Information Services Plc.
Sofia, 2 Panayot Volov Street; tel.. 943-67-10; fax 943-66-07; E-mail:office@is-bg.net

Certification Practice Statement

Version: 1.02
Published on 27 March 2003

Endorsed with Resolution №260 of March 27th, 2003
by the Communication Regulation Commission

Content

You can send you comments, concerning this CPS at the following e-mail address support@mail.stampit.org or you can send it via ordinary mail to the following address: "Information Services" Plc. – StampIT; 3 "165" Street; Izgrev, 1797 Sofia, Bulgaria; Tel: +359 2 9656244; Fax: +359 2 9656212; E-mail: support@mail.stampit.org.

"Information Services" Plc.;
Sofia, 2 "Panayot Volov" Street;
Tel. 943 6710;
Fax: 943 6607;
BULSTAT: 831641791;
Tax number: 1223007402

1 General overview

This section provides an overview of the StampIT public certification services.

1.1 Certification Service Provider

"Information Services" Plc. is a certification service provider and operates in compliance with the Electronic Document and Electronic Signature Act and its sub-acts and regulations, issued for its appliance. "Information Services" Plc. offers certification services through a Certification Authority and a network of Registration Authorities. The Certification Authority and the Registration Authorities perform their activities on providing certification services on behalf of and in benefit of "Information Services" Plc.

1.1.1 Certification Authority

StampIT is the Certification Authority of "Information Services" Plc. that issues certificates of high class to physical or legal persons. The Certification Authority performs functions associated with public key operation that include issuing, renew, suspend, revocation of certificate, keeping a register and providing access to it.

1.1.2 Registration Authorities

The Certification Authority issues certificates after user identity verification is done. In that regard "Information Services" Plc. provides its services to its subscribers through a network of Registration Authorities that have the following functions:

- Accept, verify, approve or reject the certificate requests
- Register the presented certificate requests for StampIT services
- takes part/attends all stages of subscribers identification as defined/assigned by StampIT in accordance with the type of certificate issued
- Refer official, notarized or other mentioned documents for verification of subscriber's certificate requests.
- It notifies StampIT to issue a certificate, after the approval of the certificate request.
- Register the applied requests for renew, revocation and suspend of a certificate.

The RAs act on local level on the approval and after the authorization of "Information services" Plc., in accordance with its practices and procedures.

1.2 Electronic/Digital Certificates

The electronic/digital certificates, called further for short a Certificate, are formatted data that relate an identified subscriber with a public key. A digital certificate allows a given person taking part in an electronic transaction to prove his/her identity towards other participants in such transaction.

The certificates can be used for functions that include identification, signing, authentication and encryption.

The certificates of the type StampIT Doc and StampIT Doc Pro are qualified signature certificates, according to the Electronic Document and Electronic Signature Act.

1.3 User Interaction for selecting a certification service

StampIT assists its customers in choosing the appropriate certification service. The subscribers should carefully define their requirements to the specific applications for secure communications before applying a request for a given type of certificate.

1.4 Subscribers

Subscribers are physical or legal persons that have applied a certificate request and after the successful execution of the procedure, have been issued a certificate. Prior to verification and issuance of certificate, the subscriber is just a person applying/applicant/ for StampIT certification services.

The subscriber is a titular and author of the electronic signature in cases where the certificate is issued to a physical person.

The subscriber is a titular of the electronic signature when the certificate is issued to a legal person and the author of the electronic signature keeps the private key and is authorized to represent the titular and perform acts on his/her behalf and to his/her benefit.

The relations between "Information services" Plc. as a certification service provider and the subscriber are settled by a contract in a written form.

1.5 Relying parties

Relying parties are physical or legal persons that use PKI services in relation with certificates issued by StampIT that reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a subscriber certificate.

To verify the validity of a digital certificate they receive, relying parties must at all times refer to the StampIT Directory that includes a Certificate Revocation List (CRL) prior to relying on information featured in a certificate

1.6 Certification Practice Statement

The following document "Certification Practice Statement", called for short CPS, is a public statement of the practices of StampIT and the conditions of issuance, suspension, revocation etc. of a certificate issued under StampIT's own hierarchy. Pursuant to the division of the tasks of a CA, this CPS is largely divided in the following sections: Technical, Organizational, Practices and Legal.

This CPS is developed in correspondence to the internationally acknowledged specification RFC 2527 and the Bulgarian legislation.

This CPS is publicly accessible and is available at:
http://www.stampit.org/repository/

E-mail: support@mail.stampit.org

And ordinary mail at the following address:

"Information services" Plc. - StampIT

3"165" street, Izgrev

1797 Sofia, Bulgaria

Tel.:+359 2 9656244

Fax: +359 2 9656212

E-mail: support@mail.stampit.org

2 Technology

This section defines given technological aspects of the infrastructure and StampIT PKI services.

2.1 Issuing and management of certificates

Certificate management of StampIT issued certificates generally refer to the functions that include the following:

- Verification of the identity of an applicant of a certificate.
- Issuance and renew of certificates
- Revocation and suspend of certificates
- De-commissioning of the corresponding private keys through a process involving the revocation of certificates.
- Listing certificates in an issued certificates register.
- Publishing certificates.
- Storing certificates.

StampIT performs certification management, directly or through its own agents.

2.2 StampIT Directories, Repository and Certificate Revocation List

Directly or through third party services, StampIT makes publicly available and manages directories of issued, suspended and revoked certificates to enhance the level of trust in its services. A Certificate Revocation List is such a Directory. Users and relying parties are strongly urged to consult the directories of issued and revoked certificates at all times prior to relying on information featured on a given certificate. StampIT updates its directory of revoked certificates every three hours.

StampIT also publishes provides access to repositories, comprising data and documents, concerning PKI services, including this CPS as well as any other information it considers essential to its services.

2.3 Trustworthy systems

StampIT makes use of trustworthy systems with relation to its services. A trustworthy system is computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

2.4 Types of StampIT Certificates

StampIT offers an array of digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications.

StampIT may update or extend its list of products and services, including the types of certificates it issues, in accordance with the legislation requirements.

Issued, suspended or revoked certificates are appropriately published on the CA directories

2.4.1 Object Certificates

StampIT Object Certificates are issued to legal entities and are used for signing objects such as software. StampIT Object certificates validity period is 1 year.

2.4.2 Server Certificates - StampIT Server Certificate

StampIT Server Certificates are issued to legal entities and are meant for secure communication with a web site. They enable secure web site identification to visitors and allow confidential communication. Their validity period is 1 year.

2.4.3 Personal certificates

2.4.3.1 StampIT Doc Certificates

StampIT Doc Certificates are issued to physical/natural persons and can be used for subscriber identification, secure e-mail communications and secure communications, access to personal data and online Internet transactions of any type, for example Internet subscriber services.

StampIT Doc Certificates provide a high level of identity, where subscriber's personal appearance before the RA is required, in order to prove his/her identity. The validity period of these certificates is 1 year.

2.4.3.2 StampIT DocPro Certificate

StampIT DocPro certificates are issued to physical/natural persons that are authorized to represent legal persons. They can be used for subscriber's identification, secure e-mail communications and secure communications, access to personal data and online Internet transactions.

StampIT DocPro Certificates provide a high level of identity, where subscriber's personal appearance before the RA is required, in order to submit the documents of the legal person and prove his identity. The validity period of these certificates is 1 year.

2.4.3.3 StampIT Enterprise Certificate

StampIT Enterprise Certificates are issued, after the submission of a request by StampIT corporate customers, to physical/natural persons that are corporate customer officers. The physical/natural persons are bounded with the legal person's name, but they are not authorized to make electronic statements on his behalf. The certificates could be used for identification, secure e-mail communications and communications within the organization, access to personal data and online Internet transactions.

The physical/natural persons do not personally appear before the RA, the identification process is done by a person, authorized by the corporate customer. The validity period of these certificates is 1 year.

2.5 Approval of Software and Hardware Devices

StampIT CA approves directly or through an authorized consultant the hardware and software that it uses to provide its public PKI services.

2.6 Extensions

2.6.1 Certificate Extensions

StampIT uses the standard X.509, version 3 based formats for the certificates issued by it. In correspondence to the X.509v3 the CA can define extensions to the main certificate structure.

2.6.2 Including information / data in the certificate extensions

Extensions are usually defined in the subscriber's certificate. They could also be partially defined in the certificate while the remainder to be a document which is incorporated by reference in the subscriber's certificate. Information included in such a way is publicly accessible.

2.7 Key generation process

StampIT uses a trustworthy key generation process for the generation of its private keys. StampIT distributes the secret shares of its private keys. StampIT is the legal owner and holder of the private keys that it uses through to secret sharing. StampIT has the authority to transfer such secret shares to secret-shareholders that have appropriately been authorized

2.7.1 StampIT Key Generation

StampIT securely generates and protects its own private keys, using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorized usage of it. StampIT implements and documents key generation procedures, in correspondence with this CPS. StampIT acknowledges European and commonly approved international practice standards on trustworthy systems and it uses its best endeavours to appropriately follow them.

