ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

stampit

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

General Terms and Conditions for provision of qualified certification services

eIDAS-StampIT-GTC

Version: 3.1.0.

Publication date: 7 June 2017

Contents

You may send your comments on this document by email:support@mail.stampit.org or by mail to the following address:

Information Services JSC - StampIT
11, Lachezar Stanchev Str. Izgrev
1756 Sofia, Bulgaria
Tel.: + 359 2 9656 291
Fax: + 359 2 9656 212
E-mail:support@mail.stampit.org

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 audiovisual 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 certificate 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 signature, electronic seal and qualified website authenticity
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. OVERVIEW

This section makes an overview of the practices for provision of qualified certification services of Information Services JSC

1.1. Qualified certification services provider

Information services JSC is a provider of qualified certification services that works in compliance with 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.

Certification authority

StampIT is the Certification authority of Information Services JSC which issues qualified certificates for electronic signature (QES) to natural persons and to natural persons associated with legal persons as well as qualified certificates for electronic seal (QESL) to legal persons and qualified website authentication certificates (QWA) and qualified electronic time stamps. The certification authority carries out the activities, which include the issue, renewal, suspension, resumption and revocation of qualified certificates, keeping a register and providing access to it.

Registration authorities

The certification authority issues a qualified certificate 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 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 issue a qualified certificate;
- to register the submitted requests for renewal, termination, suspension and resumption of the validity of the qualified certificates.

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

1.2. Qualified certificate for electronic signature (QES)

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

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

Types:

1.2.1. Qualified certificates for advanced electronic signature - 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 StampITEnterprisePro**

StampITEnterprisePro 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.

StampITEnterprisePro provides high level of identity and the requestor is required to prove his/her 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.

1.2.2. 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 his/her 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 StampITDocPro**

StampITDocProQES 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.

StampITDocPro QES provide high level of identity and the requestor is required to prove his/her 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.

1.3. 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 of data provided by the legal persons such as electronic documents, photos, drawing and software.

Types:

1.3.1. Qualified certificate for qualified electronic seal for a legal person StampITEnterpriseSeal - QESL (advanced)

StampITEnterpriseSeal are issued to legal persons (creators of advanced electronic seal). They may be used for identification of the subscriber/ the creator of the advanced 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.

StampITEnterpriseSeal 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.

1.3.2. Qualified certificate for qualified electronic seal for a legal person StampITeSeal - QEST (qualified)

StampITeSealare 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.

StampITeSeal 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.

1.4. Qualified website authentication certificate (QWA)

Qualified website authentication certificate is used to attest the website authenticity by binding it with the relevant natural person or legal person to whom QWA is issued.

StampIT issues two types of qualified website authentication certificates.

1.4.1. StampIT Server DVC – used for website authenticity certification;

1.4.2. StampIT Server OVC - used for certification of website authenticity and its link with specific natural person or legal person.

1.5. 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.

1.6. Relations with user for choosing certification services

StampIT renders assistance to its clients to choose appropriate certification service. Subscribers are required to determine carefully their requirements to the specific uses for protected and encrypted communications before submission of request for provision of the relevant type of qualified certification service.

1.7. 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.

1.8. 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 qualified electronic signatures/ 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.

2. TECHNOLOGY OF USE OF QES/ QESL

This section makes a review of the technology for receiving, installing and using qualified certificates for electronic signatures and qualified certificates for electronic seals. Qualified certificates are issued by StampIT on a smart card.

2.1 Preliminary preparation

The process of preliminary preparation for receiving and installing a qualified certificate and using the electronic signature/ electronic seal includes the following key steps:

- Submission of a request for issuing a qualified certificate;
- Verification of the identity of the requestor;
- Issuing a qualified certificate by StampIT;
- Receiving the qualified certificate and data for access to the smart card;
- Installing the qualified certificate of StampIT on the subscriber's hardware;
- Ensuring conditions for protection of the private key and the qualified certificate;
- Choice and installation of the applied software for using the private key and the qualified certificate;
- Settings of the applied software.

2.2 Signing/ creation of a seal

Signing with electronic signature/ creation of a seal is carried out by using applied software for using the private key.

The holder of electronic signature/ the creator of a seal shall strictly follow the instructions given by the applied software developer and shall comply with the restrictions and the conditions of use, indicated in the regulation, in this document, the Qualified certification services practice statement (CPS) and the relevant policy for provision of qualified certificates.

