ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

stampit

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

Provision of qualified certification services by
Information Services JSC

POLICY
for provision of qualified certificates for advanced electronic signature and advanced electronic seal (eIDAS-CP-AES)

Version: 2.0
Publication date: 07.06.2017
Last revision date: 07.06.2017

Contents

Information Services JSC
Sofia, 2, Panayot Volov Str.
tel. 02/ 9420340
fax 02/ 9436607
Company number (EIK) 831641791

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 an advanced 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
Qualified 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 an advanced 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
Qualified 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 audiovisual recording
Certificate for website authentication	An attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued
Qualified certificate for website authentication	A certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV 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).

CA	Certification authority
RA	Registration authority
RSA Rivers-Shamir-Adelman	Criptographic algorithm (asymmetric)
SHA2 Secure Hash Algorithm	Hash function
SHA256/RSA Signature algorithm	Algorithm for creation of advanced electronic signature by IO JSC
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	Advanced electronic signature/ seal creation device
NCP+	Extended normalized certificate policy, which includes additional requirements for qualified certificates in compliance with Regulation (EU) No. 910/2014
Common Name (CN)	public name
Certificate Policy (CP)	Policy for provision of qualified certificates for electronic signature, electronic seal and website authentication
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

1. Introduction

This document describes the general rules that Information Services JSC applies upon issuing and managing qualified certificates for advanced electronic signature and for advanced electronic seal as well as the applicable services and the scope of applicability.

For the issuing of qualified certificates for advanced electronic signature and for advanced electronic seal shall apply procedures and practices guaranteeing the highest level of security upon issuing, publishing and management of the issued qualified certificates.

1.1. Policy overview

This policy refers to the qualified certificates for advanced electronic signature and for advanced electronic seal issued by Information Services JSC in compliance with Regulation (EU) № 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 in accordance with the applicable law of Republic of Bulgaria.

The document has been structured in accordance with the recommendations defined in IETF RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

The policy is consistent with the following documents:

- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- ETSI EN 319 411-2 v2.1.1 „Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates";
- ETSI EN 319 412-5: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 5: QCStatements";
- ETSI TS 101 456: „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

Issuing qualified certificates for advanced electronic signatures and advanced electronic seals refers to:

- issuing qualified certificate to a natural person (signatory) - this is a qualified certificate for advanced electronic signature;
- issuing qualified certificate for advanced electronic seal of a legal person (creator of a seal) - this is a qualified certificate for advanced electronic seal.

The access to this document is public and its current version is published on the website of StampIT https://www.stampit.org.

Information Services JSC reserves the right to amend this document at any time and each amendment shall be entered in the new version of the document published as mentioned above.

1.2. Policy name and identifier

The issued certificates shall contain policy identifier issued in accordance with recommendation IETF RFC 3647 [I.4], clause 3.3, which may be used for their identification by the Relying parties when they are used.

The policy identifiers of qualified certificates mentioned in this document are as follows:

QCP-n

Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)

QCP-l

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)

Object identifiers (OID) in compliance with the type of the issued certificates are as follows:

Type of certificate	StampIT Policy Identifier	ETSI Policy Identifier
StampIT Enterprise Certificate	1.3.6.1.4.1.11290.1.2.1.5	0.4.0.194112.1.0
StampIT Enterprise Pro Certificate	1.3.6.1.4.1.11290.1.2.1.6	0.4.0.194112.1.0
StampIT Enterprise Seal Certificate	1.3.6.1.4.1.11290.1.2.1.7	0.4.0.194112.1.1

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.

1.3.1. Certification authority

StampIT is the Certification authority of Information Services JSC, which issues qualified certificates for advanced electronic signature (QES-advanced) to natural persons, qualified certificates for advanced electronic signature (QEST-advanced) to legal persons and qualified signatures for advanced electronic seal (QESeal - advanced). The certification authority carries out the activities, which include the issue, renewal, suspension, resumption and revocation of qualified certificates, keeping registers and providing access to them.

1.3.2. Registration authorities

The certification authority issues QES-advanced and QEST-advanced 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 in accordance with the internal rules of StampIT;
- 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 physical 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 electronic signatures/ advanced 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.

1.4. Applicability and restrictions for the use of the issued qualified certificates

1.4.1. Applicability

Issued qualified certificates for advanced electronic signature and for advanced electronic seal may be used for the creation of electronically signed documents and/ or transactions in information systems guaranteeing high level of information security.

1.4.2. Restrictions

It is forbidden to use the issued qualified certificates in any manner or for any purpose other than those specified in this policy. It is forbidden to use the issued qualified certificates for performance of activities that are restricted by the law of the Republic of Bulgaria and the applicable regulations and directives of the European Union.

