| | Position | Name, Surname | Data | Signature |
|---|---|---|---|---|
| **Approved by** | CEO | Dimitar Brankov | *10.05.2018* | |
| **Coordinated by** | IMS Representative | Emil Dautov | *10.05.2018* | |
| **Prepared by** | Cryptographic Security Administrator | Emil Dautov | *10.05.2018* | |

| | |
|---|---|
| **Date of document registration:** | *01.07.2017* |
| **Date of last correction:** | *10.05.2018* |
| **The original is stored at:** | *a* IMS Representative |

| ***Form type and №*** | | | | | |
|---|---|---|---|---|---|
| **Original** | | **Controlled copy** | **X** | **Information** | |

| | |
|---|---|
| **Dissemination of the document:** | **Subscriber:** |
| **Internal:** | |
| **Public:** | |

**This document is part of the Information Security Management System of**
**"SYSTEM FOR ELECTRONIC PAYMENTS BULGARIA/SEP BULGARIA" JSC**
**Everyone who uses this document shall carry out the ISMS requirements for work with sensitive information.**

## CONTENTS

## 1. INTRODUCTION

Policy and Practice for provision of qualified services for Time-Stamp Certification (“***Time-Stamp Certification Policy”***) is a document containing the general rules and regulations, applied by the qualified certification services Provider “SYSTEM FOR ELECTRONIC PAYMENTS BULGARIA/SEP BULGARIA“ JSC (SEP Bulgaria / Provider). This document specifies the policy and security requirements relating to the operation and management practices, used from the Time-Stamp Certification Authority (“***eSign Sep TSA***”) for issuing qualified electronic time-stamps.

In the “Time-Stamp Certification Policy” are specified the participants in the process of issuing and maintaining user qualification electronic time-stamps, as well as their responsibilities, rights and obligations. The applicable range of effect of the electronic time-stamps is also specified. A detailed description of those rules is provided in the document CPS of SEP Bulgaria..

The structure and contents of this “Time-Stamp Certification Policy” are prepare in accordance with the technical specification ETSI TS 102 023.

SEP Bulgaria fulfill the “Time-Stamp Certification Authority Policy” upon provision of electronic time-stamps and publicly provides qualified certification services for provision of qualified electronic time-stamps. It can be accessed on: http://www.eSign.bg.

The qualified electronic time-stamp is used by default for exactness of the date and hour specified by it for integrity of the data with which the date and time are connected.

The qualified time-stamp issued by SEP Bulgaria is recognized in all member states of the European Union and complies with the following requirements:

1. it binds the date and time with the data in a way that largely excludes the possibility of unnoticed data change;
2. is based on an exact time source associated with coordinated universal time;
3. is signed with an elaborated or qualified electronic signature or is stamped with an elaborated or qualified electronic stamp of SEP Bulgaria in its capacity as a qualified provider of qualified certification services.

## 2. SCOPE

“Time-Stamp Certification Authority Policy” (***Policy***) can be used by the relying parties and users of qualified certification services.

SEP Bulgaria guarantees the reliability of the provided qualified TSS through its Time-Stamp Certification Authority (eSign Sep TSA).

The provision of qualified electronic time-stamps is based on the infrastructure with a public key, secure time sources and certificates format X.509.

## 3. REFERENCES

This document is in line with standards and standardization documents, procedures, directives, national legislation and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and certification services during electronic transactions on the internal market and repealing Directive 1999/93/EC (Regulation (EU) No 910/2014), including:

1. Recommendation ITU-R TF.460-6: „Standard-frequency and time-signal emissions";
2. ISO/IEC 19790:2012: „Information technology - Security techniques - Security requirements for cryptographic modules";
3. ISO/IEC 15408 (parts 1 to 3): „Information technology - Security techniques - Evaluation criteria for IT security";
4. ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers";
5. ETSI EN 319 421: „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps";
6. ETSI EN 319 422: „Electronic Signatures and Infrastructures (ESI); Time-Stamping protocol and Time-Stamp token profiles";
7. FIPS PUB 140-2: „Security Requirements for Cryptographic Modules";
8. IETF RFC 3161 „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)";
9. IETF RFC 5816: „ESSCertIDV2 update to RFC 3161";
10. Certification Practice Statement/CPS of SEP Bulgaria.