2.3 Identification

Qualified certificates for electronic signature/ electronic seal issued by StampIT may be used for identification of the subscriber upon remote access to web server in the following manner:

- Via the browser used by the subscriber is selected the place, which is subject to remote access (most often URL);
- When connecting with the server, the subscriber is required to select and confirm the relevant QES/ QESL, which will be used for getting access to the remote resources;
- After successful completion of the session for identification, the subscriber receives the opportunity for access to the remote resources in compliance with the rights granted to it in this regard.

2.4 Verification of electronic signature/ electronic seal

The purpose of the electronic signature/ electronic seal verification is to establish that:

- the electronic signature/ the electronic seal was created with private key, which corresponds to the private key entered in the qualified certificate of the holder of electronic signature/ creator of a seal;

- the message/ the electronic document has not been changed after the creation of the electronic signature/ electronic seal.

Upon receipt of a signed electronic statement/ electronic document, confirmed with electronic seal, before deciding whether to rely on this electronic signature/ electronic seal, the addressee (the relying party) must perform at least the following actions:

- To become acquainted with the principles and the rules of StampIT for issuing and management of qualified certificates;
- To verify (with the help of the applied software) the condition of the electronic signature/ electronic seal - whether the electronic statement/ electronic document has not been changed/ after the creation of the electronic signature/ electronic seal;
- To verify the period of validity entered in the qualified certificate of the signatory/ the creator of a seal;
- To verify whether the qualified certificate, which has been used for signing the electronic statement, respectively for creation of the electronic seal, is published by StampIT;
- To download from the website of StampIT the latest copy of the public Certificates Revocation List (CRL);
- To install CRL and to update the database with revoked and suspended certificates on the local computer on which the verification is carried out;
- Visually or automatically (through the applied software) to verify the status of the qualified certificate - whether in the updated CRL is included the qualified certificate of the signatory/ the creator of a seal of the received electronic statement/ electronic document.

After performance of the specified steps, if it is considered necessary, the addressee may undertake also other actions permissible by the law for additional verification before making final decision whether to trust the electronic signature/ the electronic seal and the qualified certificate. In any case, the addressee shall rely on the electronic signature/electronic seal and the qualified certificate only to the extent reasonable for the specific circumstances.

3. TECHNOLOGY OF USE OF QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES (QWA)

Qualified website authentication certificate is installed on the relevant website for which it is issued. Upon creating a link to a website, which uses StampIT Server DVC, the relying parties receive

confirmation that the relevant domain is verified and validated. Upon creating a link to a website, which uses StampIT Server OVC, the relying parties receive confirmation that the relevant domain is verified and validated and that it is connected to a specified natural or legal person.

4. TECHNOLOGY OF USE OF QUALIFIED ELECTRONIC TIME STAMPS (QETS)

The certification of the date and time of submission of electronic document is carried out in compliance with IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) when the subscriber submits electronic request to the address, specified by StampIT. The request is submitted to Information Services JSC as certification services provider and it performs the activities for time stamping.

5. Requirements for private key storage

The private key of the asymmetric cryptographic system shall be stored in the conditions of high degree of security. This section reviews the basic requirements to storage of the private key of the signature/ the creator of a seal/ the person to whom QWA is issued.

5.1 Physical storage

After generation of the key pair on the smart card and the provision of data for activation of the smart card of the subscriber, the responsibility for the physical protection of the private key is borne entirely by it, respectively by the signatory/ the creator of a seal. The same applies also for the cases of private key storage in a file. The subscriber, respectively the signatory/ the creator of a seal must take measures to prevent any unauthorized physical access to the holder (the file or the smart card) containing the private key. Access to the carrier shall have only the signatory/ the creator of a seal/ the person to whom QWA has been issued, which will protect the private key and the qualified certificate from unauthorized access or use of the electronic signature/ electronic seal by a person other than the signatory/ the creator of a seal/ the person to whom QWA has been issued.

5.2 Reproduction

The storage of the private keys and the qualified certificate in files creates preconditions for their fast and easy reproduction by a person other than the signatory/ the creator of a seal/ the person to whom QWA has been issued. When the private key is stored on a smart card it cannot be exported, however the signatory/ the creator of a seal/ the person to whom QWA has been issued shall not provide to other persons the opportunity for access to the private key, the smart card or the electronic file provided by StampIT containing the qualified certificate.

5.3 Operational storage of the private key

In case of operation work, when the file or the smart card on which is located the private key and the qualified certificate are not used temporarily, they shall not be left unsupervised at a public place. Failure to observe such requirement creates preconditions for compromising of the private key of the subscriber.

