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

Provision of qualified certification services by
Information Services JSC

POLICY
for provision of qualified website authentication certificates (eIDAS-CP-SSL)

Version: 2.1
Publication date: 07.06.2017
Last revision date: 15.06.2018

Contents

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

TERMS AND ABBREVIATIONS

Regulation (EU) No 910/2014	REGULATION (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Directive 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Certification service	Electronic service provided by Information Service AD for pay, consisting of: a) creation and validation of electronic signatures, electronic seals and electronic timestamps as well as certificates related to such services; b) creation and validation of website authentication certificates.
Qualified certification service	Certification service that meets the applicable requirements laid down in Regulation (EC) No. 910/2014.
Signatory	A natural person who creates an electronic signature.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign
Advanced electronic signature	Electronic signature which meets the following requirements: a) it is uniquely linked to the signatory; b) it is capable of identifying the signatory; c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
Qualified electronic signature	An advanced electronic signature that is created by an advanced electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
Electronic signature creation data	Unique data which is used by the signatory to create an electronic signature.
Certificate for electronic signature	an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person,
Qualified certificate for electronic signature (QCES)	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I to Regulation (EU) No. 910/2014;
Electronic signature creation device	Configured software or hardware used to create an electronic signature
Qualified electronic signature creation device	Electronic signature creation device that meets the requirements laid down in Annex II to Regulation (EU) No. 910/2014
Creator of a seal	A legal person who creates an electronic seal.
Electronic seal	data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
Advanced electronic seal	Electronic seal which meets the following requirements: a) it is uniquely linked to the creator of the seal; b) it is capable of identifying the creator of the seal; c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

	d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
Qualified electronic seal	An advanced electronic seal, which is created by an advanced electronic seal creation device, and that is based on a qualified certificate for electronic seal
Electronic seal creation data	Unique data, which is used by the creator of the electronic seal to create an electronic seal.
Certificate for electronic seal	an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person
Qualified certificate for electronic seal	A certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III to Regulation (EU) No. 910/2014;
Electronic seal creation device	Configured software or hardware used to create an electronic seal
Qualified electronic seal creation device	Electronic seal creation device that meets the requirements laid down in Annex II to Regulation (EU) No. 910/2014
Electronic time stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
Qualified electronic time stamp	Electronic time stamp which meets the following requirements: a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; b) it is based on an accurate time source linked to Coordinated Universal Time; and c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.
Electronic document	Any content stored in electronic form, in particular text or sound, visual or audiovisual recording
Certificate for website authentication	An attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued
Qualified certificate for website authentication	A certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV to Regulation (EU) No. 910/2014 ;
Relying party	A natural or legal person that relies upon an electronic identification or a trust service
National law	The valid Bulgarian law
Supervisory authority	Supervisory authority in the meaning of article 17 of Regulation (EU) № 910/2014
IO JSC/ Provider/ Qualified trust service provider	Information Service AD in the capacity of qualified trust service provider that is granted the qualified status by a supervisory body.
Practice	Practice for provision of qualified certification services (Certification Practice Statement - CPS)
Policy	Policy for Provision of Qualified Certificates for Qualified Electronic Signature and Qualified Electronic Seal (eIDAS-CP-QES) Policy for Provision of Time-Stamping Services (eIDAS-CP-TS) Policy for Provision of Qualified Certificates for Advanced Electronic Signature and Advanced Electronic Seal (eIDAS-CP-AES); Policy for Provision of Qualified Website Authentication Certificates (eIDAS-CP-SSL).
CA	Certification authority

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

1. Introduction

This document describes the general rules that Information Services JSC applies upon issuing and managing qualified website authentication certificates as well as the applicable services and the scope of applicability.

The purpose of the services for website authentication is to prove that the domain is managed by legitimate subject or organisation.

The offered services for website authentication correspond to Regulation (EU) № 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, requirements and guidelines defined by CA/Browser Forum (https://cabforum.org/) and in compliance with the applicable law of Republic of Bulgaria.

For the issuing of qualified website authentication certificates shall apply procedures and practices guaranteeing the highest level of security upon issuing, publishing and management of the issued qualified certificates.

1.1. Policy overview

This policy refers to the qualified website authentication certificates issued by Information Services JSC in compliance with Regulation (EU) № 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and in accordance with the applicable law of Republic of Bulgaria.