## 4. DEFINITIONS AND ABBREVIATIONS

### 4.1. DEFINITIONS

1. Network Time Protocol (NTP) - a network protocol that is used by time synchronization programs on one or a network of many information systems;
2. Electronic time-stamp (Time-Stamp tamp) - data in electronic form linking other data in electronic form at a specific point in time and representing evidence that the latest data existed at that time;
3. Qualified Electronic Time-stamp - electronic time-stamp that meets the requirements of Regulation (EU) No 910/2014;
4. Time-Stamp Certification Authority ("eSign Sep TSA") - an internal infrastructure unit within ESIGN SEP that issues qualified electronic time-stamps;
5. Qualified Time-Stamping Service (TSS) - a service for verifying the date and hour of submission of the electronic document;
6. Time-Stamp tamp token profiles (TST) - Information object defined in recommendation IETF RFC 3161 (profile of an electronically signed certificate "eSign Sep TSA" for the existence of digital content of an electronic document before a specified moment specified in the certificate, and for un-changeability of this content after this moment. Attached to an electronic signature, the certificate creates irrevocability of the signature in time);
7. Relying party: recipient of a time-stamp token who relies on that time-stamp token;
8. User: entity requiring the services provided a TSA and which has explicitly or implicitly agreed to its terms and conditions
9. Time-stamp policy: named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements;
10. Time-stamp token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time;
11. Time-Stamping Authority (TSA): authority which issues time-stamp tokens

12. time-stamping unit(TSU): set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time
13. TSA system: composition of IT products and components organized to support the provision of time-stamping services;
14. Coordinated Universal Time (UTC) - Coordinated Universal Time reported in accordance with Recommendation ITU-R TF.460-6 [1];

### 4.2. ABBREVIATIONS

1. TSA - Time-Stamping Authority;
2. TSS - Time-Stamping Service;
3. TSU - Time-Stamping Unit;
4. TST - Time-stamp Token;
5. UTC - Coordinated Universal Time;
6. PKI - Public Key Infrastructure.

## 5. GENERAL CONCEPTS

### 5.1. QUALIFIED TIME-STAMPING CERTIFICATION SERVICES (TSS / TIME-STAMPING SERVICES)

The data exchange in the infrastructure of eSign SEP, which is used to issue and manage qualified electronic time-stamps, consists of two main components:

1. technological system that issues qualified electronic time-stamps , maintains a record and archive of generated time tokens for electronic time-stamps ;
2. management of the system, which monitors and controls the operations of receiving online requests, issuing, checking and approval of the issued tokens for electronic time-stamps .

The system management guarantees direct access to a UTC secure source and reliable management of the technological system components. TSS is performed by internal eSign unit - Time-Stamp Certification Authority ("eSign Sep TSA"). The Time-Stamp Certification Authority issues qualified electronic time-stamp (Qualified Time-Stamp) through which the Provider's users can certify the time for provision of electronic documents, electronic signatures, electronic transactions, etc. The qualified electronic time-stamp is proof that the data object existed at the moment of the time-stamping.

In order to do that “eSign Sep TSA”:

a) confirms existence of the data;
b) provides evidence that the electronic signature/stamp was affixed with valid pair of cryptographic keys, used for signing/stamping the electronic document or the electronic message;
c) issues a qualified electronic time-stamp in compliance with standard ETSI EN 319 422;

d) issues a qualified electronic time-stamp which does not contain errors or inexact information;

e) is not a party on the arrangements described and marked in the time certificate.

## 5.2. TIME-STAMP CERTIFICATION AUTHORITY, ESIGN SEP TSA

eSign Sep TSA is a certifying authority in the infrastructure of SEP Bulgaria, issuing qualified certificates for qualified electronic TSS s managed according to the present policy.

SEP Bulgaria confirms, that" "eSign Sep TSA" is subject to audit, at least once every 24 months from a Compliance Evaluation Authority. Within normative time the report for compliance evaluation is submitted to the Monitoring Authority – the Communications Regulatory Commission.

## 5.3. USERS

The users are the persons defined in the "Certification Practice Statement" of SEP Bulgaria.

When the user is an organization which consists of several end users or an individual end-user, some of the responsibilities related to an organization shall also be applied to the end-users. In any event, the organization is responsible if end-user obligations are not properly executed. Therefore, the organization should inform its end-users about their responsibilities and obligations.

If the user is an end consumer, he/she is liable if he/she fails to perform his/her duties correctly, under the conditions stipulated in this document.

## 5.4. GENERAL PROVISIONS

This Time-Stamp Certification Authority Policy defines a set of rules that SEP Bulgaria complies with when issuing qualified electronic time-stamps. This document complements the CPS of SEP Bulgaria.

The Provider issues qualified electronic time-stamps to any third party without any technical limitations. The issue of qualified electronic time-stamps may be paid or free of charge. Information on fees collected by SEP Bulgaria can be found on the website at: http://www.eSign.bg

1. Purpose

The Policy is published on the website of the Provider and is available to all interested parties.

