ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

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

Provision of qualified certification services by
Information Services JSC

POLICY
for provision of time-stamping services (eIDAS-CP-TS)

Version: 1.0
Publication date: 07.06.2017
Last revision date: 07.06.2017

Contents

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

1 Introduction

This document describes the general rules applied by Information Services JSC upon provision of time stamping services for issuing qualified time stamps.

For the issuing of qualified time stamps shall apply procedures and practices guaranteeing the highest level of security upon issuing, publishing and management. Additional and more detailed information for the applied rules is available in the Practice for Provision of Qualified Certification Services published on the website of StampIT https://www.stampit.org.

A qualified electronic time stamp shall meet the following requirements:

- it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
- it is based on an accurate time source;
- it is signed using a qualified electronic signature of StampIT in its role of a qualified provider of qualified certification services.

The structure and the content of this document corresponds to the requirements of the technical specification ETSI TS 102 023.

1.1 Scope

This policy refers to the qualified electronic time stamps 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.

2 References

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 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- ETSI EN 319 421: „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps“
- ETSI EN 319 422: „Electronic Signatures and Infrastructures (ESI); Timestamping protocol and Timestamp token profiles"
- IETF RFC 3161 „Internet X.509 Public Key Infrastructure: Timestamp Protocol (TSP)"
- Practice for provision of qualified certification services (CPS) of StampIT

3 Definitions 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

4 General concepts

4.1 Qualified time stamping service

The provision of qualified time stamping service and management of qualified electronic time-stamp tokens consists of two components:

- Technological systems which issues qualified electronic time-stamp tokens and maintains an archive for generated certificates for electronic time stamps.
- Management of the system that monitors and controls the operations for service provision

The management of the system ensures permanent updating and synchronization with accurate time source linked to Coordinated Universal Time (UTC) and reliable management of the technological system.

4.2 Time-stamping authority

For the issuing of certificates for qualified electronic time stamps is used time-stamping authority StampIT Global TSA, signed with qualified electronic signature StampIT, in its role of qualified provider of qualified certification services. Through the electronic time stamps the Subscribers may certify the time for submission of electronic documents and electronic messages and is a proof that the signed data object existed as at the time of applying the time stamp.

StampIT is subject to audit by independent compliance assessment authority at least once every 24 months. The purpose of the audit is to confirm that Information Services JSC in the capacity of provider of certification services and the certification services provided by the Organization meet the requirements of Regulation (EU) № 910/2014, ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1.

4.3 Subscribers

Subscribers are users of the service described in the Practice for provision of qualified certification services.

Subscribers may be end users of a group of users within an organisation.

When the subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled. Organization shall inform its end users concerning their liability in connection with the use of the present certification service.

When the user is an end user, it shall be liable for the observance of the requirements of this policy.

4.4 Overview

4.4.1 Designation

This document adds to the Practice for provision of qualified certification services the specific terms for provision of qualified time-stamping services.

4.4.2 Level of specificity

This policy describes the general approach, procedures and rules upon provision of the service for qualified time stamping regarding the technical, organizational and procedural requirements for service maintenance.

All operational documents and records maintained by StampIT have the relevant level of classification concerning the access to them and are available for review by duly authorized persons.

4.4.3 Approach

This document presents the general policy for provision of the services and does not detail the technical approaches for infrastructure realization and management. It defines the conditions and the rules observed by StampIT as a qualified provider of qualified certification services and qualified electronic time-stamps.

5 Policy of the time-stamping authority

5.1 General

The policy of the time-stamping authority is a set of rules and their application upon issuing and management of time stamps. StampIT guarantees accuracy of at least 1 second upon issuing these certificates.

The used profile for the issued qualified time stamp certificates comply with the requirements of ETSI EN 319 422.

Issuing, verification and search in the Public register of qualified time stamps is carried out through the user interface accessible for the Subscribers onhttps://tsa.stampit.org.

Issuing is possible also by https protocol in compliance with RFC 3161 and the issued certificates use the algorithms RSA 2048 / SHA256.