1.5. Approval, control of versions and content of this policy

The policy is developed by qualified employees of Information Services JSC in compliance with the applicable regulatory documents in this area. Each new version shall take effect after its coordination with the Legal Department, the director of the Technical Directorate and after its approval by the Executive Director of Information Services JSC.

The approach to the control of versions shall include incrementing a major version (upon applying major amendments in the document) and incrementing a minor version - point release - for remedy of technical errors and discrepancies.

After approval of a version, it shall be published immediately on the website of StampIT.

The users (subscribers and relying parties) shall refer to the current version of this policy as at the time of using the services of the provider.

Contact details for StampIT:

11, Lachezar Stanchev Str. Izgrev

1756 Sofia, Bulgaria

Tel.: + 359 2 9656 291

Fax: + 359 2 9656 212

Web: https://www.stampit.org

E- mail: support@mail.stampit.org

2. Public registers and management

2.1. Maintained public registers

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.

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

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

2.2. Refresh frequency

Frequency of refreshing the published qualified certificates is as follows:

	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 certificates	https://stampit.org	real time

2.3. 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 shall be accessible 24 hours per day and 7 days per week except in case of events beyond the control of StampIT.

3. Identification and check of identity data

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.

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

Issuing qualified certificate by using „pseudonym" is made only after the Registration authority collects the required statutory identifying information.

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 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.

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

- legal person (creator of a seal) - verification in the relevant registers based on submitted EIK, respectively BULSTAT;
- authorized representative of a legal person (Signatory) - verification and certification "True copy" and signature on the required documents.
- natural person (signatory) - present in person with identity document
- the required documents may be presented also in absentia (through an authorized representative) - 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

- 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).

3.2. Initial registration

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

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

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.

In case that the verification is impossible, the following shall be presented to an employee of RA:

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

3.2.3. Verification of natural persons, legal persons, representatives of a legal person

The verification of the identity of a legal person aims to prove that during the consideration of the application the legal person exists and that the legal representative who applies for qualified signature has the representative authority to request the issuing.

The following must be presented to an employee of the RA:

- Identity document of the natural person to whom QES - advanced is issued, which is associated with the legal person - original;
- Document/ power of attorney from which ensues the representative authority of the natural person for the legal person - original and copy certified by the applicant. 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 employees of the RA by presenting to the RA 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. Verification by the certification authority

After the successful completion of the identification and verification processes by the Registration authority of the persons and the conditions for issuing or management of a qualified certificate, the Certification authority shall publish immediately the issued qualified certificate in the Public register/ Depository of issued certificates, accessible through OCSP or respectively in the Certificate Revocation List - CRL.

3.3. Renewal of qualified certificate

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 is possible only if the qualified certificate is issued with term of validity of 1 (one) year or 3 (three) years 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.

If there are changes in the stated circumstances, entered in the qualified certificate, a new key pair must be generated (rekey).

3.4. Suspension and revocation of a qualified certificate

Suspension of a qualified certificate aims to stop temporarily its usage.

Revocation of a qualified certificate stops permanently the validity of the certificate.

StampIT will suspend or revoke a qualified certificate in the following cases:

- 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 this policy and the 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 this policy and the 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;
- at the request of authorities specified in a statutory instrument.

3.4.1. Request for suspension or revocation

The subscriber or any authority specified in a statutory instrument may request suspension or revocation of a qualified certificate.

The identity of the requestor and its representative authority will be confirmed depending on the nature of the requested action.

3.4.2. Effect from suspension or revocation

For the period of suspension or upon revocation of a qualified certificate, its validity is considered immediately terminated.

The validity of the 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.

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

3.4.3. Notification upon suspension or revocation of a qualified certificate

StampIT shall notify the subscriber for revocation of suspension of a qualified certificate and for the reasons for the revocation or suspension through communication means, which it considers appropriate.

3.5. Identification and verification of identity after revocation of issued qualified certificate

Renewal or reissue of a qualified certificate after its termination shall not be allowed.

In case of request by the Signatory/ the Creator of a seal for the issue of a new qualified certificate, the procedure for initial creation of a qualified certificate shall be observed.