2.7.2 Secret Sharing

StampIT uses secret sharing and multiple authorized holders of secret shares, to safeguard and improve the trustworthiness in the CA at high security level and provide key recovery.

2.8 StampIT Certificates Profile

It is obligatory that the Certificate profile contains the fields specified below:

2.8.1 Key Usage field

The Key Usage field specifies the purpose of the key contained in the certificate. This field is used when a key could be used for more than one operation and its usage must be restricted.

The possible key purposes identified by the X.509v3 standard are the following:

a) **Digital Signature**, for verifying digital signatures used for object authentication and data integrity verification and have purposes other than those identified in b), e) or f).

b) **Non-repudiation**, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in e) or f) below).

c) **Key encipherment**, for enciphering keys or other security information, e.g. for key transport.

d) **Data encipherment**, for data enciphering, but not keys or other security information as in c) above.

e) **Key certificate signing**, for verifying a CA's signature on certificates (used in CA-certificates only).

f) **CRL signing**, for verifying a CA's signature on the CRL.

2.8.2 Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or as an end-user. This extension should always be marked as critical

otherwise some implementations will ignore it and allow a user certificate to be used as a CA certificate.

2.8.3 Certificate policy

Certificate policy is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within its issuance context. A policy identifier is a unique number within a specific domain that unambiguously identifies the policy.

3 Object identifiers structure

An Object Identifier (OID) is a sequence of integer figures that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

Object Identifier					
Information Services Plc.	StampIT	Roots	Sub CAs	End Entity	Certificates
1.3.6.1.4.1.11290	1	1	1	1	StampIT Doc Pro
				2	StampIT Server
				3	StampIT Object
				4	StampIT Enterprise
				5	StampIT Doc

3.1 Object identifiers values

	Policy Identifier
Information Services Plc.	1.3.6.1.4.1.11290
StampIT	1.3.6.1.4.1.11290.1
StampIT Domestic Root CA	1.3.6.1.4.1.11290.1.1
StampIT Domestic CA	1.3.6.1.4.1.11290.1.1.1
StampIT DocPro	1.3.6.1.4.1.11290.1.1.1.1
StampIT Server Certificate	1.3.6.1.4.1.11290.1.1.1.2
StampIT Object Certificate	1.3.6.1.4.1.11290.1.1.1.3
StampIT Enterprise Certificate	1.3.6.1.4.1.11290.1.1.1.4
StampIT Doc Certificate	1.3.6.1.4.1.11290.1.1.1.5

4 Organization

This part of the document describes the organization and the trust conditions of StampIT.

4.1 StampIT Infrastructure

StampIT strives to maintain its sound organization, technology standing and framework of published practices and procedures.

4.2 Conformance to this CPS

StampIT conforms to this CPS and other obligations it undertakes through contracts when it provides its services.

4.3 Termination of CA Operations

In case of termination of CA operations for any reason, StampIT provides timely notice and transfer of responsibilities maintenance of records to succeeding entities. Before terminating its own CA activities, StampIT takes the following steps:

- Providing the Communication regulation commission (CRC) and its subscribers of valid certificates with four (4) month notice of its intention to cease acting as a CA;
- Revoking all certificates that are still unrevoked or unexpired at the end of the four-month notice period without seeking subscriber's consent;
- Giving timely notice of revocation to each affected subscriber for their certificate revocation within a month after the receipt of a notice from the Communication Regulation Commission;
- Making reasonable arrangements to preserve its records according to this CPS and the legal requirements;
- Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as StampIT's.

4.4 Form of Records

StampIT retains records in electronic and/or in paper-based format. StampIT may require its Registration authorities, subscribers, or their agents to appropriately submit documents in compliance with this requirement.

4.5 Records Storage / Retention Period

StampIT retains in a trustworthy manner records of StampIT digital certificates and associated documentation for a term of no less than 10 years. The retention term begins on the date of expiration or revocation of the certificate. Such records may be retained in electronic, in paper-based format or any other format that StampIT may see fit.

4.6 Activities Logs

StampIT maintains in a trustworthy manner logs of the following events:

- Key generation;
- Key management.

4.7 Audit of Main Functions

StampIT makes its infrastructure available to inside inspection (different from the one, mentioned in the Electronic Document and Electronic Signature Act) by persons, authorized in a defined way by it. StampIT is not obliged to endorse or approve any of the content, findings, and recommendations of such auditing reports and it may review such auditing reports with a view to additionally protect StampIT services. StampIT applies references to its judgment in accordance with the applied inside and publicly accessible policies and procedures.

4.8 Contingency Plans and Disaster Recovery

To maintain the integrity of its services StampIT implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plan is revised and updated at least once a year.

4.9 Availability of StampIT Certificates

StampIT may make available to other parties copies of certificates in which StampIT is the subject as well as any related revocation data to verify a signature that is verifiable with reference to a digital certificate.

4.10 Publication of Information on Issued Certificates

StampIT publishes all issued certificates and the whole information on revoked certificates or the validity of these certificates.

4.11 Confidentiality of Information

StampIT observes applicable rules on the protection of personal data. StampIT also treats as confidential information that includes the following:

- Subscriber agreements;
- Certificate applications archive;
- Transactions archive;
- External or internal audit trail records and reports;
- Contingency plans and disaster recovery plans;
- Internal tracks and records on the operations of StampIT infrastructure, certificate management and enrollment services and data.

StampIT does not release nor it is required to release any confidential information without an authenticated, reasonably specific request by an authorized party specifying the following:

- The party to whom StampIT imposes a duty to keep information confidential;
- The party requesting such information;
- An order or decision, taken by an authorized institution, if any.

StampIT may charge an administrative fee to process such disclosures.

4.12 Physical Protection

Physical access to the secure part of StampIT facilities is limited to appropriately authorized individuals, in correspondence to their operational obligations. Precautions are taken for protection from environmental hazards and compromising of assets, leading to interruption of business activities and also for detecting and pre-

venting attempts for compromise or theft of information and devices processing information.

4.13 Personnel Management Practices

Personnel management practices include measures that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

4.13.1 Confidential Information

All personnel that have access to confidential information are obliged to handle it in strict confidence.

4.13.2 Confidential Declarations

All employees of the certificate service provider that have access to confidential information, sign confidential declarations.

4.14 Publication of information

StampIT certificate services and StampIT repository are accessible through the following means of communication:

At web address: http://www.stampit.org/repository/

By e-mail E-mail: support@mail.stampit.org

By ordinary mail:

"Information services" Plc. – StampIT

3"165" street, Izgrev

1797 Sofia, Bulgaria

Tel.: +359 2 9656244

Fax: +359 2 9656212

E-mail: support@mail.stampit.org

5 Practices and Procedures

This part of the document presents the practices and procedures of StampIT PKI services.

5.1 Certificate Application Requirements

Prior, upon or during application for a digital certificate, applicants of certificates take the following steps prior to requesting a StampIT certificate:

- Submit a certificate application and agree with the terms of a subscriber agreement and this CPS;
- Provide proof of their identity according to StampIT standard defined procedures.

5.1.1 Delegation

An application for a StampIT digital certificate can be made in person or through an authorized person/representative depending on the type of a certificate and the requirements for its issuance. The delegation is proved by a notary endorsed letter, a document for the current status of the company and other documents, defining the connection between the titular and the authorized person/representative and his/her rights.

5.1.2 Key Pair Generation

StampIT registration authorities are exclusively responsible to generate securely the subscriber's private key pair, using a secure signature creation device. The subscriber shall attend the generation process, depending on the type of certificate and the requirements for its issuance.

5.1.3 Key Pair Protection

Subscribers are exclusively responsible to take all necessary measures to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private key.

5.1.4 Delegating Responsibilities for Private Keys

Subscribers shall be exclusively responsible for the acts and omissions of authorized by them persons or their partners they use to generate, retain, or destroy their private keys.

5.2 Subscriber Identification

Prior to issuing a certificate StampIT mandates controls to establish the identity of the future subscriber. Such controls are performed by StampIT RAs. A StampIT RA also supervises the application of such procedures on the basis of StampIT issued guidelines.

5.3 Validation Information for Certificate Applications

Applications for StampIT certificates are supported by appropriate documentation to establish the identity of an applicant as described in the product information below.

StampIT may modify the requirements related to application information for individuals to respond to its own requirements, the business context of the usage of certificates, or as it may be prescribed by law.