Management of the personnel, the physical and operational security of the activities of Provider during provision of qualified certified services, are described in the CPS of SEP Bulgaria.

2. Specifics

The Policy defines only the general rules for issuing and management of qualified electronic time-stamps.

A detailed description of the technological process is contained in additional documents which are not public.

The unpublicized documents, together with reports, results from external and internal audits are accessible only for authorized persons.

3. Approach

This Policy has been developed in a general plan and does not describe every technical detail. It specifies the rules and conditions which the Provider complies with, in its capacity as a qualified provider of certified services and is an inseparable part of the General Conditions of the contract with the users during provision of qualified electronic time-stamps.

## 6. POLICY

### 6.1. GENERAL REQUIREMENTS

The Policy defines a set of rules, which SEP Bulgaria complies with upon issuing qualified time-stamps to provide accurate time versus the Coordinated Universal Time (UTC) accurate to 0.5 seconds.

SEP Bulgaria guarantees:

1. public access to receive and verify the issued qualified time-certificates;
2. that appropriate security measures are followed, in accordance with the generally accepted international practice;
3. that appropriate security measures are followed, in accordance with the generally accepted international practice;
4. Provider's activities are organized in such a way that the issuance of qualified electronic time-stamps is separated from the other activities of the Provider;
5. electronic time-stamp token (TST) profile complies with ETSI EN 319 422;
6. TST issued by eSign Sep TSA contains information for the stamp (TST-info structure) located in the Signed-Data structure (RFC 2630), signed by eSign Sep TSA and embedded in Content-Info structure (RFC 2630). The issued time-stamps are compliant with RFC 3161 recommendations. The Qualified Time Verification Service issues RSA 2048-bit encrypted qualified electronic time-stamps using SHA256.

The certificate profile of eSign Sep TSA, which verifies the electronic time-stamp in the issued electronic TST is:

| eSign Sep TSA | | |
|---|---|---|
| Version | V3 | |
| Signature algorithm | sha256RSA | |
| Signature hash algorithm | sha256 | |
| Issuer | CN | eSign Sep QES CA |
| | OU | SEP Bulgaria JSC Qualified QES Authority |
| | 2.5.4.97 (organizationIdentifier) | NTRBG-131107204 |
| | O | Sep Bulgaria JSC |
| | C | BG |
| Validity | 5 years | |
| Subject | CN | Common Name |
| | *2.5.4.97 (organizationIdentifier) | Legal entity ID NTRYY-xxxxxxxxx / national identification code / VATYY-xxxxxxxxx /VAT Number/ |

| | | |
|---|---|---|
| | | YY – country code |
| | O | Organization |
| | L | Locality |
| | C | Country |
| Public key | RSA 2048 bits | |
| Authority Information Access | [1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://www.esign.bg/bg/services/public-register/eSign_Sep_QES_CA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.esign.bg/ocsp | |
| Certificate Policies (Non Critical) | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.30299.3.1.2<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>https://www.esign.bg/bg/useful/documents/ | |
| CRL Distribution Points (Non Critical) | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://crl.sep.bg/eSignSepQESCA.crl | |
| Basic Constraints (Critical) | Subject Type=End Entity<br>Path Length Constraint=None | |
| Key Usage (Critical) | Digital Signature (80) | |
| Enhanced Key Usage (Critical) | Time Stamping (1.3.6.1.5.5.7.3.8) | |

## 6.2. POLICY IDENTIFIER (OID)

Through the inclusion of this object OID identified in the issued tokens for electronic time-stamp, SEP Bulgaria confirms compliance with this Policy.

The OID described above is in compliance with ETSI BTSP (Best Practices Policy for Time-Stamp) OID=0.4.0.2023.1.1, in accordance with the ETSI EN 319 421.

The OID of eSign Sep TSA is: 1.3.6.1.4.30299.3.1.2

## 6.3. APPLICABILITY OF ELECTRONIC TIME-STAMP

The qualified TSS allows certification of the date and hour of provision of the electronic signature/stamp of every document signed with electronic signature/stamp.

This document does not specify any limitations in the applicability of the token for electronic time-stamp (TST), issued in compliance with this policy.

The Policy is directed towards execution of the requirements for qualified time-stamps with long validity term (ETSI EN 319 122 [6]), but it is applicable to every other use of time-stamps with equivalent requirements.