The profile of StampIT Global TSA certificate is the following:

StampIT Global TSA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Qualified CA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	
	2.5.4.97 (Organizationidentifier)	NTRBG-831641791	EIK
Validity	5 years		
Subject	CN	StampIT Global TSA	Name
	C	BG	State
	O	Information Services JSC	Organization
	L	Sofia	District
	2.5.4.97 (OrganizationIdentifier)	NTRBG-831641791	EIK
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature		
Friendly Name	StampIT Global TSA		
Extended key usage (Critical)	Time Stamping (1.3.6.1.5.5.7.3.8)		
Basic constrains (Critical)	End entity		

Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.stampit.org/repository/stampit_global_qualified.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/
CRL Distribution Point/Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global_qualified.crl
Certificate Policies (Non Critical)	Policy identifier = **1.3.6.1.4.1.11290.1.2.1.1** Repository = http://www.stampit.org/repository/

5.2 Policy identifier

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

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

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1)

baseline-ts-policy (1)

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

Type of certificate	StampIT Policy Identifier	ETSI Policy Identifier
StampIT Global TSA	1.3.6.1.4.1.11290.1.2.1.1	0.4.0.2023.1.1

5.3 Applicability of the electronic time stamp

This policy aims to cover the requirements for qualified electronic time stamps (ETSI EN 319 122) but it is applicable to any other use of time stamps with equivalent requirements.

The qualified time stamping service allows that for each signed object the date and time of submission is attested.

5.4 Compliance

The activities for issuing and managing the qualified electronic time stamps comply with the requirements of:

- Regulation (EU) No 910/2014
- ETSI TS 119 421
- RFC 3161
- RFC 5816

6 Obligations and liability

6.1 Obligations

6.1.1 General

StampIT shall:

- observe its internal rules and public practice, policies and procedures;
- observe Regulation (EU) No. 910/2014 and the national law
- ensure reliable mechanisms including the mechanism for generation of keys, the protected mechanism for electronic signature creation and the procedures for distribution of the secret parts with regard to its own infrastructure
- notify the parties in case of compromising of its private keys
- manage the life-cycle of StampIt Global TSA certificate;
- issue qualified time stamps in compliance with the policy and the practice and shall meet the obligations specified in them.

6.1.2 Obligations toward Subscribers

StampIT shall:

- ensure uninterrupted access to the qualified time stamp service except during scheduled preventive maintenance and force majeure situations;
- ensure qualified electronic time stamps with accuracy better than 1 second;
- ensure support for the subscribers and the relying parties;
- provide copies of its practice and policies as well as the other valid documents for public access.

6.2 Obligations of Subscribers

Subscribers shall:

- verify the issued qualified electronic time stamps including by checking the CRL list or through OCSP interface;
- not misuse the provided interface;
- perform their obligations described in the Practice for provision of qualified certification services.

6.3 Obligations of the relying parties

The relying parties shall:

- verify the issued qualified electronic time stamps including by checking the StampIT Global TSA certificate in the CRL list or through OCSP interface;
- check the applicability of the cryptographic algorithms used for the creation of the certificate;

- perform their obligations described in the Practice for provision of qualified certification services.

6.4 Liability

In connection with the risk for liability for caused damages in compliance with Regulation (EU) № 910/2014 StampIT shall maintain sufficient financial resources and/ or shall conclude appropriate liability insurance in accordance with the national law.

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

- missed benefits
- loss of data
- other indirect damages ensuing from or in connection with the use, validity or inoperability of the qualified time stamping service
- the use of qualified time stamp, which exceeds certain limitations specified therein or in this policy
- the security, use, integrity of products, including hardware and software , which the subscriber uses

7 Requirements to the time-stamping authority practice

StampIT shall exercise reliable and secure control on the performance of the requirements of this policy. All events are registered in the systems in system journals, which are archived and stored securely.

7.1 Practice and procedures of the time-stamping authority

7.1.1 Practice

Procedures and mechanisms for control upon provision of qualified time stamping services are described in the document Practice upon provision of qualified certification services published on ‼HYPERLINK "https://www.stampit.org" ¶https://www.stampit.org┴.