Such documentation shall include the following identification elements, in correspondence to the type of certificate and the requirements for its issuance:

- Name of the applicant;
- Personal ID number;
- Name of the legal representative and authorization letter;
- Domain name;
- Name of the organization/legal person;
- Organizational unit;
- Address, city/town, zip code, country;
- Technical and billing contact persons and legal representative;
- National Tax Register number;
- BULSTAT ID code;
- Server Software;
- Payment Information;
- Proof of right to use name;
- Proof of Organization registration;
- Organizational status document, issued not earlier than 1 month before the certificate application submission, a formal letter from office of Dean or Principal (for Educational Institutions), official letter from an authorized representative of a local government organization;
- Registration form properly filled in and signed;
- Certificate request signed;
- Subscriber agreement signed.

5.4 Validation Requirements for Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information, StampIT confirms the following information:

- the certificate applicant is the same person as the person identified in the certificate request;
- the certificate applicant holds the private key corresponding to the public key to be included in the certificate;
- the information to be published in the certificate is accurate, except for non-verified subscriber information;
- any authorized person/representative who applies for a certificate should be duly authorized to do so.

StampIT controls the accuracy of the information published as submitted by the applicant at the moment the certificate is issued.

In all cases and for all types of StampIT certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify StampIT of any changes in it after the issuance of the certificate.

5.4.1 Personal Appearance/Presence

To establish the link between the applicant and the applicant's public key StampIT may require the personal presence of the applicant before a RA for certain types of certificates.

5.4.2 Third-Party Confirmation of Information of a Given Legal Entity

StampIT may require a third party to confirm information on a legal entity that applies for a StampIT digital certificate. StampIT accepts confirmation from third party organizations, third party databases and government entities while it may examine other third party references which business is related to the applicant's one.

StampIT controls include Trade Registry verifications or other databases that confirm the registration of the legal person/entity.

StampIT may use any means of communication at its disposal to ascertain the identity of a legal person/entity.

5.4.3 Serial Number Assignment

StampIT has discretion to assign Relative Distinguished Names (RDNs) and certificate serial numbers that are included in a certificates issued by StampIT.

5.5 Time to Issue a Certificate

StampIT makes reasonable efforts to confirm certificate application information and issue a digital certificate within 5 work days after the receipt of the documents.

5.6 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application StampIT approves an application for a digital certificate.

If the validation of a certificate application fails, StampIT rejects the certificate application. Upon such rejection StampIT promptly notifies the applicant and provides a reason for such failure. Applicants whose applications were rejected can apply a certificate request again.

5.7 Certificate Issuance and Subscriber Consent

StampIT issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid the moment a subscriber accepts it. Issuing a digital certificate means that StampIT accepts a certificate application.

StampIT issues a certificate pursuant to an applicant's consent. Consent to issue a certificate is demonstrated by submitting an application notwithstanding the fact that acceptance notice of a certificate has not yet occurred.

Upon fulfillment of a certificate request, the applicant accepts the certificate content.

The certificate service provider immediately publishes the certificate in the supported by it register.

5.8 Certificate Validity

Certificates are valid upon issuance by StampIT and their acceptance by the subscriber.

5.9 Certificate Acceptance by the Subscriber

A subscriber is deemed to have accepted a certificate when:

- Subscriber's approval of the certificate is manifested to StampIT by means of an on-line or email notice sent to StampIT by the subscriber;
- The certificate is used for the first time by the subscriber;
- 15 days pass from the date of the issuance of a certificate, in case the subscriber has not put in a claim for the certificate's content.

5.10 Publication of Issued Certificates

StampIT publishes a copy of the certificate in a StampIT repository. While StampIT may publish a certificate on other repositories, as it might see fit it assumes no

responsibility for the validity, completeness or availability of directories supported by such third parties. Subscribers on their turn may also publish their StampIT certificates in other repositories.

5.11 Digital Signatures Verification

Verification of a digital signature aims at determining that:

- the digital signature was created by the private key corresponding to the public key listed in the signer's certificate;
- the associated message has not been altered since the digital signature was created.

5.12 Reliance on Digital Signatures

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the verifier. A digital signature can be trusted to rely upon if:

- The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate;
- Reliance is reasonable under the circumstances.

5.13 Renewal

The validity period of StampIT certificates is indicated on the appropriate certificate field and it is one year (365 days) from the date of issuance. While renewal requirements may vary from those originally required to subscribe to the service, StampIT publishes and updates a conditional renewal of digital certificates it has issued. Renewal is allowed only if all data on a certificate remains correct as per the initial application.

Certificate renewal is done in accordance with the current conditions at the moment of renewal.

The subscriber must at all times control the correctness and accuracy of the information published in a renewed certificate. Requests for renewal must be addressed to StampIT at least 10 days prior to expiration date.

5.14 Notice Prior to Expiration

To keep intact the capacity of users of digital certificates to digitally sign, approximately thirty (30) days prior to the expiration of a digital certificate, StampIT shall make reasonable efforts to notify subscribers via e-mail, of the imminent expiration of a digital certificate.

5.15 Certificate Suspension and Revocation

Suspension of a certificate is to make it temporarily inoperable. Revocation of a certificate is to permanently end the operational period of a certificate. StampIT suspends or revoke digital certificates if:

- Availability of sound information/proof and conditions that show there has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key;
- The certificate's titular/subject (whether StampIT or a subscriber) has breached their obligation under this CPS;
- The performance of an obligation under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause

beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- There is a modification of the information that is included in the subscriber's certificate content;
- Under the request of the institutions mentioned in the legislation acts/regulations.

5.15.1 Suspension or Revocation Request

The subscriber or other appropriately authorized parties can request suspension or revocation of a certificate. Suspension or revocation can be done through StampIT web site, by email or phone. The identity of the requesting party shall be verified as appropriate.

5.15.2 Effect of Suspension or Revocation

During suspension, or upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The validity of the certificate is resumed with the expiration of the suspension/revocation term in case the reasons for it are declined or if the subscriber requests it in compliance with the legal acts.

5.15.3 Certificate Suspension and Revocation Notice

StampIT informs the subscriber about the certificate suspension or revocation via communication means it finds appropriate.

5.16 Certificate Management Procedures

5.16.1 Renewal of StampIT Certificates

Renewal of a certificate, issued by StampIT, could be done only in case all the data in the certificate content remains unchanged, as in the initial certificate issuing request. The content of the renewed certificate is identical with the one in the current certificate besides the validity term, which starts on the renewal date, written in the certificate.

In correspondence to the renewal requirements StampIT RA operator may require current documents, proving the accuracy and correctness of the information included in the certificate content at the moment. The applicant signs a declaration that the initially submitted data and the data written in the certificate content are accurate, correct and unchanged at the moment.

Upon availability of any changes in the data and circumstances, concerning the physical and/or legal person, the applicant should apply a certificate issuing request for a new certificate.

5.16.1.1 Documents for Renewal of StampIT Certificates:

The documents that could be required by the subscriber include but are not limited to the following:

1. Official Company Registration Decision/proof – original and copy, signed by the applicant.
2. Tax registration document/proof - original and copy, signed by the applicant.
3. BULSTAT registration document/proof - original and copy, signed by the applicant.

4. Proof of organizational status, issued not earlier than a month before applying a certificate renewal request– original and copy, signed by the applicant.
5. Personal Identification document (Personal ID card) of the physical person that applies for a renewal of a certificate– original and copy signed by the applicant.
6. Notary signed power letter, proving that the physical person is authorized by the legal person to represent it – original and copy signed by the applicant. This document is required in case the authorization reason is not included in the other documents about the status of the legal person.
7. Signed certificate renewal request.
8. Payment document.

5.16.1.2 Certificate Renewal procedure

The following steps describe the certificate renewal process:

1. The applicant personally appears before the RA and applies a "Renewal Request", accompanied by certificate renewal documents.
2. The applicant's identity is verified and the compliance of the data and the circumstances, concerning the the applicant at the moment of renewal.
3. The RA operator checks the submitted documents and applies a certificate renewal request to the CA.
4. The CA renews the certificate and sends it back to the RA.
5. The certificate is stored on a smart card and it is delivered to the subscriber.
6. The renewed certificate is published in StampIT public LDAP directory structure.
7. Acceptance of the certificate by the subscriber – the renewed certificate is considered accepted with the act of its issuance as its content was confirmed when the "Renewal Request" was applied by the subscriber.

Renewal of certificates could be done only for certificates that are valid at the moment a renewal request is applied at the CA. That is why the renewal request should be received not later than 10 days before the expiration of the certificate validity.

5.16.2 Revocation of a certificate

Revocation of a certificate is done by StampIT after the application of a Revocation Request by the RA. To make this request the RA operator is obliged to verify the identity and authorization of the subscriber.