4. Operational activities

Activities connected with the provision of certification services shall be performed according to the following procedures:

- registration and processing of a request for issuing a qualified certificate
- issuing a qualified certificate
- submission to the Subscriber of the issued qualified certificate
- renewal of a qualified certificate by keeping (renew) or generating a new key pair (rekey)
- suspension/ resumption of the validity of a qualified certificate

- revocation of a qualified certificate

Registration

Request for registration of Subscriber of qualified certification services shall be submitted to the Registration authority by natural persons, legal persons or their authorized representatives and shall include
the following information:

- full name of the Signatory/ the Creator of a seal or an authorized representative of the legal person
- full name of the legal person associated with the Signatory
- evidence of representative authority of the Signatory toward the legal person - where applicable.
- identifiers: EIK, Personal number, BULSTAT, etc.
- full mailing address of the person
- contact telephone
- email address
- type of requested qualified certificate
- identifier (OID) of the policy on which basis the certificate is issued
- private key and corresponding to a public key
- additional information requested for inclusion in the certificate
- signing Contract for qualified certification services and consent with the conditions of this Policy and the Practice upon provision of qualified certification services

Renewal

Renewal is possible only subject to available qualified certificate of Signatory/ Creator of a seal in accordance with this Policy and the Practice of StampIT.

The renewal of qualified certificate keeps the information for the Signatory/ the Creator of a seal from the current certificate and in the renewed certificate is changed only the period of validity.

Revocation

Request for revocation by a Subscriber of a qualified certificate shall be submitted to the Registration authority by natural persons, legal persons or their authorized representatives in person to RA.

StampIT may terminate a qualified certificate in the following cases:

- death/ putting under judicial disability of the Signatory/ Creator of a seal
- termination of the representative authority of the Signatory toward the Subscriber
- identification of incorrect data upon issuing the certificate
- identified untrue certified information;
- in case of change in certified data of Signatory/ Creator of a seal
- private key compromising
- default of payment of the remuneration due
- request for revocation on the part of the Signatory/ Creator of a seal

The subscriber or its legal representative shall inform StampIT in case of occurrence of any of the above events.

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

4.1. Valid use of issued qualified certificates

4.1.1. On the part of the subscribers

The subscribers shall use the issued qualified certificates only in compliance with the Policy according to their designation in the term of their validity and in case that they are not suspended/ revoked.

The Signatory/ the Creator of a seal shall be responsible for the usage of the private key.

4.1.2. On the part of the relying parties

Relying parties shall use the public keys and their relevant certificates only in compliance with their designation, after performance of the following verifications:

- verification of the status of the certificate through OCSP or CRL
- verification of the electronic signature of the Certification authority including its status through OCSP or ARL
- verification of the time validity of the certificate

4.2. Renewal and reissue of qualified certificates

Renewal of qualified certificates issued by StampIT may be performed only if all data in the certificate are unchanged as in the initial request for issuing. The content of the renewed qualified certificate is identical to the one of the current certificate except the term of validity which shall start on the date of renewal entered in the certificate.

In compliance with the requirements for renewal the Registration authority of StampIT may request updated documents proving the correctness and of the information included in the content of the qualified certificate at the current moment.

The requestor declares that the data provided upon the initial issue and those entered in the qualified certificate are true, correct and not changed at present.

If there are changes in the data and circumstances relating to the natural and/ or legal person, the requestor shall submit request for the issue of a new qualified certificate.

The documents required for renewal of qualified certificates are published on the website of StampIT: https://www.stampit.org.

4.2.1. Procedure for renewal of qualified certificates

The following steps describe the process of renewal:

1. The requestor shall submit Request for renewal accompanied by documents for renewal by appearing in person, through duly authorized representative or by electronic way by using a valid qualified certificate for electronic signature.
2. The identity is verified, respectively the identity of the requestor and the compliance of data and circumstances relating to the Subscriber as at the time of renewal.
3. The operator of the Registration authority of StampIT shall verify the presented documents and shall submit the request for renewal of the qualified certificate to the Certification authority.
4. The certification authority shall renew the qualified certificate, which shall be sent back to the Registration authority of StampIT in order to notify the subscriber about the existence of the renewed qualified certificate.
5. The qualified certificate shall be recorded in a secure device for creation of electronic signature/ electronic seal.
6. The renewed qualified certificate shall be published in the public register maintained by StampIT.

Renewal of a qualified certificate may be carried out only for certificates, which are valid as at the time of submission of the request to the Certification authority. For this reason the request for renewal as well as the required documents must be received in the Registration authority before expiry of the term of validity of the qualified certificate.

4.3. Change of information in the qualified certificates

Change of information for issued and published qualified certificate is not allowed.

At the request of the Subscriber, the issued qualified certificate may be revoked and a new one may be issued, with a new key pair and for payment in accordance with the procedure for the initial issue.

4.4. Suspension of qualified certificates

The validity of a qualified certificate issued by StampIT may be suspended upon availability of the relevant grounds, for the required term according to the circumstances, however for up to 48 hours.

For the period of the suspension of the qualified certificate, it shall be considered invalid.

