records meet the requirements of the international standards ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, Regulation (EU) No. 910/2014, the statutory instruments, the requirements to information security, the requirements to IT services, whether they are implemented and maintained efficiently and whether they are performed according to the expectations. Internal audits cover all registration authorities in the structure of the Organization.The management of Information Services JSC

assigns the performance of regular internal audits for compliance of the activity with the approved Practices and Policies upon provision of certification services.

The management of Information Services JSC carries out ongoing operational control on the employees for the strict compliance of the operating instructions.

8.1 Audit planning

8.1.1 Internal audits

Internal audits are planned, conducted and documented according to procedure PU 08-01 Internal audits, which purpose is to determine the order and the procedure for performance of internal audits of the Integrated system of management of quality, information security and services in Information Services JSC.

The internal audits are carried out by audit teams, by preliminary prepared annual Programme for internal audits of ISU DK 08-01-01. The programme is prepared by the Management representative for the Integrated Management System with the assistance of the Information Security Manager and the Services Manager and is confirmed by the Executive Director. The annual programme for conducting internal audits is prepared in accordance with the condition and the importance of the audited zones and processes, which are carried out in them by taking into account the results from previous audits.

Upon preparation of the internal audits and determination of the audit team, the condition for independence of the auditors shall be considered to ensure their objectiveness and impartiality to the activity, which should be audited.

The management of Information Services JSC carries out ongoing operational control on the employees for the strict compliance of the operating instructions.

8.1.2 Compliance assessment audits

Information Services JSC is subject to audit by independent compliance assessment authority once a year.

The purpose of the audit is to confirm that Information Services JSC in the capacity of provider of certification services and the certification services provided by the Organization meet the requirements of Regulation (EU) № 910/2014, ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1.

Information Services JSC shall present to the Supervisory authority the compliance assessment reports related to Regulation (EU) № 910/2014, ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1.

The supervisory authority may at any time perform audit or request that an independent compliance assessment authority perform compliance assessment of Information Service JSC.

8.2 Qualification of auditors

The internal audit manager of the Integrated Management System may be an employee of the organisation with qualification of an auditor according to ISO 27001, ISO 9001 and ISO 20000-1.

The internal audits in the Information Services JSC are carried out by employees of the Organisation with qualification and experience of an auditor according to ISO 27001, ISO 9001, ISO 20000-1.

For the purposes of auditing, Information Services JSC has employees who possess the necessary expertise and knowledge related to public key infrastructure, with the reliable and secure operation of the technology system, information security, as well as the presence of a large practical experience in auditing.

The independent Authorities for compliance assessment are subject to accreditation by the relevant state authority for accreditation (IA Bulgarian Accreditation Agency). The system for accreditation and competence of the auditors are specified in Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93ISO/IEC 17065:2012 „Compliance assessment. Requirements to the authorities for certification of products, processes and services".

The supervisory board has the authorities to audit the certification services provider at any time through authorized experts.

8.3 Relations of the external auditors with Information Services JSC

Based on the principles of audit, the external auditors must be independent and objective and must not be directly or indirectly connected with the Information Services JSC and must not have any conflict of interests with the company.

The relations of the Information Services JSC and the external auditors shall be settled by contract.

8.4 Scope of the audit

The internal audits of Information Services JSC cover audit of the activity of the provider and the compliance with the Policy and the Practice upon provision of certification services, comparison of the practices and procedures indicated in this document with their practical realization upon performance of the activity of the Organization, inspection of the activity of the Registration authority, other circumstances, facts and activities connected with the infrastructure of Information Services JSC at the discretion of the management.

The scope of the internal audits also verifies the maintenance and the application of the requirements of the Integrated system for management of quality, information security and services in the activity of the structural units in compliance with EN ISO 9001:2008, ISO/IEC 27001:2013, ISO/IEC 20000-1:2011.

The inspection by the Supervisory body covers the statutory requirements for the activities of Information Services JSC according to the applicable legislation in the sector of qualified certification services.

External audit by the Compliance Assessment Body covers the entire activity of Information Services JSC for the provision of qualified certification services and implementation of all standards related to Regulation (EU) No 910/2014: Documentation; Archives; Information data related to the issuance and management of qualified certificates; Physical and information security and reliability of the technological system and management; Certification Authorities as well as with the requirements of the international standards ISO 27001, ISO 9001, ISO 20000-1.