5.4 Key word and personal identification number (PIN)

The access to the private key and the qualified certificate provided by StampIT is limited through a key word (password) or PIN code. Only the signatory/ the creator of a seal/ the person to whom QWA is issued should know and use the key word for access to the file or the PIN code for access to the smart card. If a wrong PIN code is entered three times, the smart card is blocked. The signatory/ the creator of a seal/ the person to whom QWA is issued shall undertake the required activities to prevent the opportunity that each person receives information about the key word or PIN code.

5.5 Use of the private key

The smart card shall be placed in the card reader each time when the private key and the qualified certificate is used. To prevent the hazard of unauthorized use of the private key and the qualified certificate by other persons, the card must not be left without supervision in the card reader. In case that the personal computer will not be used for a longer period of time, the smart card must not be left in the card reader and the personal computer must be switched off and/ or adequate measures must be taken to prevent the opportunity for unauthorized access to it by means of the hardware and the operational system.

5.6 Loss or destruction

In case of loss or destruction of the private key, the signatory/ the creator of a seal/ the person to whom QWA has been issued shall lose the opportunity to use the qualified certificate. StampIT is not able to restore any lost or destroyed key pair because it is not able to copy it. When it is generated on a smart card, the private key may not be exported thereof. In the cases when the private key and the qualified certificate are stored in a file, StampIT will not get access to the private key because the electronic request for signing the qualified certificate, which is received by the subscriber, does not contain a private key. Loss or destruction or the private key or the smart card on which the private key is stored shall lead to the inability for further use of the electronic signature/ electronic seal.

5.7. Signing/ creation of a seal

Upon signing/ creation of a seal the signatory/ the creator of a seal uses its private key and the

qualified certificate in order to create electronic signature/ electronic seal. The signatory/ the creator of a seal must take the required measures to prevent the opportunity that third persons get access to the carrier containing the private key because this will result in compromising of the private key.

5.8 Encryption and decryption

The public key of the subscriber is used for encryption and for decryption the corresponding private key. The subscriber uses its private key for the purpose of decrypting an encrypted electronic document. The subscriber and all shareholders must be aware that in case of loss or destruction of the private key for decryption, the electronic documents processed in that way become inaccessible.

5.9 Cryptographic algorithms

The use of cryptographic algorithms, which do not provide sufficient level of security for the needs of the subscribers is considered a breach of the security requirements. At present in the world practice are considered secure and are recommended for use the RSA algorithm for signing, SHA1 (160bit) for hashing and 3DES algorithm for data encryption. The subscribers must use only algorithms with high degree of security and in compliance with the regulations governing their use.

5.10 Applied software

The use of qualified certificates for electronic signature/ electronic seal shall be carried out through software applications. The subscriber and the relying parties must use only licensed software with proven origin, which meets the generally accepted in the practice information security standards. The use of unlicensed software is in breach of the security requirements.

6. STATUS OF A QUALIFIED CERTIFICATE

This section presents the rules for updating and verification of the status of the qualified certificates issued by StampIT.

6.1 Issuance and validity of the qualified certificate

StampIT shall issue a qualified certificate after satisfaction of the request for issuing a qualified certificate. The qualified certificates are valid upon their issuance by StampIT and their acceptance on the part of the subscribers.

6.2 Acceptance of the qualified certificate by the Subscriber

It is assumed that the qualified certificate is adopted by the subscriber subject to any of the

following preconditions:

• the approval of the subscriber is shown to StampIT on-line or by electronic message sent by the subscriber;

• the qualified certificate is used by the subscriber for the first time;

• upon expiration of 3 days from the date of issuing the qualified certificate if in this term the subscriber has not made any claim concerning the content of the qualified certificate..

6.3 Publication of issued qualified certificates

StampIT publishes a copy of the issued qualified certificates in its repository in case that the subscriber respectively the signatory/ the creator of a seal does not express its disagreement for publication. StampIT may publish qualified certificates in other repositories, 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 their qualified certificates issued by StampIT in other repositories.

6.4 Relying on electronic signatures/ electronic seals

The ultimate decision whether to rely on electronic signature/ electronic seal must be made by the relying party subject to the availability of the following preconditions:

• the electronic signature/ electronic seal has been created in a period when the qualified certificate was valid, which may be verified by making a check for validity of the qualified certificate;;

• the verifying parties agrees with the terms and conditions under which the certificate of the signatory/ the creator of a seal has been issued;

• the reliance is reasonable for the specific circumstances.