4.4.1. Grounds for suspension

The validity of a qualified certificate issued by StampIT may be suspended:

1. At the request of the Subscriber. The request may be submitted to the Registration authority of the provider or through other communication means including telephone, fax, email.
2. At the request of a person for whom there are circumstances evidencing that it may be aware of breaches of the security of the private key, such as a representative, a partner, an employee, a family member, etc.
3. By order of the Supervisory authority - upon immediate hazard for the interests of third persons or in case of existence of sufficient data for breach of the law.

4.4.2. Procedure for suspension

The following steps describe the process of suspension of the validity of a qualified certificate:

1. The Certification authority receives request for suspension.
2. The Certification authority shall suspend the validity of the certificate by including it in the list of revoked qualified certificates, which is publicly accessible.
3. The certification authority shall immediately notify the subscriber and the signatory/ the creator for the suspension of the validity of the qualified certificate.

4.5. Resumption of qualified certificates

The validity of a qualified certificate is resumed upon expiration of the term of suspension if the ground for suspension is not valid any more or at the request of the subscriber, after StampIT, respectively the Supervisory authority is convinced that it has become aware of the reason for the suspension and the request for resumption is made after such awareness.

The certification authority shall resume the validity of the qualified certificate and shall remove it from the Certificates Revocation List.

4.5.1. Grounds for resumption

1. By order of the Supervisory authority - when the reason for the suspension of the activity is order of the Supervisory authority.
2. Upon expiration of the term for suspension of the validity of the certificate;
3. At the request of the Subscriber.

4.5.2. Procedure for resumption

1. By order of the Supervisory authority – StampIT shall receive the order of the Supervisory authority for resumption of the validity of the qualified certificate. The certification authority shall resume the validity of the certificate by removing it from the Certificates Revocation List.
2. After expiration of the term of suspension of the validity of the certificate - after expiration of 48 hours from the moment of suspension of the validity of the qualified certificate, its validity is resumed automatically by the Certification authority if until that time a valid request for revocation is not received by the procedure for revocation of a qualified certificate.
3. At the request of the subscriber - after StampIT becomes convinced that it has become aware of the reason for the suspension and the request for resumption is made on the basis of such awareness. Request for resumption of the validity of the qualified certificate on the part of the subscriber is realized by the following procedure:
    - the requestor/ the legal representative/ the authorized representative of the requestor shall appear in person to the Registration authority and shall submit Request for Resumption, accompanied by documents that prove its identity and representative authority.

- The operator of the Registration authority shall verify the presented documents and shall submit request for resumption of the qualified certificate to the Certification authority.
- The certification authority shall resume the validity of the qualified certificate.

If in the period of suspension of the qualified certificate in the Certification authority is received a valid request for its revocation, then StampIT shall revoke the certificate in compliance with the approved procedures.

4.6. Termination of the qualified certificates

StampIT shall terminate the validity of a qualified certificate after submission of a request for termination by the Registration authority. To make such request, the operator of the Registration authority shall verify the identity of the requestor/ the legal/ the authorized representative of the requestor as well as the representative authority of the legal/ authorized representative of the requestor. Request for termination may be submitted to the Registration authority by the Subscriber.

4.6.1. Ground for revocation

The grounds for revocation of a qualified certificate may include the following but not limited to:

1. 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.
2. termination of the representative authority of the natural person toward the legal person entered in the content of the certificate.
3. Termination of the legal person of the subscriber.
4. Death or putting under judicial disability of the natural person.
5. evidence that the qualified certificate is issued on the basis of false data.
6. In case of change in the information, which is submitted initially and is contained in the qualified certificate of the Subscriber;
7. In case of default of the duties of the subscriber under the contract for qualified certification services.
8. At the request of the subscriber, after verification of the identity and the representative authority of the requestor.

All qualified certificates issued by StampIT shall be revoked unconditionally upon termination of the activity of StampIT.

The documents required for revocation/ suspension of qualified certificates are published on the website of StampIT: https://www.stampit.org.

4.6.2. Procedure for revocation

The following steps describe the process of revocation of a qualified certificate:

1. the requestor/ the legal/ the authorized representative of the requestor shall appear in person to the Registration authority and shall submit Request for Revocation, accompanied by documents that prove its identity and representative authority.
2. The operator of the Registration authority shall verify the identity of the requestor and its representative authority as at the time of submission of Request for Revocation.

3. The operator of the Registration authority shall submit request for revocation to the Certification authority.
4. The certification authority shall revoke the qualified certificate.
5. The revoked certificate shall be included in the Certificates Revocation List maintained by StampIT, which is publicly accessible.