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

The policy is consistent with the following documents:

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

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

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

1.2. Policy name and identifier

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

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

DVCP/Domain Validation Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)

OVCP/Organizational Validation Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)

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

Type of certificate	StampIT Policy Identifier	ETSI Policy Identifier
StampIT Server DVC	1.3.6.1.4.1.11290.1.2.1.8	0.4.0.2042.1.6
StampIT Server OVC	1.3.6.1.4.1.11290.1.2.1.9	0.4.0.2042.1.7

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

Information services JSC is a trusted provider of qualified certification services, which meet the requirements specified in Regulation (EU) № 910/2014 and the valid national law. Information services JSC provides qualified certification services through ***certification authority*** and a network of ***registration authorities***. The certification authority and the registration authorities perform their activities for provision of qualified certification services on behalf of and on the account of Information Services JSC.

1.3.1. Certification authority

StampIT is the certification authority of Information Services JSC, which issues qualified website authentication certificates (QWAC). The certification authority carries out the activities, which include the issue, renewal, suspension, resumption and revocation of QWAC, keeping registers and providing access to them.

1.3.2. Registration authorities

The certification authority issues QWAC after verification of the subscriber's identity. In this regard Information Services JSC provides its services to the subscribers through a network of Registration authorities that have the following functions:

- to accept, verify, approve or reject requests for issuing QWAC in accordance with the internal rules of StampIT;
  - to register the submitted requests for qualified certification services of StampIT;
  - to take part in all phases upon identification of the subscribers as specified by StampIT depending on the type of qualified certificate, which they issue;
  - to refer to formal, notarized or other specified documents to verify the request submitted by the applicant;

- after approval of the request to notify StampIT in order to initiate the issue of a qualified certificate;
- to register the submitted requests for renewal, termination, suspension and resumption of the validity of a qualified certificate.

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

1.3.3. Subscribers

Subscribers are natural or legal persons who have submitted request and after successful completion of the procedure have received a qualified certificate. Before the verification and issue of a qualified certificate, the subscriber is only an applicant for the qualified services of StampIt.

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

1.3.4. Relying parties

Relying parties are natural and legal persons who use the certification services with qualified certificates issued by StampIT and rely on these qualified certificates upon establishing a link to a website.

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

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

1.4.1. Applicability

The issued qualified website authentication certificates may be used only for website authentication in accordance with the restrictions of the type of the issued qualified certificate.

1.4.2. Restrictions

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

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

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

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

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

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

Contact details for StampIT:

11, Lachezar Stanchev Str. Izgrev

1756 Sofia, Bulgaria

Tel.: + 359 2 9656 291

Fax: + 359 2 9656 212

Web: https://www.stampit.org

E- mail: support@mail.stampit.org

2. Public registers and management

2.1. Maintained public registers

StampIT publishes the issued qualified certificates in the register of issued certificates. StampIT may publish qualified certificates in other registers, which are considered appropriate however it shall not be liable for the validity, accuracy and availability of directories maintained by third parties. Subscribers on their hand may also publish qualified certificates issued by StampIT in other registers. The subscriber may prevent the publication of the issued certificate in the maintained registers by explicit declaration of will upon conclusion of the contract for qualified certification services.

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

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

2.2. Refresh frequency

Frequency of refreshing the published qualified certificates is as follows:

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

2.3. Access

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

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

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

3. Identification and check of identity data

3.1. Name

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

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

The field "Subject" contains unique name of the web server.

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

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

3.1.1. Web server name

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

- C – two-letter abbreviation of the country's name according to ISO 3166-1 alpha2;
- CN – domain name (qualified DNS name) or public IP address;
- GN – full name of the natural person Optional;
- SN – family name of the natural person Optional;
- O – name of the organisation represented by the person Required when issuing OVC type;
- organizationIdentifier – identifier of organisation. Required when issuing OVC type;
- OU – organisational unit. To be filled in upon issuing of OVC type following due certification Optional;
- SA - address: To be filled in upon issuing of OVC type following due certification Optional;
- L – location. To be filled in upon issuing of OVC type following due certification Optional;
- SerialNumber – unique identifier of the natural person
- Other fields, which are described in details in the profiles of the qualified certificates

3.1.2. Alternative names (Subject Alt Name)

Non-critical expansion, which must contain at least the CN record as well as adding additional domains/ public IP addresses under the Subscriber's control.