6.5 Suspension and revocation of qualified certificates

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, respectively the subscriber has violated its obligations under CPS;
- the performance of any obligation under CPS 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.

6.5.1 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.

6.5.2 Effect of 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.

6.5.3 Notification upon suspension and 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.

6.5.4 Revocation of a qualified certificate

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.

6.5.4.1 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 certification service.
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.

6.5.5 Suspension of the validity of the qualified certificates of StampIT

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.

6.5.5.1 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.

6.5.6 Resumption of a qualified certificate

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 by removing it from the Certificates Revocation List.

6.5.6.1 Grounds for resumption of a qualified certificate

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.

7. LEGAL CONDITIONS AND PROCEDURE FOR USE OF QUALIFIED CERTIFICATES

This part of the document describes the legal guarantees, the grounds and the restrictions connected with the qualified certificates issued by StampIT.

7.1 Administrative order and terms for use of qualified certificates

StampIT issues qualified certificates to natural and legal persons. Natural persons who request and use qualified certificates of the type StampIT Doc Certificate are governed by the terms and conditions for use specified in this document and in CPS of StampIT. For the qualified certificates, which are issued to legal persons or to natural persons associated with legal persons, it is expedient that the legal person - subscriber develops internal regulation. Within the internal rules of the legal person, such document shall govern the field of application, the rights, the obligations and the responsibilities of the employees of the legal person with regard to their electronic statements and the use of qualified certificates from them.

7.2 Identity

The persons who use qualified certificates and the relying parties must know the rules and procedures for determination of the identity of the subscribers of qualified certificates issued by StampIT, which will allow them to make the relevant decision for use, verification and relying on the electronic signatures/ electronic seals and the qualified certificates.

7.3 Requirements to the requestors of qualified certificates

Before or during the process of requesting qualified certificates, the requestor of qualified certificates shall do the following:

- submit request for the issuance of a qualified certificate and accept the conditions of the Contract for certification services and CPS;
- produce evidence for their identity/ representative authority according to the standard

procedures of StampIT.

7.3.1 Authorization

Request for a qualified certificate of StampIT may be submitted in personal or through an attorney/ authorized representative depending on the type of the qualified certificate and the conditions for its issuance. Authorization shall be proven by notarized power of attorney, certificate of good standing (if applicable) and other documents establishing the connection between an authorizer and an authorized representative/ attorney and its rights.

7.3.2 Generation of the key pair

The registration authorities of StampIT shall be fully liable for the safe generation of the key pair of the subscriber, when for that purpose is used protective mechanism for creation of electronic signature/ electronic seal (smart card). Depending on the type of the qualified certificate and the conditions for its issuance, the subscriber may be present at the process of generation. When a key pair is generated for qualified certificates for qualified electronic signature/ qualified electronic seal, in all cases is used secure electronic signature/ electronic seal creation device with the relevant required level of security according to Regulation (EU) No. 910/2014. In the cases when the key pair is generated with the Signatory/ the Creator or the Subscriber, the Registration authority shall perform inspection of the requirements for the security level of the electronic signature/ seal creation device and verification for compliance with the cryptographic requirements.

7.3.3 Protection of the key pair

The subscribers are fully liable for the prevention of 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 carrier storing the key pair.

If the subscriber is a legal person, the responsibility for protection of the key pair is to the signatory respectively the creator of a seal.

7.3.4 Delegation of responsibilities for the private key

The subscribers are fully responsible for the missions or omissions of their attorneys or the partners, which the use for keeping, storage or destruction of their private keys.

7.4 Publication of data from the qualified certificate

StampIT shall publish the qualified certificate or data from the certificate on any accessible repository such as LDAP (Lightweight Directory Application Protocol) directories and Certificates Revocation List - CRL unless the subscriber has explicitly stated its disagreement for publication.

StampIT shall manage directories of qualified certificates with specific characteristics in order to increase the level of confidence in the offered services. The users and the relying parties must check in these directories with issued, revoked and suspended qualified certificates any time before making decision whether to rely on the information contained in the certificates.

7.5 Obligation concerning the provided information

In any cases and for all types of qualified certificates issued by StampIT, the subscriber (and not StampIT) has the permanent obligation to monitor the accuracy, the correctness and the completeness of the information provided upon the issuance of the qualified certificate and upon occurrence of changes to notify immediately StampIT about them.