4.7. Status of issued qualified certificates

Information about the status of the qualified certificates issued by StampIT is available 24 hours per day, 7 days per week as follows:

4.7.1. Automated, through the Certificate Revocation List (CRL)

StampIT shall maintain Certificate Revocation Lists accessible on the website of the Provider in accordance with the requirements of RFC 6818. CRL lists shall be refreshed at least every 3 hours or immediately upon occurrence of any event. The specific addresses of the CRL lists are available in the CRL Distribution Point (CDP) attribute of the certificates.

4.7.2. Automated, through the Online Certificate Status Protocol (OCSP)

StampIT shall maintain automated service for online certificate status protocol (OCSP) in accordance with the requirements of RFC 6960.

The address for verification of the status of the issued certificates is described in Authority Information Access (AIA) extension of the qualified certificates..

4.7.3. Manually, through the website of StampIT

StampIT shall maintain web-based interface for manual verification of the status of the issued certificates accessible on https://www.stampit.org.

5. Physical and organizational security

5.1. Physical security

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.

Information Services JSC has implemented and maintains Integrated Management System certified by external certification authority under the standards ISO 27001:2013 for information security management, ISO 20000-1:2011 for management of the provided ИТ services and ISO 9001:2015 for quality management.

5.1.1. Secure premises

For the needs of StampIT shall be maintained specially built secure premises property of the Company in which are accommodated the infrastructural components of StampIT. In the premises will be provided real time monitoring of the basic characteristics of the environment (temperature and humidity) as well as sensors for movement, seismic activity, video surveillance and etc.

Unarmed security guards are available 24 hours per day, 7 days per week who control and monitor the access to the premises. The secure premises used for the provider's infrastructure have separate alarm system in addition to the basic one used for the access to the buildings of the Company.

The access to the premises is organized through two-factor authorization and each entry and exit from the premises shall be registered.

5.1.2. Data storage

Specially equipped archival premise shall be build for customer data storage. The technical carriers shall be stored in fire-resistant strong boxes.

5.1.3. Secure data destruction

Upon data destruction, the security policy of the Company shall be complied with. Paper documents shall be destructed by paper shredders with high level of security and for the technical data carriers shall apply DBAN method and physical destruction of the carrier. Activities shall be duly documented by registering audit trail for the performed activities.

5.2. Organisational security

Implemented organizational measures for information security management shall comply with the requirements of the valid law, the technical standards and the Integrated Management System implemented in the Company.

The activities shall be performed by properly qualified employees with a role in the relevant process in order to minimize the possibility for compromising the implemented controls, leaking of confidential information and avoidance of conflict of interests. Roles are laid down in the internal rules of StampIT and in the job descriptions of each employee related with the operations of the Provider.

5.3. Personnel security

The practices for personnel management include measures, which give guarantees for reliability and competence of the employees and for performance of their duties.

All employees who have access to information shall strictly observe the requirements for confidentiality and personal data protection.

Employees of the provider who have access to confidential information shall sign declarations for confidentiality and non-disclosure of information.

Employees of the provider who have access to personal data shall sign declarations for non-disclosure of personal data.

5.3.1. Personnel training

Employees working on the management and operation (PO) of the infrastructure of StampIT shall undergo training on the practice and the policies for issuing the different types of certificates and administration of different types of cryptographic devices. In the training shall be included also the requirements of the Integrated Management System relevant to the role of the employee.

Specific process documentation has been also developed describing the process parameters of the specialized software for infrastructure management and the required client's installations.

The company shall develop plans for process development and specialized training of employees. Assessment of the impact on the work and the awareness of the employees shall be carried out for each training.

5.4. Records and journals management

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 operational instruction 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 a 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.

5.5. Archives management

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 the users
- the whole information about the users
- 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

5.6. Certification authority termination

In case of termination of the operations of the Certification authority, for whatever reason, StampIT shall promptly notify and transfer its duties for archives maintenance to the successors.

Before termination of its operations as Certification authority, StampIT shall perform the following activities:

- to inform about its intentions the Supervisory board and the subscribers who have valid qualified certificates at least four months before the date of termination of its operations;

- to terminate all qualified certificates which are still not terminated or are still valid at the end of the four-month period of time without asking for the consent of its subscribers - if the operations will not be transferred to another provider;
- to perform the required activities for archives storage in compliance with this policy and the regulatory requirements - if the activity will not be transferred to another provider;
- in case that it transfers its operations to another provider, StampIT will hand over to the assignee the whole documentation related to its operations as certification services provider and the right to use the public key infrastructure of StampIT with a view to the management of already issued qualified certificates for a term, which is not longer than six months.