5.16.2.1 Revocation reasons

Revocation reasons for termination of a certificate could be, but are not limited to the following:

1. Reasonable information and circumstances proving that there is loss, theft, change, unauthorized disclosure or other private key compromise are available.
2. Termination of the physical person's authorization towards the legal person, written in the certificate content.
3. Termination of the subscriber's legal person.
4. Death or injunction of the physical person.
5. Proof that the certificate was issued on the base of incorrect data.
6. Change of the information that was initially submitted and included in the subscriber's certificate.
7. In case of not keeping subscriber's obligations on the certificate service contract.

8. Under the subscriber's request after a verification of his identity and authorization.

The validity of all the certificates issued by StampIT is unconditionally terminated in case of StampIT activity cessation.

5.16.2.2 Documents for revocation of StampIT certificates:

The documents that could be required from the subscriber in case of applying a certificate revocation request include but are not limited to the following:

1. Document for personal identification (ID card) of the physical person requesting revocation of the certificate – original and copy signed by the subscriber.
2. For legal persons – document that shows the physical person's authorization by the legal person - original and copy signed by the subscriber.
3. Signed certificate revocation request.

5.16.2.3 Certificate revocation procedure

The following steps describe the certificate revocation:

1. The subscriber personally appears before the RA and applies a certificate revocation request accompanied by the documents proving his/her identity and authorization.
2. The RA operator verifies the subscriber's identity and authorization at the moment of applying a certificate revocation request.
3. The RA operator submits the certificate revocation request to the CA.
4. The CA revokes the certificate.
5. The revoked certificate is included in the StampIT certificate revocation list which is publicly accessible at the following address http://www.StampIT.org/CRL/StampIT.crl

After the certificate revocation the subscriber can apply a new certificate issuing request and after payment of the due fees and successful completion the issuing procedure the subscriber can receive a new StampIT certificate.

5.16.3 Suspend of StampIT certificates

If certain reasons are available StampIT certificates could be suspended for the required period of time but it should not be longer than 48 hours.

The certificate is considered invalid for the time it was suspended.

5.16.3.1 Suspend Reasons

StampIT certificates could be suspended only after an order by the Communication Regulation Commission – in case third parties' interests are endangered or in case there exists evidence for breaking the law.

5.16.3.2 Certificate suspension procedure

The following steps describe the certificate suspension process:

1. The CA receives an order in written form by the Communication Regulation Commission for suspend of the certificate.
2. The CA suspends the certificate and publishes it in the certificate revocation list that is publicly accessible at the following address:http://www.StampIT.org/CRL/StampIT.crl.
3. The CA immediately informs the subscriber for the suspend of the certificate.

5.16.4 Renew / Renovation of a certificate

The certificate is renewed/renovated after expiration of the suspension term in case the suspension reasons no longer exist or under the subscriber's request after StampIT, respectively the Communication Regulation Commission are assured that the subscriber was informed about the suspension reason, and the renewal/renovation request was applied as a result of the above. The CA renews the certificate by removing it from the certificate revocation list. The moment the certificate is renewed it is considered valid.

5.16.4.1 Reasons for certificate renew

1. Under the order of the Communication Regulation Commission – when the suspension was performed by their order.
2. After the expiration of the suspend period of the certificate.
3. By subscriber's request.

5.16.4.2 Certificate Renovation procedure

1. Under the order of the Communication Regulation Commission – StampIT receives the certificate renovation order given by the CRC. The CA renovates the certificate by removing it from the certificate revocation list.
2. After the expiration of the suspend term – after the expiration of a period of time of 48 hours from the moment of the certificate suspend, the certificate is automatically renovated by the CA, in case a valid certificate revocation request is not received according to the procedure.
3. Under the subscriber's request – after StampIT, respectively CRC, is assured that the subscriber was informed about the suspend reason and the renovation request was applied as a result of the above mentioned. The certificate renovation request could be applied after the personal appearance of the subscriber before the RA. The certificate renovation request by the subscriber is realized under the following procedure:
    - The subscriber personally appears before the RA and applies a renovation request accompanied by the documents that prove his/her identity and authorization;
    - Verification of subscriber's identity and authorization;
    - The RA operator examines the submitted documents and sends a certificate renovation request to the CA;
    - The CA renovates the certificate.

The moment the CA renovates the certificate the certificate is considered valid. If the CA receives a valid certificate revocation request within the suspend period, StampIT revokes the certificate in accordance with the approved procedures.

6 Legal Conditions of Certificate Issuance

This part describes the legal representations, warranties and limitations associated with StampIT digital certificates.

6.1 StampIT Service Representations

StampIT makes to all subscribers and relying parties certain representations regarding its public service, as described below. StampIT reserves its right to modify such representations as it sees fit or required by law.

6.2 Information Incorporated by Reference into a Digital Certificate

StampIT incorporates by reference the following information in every digital certificate it issues:

- general conditions for the provided services;
- an applicable certificate policy;
- the extensions content that is not completely explained in the certificate;
- reference to the certification service provider's registration at the Communication Regulation Commission;
- any other information/data that should be included in the certificate fields.

6.3 Pointers to Incorporate by Reference

To incorporate information by reference StampIT uses URLs (Universal Resource Locators), OIDs (Object Identifiers) or any other means to incorporate information by reference, as they may become available.

6.4 Limitations and Liability

StampIT certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, intended purpose of the certificate and disclaimers of warranty. Such information may be displayed through a hypertext link. To communicate required information StampIT may use:

- State field – for subscriber's data insertion;
- Issuer alternative name – for the certificate type;
- StampIT standard resource index/register for the certification policy;
- Other appropriate fields in the certificate's content;
- Private or other registered authorizations.

6.5 Publication of Certificate Data

StampIT reserves its right and the subscriber agrees to publish a certificate and certificate related data in any accessible repository as LDAP (Light Directory Application Protocol) directories, CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol).

StampIT manages directories of featured certificates to enhance the level of trust in its services. Users and relying parties are strongly advised to consult the directories of issued and revoked certificates at all times prior to relying on information featured on a certificate.

6.6 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of StampIT certificates the subscriber (not StampIT) has a continuous obligation to monitor the accuracy, genuineness and completeness of the submitted information and immediately notify StampIT of any such changes at their occurrence.

6.7 Publication of Information

Public information, concerning StampIT operation, may be periodically updated. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

6.8 Interference with StampIT Operation

Subscribers, relying parties and any other parties shall refrain from monitoring, interfering with, or reverse engineering the information systems of StampIT services including the key generation process, the public web site and StampIT repositories except as explicitly permitted by this CPS or upon prior written approval of StampIT.

6.9 Standards

StampIT assumes that user software that is claimed to be compliant with X.509v3 and other applicable standard enforces the requirements set out in this CPS. StampIT cannot warrant that such user software will support and enforce controls required by StampIT while the user should seek appropriate advice.

6.10 StampIT Partnerships Limitations

Contracting partners of StampIT shall refrain from undertaking any actions that might imperil, put in doubt or reduce the trust associated with StampIT products and services.

6.11 StampIT Limitation of Liability for a StampIT Contracting Partner

StampIT network may include RAs that operate under StampIT practices and procedures. StampIT warrants the integrity of any certificate issued under its own CA within the limits of StampIT CPS.

6.12 Secret Shares

StampIT uses secret shares to protect its private key.

6.13 Choice of Cryptographic Methods

Parties acknowledge that they are solely responsible for and have exercised independent judgment in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques in compliance with the legal acts.

6.14 Reliance on Unverified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against a CRL or any other available

directory published by StampIT. Relying parties are alerted that an unverified digital signature cannot be assigned as the signature of the subscriber.

StampIT adequately informs relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository.

6.15 Invalid Certificates

An applicant for a StampIT certificate that the applicant or StampIT does not accept as a valid one for any reason whatsoever, does not have the right to create a digital signature using a private key corresponding to the public key included in a certificate. In that case there are no conditions of relying upon such certificate.

6.16 Refusal to Issue a Certificate

StampIT reserves its right to refuse to issue a certificate to any person that does not comply with the issuance procedures and/or does not submit the required documents for issuing a certificate, without incurring any liability or responsibility for any damages arising out of such refusal.

6.17 Subscriber Obligations

Unless otherwise stated in this CPS, StampIT subscribers and not StampIT shall exclusively be responsible of the following:

- Have knowledge on using digital certificates and PKI;
- When generating the key pair, ensure that the public key submitted to StampIT corresponds to the private key used;
- Provide correct, accurate and complete information to StampIT;
- Re-apply for a certificate if at the stage of certificate renewal any information originally submitted has changed since it had been originally submitted to StampIT;
- Read, understand and agree with all terms and conditions in this StampIT CPS and associated with it documents published in StampIT Repository;
- Use StampIT certificate only for legal purposes and in compliance with this StampIT CPS;
- Notify StampIT or a StampIT RA of any changes and incompleteness in the information submitted;
- Cease using a StampIT certificate if any information in it becomes misleading, obsolete or invalid;
- Cease using a StampIT certificate if such certificate is expired and remove it from any applications or devices it has been installed on;
- Prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published on a StampIT certificate;
- Request revocation of a certificate in case of an occurrence that materially affects the integrity of a StampIT certificate;
- Request revocation of a certificate if any part of the information in it becomes misleading obsolete or invalid;
- For acts and omissions of partners they use to generate, retain, or destroy their private keys;
- To refrain from submitting to StampIT or materials that contain statements that are libelous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive.