3.1.3. Meaningful names

Names must be connected to the service, which the present. StampIT may refuse to issue qualified certificate at its own discretion..

3.1.4. Anonymity and pseudonyms

As described in Practice for provision of qualified certification services

3.1.5. Interpretation of different forms of names

StampIT shall render assistance to the Subscriber when it is necessary to interpret data connected with the issue of a qualified certificate.

3.1.6. Unique names

The issued qualified certificates must be unique within the register kept by StampIT. If necessary, additional identifier may be added to guarantee the uniqueness.

3.1.7. Authenticity and trademark Resolution of disputes

As described in Practice for provision of qualified certification services

3.2. Initial registration

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

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

3.2.1. Verification for public key possession

As described in Practice for provision of qualified certification services

3.2.2. Verification of legal persons

As described in Practice for provision of qualified certification services

3.2.3. Verification of natural persons

As described in Practice for provision of qualified certification services

3.2.4. Verification by the certification authority

As described in Practice for provision of qualified certification services

3.2.5. Interoperability assurance

Upon performance of its activities, StampIT may cooperate with third persons including certification services providers except in the following hypotheses:

- possible conflict of interests;
- objective possibility to breach the rights of Subscribers;

- specific legal or other provision.

3.2.6. Verification of domain and/ or IP address

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

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

3.2.7. Compliance criteria

As described in Practice for provision of qualified certification services

3.3. Renewal of qualified certificate

As described in Practice for provision of qualified certification services

3.4. Suspension and revocation of a qualified certificate

As described in Practice for provision of qualified certification services

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

As described in Practice for provision of qualified certification services

4. Operational activities

As described in Practice for provision of qualified certification services

4.1. Valid use of issued qualified certificates

4.1.1. On the part of the subscribers

As described in Practice for provision of qualified certification services

4.1.2. On the part of the relying parties

As described in Practice for provision of qualified certification services

4.2. Renewal and reissue of qualified certificates

As described in Practice for provision of qualified certification services

4.2.1. Procedure for renewal of qualified certificates

As described in Practice for provision of qualified certification services

4.3. Change of information in the qualified certificates

As described in Practice for provision of qualified certification services

4.4. Suspension of qualified certificates

As described in Practice for provision of qualified certification services

4.4.1. Grounds for suspension

As described in Practice for provision of qualified certification services

4.4.2. Procedure for suspension

As described in Practice for provision of qualified certification services

4.5. Resumption of qualified certificates

As described in Practice for provision of qualified certification services

4.5.1. Grounds for resumption

As described in Practice for provision of qualified certification services

4.5.2. Procedure for resumption

As described in Practice for provision of qualified certification services

4.6. Revocation of the qualified certificates

As described in Practice for provision of qualified certification services

4.6.1. Ground for revocation

StampIT may revoke at its own discretion any issued qualified certificate in case of reasonable doubts for compromising the private key or when using it for illegal activities.

As described in Practice for provision of qualified certification services

4.6.2. Procedure for revocation

As described in Practice for provision of qualified certification services

4.7. Status of issued qualified certificates

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

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

As described in Practice for provision of qualified certification services

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

As described in Practice for provision of qualified certification services

4.7.3. Manually, through the website of StampIT

As described in Practice for provision of qualified certification services

5. Physical and organizational security

5.1. Physical security

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

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

5.1.1. Secure premises

As described in Practice for provision of qualified certification services

5.1.2. Data storage

As described in Practice for provision of qualified certification services

5.1.3. Secure data destruction

As described in Practice for provision of qualified certification services

5.2. Organisational security

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

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

5.3. Personnel security

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

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

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

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

5.3.1. Personnel training

As described in Practice for provision of qualified certification services

5.4. Records and journals management

As described in Practice for provision of qualified certification services

5.5. Archives management

As described in Practice for provision of qualified certification services

5.6. Certification authority termination

As described in Practice for provision of qualified certification services

6. Technical security control

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

As described in Practice for provision of qualified certification services

6.2. Generation of key pair of Subscriber

Algorithms used to generate the key pair must meet the minimum requirements defined in ETSI TS 119 312.