6. Technical security control

6.1. Generation and putting in operation of the key pair of Certification authority

StampIT uses reliable process for generation in order to generates its private keys. StampIT divides its private keys to 3 (three) secret parts. StampIT is the legal owner and holder of the private keys for which it uses the procedure for division of secret parts. StampIT may transfer such secret parts to different persons who are explicitly authorized.

StampIT shall generate securely and shall protect its own private keys by using reliable system and shall take the required measures to prevent compromising or their unauthorized use. StampIT implements and documents the procedure of key generation in compliance with this policy. StampIT implements the European and the generally recognized in the international practice standards for reliable systems including the information security standards and makes everything possible to observe them.

StampIT applies triple division to secret parts and distributes them between authorized persons who take care of storing the secret parts in order to increase the confidence in the Certification authority with high degree of security and to ensure key restoration.

6.2. Generation of key pair of Subscriber

The key pair of the Subscriber is generates in a secure environment in accordance with the requirements of Regulation (EU) № 910/2014 and the ETSI specifications. A key pair may be generated with the Subscriber in compliance with the above requirements and with the RA of StampIT in the presence of the Subscriber. The key pair may be also generated through advanced electronic signature/ seal creation device (QSCD), verified for level of security and for interoperability with the systems of StampIT.

The private key is controlled through access code - PIN code or equivalent.

The subscriber shall be liable for the private key controlled by it.

6.2.1. Requirements to devices

The certification authority of StampIT approves directly or through authorized consultants the hardware and the software, which it uses in order to provide qualified certification services.

6.2.2. Provision of the key pair to the Subscriber

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.

6.2.3. Minimum lengths of key pairs

The length of the key pair for advanced electronic signature and advanced electronic seal generated through the infrastructure of StampIT shall be at least 2048 bits, with combination of hash and asymmetric algorithms sha256-with-RSA.

6.2.4. Public key parameters

The subscriber is responsible for verification of the quality of the parameters of the generated private key. It has to verify the ability of the key to create valid advanced electronic signature/ advanced electronic seal and its subsequent verification.

The devices StampIT have security level CC EAL 4+ and FIPS 140-2 Level 3.

All devices for advanced electronic signature creation and advanced electronic seal creation (QSCD), used by the Subscriber outside the infrastructure of StampIT must be certified for security level CC EAL 4+ and higher.

6.2.5. Private key management

6.2.5.1. Private key storage

The subscriber shall store the private key in a reliable system guaranteeing its security. When StampIT generates the key pair, at the request of the Subscriber, the key pair shall be delivered in a secure form to the Subscriber.

StampIT shall not create copies of the private keys of the Subscriber.

6.2.5.2. Private key activation

Private key activation shall be carried out by entering of a valid PIN code giving access to the functionality for performance of cryptographic operations with the private key.

6.2.5.3. Private key deactivation

Deactivation shall be carried out through the relevant functionality of the environment in which the private key is stored.

6.2.5.4. Private key destruction

It is carried out through the functionality of the environment storing the private key. The use of the certificate must be impossible after performance of this operation.

6.3. Key pair management

6.3.1. Public key archiving

The public keys of the Subscribers are available in the registers of StampIT. The registers of the provider are archived by the procedures for information security management performed and observed by the expert panel of StampIT.

6.3.2. Validity and use of issued certificates

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

6.4. Private key activation

Upon performance of the activities in the Registration authority, data for private key activation are entered by the User in a protected manner, in the presence of an operator.

When the Subscriber generates the key pair for qualified certificate, the Subscriber is responsible for management of the activation data.

6.4.1. Generation and provision of activation data

The key pair of the Signatory/ the Creator of qualified certificate for advanced electronic signature/ seal shall be generated in approved by StampIT advanced 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 advanced electronic signature/ seal. When generation is carried out in environment under the control of the Subscriber, then it shall be liable for the compliance with the requirements of Regulation (EU) № 910/2014 and ESTI specifications in this area.

6.4.2. Activation data protection

The signatory/ creator shall store and protect from compromising the access codes to the advanced electronic signature/ seal creation devices and environments.

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

6.5. Security of the used computer systems

StampIT uses reliable and redundant systems upon provision of its services. The reliable system represents computer hardware, software and procedures, which ensure acceptable level of protection against risks connected with security, provides reasonable level of operability, reliability, correct operation and realization of the security requirements.

The complex of software and hardware used for the activity of StampIT is made of highly reliable and secure components. The concept Security by design is applied and for each component are included the available factors and configurations for security.

StampIT applies the procedures and the policies for information security management, a part of the Integrated management system maintained by Information Services JSC.

6.6. Change management in the system of StampIT

The change management in the system of StampIT is subject to the procedures and the policies for information security management, a part of the Integrated management system maintained by Information Services JSC.