6.18 Subscriber's Representations upon Acceptance

Upon accepting a certificate the subscriber represents to StampIT and to relying parties that at the time of acceptance and until further notice will comply with:

- All representations made by the subscriber to StampIT regarding the information contained in the certificate are accurate and true;
- All information contained in the certificate is accurate and true while the subscriber shall act promptly to notify StampIT of any material inaccuracies and changes in such information;
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS;
- Use a StampIT certificate only in conjunction with its purpose;
- The subscriber retains control of his/her private key, uses trustworthy systems, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use;
- The subscriber is an end-user subscriber and does not have the right to use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as an CA unless expressly agreed in writing between subscriber and StampIT;
- subscriber accepts the terms and conditions of this CPS.

6.19 Obligations of StampIT Registration Authorities

StampIT RAs obligations are as follows:

- Receive applications for issuing and renewing StampIT certificates in accordance with this StampIT CPS;
- Perform all actions prescribed by StampIT procedures and this CPS;
- Receive, verify and relay to StampIT all requests for revocation and suspension of a StampIT certificate in accordance with StampIT procedures and this CPS.

6.20 Information for a Relying Party

A party relying on a StampIT certificate should comply with the generally acknowledged by the international practice rules as follows:

- Have knowledge on using digital certificates and PKI;
- Study the limitations to the usage of digital certificates;
- Get to know the terms of StampIT CPS;
- Verify a StampIT certificate by using among others accepted means the CRL;
- Trust a StampIT certificate only to a reasonable extent for the given circumstances.

6.21 Correctness, accuracy and completeness of the information

Subscribers shall be responsible for the correctness, accuracy and the completeness of the information they present for use in certificates issued under this CPS.

6.22 Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties that,

reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

6.23 Duty to Monitor Subscriber's representatives/authorized persons

The subscriber has the obligation to constantly control the data that their representative supplies to StampIT. The subscriber must promptly notify the issuer of any misrepresentations and omissions made by their representative.

6.24 Use of Representatives

For certificates issued at the request of a subscriber's representative, both the representative and the subscriber shall jointly and severally indemnify StampIT, and its representatives and contractors.

6.25 Usage Conditions of StampIT Repository and Web site

Parties (including subscribers and relying parties) accessing StampIT Repository and web site agree with the provisions of this CPS and any other conditions of usage that StampIT may make available except for information provided in or used for demo, free of price and test certificates. Parties demonstrate acceptance of the conditions of usage by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any information or services provided. Conditions of usage of StampIT Repository include:

- Information provided as a result of the search for a digital certificate;
- Providing the possibility for verification of the status of digital signatures created with a private key corresponding to a public key included in a certificate;
- Information published on the web site of StampIT;
- Any other services that StampIT might advertise or provide through its web site.

6.26 Reliance at Own Risk

It is the sole responsibility of the parties that access information featured in StampIT Repository and web site to assess and rely on information featured therein.

Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate.

6.27 Accuracy of Information

StampIT recognizing its trusted position makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information.

6.28 Failure to Comply With the Conditions

Failure to comply with the conditions of usage of StampIT Repositories and web site may result in terminating the relationship between StampIT and the party.

6.29 StampIT Obligations

To the extent specified in the relevant sections of the CPS, StampIT is obliged to:

- Comply with this CPS and its internal or public policies and procedures;

- Comply with applicable laws and regulations;
- Provide infrastructure and certification services, including the establishment and operation of StampIT Repository and web site for the operation of PKI services;
- Provide Trust mechanisms, including a key generation mechanism, secure signature creation device, and secret sharing procedures regarding its own infrastructure;
- Provide prompt notice in case of compromise of its private keys;
- Publicly provide and validate application procedures for the various types of certificates;
- Issue and renew digital certificates in accordance with this CPS and fulfill its obligations presented herein;
- Upon receipt of a request from a RA operating within StampIT network act promptly to issue a StampIT certificate in accordance with this StampIT CPS;
- Upon receipt of a request for revocation from an RA it acts to revoke a certificate in accordance with this CPS;
- Publish certificates in accordance with this CPS;
- Provide support to subscribers and relying parties as described in this CPS;
- Revoke, suspend and renew certificates according to this CPS;
- Provide information on the validity expiration and renewal of certificates according to this CPS;
- Make available copies of this CPS and its applicable documents to public access.

StampIT acknowledges that it has no further obligations under this CPS.

6.30 Correspondence to a Particular Purpose

StampIT disclaims all warranties and obligations, in case its products and/or services are used not in accordance with their predefined purpose/function , and any warranty of the accuracy of provided but unverified information.

6.31 Other Warranties

Except as it may have otherwise been stated in the Bulgarian legislation on electronic signatures, StampIT does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or disseminated by or on behalf of StampIT except as it may be stated in the relevant product description below in this StampIT CPS;
- The accuracy, authenticity, completeness or fitness of any information contained in free, test or demo certificates, issued by StampIT;
- Representation of information in a certificate if otherwise stated in the relevant product description in this CPS;
- Quality, functions or performance of any software or hardware devices;
- Although StampIT is responsible for the revocation of a certificate it cannot be held liable if it cannot execute it for reasons outside its own control;
- The validity, completeness and availability of directories of certificates and CRLs, supported by third parties unless that is explicitly stated by StampIT.

6.32 Non Verified Subscriber Information

Non-verified information will be considered the one that is not included in the scope of the obligatory data in the certificate content, in compliance with Article 24 of the Electronic Document and Electronic Signature Act and that cannot be verified by the certificate service provider by official documents or in another way accepted by law. The scope of the non-verified information may include but it is not limited to:

- E-mail address;
- Telephone and/or fax;
- Organizational unit;
- Authorized physical person's position.

6.33 StampIT Liability Limitation

In no event except for wilful misconduct shall StampIT be liable for:

- Missed profits;
- Loss of data;
- Any other indirect, consequential damages arising from or in connection with the use, delivery, license, performance or non performance of certificates and digital signatures;
- Any other damages except for those due to reliance on the information featured on a given certificate, based on the verified information in the certificate;
- A fault in the verified information that is due to fraud or wilful misconduct of the applicant;
- Usage of a certificate that has not been issued or used in conformance with this CPS;
- Usage of a certificate that is not valid;
- Usage of a certificate that exceeds given limitations stated upon it or on this CPS;
- Security, usability, integrity of products, including hardware and software used by the subscriber;
- Compromise of a subscriber's private key.

6.34 Damage Limitations

In no event (except for wilful misconduct) will the aggregate liability of StampIT to all parties including without any limitation a subscriber, an applicant, a recipient, or a relying party for all digital signatures and transactions related to such certificate exceeds the limit for such certificates that is stated in this CPS.

6.35 CPS Application

When this CPS conflicts with other rules, guidelines, or policies, this CPS conditions shall prevail and bind the subscriber except as to other contracts signed before the publishing of this CPS.

6.36 Intellectual Property Rights

StampIT or its contracting partners own all intellectual property rights associated with its databases, web sites, StampIT digital certificates and any other publication originating from StampIT including this CPS.

6.37 Infringement and Damages

StampIT subscribers are obliged when submitting to StampIT and use a domain and distinguished name (and all other certificate application information) not to interfere with or infringe any rights of any third parties with respect to their trademarks, trade names, or any other intellectual property right. StampIT subscribers are obliged not to use the domain and distinguished names for any unlawful purpose, unfair competition, and not submitting, confusing or misleading information to a person, whether natural or incorporated.

Subscribers should indemnify StampIT for any loss or damage resulting from any such interference or infringement.

6.38 Ownership

Certificates are property of StampIT. StampIT gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates shall not be published in any publicly accessible repositories or directories without the express written permission of StampIT.

The scope of this restriction is also intended to protect subscribers against the unauthorized publication of their personal data featured on a certificate.

Private and public keys are property of the subscribers who rightfully issue and hold them.

Secret shares of StampIT private key remain property of StampIT.

6.39 Applicable Legislation / Governing Law

This CPS is issued by, and construed in accordance with the Bulgarian legislation. This choice of legislation is made to ensure uniform interpretation of this CPS, regardless of the place of residence or subscriber's place of use of StampIT digital products and services. The Bulgarian legislation applies in all StampIT contractual relationships in which this CPS may apply in relation to StampIT products and services where StampIT acts as a provider, supplier, beneficiary receiver or otherwise.