8.5 Actions taken as a result of conducted audit

The reports of internal and external audits are documented in reports.

The audit reports are submitted to the management of Information Services JSC.

Audit report, prepared by compliance assessment authority, is submitted to the Supervisory body.

Based on the findings and the assessments made in the audit report, the management of Information Services JSC shall outline measures, terms and persons responsible for remedy of the reasons for identified inconsistencies and undertaking activities for remedy potential inconsistencies or other undesired events.

8.6 Storage of results

The results of the performed internal and external audits are stored in the Information Services JSC in the duly established order.

The certificates of Information Services JSC received from the compliance assessment authority are published on the website of the company.

9. Other business and legal issues

9.1 Prices

The prices of the qualified certification services, the prices of the hardware devices, which are offered in connection with these services, as well as the prices of the consulting services are indicated in the Price List of Goods and Services provided by Information Services JSC as a provider of qualified certification services, which is approved by the executive director of Information Services JSC and is publicly accessible on https://www.stampit.org.

Information Services JSC is entitled to change the prices by publishing the updated Price list of https://www.stampit.org. The new prices enter into force on the date of publication unless in the Price list is specified another later date.

9.1.1 Price of the contract for qualified certification services. Invoicing and payment

The price under the contract for qualified certification services includes prices of goods and services, which are included in the scope of the contract:

- the price for issuing/ renewal and use of the qualified certificate;
- the price of the hardware devices, which are provided in connection with the certification services (if applicable);
- the price of other services, which are provided in connection with the certification services (if applicable);

Payment of the price under the contract for qualified services is carried out by the Subscriber by one of the following methods:

1. in cash or through POS terminal (if such is available in the Provider's office) - upon contract conclusion. These methods of payment are possible for all Subscribers;

2. by bank transfer – within 3 (three) – days after conclusion of the contract and issuing an original invoice. Payment is made to the bank account of the Provider specified in the invoice. This method of payment is possible only for Subscribers - legal persons or sole traderships. In case that the

Subscriber fails to carry out payment in the agreed term, the contact and the certificate(s) shall be revoked.

In case of earlier revocation of the qualified certificate and/ or the contract for qualified certification services for reasons beyond the responsibility of the Provider, price refund shall not be due to the Subscriber for the remaining term of the revoked qualified certificate.

The price under the contract for qualified certification services does not include the expenses of the Subscriber for bank transfers and for assurance of communications of the Subscriber in connection with the use of the qualified certification services. These costs are due by the Subscriber to the provider of the relevant service.

Upon provision of consulting services the total price due is determined on the basis of the worked time, based on signed record of handover for the provided services and shall be paid within 3 (three) days after signing the record and issuing an original invoice.

The provider issues invoice for the services according to the national law.

In case of late payment after expiration of the term, specified in the contract for qualified certification services, the Subscriber shall pay to the Provider compensation equal to the legal interest in case of full repayment of the obligation.

9.1.2 Free services for the Subscribers/ the Relying parties

Information Services JSC shall provide free access to the following services connected with the issuance and the use of qualified certificates:

- check-up of a certificate published in the Register of issued qualified certificates;
- validity check-up of an issued certificate;
- Real-time verification of the status of a certificate;
- issuing time certificate for provided content/ electronic statement through user interface by Subscriber of StampIT holding a valid qualified certificate;
- download of valid Certificate Revocation List (CRL);
- access to the archive of Certificate Revocation List (CRL);
- download of the operational certificates of StampIT;
- download of public documents of StampIT;
- other services

9.1.3 Return of certificate and price refund

When the issued qualified certificate contains gaps or errors, the signatory/ the creator respectively the subscriber may object within 3 days after its publication in the register of the issued certificates.

If the gaps or errors are omitted due to gaps or errors of the operator of the Registration authority, they shall be remedied immediately by the provider through issuing a new qualified certificate without paying a fee.

If gaps or errors are omitted due to submission of incorrect data by the Subscriber, the qualified certificate shall be revoked and the Provider shall not refund price.

When the Subscriber refuses to accept the issued qualified certificate with true content, the qualified certificates shall be revoked and no price refund shall be due.

9.2 Financial liability

StampIT shall not be liable for the provided qualified certification services to the signatory of electronic signature/ the creator of stamp/ to the subscriber and to any third persons who rely on the qualified certificates issued by StampIT.