All changes are managed by the relevant authorized employees of the Company. Upon adding new components to the system (hardware or software), the required technical and operational documentation shall apply to them.

Upon withdrawal of components from the systems, the secure destruction of the data on them is guaranteed by the Provider.

6.7. Network security control

Information Services JSC has highly developed network infrastructure, which components provide opportunity for protection of different types of network attacks. There are devices for protection from DDoS, new generation firewalls (ng-firewalls) and highly efficient active network devices.

Network operations centre (NOC), which operates 24 hours per day, 7 days per week, in which is carried out observation and early notification in case of events, which may influence the activity of StampIT.

7. Certificates profiles

7.1. 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 JSC	Organization
	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=0		
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/		

7.2. Profile of StampIT 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 (Critical)	Subject Type=CA 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/		

7.3. Profile of qualified certificate for advanced electronic signature StampIT Enterprise, which is issued to a natural person

Профил на StampIT Enterprise			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	term determined in the contract for the certification service (one or three)		
Subject	*C	Country	State
	L	Locality	Town/ District
	*CN	Common Name	Full name or Friendly name
	*G	Given	name of the natural person, written in the Roman alphabet
	*Sn	Surname	surname of the natural person, written in the Roman alphabet
	Pseudonym (2.5.4.65)	Pseudonym	Pseudonym
	*E	E- mail:	Post address

	*SerialNumber		Unique identifier of the natural person: For Bulgarian citizen: PNOBG-xxxxxxxxxx /personal number/ PASBG-xxxxxxxxx /passport number/ TINBG-xxxxxxxxxx/VAT number/ For a foreign person: PNOYY-xxxxxxxxxx /personal number/ PASYY-xxxxxxxxx /passport number/ IDCYY-xxxxxxxxx /national card/ YY-country code
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Non-Repudiation Key Encipherment		
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/		
Extended key usage (Non Critical)	Client Authentication E-Mail Protection Smart Card Logon Document Signing		
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Natural(oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.stampit.org/pds/pds_en.pdf language=en		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=**1.3.6.1.4.1.11290.1.2.1.5** Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=https://www.stampit.org/repository [2] Certificate Policy: Policy Identifier= 0.4.0.1456.1.2 [3] Certificate Policy: Policy Identifier=0.4.0.194112.1.0		

7.4. Profile of qualified certificate for advanced electronic signature for a natural person associated with a legal person StampIT Enterprise Pro

Profile of Enterprise Pro			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	term determined in the contract for the certification service (one or three years)		
Subject	*C	Country	State
	L	Locality	Town/ District
	*CN	Common Name	Full name or Friendly name
	*G	Given	name of the natural person, written in the Roman alphabet
	*Sn	Surname	surname of the natural person, written in the Roman alphabet
	Pseudonym (2.5.4.65)	Pseudonym	Pseudonym
	*E	E- mail:	Post address
	*SerialNumber		Unique identifier of the natural person: For Bulgarian citizen: PNOBG-xxxxxxxxxx /personal number/ PASBG-xxxxxxxxx /passport number/ TINBG-xxxxxxxxxx/VAT number/ For a foreign person: PNOYY-xxxxxxxxxx /personal number/ PASYY-xxxxxxxxx /passport number/ IDCYY-xxxxxxxxx /national card/ YY-country code
	O	Organization	Name of legal person
	*OrganizationIdentifier (2.5.4.97)	2.5.4.97	Legal person identifier NTRYY-xxxxxxxxx /national identification code/ VATYY-xxxxxxxxx /tax number/ YY – country code
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Non-Repudiation Key Encipherment		
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/ [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://stampit.org/repository/stampit_global_qualified.crt		

Extended key usage (Non Critical)	Client Authentication E-Mail Protection Smart Card Logon Document Signing
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Natural(oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.stampit.org/pds/pds_en.pdf language=en
Basic constrains (Critical)	End entity
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.6 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=http://www.stampit.org/repository [2] Certificate Policy: Policy Identifier= 0.4.0.1456.1.2 [3] Certificate Policy: Policy Identifier=0.4.0.194112.1.0

7.5. Profile of qualified certificate for advanced electronic seal for a legal person StampIT Enterprise Seal

Profile of StampIT Enterprise Seal			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	term determined in the contract for the certification service (one or three years)		
Subject	*C	Country	State
	L	Locality	Town/ District
	*E	E- mail:	Post address
	*O	Organization	Name of legal person
	*OrganizationIdentifier (2.5.4.97)	2.5.4.97	Legal person identifier NTRYY-xxxxxxxxx /national identification code/ VATYY-xxxxxxxxx /tax number/ YY – country code
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Non-Repudiation Key Encipherment		
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/ [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://stampit.org/repository/stampit_global_qualified.crt		

Extended key usage (Non Critical)	Client Authentication E-Mail Protection Document Signing Code Signing
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Legal(oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.stampit.org/pds/pds_en.pdf language=en
Basic constrains (Critical)	End entity
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.7 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=http://www.stampit.org/repository [2] Certificate Policy: Policy Identifier= 0.4.0.1456.1.2 [3] Certificate Policy: Policy Identifier=0.4.0.194112.1.1

8. Control of Provider's activities

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.