6.40 Jurisdiction

Settlement of all disputes that may arise from or in connection with this CPS, or while providing StampIT PKI services will be referred to the competent District Court of Sofia.

6.41 Dispute Resolution

If a dispute arises in connection with issuance, renewal, suspension or revocation of a StampIT certificate, the persons involved can lodge a complaint.

The complaints should be lodged in written form to the Chief Executive Director of "Information Services" Plc., via the Director of PKI Department at the following address: Sofia – 1797, Izgrev, 3 "165" street.

Within 7 days after the receipt of the complaint the Director of PKI Department sends the complaint and a written statement on it to the Chief Executive Director of "Information Services" Plc.

The Chief Executive Director of "Information Services" Plc. considers the complaint and comes up with a decision within 14 days after its receipt and informs the person that lodged it in written form.

6.42 Assignation

The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer) or otherwise, provided such assignment is undertaken consistent with this CPS, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

6.43 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to effect the original intention of the parties.

EACH AND EVERY PROVISION OF THIS CPS THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF OR LIMITATION UPON ANY WARRANTIES OR OTHER OBLIGATIONS, OR EXCLUSION OF DAMAGES IS INTENDED TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND IS TO BE ENFORCED AS SUCH.

6.44 Interpretation

This CPS shall be interpreted within the boundaries of the commonly accepted business practices under the circumstances and intended usage of a product or service. In interpreting this CPS parties shall also take into account the scope and application of the services and products of StampIT and its network of Registration Authorities as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS, are for all purposes an integral and binding part of the CPS.

6.45 Waiver

This CPS shall be enforced, as a whole while failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision.

6.46 Notice

StampIT accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from StampIT the sender of the notice shall deem communication effective. If the sender does not receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

"Information Services" Plc.

3 "165'" street, Izgrev

1797 Sofia, Bulgaria

Tel.: + 359 2 9656244

Fax: + 359 2 9656212
E-mail: support@mail.stampit.org

6.47 Fees

StampIT may charge subscriber fees for the use of StampIT products and services as published on its web site. StampIT retains its right to effect changes to such fees.

6.48 Continuation of CPS operability

The obligations and restrictions contained under sections entitled: *"Audit of main activities", "Confidential Information"," Obligations of StampIT", and "Limitations Upon Such Obligations, Indemnity by the Subscribe"r* retain their operability after the termination of this CPS.

7 Products and Services Provided by StampIT

7.1 General

StampIT certificates offer identity assurance requiring personal presence before a registration authority for certificates issued to physical persons. For issuing certificates to legal persons and corporate customers StampIT requires corporate documentation to verify the identity of the legal person applying for a certificate.

StampIT certificates are issued to physical persons or legal persons.

The typical validity period of StampIT certificates is 1 year or as indicated on StampIT web site.

7.2 Submitted Documents to Identify the Applicant

In all cases, the applicant must submit to StampIT Registration Authority a signed registration form, signed request form, signed subscriber agreement and a copy of identity proof as indicated in the registration procedure. Depending on the class of certificate the applicant must additionally submit documents identifying the legal person and authorization reasons.

StampIT may require additional proof for verification of the applicant's identity and/or the legal person.

For certificates issued to physical persons that are authorized to represent legal persons/entities, the applicant should submit a signed registration form, certificate issuing request, Subscriber's Agreement, legal person's/entity's documents and all other required documents in that regard before StampIT.

For certificates issued to Government institutions, organizations and schools, besides the above mentioned documents, the applicant should submit a notary signed power letter that authorizes him to apply a certificate issuing request before StampIT.

7.3 Time to Confirm Submitted Data

StampIT makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames that may vary from one (1) to five (5) working days.

7.4 Personal StampIT Doc certificates

StampIT Doc certificates are issued to physical persons and could be used for identification, secure e-mail messaging and secure e-mail communications, personal financial information access and online Internet transactions of any type, for example Internet Subscribe Services.

7.4.1 Content

The content of the information published in the certificate may include the following elements:

- Subscriber's e-mail address;
- Subscriber's name;
- Permanent address;
- Subscriber's data;
- Public key;
- Country/zip code;
- Issuing CA(StampIT);

- StampIT electronic/digital signature;
- Type of the algorithm;
- Certificate validity;
- Certificate serial number.

7.4.2 Documents for issuing a StampIT Doc certificate:

1. Identification document (ID card) of the physical person, whose name is filled in the certificate content – original and copy, signed by the applicant.
2. Signed Subscriber Agreement.
3. Signed Certificate issuing request.
4. Registration form signed and filled in Roman alphabet.
5. Payment document/proof.

7.4.3 Certificate issuing procedure

The following steps describe the certificate request process:

1. The applicant must personally appear before the StampIT RA and apply a "Certificate Request", accompanied by a signed registration form and documents for issuing a certificate.
2. Verification of subscriber's identity and completeness of submitted documents.
3. The RA operator generates the key pair on a smart card in the subscriber's presence and submits a request before the CA for issuing a certificate.
4. After a formal verification of subscriber's data, the CA issues a certificate, which is sent back to the RA.
5. The certificate is stored on a smart card and the smart card is delivered to the subscriber.
6. The subscriber receives the software for smart card access and he/she is obliged to change the smart card access PIN before the first usage of the certificate.
7. The smart activating data is sent to the subscriber via ordinary mail – by courier services or registered mail to a mentioned by the subscriber address.
8. The issued certificate is published in the StampIT public LDAP directory STRUCTURE.

7.4.4 Certificate profile:

StampIT Doc Certificate			
Signature Algorithm	Sha1/RSA		
Issuer	CN	StampIT Domestic CA	
	C	BG	
	O	Information Services Plc.	
	OU	StampIT	
Validity	1 Year		
Subject	C	Country	
	L	Locality	
	CN	Common Name	
	E	E-Mail	
	POC	Postal Code	
	STA	Address	
	S	State	EGN:[ЕГН]
	PN	Phone	
Public Key Length/Type	RSA 1024 bits		
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment		
Issuer Alternative Name (Non Critical)	/OU=Doc Certificate		
Extended Key Usage Field (Non Critical)	Client Authentication, E-Mail Protection		
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]		
Subject Key Identifier (Non Critical)	[Subject Key ID]		
Basic Constrains (Critical)	No (End Entity)		
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl		
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.5 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/		

7.5 Personal StampIT DocPro certificates

StampIT DocPro certificates are issued to physical persons that are authorized to represent legal persons. The certificates could be used for identification, secure e-mail messaging and secure e-mail communications, personal financial information access and online Internet transactions of any type, for example Internet Subscribe Services.

7.5.1 Content

The information published in the certificate content may include, but it is not limited to the following elements:

- E-mail address of the authorized representative;
- Name of the authorized representative;
- Public key;
- Country/zip code;
- Name of the legal person;
- Headquarters address of the legal person;
- Legal person data;
- Issuing CA;
- StampIT digital/electronic signature;
- Type of the algorithm;
- Certificate validity;
- Certificate serial number.

7.5.2 Documents for issuing a StampIT DocPro certificate:

1. Official/Court Company Registration Decision – original and copy, signed by the applicant.
2. Tax registration document/proof - original and copy, signed by the applicant.

3. BULSTAT registration document/proof - original and copy, signed by the applicant.
4. Proof of organizational status, issued not earlier than a month before applying a request for a certificate – original.
5. Identification document (Personal ID card) of the physical person that is filled in the certificate content and is authorized to represent the legal person – original and copy, signed by the applicant.
6. Notary signed power letter, proving that the physical person is authorized by the legal person to represent it – original and copy, signed by the subscriber. This document is necessary in case the authorization reason is not included in the other documents concerning the status of the legal person.
7. Signed Subscriber Agreement.
8. Signed Certificate issuing request.
9. Registration form signed and filled in Roman alphabet
10. Payment document/proof.

7.5.3 Certificate issuing Procedure

The following steps describe the certificate request and issuing procedure:

1. The applicant must personally appear before the StampIT RA and apply for a certificate and submit a "Certificate Request", accompanied by a signed registration form and documents for issuing a certificate.
2. Verification of subscriber's identity and completeness of submitted documents.
3. The RA operator generates the key pair on a smart card in the subscriber's presence and submits a certificate issuing request before the CA.
4. After a formal verification of subscriber's data, the CA issues a certificate, which is sent back to the RA.
5. The certificate is stored on a smart card and the smart card is delivered to the subscriber.
6. The subscriber receives the software for smart card access and he/she is obliged to change the smart card access PIN before the first usage of the certificate.
7. The smart card activating data is sent to the subscriber via ordinary mail – by courier services or registered mail to a mentioned by the subscriber address.
8. The issued certificate is published in the StampIT public LDAP directory STRUCTURE.