The activities for management, maintenance and improvement of the services provided by the time stamping authority (including risk assessment procedures) are carried out in compliance with the requirements of the Integrated management system implemented in Information Services JSC, certified by external certifying authority under the standards ISO 27001:2013 for information security management, ISO 20000-1:2011 for management of the provided IT services and ISO 9001:2015 for quality management.

7.1.2 Accessibility

The general practices for provision of qualified time stamping services are described in the document Practice upon provision of qualified certification services published on ‼HYPERLINK "https://www.stampit.org" ¶https://www.stampit.org┴.

To ensure high quality and availability of the service, all system components and communication connectivity are at least double redundant. Infrastructures are built for ensuring uninterrupted

power supply based on uninterrupted power supply units (UPS) and diesel generators of power supply.

7.2 Time-stamping authority key management

7.2.1 Time-stamping authority key generation

StampIT generates securely and protects the key pair by using a reliable system (HSM with security level FIPS 140-2, level 3+) and takes the required measures to prevent their compromising or unauthorized use. StampIT implements and documents the procedure of key generation in compliance with this policy. StampIT implements the European and the generally recognized in the international practice standards for reliable systems including the information security standards and makes everything possible to observe them.

The requirements to the used algorithms and the length of the subscribing private key are consistent with ETSI TS 119 312.

7.2.2 Time-stamping authority private key protection

The time-stamping authority private key is stored and protected only through HSM cryptographic module certified in accordance with the requirements of FIPS 140-2, level 3+.
In specially protected fire-resistant strong boxes are stored separately through key escrow the keys for time-stamping authority private key restoration. This is done for the purpose of restoration in case of force majeure events.

7.2.3 Time-stamping authority public key distribution

The public key of the certificate StampIT Global TSA is published on the website of StampIT !! HYPERLINK "https://www.stampit.org" ¶https://www.stampit.org⊥.

7.2.4 Rekeying the time-stamping authority's key

StampIT Global TSA is issued for a term of 5 years. If during that period reasonable grounds occur for cryptographic deficiencies or the requirements change, a new key pair shall be generated. Upon expiration of the period of validity a new key pair is generated and a new qualified certificate is issued.

7.2.5 Time-stamping authority private key destruction

Upon expiration of the term of validity or revocation, the private key shall be stored for a period of 10 years. Upon expiration of that term, the private key of such certificate is destroyed securely to ensure that it will not be reused.

7.2.6 Life cycle management of cryptographic module used to sign time-stamps

The staff of StampIT shall inspect the cryptographic module to ensure the integrity of the packing when it is received and stored.

The installation, configuration and activation of the module is made by employees with the relevant roles according to the procedures of the manufacturer in the secure premises of Information Services JSC.

Employees shall perform the technological procedures for verification of the status of the equipment.

Upon withdrawal or replacement, the employees of StampIT shall erase in a secure manner the private keys available in the module in compliance with the documentation provided by the manufacturer.

7.3 Requirements to the time-stamping authority practice

The time stamping services shall be carried out in accordance with the requirements of ETSI

TS 101 861 Time Stamp Profile и RFC 3161.

Communication with the Subscribers is carried out via the protocols HTTP and HTTPS.

7.3.1 Electronic time stamp token (TST)

Profiles of requests for issuing TST and responses are the following:

Time Stamp Query (TSQ)		
Version	1	
MessageImprint	Hash Algorithm	OID SHA256 2.16.840.1.101.3.4.2.1
	Hash Value	Hash value on data
RequestedPolicy		OID StampIT Global TSA 1.3.6.1.4.1.11290.1.2.1.1
Nonce		Option
CertReq	True/False	For inclusion of StampIT Global TSA certificate in TSR:

Time Stamp Response (TSR)		
Version	1	
MessageImprint	Hash Algorithm	OID SHA256 2.16.840.1.101.3.4.2.1
	Hash Value	Hash value on data
Policy		OID StampIT Global TSA 1.3.6.1.4.1.11290.1.2.1.1
SerialNumber		Serial number of TSR
GeneratedTime		Time stamp based on UTC
Accuracy		min 999ms
Nonce		If present in the request
TSA		If requested

7.3.2 Accurate time synchronization with UTC

Accurate time synchronization is carried out via NTP/NTPS protocol through a link to at least two different stratum-1 and ultimately to stratum-2 servers. Synchronization is carried out at least twice a day automatically, by registering the deviations.