7.6 Publication of information

The public information connected with the activity of StampIT may be updated from time to time. Such updates shall be indicated via appropriate numbering of the versions and date of publication of each new version.

7.7 Standards

StampIT accepts that the software of the subscribers is compatible with the standard X.509v3 and the other applicable standards and performs the requirements specified by CPS. StampIT may not guarantee that the software of the subscribers will maintain and implement the controls required by StampIT. If necessary, the subscriber may seek appropriate consultation.

7.8 Choice of cryptographic methods

The parties agree that they are the only responsible and have made independent decision for the choice of software, hardware and algorithms for encryptions/ electronic signature/ electronic seal, including their parameters, procedures and techniques in compliance with the requirements of Regulation (EU) No. 910/2014.

7.9 StampIT directories, repositories and certificates revocation list

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 updates the certificates revocation list automatically for any event or every three hours.

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.

7.10 Relying on unverified electronic signatures/ electronic seals

The relying parties must verify the electronic signature/ electronic seal by verifying every time the validity of the qualified certificate in the directory of CRL or any other available directory, which is published by StampIT. The relying parties are notified that unverified electronic signature/ electronic seal may not be defined as electronic signature/ electronic seal of the subscriber.

StampIT informs appropriately the relying parties for the use and the verification of the electronic signatures/ electronic seals through its CPS and other documents published in its public repository.

7.11. Certificates Revocation List (CRL)

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, suspended and revoked qualified certificates before deciding whether to trust the information entered in a qualified certificate. StampIT updates the certificates revocation list automatically for any event or every three hours. The certificates revocation list (CRL) is publicly accessible on addresshttp://www.stampit.org/crl/.

7.11.1. Profile of the Certificate Revocation List (CRL)

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)

7.11.2. Codes for suspension/ revocation of a qualified certificate

1. **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.
2. **CA Compromise** – compromised is the private key of the Certification authority, which is used for signing the qualified certificates of the subscribers;.
3. **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; .
4. **Superseded** – the qualified certificate has been superseded by another qualified certificate.
5. **Cessation of Operation** – the activities connected with the initial issue of a qualified certificate are terminated.
6. **Certificate Hold** – the activity of the qualified certificate is suspended (certificate is invalid at present).
7. **Unspecified** – the qualified certificate is revoked with specifying the reason when there is valid request for termination.

7.12. Obligations of the subscriber

Unless otherwise specified in the 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 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 the 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.

7.13 Accuracy, correctness and completeness of information

The subscriber shall be fully liable for the accuracy, correctness and completeness of the information, which provides for the use of a qualified certificate according to CPS.

7.14 Liability of the subscriber to the relying party

Without prejudice to the other obligations of the subscribers, specified in CPS, the subscribers are liable for any incorrect statements made by them upon issuance of the qualified certificate to third parties, which reasonably rely on the information specified therein.

7.15 Relying on one's own risk

The responsibility for assessing and relying on the information in the repository and the website of StampIT is borne by the parties that use such information.

The parties agree that they have received the required information in order to decide whether to rely on the information contained in the qualified certificate.

7.16. Obligations 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 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 CPS;
- upon receiving request for revocation of a qualified certificate by the Registration authority, revoke the certificate in accordance with CPS;
- publish the qualified certificate in accordance with CPS;
- provide support to subscribers and relying parties as described in CPS;
- revoke, suspend and resume the qualified certificate in accordance with CPS;
- ensure information about the expiration of the term of validity and resumption of the qualified certificate in accordance with CPS;
- provide public access to CPS and to the valid documents.

7.17 Other guarantees

Except as specified in Regulation (EU) № 910/2014 and the national law, StampIT shall not give guarantees for:

- the accuracy, authenticity, completeness or compliance for any unverified information, which is contained in the qualified certificate or is distributed by StampIT or on its behalf as specified in the relevant description of the products in the CPS of StampIT;
- the accuracy, authenticity, completeness or compliance of any information, which is contained in test or demonstration qualified certificates issued by StampIT;
- provision of information in the qualified certificate unless otherwise specified in the relevant description of the products in CPS;
- although StampIT has the obligation to terminate a qualified certificate, it shall not be liable if it may not terminate it for reasons, which are beyond its control;
- the validity, the accuracy and the availability of directories with issued qualified certificates and certificates revocation list maintained by third parties unless this is explicitly specified by StampIT.

7.18. 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 CPS.