7.5.4 Certificate Profile:

StampIT DocPro Certificate			
Signature Algorithm	Sha1/RSA		
Issuer	CN	StampIT Domestic CA	
	C	BG	
	O	Information Services Plc.	
	OU	StampIT	
Validity	1 Year		
Subject	C	Country	
	L	Locality	
	O	Organization	
	OU	Organization Unit	
	CN	Common Name	
	E	E-Mail	
	POC	Postal Code	
	STA	Address	
	T	Job Function	
	S	State	B:[БУЛСТАТ] T:[Данъчен номер] C:[Съдебна регистрация] F:[овластяване] EGN:[ЕГН]
	PN	Phone	
Public Key Length/Type	RSA 1024 bits		
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment		
Issuer Alternative Name (Non Critical)	/OU=DocPro Certificate		
Extended Key Usage Field (Non Critical)	Client Authentication, E-Mail Protection		
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]		
Subject Key Identifier (Non Critical)	[Subject Key ID]		
Basic Constrains (Critical)	No (End Entity)		
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl		
Certificate Policies (Non Critical)	Policy Identifier = OID 1.3.6.1.4.1.11290.1.1.1.1 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/		

7.6 Personal StampIT Enterprise Certificates

StampIT Enterprise Certificates are issued under the request of corporate StampIT customers to physical persons that are corporate customer officers. The name of the legal person is filled in the certificate content; however the officers are not authorized to make electronic statements on behalf of the customer.

The corporate customer authorizes its representative that prepares the certificate issuing documents, verifies the officers' identity and represents the corporate customer before StampIT.

7.6.1 Content

The information published in the certificate content may include, but it is not limited to the following elements:

- Officer's e-mail address;
- Officer's name;
- Public key;
- Country/zip code;
- Name of the legal person;
- Headquarters address of the legal person;
- Issuing CA;
- StampIT electronic signature;
- Type of algorithm;

- Certificate validity;
- Certificate serial number.

7.6.2 Documents for issuing a StampIT Enterprise certificate:

1. Official Company Registration Decision/proof – original and copy, signed by the applicant.
2. Tax registration document/proof - original and copy, signed by the applicant.
3. BULSTAT registration document/proof - original and copy, signed by the applicant.
4. Proof of organizational status, issued not earlier than a month before applying a request for a certificate – original.
5. Signed and stamped list with the subscriber officers' data on a paper or electronic document, containing the registration forms' data.
6. Notary signed power letter, proving that the corporate customer has authorized a representative that will represent it before StampIT for all the activities concerning the certificate issuance and management, issued to the corporate customer officers' – original.
7. Identification document (Personal ID card) of the physical person that is authorized to apply the certificate issuance request under clause 6 – original and copy signed by the applicant.
8. Signed Subscriber Agreement.
9. Signed Certificate issuing request.
10. Registration form signed, stamped and filled in Roman alphabet for each of the officers that will be issued a certificate.
11. Payment document/proof.

7.6.3 Certificate Issuing Procedure

The following steps describe the certificate request and issuing procedure:

1. Signing a contract/agreement for issuing certificates to a corporate customer.
2. The authorized representative of the corporate customer (subscriber) applies "Certificate issuing request", accompanied by registration forms – on paper or electronic document. Each page of the paper document is signed and stamped; while for the electronic document a CD ROM (only writeable) is used.
3. Within the agreed term after the application of the certificate issuing request, StampIT issues certificates to the corporate customer officers whose files and data lists are processed in a batch mode.
4. The certificates bear a date consequent to the agreed delivery date of the ready smart cards to the authorized corporate customer representative.
5. The issued certificates are published in the public LDAP directory structure supported by the CA.
6. The authorized corporate customer representative receives the certificates issued on smart cards and the smart cards' activation data in sealed and named envelopes with a Delivery Protocol.
7. The envelopes are personally delivered to the relevant officer, listed in the certificate content, by the authorized corporate customer representative.
8. The corporate customer receives the smart card access software via its authorized representative and binds its officers to change the smart card access PIN before the first usage of the certificates.

7.6.4 Certificate Profile:

StampIT Enterprise Certificate			
Signature Algorithm	Sha1/RSA		
Issuer	CN	StampIT Domestic CA	
	C	BG	
	O	Information Services Plc.	
	OU	StampIT	
Validity	1 Year		
Subject	C	Country	
	L	Locality	
	O	Organization	
	OU	Organization Unit	
	CN	Common Name	
	E	E-Mail	
	POC	Postal Code	
	STA	Address	
	S	State	EGN:[ЕГН]
	PN	Phone	
Public Key Length/Type	RSA 1024 bits		
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment		
Issuer Alternative Name (Non Critical)	/OU=Enterprise Certificate		
Extended Key Usage Field (Non Critical)	Client Authentication, E-Mail Protection		
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]		
Subject Key Identifier (Non Critical)	[Subject Key ID]		
Basic Constrains (Critical)	No (End Entity)		
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl		
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.4 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/		

7.7 Secure Server StampIT Server Certificate

Server certificates are meant for secure communication with a web site. The applicant is a legal person/entity that has a web site. Server certificates are used to assure the web sites identity to the visitor and to assure confidential communication with the web site. Secure server certificates are issued to legal entities.

To enable issuing the StampIT server certificate, the RA needs to be in the batch mode. That is an automated process for reading certificate requests and issuing certificates.

7.7.1 Content

The content of the information published in the certificate may include the elements as follows:

- Server name;
- Public key;
- Country code;
- Legal person/entity name;
- Issuing CA (StampIT);
- StampIT electronic signature;
- Type of algorithm;
- Certificate validity;
- Certificate serial number.

7.7.2 Documents for issuing a StampIT Server certificate:

1. Official/Court Company Registration Decision – original and copy, signed by the applicant.

2. Tax registration document/proof - original and copy, signed by the applicant.
3. BULSTAT registration document/proof - original and copy, signed by the applicant.
4. Proof of organizational status, issued not earlier than a month before applying a request for a certificate – original.
5. Proof of domain's name usage rights – copy signed by the applicant.
6. Notary signed power letter, proving that the physical person is authorized by the legal person to represent it before StampIT for all the activities concerning certificate issuing and management– original.
7. Identification document (Personal ID card) of the physical person that is authorized to represent the legal person – original and copy, signed by the applicant
8. Signed Subscriber Agreement.
9. Signed Certificate issuing request.
10. Registration form signed and filled in Roman alphabet.
11. Payment document.

7.7.3 Certificate issuing procedure

The following steps describe the certificate request:

1. The applicant, who applies for a StampIT Server Certificate on behalf of legal person/entity, must generate the CSR file (Certificate Signing Request) with the appropriate application tool. This process includes the Key Pair generation using the web server software utility.
2. The applicant stores the CSR file, containing the public key of the generated key pair, on a floppy disk.
3. The applicant must personally appear before the StampIT RA.
4. The applicant submits personal and legal person'/entity's information that proves its identity and relationship with the organization.
5. After validation of the documents StampIT RA processes the applicant CSR file and sends it to the StampIT CA.
6. StampIT CA formally verifies the data, issues, and publishes the certificate.
7. StampIT CA sends back the signed certificate to the StampIT RA.
8. StampIT RA operator stores the signed certificate on the applicant's given media and delivers it to the legal person's/entity's representative.

7.7.4 Certificate profile:

StampIT Server Certificate		
Signature Algorithm	Sha1/RSA	
Issuer	CN	StampIT Domestic CA
	C	BG
	O	Information Services Plc.
	OU	StampIT
Validity	1 Year	
Subject	C	Country
	L	Locality
	O	Organization
	OU	Organization Unit
	CN	Common Name
Public Key Length/Type	RSA 1024 bits	
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	
Issuer Alternative Name (Non Critical)	/OU=Server Certificate	
Extended Key Usage Field (Non Critical)	Server Authentication	
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]	
Subject Key Identifier (Non Critical)	[Subject Key ID]	
Basic Constrains (Critical)	No (End Entity)	
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl	
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.2 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/	

Because of the specificity of the issuing procedure of the secure server certificates they are issued only by the StampIT RA, located in Sofia.

7.8 StampIT Object Signing Certificates

Object Signing Certificates are used for signing objects, for example software. Object Signing Certificates are issued to legal entities.

7.8.1 Content

The content of the information published in the certificate may include but it is not limited to the following elements:

- Legal person's name;
- Legal person's data;
- Public key;
- Country code;
- Issuing CA (StampIT);
- StampIT electronic signature;
- Type of algorithm;
- Certificate validity;
- Certificate serial number.

7.8.2 Documents for issuing a StampIT Object certificate:

1. Official/Court Company Registration Decision – original and copy, signed by the applicant.
2. Tax registration document/proof - original and copy, signed by the applicant.
3. BULSTAT registration document/proof - original and copy, signed by the applicant.
4. Proof of organizational status, issued not earlier than a month before applying a request for a certificate – original.