StampIT will be responsible for all damages causes through its fault or through the fault of any external Registration authority.

In case of any damages for which StampIT is liable, it will pay compensation to the Subscriber up to the amount of the damages.

StampIT shall not be liable for damages that occurred as a result of usage of qualified certificate in the period of it validity (between the start date and the end date of validity) and only if there are no circumstances excluding the liability of StampIT.

9.2.1 Guarantees for payment of compensations

In connection with the risk for liability for caused damages in compliance with Regulation (EU) № 910/2014 StampIT shall maintain sufficient financial resources and/ or shall conclude appropriate liability insurance in accordance with the national law. Upon conclusion of insurance contract StampIT shall publish information for the insurer and and the term of the insurance on the website of StampIT.

9.2.2 Procedure for payment of compensations

The term for submission of any claim by subscribers or relying parties to StampIT or the insurer is 7 (seven) days after the date of becoming aware of damage occurrence. StampIT shall also cover claims, which are laid within 15 (fifteen) days after the end date of validity of the qualified certificate and is based on damages that occurred during the validity of the certificate.

The subscribers shall:

- send immediately notice in writing for any identified error and damages by registered letter or courier service;
- render assistance to StampIT and the insured of StampIT it order to establish the facts confirming the claim for compensation.

9.2.3 Maximum limit of compensation

For the purpose of limiting the activity of the qualified certificates, StampIT shall determine the maximum limit of compensation for incurred damages caused by the use of a qualified certificate issued by it, up to the maximum limit determined according to the national law.

StampIT may refuse payment of amount exceeding the maximum limit of the compensation for damages.

In the relations of StampIT with the subscribers and all third parties will apply these limits of compensation and conditions, which are in force as at the date of damage occurrence.

9.3 Confidentiality of business information

StampIT observes all applicable rules for protection of the information collected with the view of the business.

9.3.1 Confidential information

StampIT considers confidential any information contained in:

- contract for qualified certification service;
- archives of requests for qualified certificates and qualified electronic time stamps;
- archives of transactions;
- records of external and internal audits and reports (except reports which are public);

- emergency response and disaster recovery plans;
- internal tracking and records of operations of the infrastructure of StampIT, the management of qualified certificates, services of entry and data.

StampIT will not disclose or will not be required to disclose confidential information without available authenticated reasonable request by the Signatory/ the Creator. the Subscriber or another authorized party, which contains:

- the party to which StampIT imposes the responsibility for keeping the confidentiality of information;
- the party requesting such information;
- disposal or decision of authorized bodies, if any.

9.3.2 Non-confidential information

Non-confidential is any information included in the contents of the qualified certificates and in the Certificate Revocation List (CRL).

The following information in the repository is available to the public:

- Current and previous versions of all documents that are subject to publication including: Qualified Certification Services Practice Statement of Information Services JSC, Policies for provision of qualified certification services, Policy for provision of time stamping services, rules, procedures and documents, which are intended for the Subscribers and the Relying parties;
- Audit reports carried out by the compliance assessment authorities and the supervisory authorities;
- Additional information, which the provider has to publish.

9.3.3 Protection of confidential information

Information Services JSC shall store confidential information in strict compliance with the policies and the procedures for the Integrated Management Systems of Information Services JSC.

The subscriber under the contract for qualified certification services shall not disseminate or allow dissemination of confidential information, which has been provided to its in connection with the contract conclusion and performance, without the consent of StampIT.

9.4 Personal data privacy

Information Services JSC is a personal data administrator registered according to the national law and ensures lawful processing of personal data, provided in connection with the qualified certification services, in compliance with Directive 95/46/EU and the national law.

Personal data are collected, stored and processed in compliance with the rules for confidentiality contained in the Instruction on the measures for personal data protection, approved by the executive director of Information Services JSC.

9.4.1 Privacy statement

Information Services JSC stores and processes the personal data that have been provided to it in the capacity of qualified provider of qualified certification services in accordance with the Personal Data Protection Act.

The type and the quantity of the collected personal data are consistent with their purpose and use. Personal data are used only in connection with the provision of qualified certification services.

9.4.2 Personal Information

Information Services JSC accepts that each information about the Subscribers, which is not publicly accessible according to item 9.3.2 is personal.