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.

Information Services JSC is subject to audit by independent compliance assessment authority at least once every 24 months. 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.

The report of the compliance assessment authority shall be delivered to the Supervisory authority within 3 (three) business days after it is handed over. Based on the audit results shall be planned

the activities for remedy of the possible non-conformities and zones for improvement by specifying the particular tasks and the time for their completion.

9. Business and legal issues

9.1. Prices

StampIT determines the prices for using the products and the services of StampIT, which are published on its website. StampIT reserves the right to change these prices.

9.1.1. Remedy of discrepancies and restoration of effected payment

The subscriber may object to any inaccuracy or incompleteness of the content of the issued certificate within 3 days after its publication in the Public Register.

If the reason for the untrue content of a qualified certificate is a technical error omitted by the Registration authority, StampIT shall terminate the certificate and shall issue a new one with true content on its own account or shall restore the effected payment for the cancelled certificate with untrue content.

If the reason for the untrue content of a qualified certificate is through the fault of the Subscriber, StampIT shall terminate the certificate and may refuse reimbursement of the effected payment.

9.2. Financial liability

StampIT shall be liable to the Subscribers for the provided certification services in case that any harms have occurred as a result of the incorrect application of the policies and the practice by the Provider's employees.

If it is confirmed and is accepted that such event has occurred, then StampIT agrees to pay damages up to the maximum amount specified in the certificates however without exceeding the amount of damages.

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.

9.3. Personal data protection

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

All employees who have access to information shall strictly observe the requirements for confidentiality and personal data protection.

Employees of the provider who have access to confidential information shall sign declarations for confidentiality and non-disclosure of information.

Employees of the provider who have access to personal data shall sign declarations for non-disclosure of personal data.

9.4. Intellectual property rights

StampIT holds the intellectual property rights concerning the database, the websites, the qualified certificates of StampIT and any other publications made by StampIT including the developed practices, policies and other accompanying documents.

9.4.1. Title on the key pairs

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.

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.

9.5. Responsibilities and duties of StampIT

Up to the level determined in the relevant field in the issued certificate StampIT shall:

- observe its internal and public practice, 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 the policy and the practice and shall meet the obligations specified in them
- upon obtaining the request of the Registration authority, shall issue and renew qualified certificates in compliance with the practice and the policies
- upon receiving request for termination of a qualified certificate by the Registration authority, terminate the certificate in accordance with the practice and the policies
- publish the qualified certificate in accordance with the policies and the practice
- ensure support for the subscribers and the relying parties
- revoke, suspend and resume the qualified certificate in accordance with the policies and the practice
- ensure information about the expiration of the term of validity and resumption of the qualified certificate in accordance with the practice and the policies

- provide copies of its practice and policies as well as the other valid documents for public access

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

9.5.1. Liability to the Subscriber

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-performance of the statutory requirements to the activity of the qualified provider of qualified certification services
- Default of the statutory obligations of the qualified provider of qualified certification services governing the issue, management and 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

9.5.2. Limits of liability of the registration authority

The network of StampIT may include Registration authorities which operate in compliance with the approved practices and procedures of StampIT.

StampIT guarantees the integrity of each qualified certificate issued by its own Certification authority within the conditions specified in this policy.

9.6. Obligations of the subscriber

Unless otherwise agreed, 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 that policy 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 policy
- 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 deinstall it from the applications, devices or environments 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 or the environment 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

9.7. Disclaimer

Unless in case of gross negligence, StampIT shall not be liable for:

- missed benefits
- loss of data
- other indirect damages ensuing from or in connection with the use, validity or inoperability of the qualified certificate.
- any other damages unless those which are connected with relying on the information specified in the qualified certificate based on the confirmed information in the certificate
- error in the confirmed information, which is a consequence from fraud or intentional incorrect statement of the requestor
- the use of a qualified certificate, which has not been issued or used in compliance with this policy
- the use of qualified certificate. which is invalid
- the use of qualified certificate, which exceeds certain limitations specified therein or in this policy
- the security, use, integrity of products, including hardware and software , which the subscriber uses
- Subscriber's private key compromising