As described in Practice for provision of qualified certification services

6.2.1. Requirements to the devices/ the system

As described in Practice for provision of qualified certification services

6.2.2. Provision of the key pair to the Subscriber

As described in Practice for provision of qualified certification services

6.2.3. Minimum lengths of key pairs

Used length of the key pair must meet the minimum requirements defined in ETSI TS 119 312.
As described in Practice for provision of qualified certification services

6.2.4. Public key parameters

As described in Practice for provision of qualified certification services

6.2.5. Private key management

6.2.5.1. Private key storage

As described in Practice for provision of qualified certification services

6.2.5.2. Private key activation

As described in Practice for provision of qualified certification services

6.2.5.3. Private key deactivation

As described in Practice for provision of qualified certification services

6.2.5.4. Private key destruction

As described in Practice for provision of qualified certification services

6.3. Key pair management

6.3.1. Public key archiving

As described in Practice for provision of qualified certification services

6.3.2. Validity and use of issued certificates

As described in Practice for provision of qualified certification services

6.4. Private key activation

As described in Practice for provision of qualified certification services

6.4.1. Generation and provision of activation data

As described in Practice for provision of qualified certification services

6.4.2. Activation data protection

As described in Practice for provision of qualified certification services

6.5. Security of the used computer systems

As described in Practice for provision of qualified certification services

6.6. Change management in the system of StampIT

As described in Practice for provision of qualified certification services

6.7. Network security control

As described in Practice for provision of qualified certification services

7. Certificates profiles

7.1. Profile of StampIT Root certificate of Information Services JSC

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

Friendly Name	StampIT Global Root CA
Basic constrains (Critical)	Subject Type=CA Path Length Constraint=0
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.stampit.org/repository/

7.2. Profile of StampIT Subordinate certificate of Information Services JSC

StampIT Global Qualified CA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Root CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Validity	20 years		
Subject	CN	StampIT Global Qualified CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	District
	2.5.4.97 (organization Identifier)	NTRBG-831641791	EIK
Public Key	RSA 4096 bits		
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)		
Friendly Name	StampIT Global Qualified CA		
Basic constrains (Critical)	Subject Type=CA Path Length Constraint=0		
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.stampit.org/repository/stampit_global_root_ca.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/		
CRL Distribution Point	[1]CRL Distribution Point		

/Non Critical/	Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.stampit.org/repository/

7.3. Profile of qualified website authentication certificate StampIT Server DVC

StampIT Server DVC Profile			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG- 831641791	
Validity	365 Days or 825 Days		
Subject	*C	Country	
	L	Locality	
	*CN	Common Name	
	E	E-mail	
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Key Encipherment		
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://www.stampit.org/repository/stampit_global_qualified.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/		
Extended key usage (Non Critical)	Server Authentication		
Subject Alternative Name	DNS Name=www.Common Name DNS Name=Common Name		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.8 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=https: /www.stampit.org/repository/		

Fields with * are mandatory

7.4. Profile of qualified website authentication certificate StampIT Server OVC

StampIT Server OVC Profile

Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	365 Days or 825 Days		
Subject	*C	Country	
	L	Locality	
	*CN	Common Name	
	E	E-mail	
	*O	Organization	
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Key Encipherment		
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/ [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://stampit.org/repository/stampit_global_qualified.crt		
Extended key usage (Non Critical)	Server Authentication		
Subject Alternative Name	DNS Name=www.Common Name DNS Name=Common Name		
Basic constrains (Critical)	End entity		
CRL Distribution Point /Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.9 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=https://www.stampit.org/repository		

Fields with * are mandatory

8. Control of the activities of the Provider

As described in the Practice for provision of qualified certification services

9. Business and legal issues

9.1. Prices

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

9.1.1. Remedy of discrepancies and restoration of effected payment

As described in Practice for provision of qualified certification services

9.2. Financial liability

As described in Practice for provision of qualified certification services

9.2.1. Guarantees for payment of compensations

As described in Practice for provision of qualified certification services

9.3. Personal data protection

As described in Practice for provision of qualified certification services

9.4. Intellectual property rights

As described in Practice for provision of qualified certification services

9.4.1. Title on the key pairs

As described in Practice for provision of qualified certification services

9.5. Obligations and liability of StampIT

As described in Practice for provision of qualified certification services

9.5.1. Liability to the Subscriber

As described in Practice for provision of qualified certification services

9.5.2. Limits of liability of the registration authority

As described in Practice for provision of qualified certification services

9.6. Obligations of the subscriber

As described in Practice for provision of qualified certification services

9.7. Disclaimer

As described in Practice for provision of qualified certification services