Information contained in the qualified certificates published by StampIT is not considered personal information.

9.4.3 Responsibility for personal data protection

Information Services JSC is responsible for the protection of the personal data of the Signatory/ the Creator/ the Subscriber and the authorized persons and does not allow their disclosure to third persons. Providing access to personal information is only in accordance with the requirements of the Personal Data Protection Act.

9.4.4 Consent for use of personal data

Unless otherwise specified in the relevant Policy, the personal data of the Signatory/ the Creator/ the Subscriber and the authorized persons may not be used without their consent except in the cases provided for by law.

9.5 Intellectual property rights

Data included in the qualified certificates issued by StampIT or published in the Public Register/repository are subject to intellectual property rights and other tangible and intangible rights. Relations on the occasion of these rights shall be governed by the national law.

All rights on trademarks used by Information Services JSC are and remain property of the company.

Information Services JSC holds the intellectual property rights concerning the database, the websites, QES of StampIT and any other publications made by StampIT including this CPS.

All rights on names and trademarks used by the subscribers, included in the content of the qualified certificates, shall remain for their holder and their inclusion in the content of the qualified certificates and their use for the provision of certification services is not considered a breach.

9.5.1 Right to ownership of data in qualified certificates

Qualified certificates are property of StampIT. StampIT allows that the qualified certificates are reproduced and distributed free of charge and without exclusive right provided that they have been reproduced and distributed entirely. This does not refer to qualified certificates, which should not be published in any public storages or directories without the explicit written permission of StampIT.

The scope of such restriction aims to protect the subscribers from unauthorized publication of personal data specified in the qualified certificate.

9.5.2 Right to ownership of names and trademarks

Information Services JSC is the owner of the trademark StampIT registered according to the national law. The trademark may not be used by third persons without the explicit consent in writing of Information Services JSC.

The subscribers of StampIT, when they provide to StampIT and use domain and distinguished name (and any other information upon submission of a request), must not violate the rights of third parties with regard to their trademarks, trade names and other intellectual property rights.

The subscribers of StampIT reserve the rights on the names and trademarks, which are their property and are included in the content of the qualified certificates.

9.5.3 Right to ownership of a key pair

Private and public keys are property of the subscribers who use them and store them correctly.

Secret parts of the private keys of StampIT are property of StampIT.

9.6 Obligations and guarantees

The obligations, liabilities and guarantees of the Provider, the Subscribers and the relying parties are settled in Regulation (EU) № 910/2014, in the national law, in this Practice, in the Policies of the Provider, in the contracts for qualified certification services as well as in other documents of the Provider only to the extent they are publicly declared and accessible.

The contracts for provision of qualified certification services shall be concluded in writing in compliance with Regulation (EU) No. 910/2014, in the national law.

9.6.1 Obligations, liability and guarantees of StampIT

Up to the level determined in the relevant section of the CPS, StampIT shall:

- observe this CPS and its internal and public policies and procedures;
- observe Regulation (EU) No. 910/2014 and the national law
- ensure the infrastructure and the certification services including the building and commissioning of the storage and the website of StampIT for provision of certification services
- ensure reliable mechanisms including the mechanism for generation of keys, the protected mechanism for electronic signature creation and the procedures for distribution of the secret parts with regard to its own infrastructure
- notify the parties in case of compromising of its private keys
- make available publicly the procedures for declaring different types of qualified certificates

- issue and renew qualified certificates in compliance with this CPS and shall meet the obligations specified in it;
- upon receiving the request of the Registration authority, issue and renew qualified certificates in compliance with this CPS;
- upon receiving request for revocation of a qualified certificate by the Registration authority, revoke the certificate in accordance with this CPS
- publish the qualified certificate in accordance with this CPS;
- provide support to subscribers and relying parties as described in this with this CPS;
- revoke, suspend and resume the qualified certificate in accordance with this CPS;
- ensure information about the expiration of the term of validity and resumption of the qualified certificate in accordance with this CPS;
- provide copies of this CPS and its valid documents for public access.

StampIT declares that it has no other duties under this CPS.