Clock synchronization is monitored and registered and different notifications are issued when the deviation exceeds 50 ms.

7.4 Time-stamping authority management and operation

7.4.1 Security management

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.

7.4.2 Assets classification and risk assessment

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

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

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

7.4.3 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.

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.

7.4.4 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.

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

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

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

7.4.5 Operations management

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

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

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

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

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

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

Information Services JSC has highly developed network infrastructure, which components provide opportunity for protection of different types of network attacks. There are devices for

protection from DDoS, new generation firewalls (ng-firewalls) and highly efficient active network devices.

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

Additional and more detailed information for the applied rules is available in the Practice for Provision of Qualified Certification Services available on the website of StampIT https://www.stampit.org.

7.4.6 Access management

The security management of the qualified time stamping service is subject to a number od technical and administrative controls for access management. Technical controls apply on network (rules of ng-firewall devices and similar), system and local level.

User administration is carried out by the employees with the relevant authorized roles, as described in the security policies, a part of the Integrated Management System of the Company.

All activities carried out within the infrastructure of StampIT are allowed only subject to due authorization of the employees for which due information is stored in the system journals.

For each security breach, which has significant influence on the offered service, the Supervisory authority shall be informed.

7.4.7 Use of secure devices

Issued qualified time stamps is carried out through HSM cryptographic module with security level FIPS 140-2, level 3+. It incorporates a number of technical controls against unauthorized access and modification on physical and logical level.

7.4.8 Private key compromising

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

In case of time-stamping authority private key compromising, the following measures shall be taken:

- the certificate of StampIT Global TSA shall be revoked and shall be included in the CRL list;
- certificate with a new key pair shall be issued;
- the Subscribers and the Relying parties that may be affected shall be informed;
- detailed security audit of StampIT shall be performed for the purpose of identification of possible damages and analysis of the reasons for compromising;

- corrective actions shall be taken, which shall be documented, performed and validated.

7.4.9 Time-stamping authority termination

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

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

- to inform about its intentions the Supervisory authority and the subscribers for the service at least four months before the date of termination of its operations;
- to terminate the certificate of the time stamping authority - if the operations will not be transferred to another supplier;
- to perform the required activities for archives storage in compliance with this policy and the regulatory requirements - if the activity will not be transferred to another provider;
- in case that it transfers its operations to another provider, StampIT will hand over to the assignee the whole documentation related to its operations as time stamping services provider and the right to use the public key infrastructure of StampIT with a view to the management of already issued qualified certificates for a term, which is not longer than six months.

7.4.10 Compliance with the legal requirements

For all issues unsettled herein shall apply the provisions of the valid of Regulation (EU) № 910/2014 and the valid national law. All requirements for provision of qualified electronic time stamps ensuing from this document shall comply with the requirements of the standards and the technical requirements of ETSI.

7.4.11 Recording of events connected with the time-stamping authority

All events connected with the operations of the time stamping authority shall be registered in a due and secure manner. This includes storing requests for issuing TST (TSQ) and responses (TSR). For the records shall be ensured control of confidentiality and integrity during their life-cycle - during systems operation (data in use), during transfer/ relocation (data in transit) and upon archiving (data at rest). Information from these records may be requested by the competent authorities in due order.

In addition to the system records shall be also carried out:

- Time-stamping authority key management records;
- accurate time synchronization records

Journals shall be stored for a period of at least 2 years.

Issued qualified electronic time stamps shall be stored for a period of at least 10 years.

7.5 Operations organization

For the organization of the operations of the time stamping authority, 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 IT services and ISO 9001:2015 for quality management.

The documents managed by the Integrated Management System as well as the policies and the practices contain all operational controls and procedures.

The activity is subject to control for compliance by external Compliance assessment authority pursuant to the requirements of the technical specification ETSI TS 119 421.