5. Notary signed power letter, proving that the physical person is authorized by the legal person to represent it before StampIT for all the activities concerning certificate issuing and management– original.
6. Identification document (Personal ID card) of the physical person that is authorized to represent the legal person before StampIT– original and copy, signed by the applicant.
7. Signed Subscriber Agreement.
8. Signed Certificate issuing request.
9. Registration form signed and filled in Roman alphabet.
10. Payment document.

7.8.3 Certificate issuing procedure

The following steps describe the certificate request:

1. The applicant, must personally appear before the StampIT RA and apply a certificate issuing request, accompanied by a registration form and the certificate issuing documents.
2. Applicant's identity is verified, respectively the complexity of the submitted documents.
3. StampIT RA Officer generates the key pair on a smart card in the applicant's presence and sends the certificate issuing request to the CA.
4. StampIT CA formally verifies the subscriber's data, issues, the certificate and sends it back to the RA.
5. The certificate is stored on a smart card and delivered to the subscriber against his signature.
6. The subscriber receives the smart card access software and he is obliged to change the smart card access PIN before the first usage of the certificate.
7. The smart card activation data (the PIN code) is sent to the subscriber via ordinary mail – courier services or registered letter to an address submitted by the applicant.
8. The issued certificate is published in the StampIT public LDAP directory structure.

7.8.4 Certificate profile:

StampIT Object Certificate		
Signature Algorithm	Sha1/RSA	
Issuer	CN	StampIT Domestic CA
	C	BG
	O	Information Services Plc.
	OU	StampIT
Validity	1 Year	
Subject	C	Country
	L	Locality
	O	Organization
	OU	Organization Unit
	CN	Common Name
Public Key Length/Type	RSA 1024 bits	
Key Usage (Critical)	Digital Signature, Non-Repudiation	
Issuer Alternative Name (Non Critical)	/OU=Object Certificate	
Extended Key Usage Field (Non Critical)	Code signing	
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]	
Subject Key Identifier (Non Critical)	[Subject Key ID]	
Basic Constrains (Critical)	No (End Entity)	
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl	
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.3 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/	

Because of the specificity of the issuing procedure of the secure server certificates they are issued only by the StampIT RA, located in Sofia.

7.9 Time Stamping

StampIT provides to its subscribers the time-stamp service that certifies the time and date of submitting an electronic document, signed with the private key corresponding to the public key in the StampIT certificate.

7.9.1 Assurance for the subscribers and third parties

Using the time-stamp service that certifies the time and date of submitting an electronic document the subscribers and third parties are assured that this electronic document existed in this form at the time certified by StampIT.

7.9.2 Technology

Time and date certification of the submission of an electronic document is done in correspondence with IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) after the subscriber submits an electronic request at an address mentioned by StampIT. The request is forwarded to "Information Services" Plc as a certificate service provider and processes the time-stamp operations.

7.10 Certificate Revocation List (CRL)

StampIT supports and updates every three hours the Certificate Revocation List which is publicly accessible at the following address: http://www.StampIT.org/crl/StampIT.crl

7.10.1 Certificate Revocation List Profile:

StampIT CRL		
Version	Version 2	
Issuer Name	CN	StampIT Domestic CA
	C	BG
	O	Information Services Plc.
	OU	StampIT
Effective date	[Date of CRL issuance]	
Next Update	[Next update]	
Signature algorithm	Sha1/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)

7.10.2 Certificate Revocation Codes:

1. **Key Compromise –** the private key, corresponding to the public key, included in certificate content, is compromised, therefore there are no reasons relying to this certificate.
2. **CA Compromise –** The CA private key used for signing subscribers' certificates is compromised.
3. **Affiliation Changed –** changes in the affiliation – the subject filled in the certificate has a changed status concerning the legal person/entity.
4. **Superseded** – the certificate is superseded by another certificate.
5. **Cessation of Operation** – all the activities concerning the initial issuing of the certificate are ceased.
6. **Certificate on hold** – the validity of the certificate is on hold (the certificate is not valid at the moment).

8 Limitation of the Certificates Operation

This section defines the specific limitation of the certifications operation in regard of the damage compensations owed by the certificate service provider, respectively the insurer for damages that occurred as a result of issuance and usage of electronic signatures with certificates, issued by StampIT.

The Certificate Service Provider is liable for damages before the titular of the advanced electronic signature and all third parties in correspondence with the regulation of Article 29 of the Electronic Document and Electronic Signature Act.

8.1 Damage Limits and Transactions Limits

The maximum damage limits mentioned in Section 8.8, are also maximum transaction limits when StampIT certificates are used.

8.2 Subscribers

StampIT subscribers are physical and/or legal persons that have been issued a certificate of one of the following types:

- StampIT Doc Certificate
- StampIT DocPro Certificate
- StampIT Enterprise Certificate
- StampIT Object Certificate
- StampIT Server Certificate

8.3 Free and Test Certificates

StampIT has no liability about the way the free and test certificates, which could be provided for purposes including demos, training and tests, are used.

8.4 Insurance Subject

Subject of the certificate service provider insurance is the liability of "Information Services" Plc. as a certificate service provider, in accordance with Article 29 of the Electronic document and electronic signature act.

8.5 Limitation of the Certificates Operation

StampIT limits the operation of the certificates and is not liable for damages that occur as a result of the following:

- Concrete obligations undertaken by the subscriber, e.g. liability against third parties, contractual sanctions, etc.;
- Compensations for legal/lawsuit, administrative or disciplinary sanctions and also adjudged lawsuit expenses to the subscriber;
- Declare bankruptcy of the subscriber or third party;
- Delay or inability of the subscribers to submit a StampIT certificate revocation request;
- Subscriber's negligence in avoiding private key compromise or loss;
- Non-observance of the CPS requirements and obligations by the subscribers;
- Not applying verification of the subscriber's electronic signature;
- Not applying appropriate security measures before or during the creation and further processing of encrypted messages;

- Illegal actions of the subscribers and third parties. StampIT has the right of damage compensations that occurred as a result of similar illegal acts;
- Damages that are out of StampIT control, including energy or telecommunication failures that are out of StampIT control;
- Using certificates for sensitive equipment operation, including but not limited to nuclear equipment, aviation navigation or communication systems, air traffic control systems, weapon control systems and all cases that could lead to death, injuries or environmental damages;
- Subscribers or third parties' abuse of Internet, telecommunications or value added networks, including the usage or reproduction of computer viruses;
- Force major

8.6 Term

The term for lodging a claim by the subscribers or the relying parties against StampIT or the insurer is 7 days of the date of receiving information about the damage occurrence.

8.6.1 Insurance Term

All claims under the previous section should be reported to StampIT during the insurance term. The insurance term is the time between dates setting the beginning and the end of the certificate validity.

8.6.2 Extending the Insurance Term

StampIT insurance also covers written claims, that are brought against StampIT within 15 days after the end of the certificate validity and they are based on damages that occurred during the certificate validity.

8.7 Subscribers' Obligations

The subscribers are obliged to:

- in case they find out errors and damages to send immediately written notice via registered letter or courier services;
- to cooperate StampIT and StampIT Insurer, in order to determine the facts that confirm the damage claim.

8.8 Maximum Damage Limit

With the aim to limit the performance of the certificates StampIT determines a maximum damage limit for the suffered damages, caused by the usage of a certificate, issued by StampIT. The limits are specified in accordance with the type of certificate, as shown in the table below:

Maximum Damage Limit	
StampIT Doc Certificate	40 000 levs
StampIT DocPro Certificate	40 000 levs
StampIT Enterprise Certificate	3 000 levs
StampIT Object Certificate	40 000 levs
StampIT Server Certificate	40 000 levs

When there are damages that exceed the set damage limit for any certificate, the earliest received claims are indemnified first until final allocation is reached. StampIT has the right to refuse paying off an amount that exceeds the maximum damage limit for damages from one certificate.

The maximum damage limit remains unchanged, despite the subscribers' number, relying parties, electronic signatures, the amount of the transactions or the claims, related to the certificate. The maximum damage limit concerns damages caused to all subscribers, applicants recipients or relying parties that occur as a result of relying to StampIT certificate verified information.

8.9 Applicable Insurance

In the relations between StampIT and its subscribers, and all third parties, all damage limits and conditions applicable at the moment of occurrence of the damage should be applied.

8.10 Force major events

The occurrence of force major events abrogates all the rights under this CPS.

8.11 Jurisdiction

Any disputes that may arise out of or in connection with the provision of StampIT certification services should be settled by the District Court of Sofia.

8.12 Applicable legislation

For all unsettled disputes under the following section the Bulgarian legislation should be applied.