StampIT is liable to the signatory of electronic signature/ the creator of a seal/ respectively to the Subscriber and to all third persons for any damages caused by:

- non-observance of the statutory requirements to the activities of the certification services provider;
- non-observance of the obligations of the certification services provider according to Regulation (EU) No. 910/2014 and the national law governing the issue, the management and the content of the qualified certificate;
- incorrect or missing data in the qualified certificate as at the time of its issuing
- algorithmic non-conformity between the private key and the public key entered in the qualified certificate
- unavailability at the time of issuing the qualified certificate of the private key corresponding to the public key with the person indicated as Signatory/ Creator;
- omissions in the establishment of the identity of the Signatory/ the Creator/ the Subscriber.

9.6.2 Obligations, liability and guarantees of the Registration authorities

The Registration authorities of StampIT shall have the following obligations:

- to receive requests for the issuing and renewal of qualified certificates of StampIT in compliance with this CPS;
- perform all activities prescribed by the procedures of StampIT and this CPS;
- receive, verify and submit to StampIT requests for revocation, suspension and resumption of the validity of the qualified certificate issued by StampIT in compliance with the procedures of StampIT and this CPS;
- observe this CPS and its internal and public policies and procedures;
- observe Regulation (EU) No. 910/2014 and the national law
- use reliable and secure devices and software;
- strictly perform the procedures for correct identification of requestors,
- enter correctly the data in the database of EUROTRUST and update this information at the time of data confirmation'
- enter correctly the information contained in the certificates;
- ensure personal data protection in compliance with the Personal Data Protection Act.
- ensure storage of the private keys of the operators in accordance with the requirements for security laid down herein;
- ensure that the private keys of the operators are used only for the purpose indicated in this CPS

In the cases when the obligations of the Registration authorities are assigned to external persons (legal or natural persons), they shall the following obligations in addition to the above specified:

- to observe the rules and procedures of StampIT for verification of identity, respectively the identity and the representative authority of the requestors of qualified certificates and the compliance of the data and circumstances regarding the service users;
- to follow strictly the sequence and to request and verify all required documents according to the standard procedures described in details in this CPS;
- to ensure access to all places and activities, including archives of documents and technical equipment connected with their activity as Registration authorities/ network of registration authorities, upon performance of overall audits or sudden and thematic audits as well as upon performance of audits and inspections by the controlling authorities determined according to the national law without hindering or preventing in any manner the auditors;
- to ensure the required technical equipment in connection with the performance of their activity as Registration authorities of StampIT;

- At the end of each quarter to send to the Provider a list of all documents presented with regard to submitted requests for issuing of qualified certificates;
- to observe strictly the internal rules and procedures of StampIT in connection with the collection, storage and archiving of documents under submitted requests and issued qualified certificates;
- not to disseminate to the third parties and not to use unlawfully any commercial secrets, know-how or other confidential information of which they have become aware upon performing their activity as Registration authorities.

9.6.3 Obligations of subscribers

Unless otherwise specified in this CPS, the subscribers of StampIT bear full responsibility for the following:

- to be aware of the use of qualified certificates
- to provide true, correct and full information to StampIT
- to become aware of and accept the terms and conditions of this CPS of StampIT and the related documents published in the storage of StampIT
- to use the qualified certificates issued by StampIT only for legal purpose and in compliance with this CPS of StampIT;
- to notify StampIT or the Registration authority of StampIT for changes and gaps in the provided information
- to stop the use of the qualified certificate if any part of the information proves to be obsolete, changed, incorrect or untrue
- to stop the use of the qualified certificate if it has expired and to uninstall it from the applications or devices where it has been installed
- to prevent compromising, loss, disclosure, modification or other unauthorized use of the private key, which corresponds to the public key published in the qualified certificate through reliable protection of the personal identification code (PIN) for work with the key pair and/ or the physical access to the carrier storing the key pair.
- to declare termination of the qualified certificate in case of any doubts concerning the integrity of the issued certificate
- to declare termination of the qualified certificate if any part of the information included in the certificate proves to be obsolete, changed, incorrect or untrue

- for missions or omissions of third parties to whom they have unlawfully provided their private key
- to refrain from provision to StampIT of materials with defamatory, lewd, pornographic, offensive, fanatical or racial character

9.6.4 Obligations of the relying parties

The party that relies on a qualified certificate issued by StampIT shall adhere to the following generally recognized rules in the international practice:

- to be aware of the use of qualified certificates
- to be aware of the restrictions on the use of qualified certificates laid down in the Policy on which basis the relevant certificate has been issued;
- to become aware of the conditions of the CPS of StampIT;
- to verify the qualified certificate issued by StampIT by using any permissible means as well as CRL (including StampIT CRL);
- to rely on the qualified certificate only to the extent reasonable for the specific circumstances;
- to use mechanism for secure verification of the electronic signature/ electronic seal, which guarantees: verification of the public key, verification of the private key, verification of the content of the signed electronic document; verification of the authenticity and validity of the qualified certificate as at the time of signing, the correct presentation of the results from the verification and the possibility to establish any changes relevant to the security.
- Information Services JSC shall not be liable for any damages that have occurred for the Relying party due to failure to render due care.

9.6.5 Obligations of other parties

9.6.5.1 Obligations of the qualified time-stamping authority

The Qualified Time-Stamping Authority StampIT Global TSA issues qualified time-stamping certificates in accordance with the requirements laid down in Regulation (EU) No 910/2014, the applicable standards and the national law and upon observance of the relevant Policy.

Upon provision of the service, StampIT:

- uses the technology for binding the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
- base itself on an accurate time source linked to Coordinated Universal Time;
- uses reliable devices and software in compliance with the requirements of the applicable technical standards and recommendations;
- sign with qualified electronic signature of StampIT;
- provides opportunity for proving in subsequent period of time (upon expiration of the period of validity of QETS) of the fact of signing/ sealing an electronic document/ another object;
- provide uninterrupted access (24/7/365) to the service (except the time for technical preventive maintenance);
- issue qualified electronic time stamps in compliance with ETSI EN 319 422 Time-stamping protocol and electronic time-stamp profiles.

9.6.5.2 Obligations of the qualified operational Certification authority for qualified electronic signatures/ qualified electronic seals

The qualified operational Certification authority for qualified electronic signatures/ qualified electronic seals StampIT Global Qualified CA carries out its functions in accordance with the requirements laid down in Regulation (EU) No 910/2014, the applicable standards and the national law and in compliance with the relevant Policy and the technical requirements for creation and verification of qualified electronic signatures/ seals.

The procedures apply by StampIT exclude any opportunity for tampering the certificates or data.

9.6.5.3 Obligations of StampIT regarding the public registers / the repository

StampIT manages and controls the public registers as follows:

- publishes and archives qualified certificated of the Qualified Root Certification Authority "StampIT Global Root CA", Qualified Operational Certification Authority StampIT Global Qualified CA", Qualified Time-Stamping Authority StampIT Global TSA and Qualified Certification Authority for verification of the status of the certificates „StampIT Global OCSP";
- publishes and archives the policies and the practice statements upon provision of qualified certification services, forms of contracts for qualified certification services, the general terms and conditions, lists of Registration authorities, reports from audits performed by the

compliance assessment authorities and supervisory authorities as well as other documents connected with the activity of qualified provider of qualified certification services;

- provides access to issued qualified certificates only in cases where the subscriber has not expressed disagreement for publication;
- provides access to information concerning the status of the qualified certificates; by publishing Certificates Revocation List – CRL.and through the interface about the status of issued qualified certificates – OCSP;
- provides non-stop access to the information in the public register of a Certification Authority, Registration Authority, subscribers and relying parties;

The parties (including subscribers and relying parties), which have access to the repository and the website of StampIT accept the clauses of this CPS and the other terms of use specified by StampIT, except the information, which is provided in demonstration and test qualified certificates. The parties accept the conditions of use when the make inquiry about the status of the qualified certificate or by using or relying on the provided information or services.

9.7 Waiver of liability

StampIT shall not be held liable also in cases of any damages caused by:

- specific commitments of the subscriber, for example assuming responsibility to a third party, liquidated damages and etc.
- compensations for legal, administrative and disciplinary penalties as well as legal expenses awarded to the subscriber;
- declaring the subscriber or a third party insolvent;
- delay or inability of the subscribers to submit request for termination of the validity of a qualified certificate of StampIT;
- failure of the subscribers to render the due care to prevent compromising or loss of the private key;
- non-observance on the part of the subscribers of the requirements and the obligations indicated in the Qualified Certification Services Practice Statement (CPS);
- failure to verify a subscriber's electronic signature;

- failure to apply appropriate measures for security before and during the creation and further processing of encrypted messages;
- unlawful actions on the part of the subscribers and third parties. StampIT is entitled to compensation for damages caused as a result of such unlawful actions;
- damages that are beyond the control of StampIT, including power supply and telecommunication failures beyond the control of StampIT;
- the use of qualified certificates for the operation of sensitive equipment including but not limited to: nuclear equipment, navigation or communication systems in the aviation, air traffic management systems, arms management systems and any cases that may result in death, bodily injuries or may cause harm to the environment;
- misuse on the part of the subscribers and third parties of Internet, telecommunications or added value networks, including by using or reproducing computer viruses;
- force majeure circumstances.

9.8 Limitation of Liability

The maximum limit of compensation for incurred damages caused by the use of a qualified certificate issued by StampIT, is up to the maximum limit determined according to the national law.

9.9 Liability of the Subscriber

The Subscriber/ Signatory/Creator shall be held liable to the Provider and all relying persons:

- if in creating the key pair he/she has used an algorithm and electronic signature/electronic seal creation devices that do not meet the requirements of Regulation (EU) No 910/2014;
- if he/she has not complied with the security requirements, specified by the Provider;
- if he/ she has not requested suspension and revocation of the certificate after he/she has become aware that the private key was used improperly or is in danger of unauthorized use;
- for any false statements made upon the issuance of the qualified certificate;

The subscriber/ the signatory/ the creator shall be liable to the Provider:

- when he/she has not stored properly the private key corresponding to the public key specified in the certificate.

- if upon the issuance of the qualified certificate it has provided incorrect data/ has concealed data, which are relevant to the content or to the procedure of issuing the certificate.

9.10 Term and termination of this document

This Practice enters into force when approved by the executive director of Information Services JSC and its publication on website: http://www.stampit.org/repository/.

This document may be amended by Information Services JSC at any time and each change shall be entered in the new updated version of the document, which enters into force after its publication on website: https://www.stampit.org/repository/.

N respect of the Subscribers and third parties will only be valid the version applicable as at the time of using the services of Information Services JSC.

The validity of the Practice shall be terminated upon termination of the activity of StampIT.

Upon termination of the validity of a version of this document, it shall be stored in the repository of documents of StampIT.

9.11 Notices and communications

The communication between StampIT and the Subscribers/ the Signatories/ the Creators, the relying parties and third persons may be carried out by mail, telephone, fax and network protocols - depending on the type of the exchanged information and used services.

Information about breaks in security as well as any other information, which is subject to public disclosure, shall be announced on http://www.stampit.org.

9.12 Amendments of the Practice

If any clause of this CPS or its application proves to be invalid or unenforceable to specific extent or for any reason, the remaining part of the conditions of this CPS (and the application of this clause concerning other persons or circumstances) will be interpreted in such manner that they meet the national law and the initial intentions of the parties.

Each clause of this CPS, which provides for limitation of liability, rejection or limitation of guarantees or other obligations or exclusion of damages is considered by the parties to be independent and separate from the other clauses and must be applied as such.

The Provider may proceed to amendments in the Practice in case of regulatory, technological and procedural changes.

Amendments to the Practice, which result in new revisions or new versions of the document are published on: https://www.stampit.org/repository/.

9.13 Procedures for resolution of disputes

Disputes between the Provider and the Subscribers connected with qualified certification services of Information Services AD first will be settle by mutual agreement.

Information Services JSC will consider only claims in writing sent to: Sofia city 1504, Oborishte region, 2, Panayot Volov Str., fax +359 2 943 6607.

The claims will be considered by the legal department of Information Services JSC. The claimant shall receive a response to his/ her claim within 14 days.

If it is impossible to settle the dispute by negotiations within 30 days, the parties may refer the dispute for resolution to the relevant competent court based in Sofia.

9.14 Governing law

For any matters unsettled in this Practice will apply the national law.

9.15 Compliance with the applicable law

This CPS is issued and interpreted in compliance with Regulation (EU) No. 910/2014 and the national law. The choice of law is made to guarantee non-contradicting interpretation of this CPS regardless of the place of residence or the domicile of the subscriber or the place of use of the qualified certificate or other products and services provided by StampIT. The national law applies to all contractual relations of StampIT, in which this CPS may be applied in connection with the products and the services of StampIT.

9.16 Other provisions

The Practice does not specify other provisions.