### 6.4. COMPLIANCE

The issued TST includes the OID, described in clause 6.2.

eSign SEP TSA executes only requests for electronic time-stamps, issued in compliance with this Policy.

eSign SEP TSA conducts its activities in accordance with the applicable legislation and standards:

1. Regulation (EU) № 910/2014;
2. ETSI TS 119 421;
3. IETF RFC 3161;
4. IETF RFC 5816.

## 7. OBLIGATIONS

### 7.1. GENERAL OBLIGATIONS OF ESIGN SEP TSA

SEP Bulgaria guarantees compliance of the procedures in this Policy with the requirements of Regulation (EU) № 910/2014 and the legislation acts applicable to it, as well as with the national legislation.

The procedures are subject to control from the Conformity Assessment Body and the Supervisory Body.

SEP Bulgaria guarantees public permanent assess to the Qualified TSS (24/7/365), excluding the time of regular technical maintenance of the technological system for receiving and audit of the issued qualified time-stamp tokens. The service for issuing qualified electronic time-stamps is with exactness of up to 0.5 (half) second and guarantees the users exactness, even during multiple connections at the same time (for example 100 users) and the Provider guarantees:

1. the provided services are complied with commonly accepted international standards and documents, described in “Practice during provision of qualified certification services;
2. uses reliable and secure technological equipment (hardware and software) for provision of the qualified certification service;
3. conducts their activities in accordance with the legislation;
4. the issued electronic TST does not contain any untrue data or errors;
5. does not breach licenses, intellectual property or other rights in the issued electronic time-stamp tokens TST;
6. does not allow modification of the digital data after issuing the time-stamp token TST, without establishing it.

### 7.2. OBLIGATIONS OF THE USERS

The users are obliged to check the validity of the electronic signature of the eSign Sep TSA and/or the Certificate Revocation List (CRL) upon extraction of the time-stamp token (TST). The updated lists (CRLs) are published on the web page of SEP Bulgaria on: http://www.eSign.bg.

Check of the certificate of the eSign Sep TSA can also be made by using the service Online Check of the Certificate Status (OCSP): http://www.eSign.bg..

Additional obligations of the users are described in clause CPS of SEP Bulgaria.

### 7.3. OBLIGATIONS OF THIRD PARTIES

The relying party should have the necessary minimum of technical knowledge for using the qualified TSS and take the necessary care. The main obligation of the relying party is to check the signature on the electronic TST. The relying party should check the validity of the certificate of eSign Sep TSA, as well as the validity term of this certificate. In case of check of time-stamp, after expiration of the validity term of the certificate of eSign Sep TSA, the third parties should:

1. make a check in the CRL of the certificate of eSign Sep TSA;
2. to make check for the applicability of the used hash algorithm;
3. to make sure in the security of the used electronic signature by checking the applicable combination of asymmetric and hash algorithms.

Using time-stamps should correspond to the requirements of this Policy and the CPS.

## 8. RESPONSIBILITY OF ESIGN SEP TSA

The responsibility of every person who is participant in the activity for provision and using qualified certification service is settled by the law or is settled in the contract between the Provider and the user.

SEP Bulgaria is responsible before the users of certification services who count on its activity, for damages caused with intent and gross negligence. The responsibility of the provider is applicable only, if the damages were caused as direct and immediate consequence of guilty behavior of SEP Bulgaria or of the parties, to whom conducting functions in relation to the provision of TSS s was assigned.

If the Provider confirms and approves that there were damages, it engages to remedy the damaged person. SEP Bulgaria is liable only to the amount of the real damages.

The obligatory insurance covers the liability of SEP Bulgaria to users, correspondingly third parties, for caused property and non-pecuniary damage up to the limits, specified in the national legislation and this Policy.

## 9. REQUIREMENTS TO ESIGN SEP TSA

SEP Bulgaria guarantees that it realizes securely, reliably and legally the management of its activities, by controlling all parties, related in some way with the procedures for time reporting, records the information and manages the personnel in appropriate

manner in order to execute its obligations correctly. All documents related to the registered information and events are recorded in journal and are archived. Storage of these records is executed in an appropriate manner. Only authorized employees of the Provider have access to the data.

eSign Sep TSA exercises control on its activities, which allows provision of qualified certification service in compliance with the provisions of this Policy. In order to control the effective functioning of the technological time reporting system, user profiles and personnel activity, all events in the system are registered.

## 10. PRACTICE OF ESING SEP TSA

### 10.1. PRACTICE

Security management and infrastructure management, procedures, control mechanisms of SEP Bulgaria are described in detail in the CPS.

The obligations and responsibility of eSign Sep TSA are described in clause 7.1 of this Policy and are in the base of the functioning of the Certifying Authority.

The audits allow constant audit of the integrity of the technological system, respectively update and troubleshooting. The exercised monitoring on the functionality of the technological system guarantees that it works correctly and in compliance with the provided production configuration.

### 10.2. SERVICE ACCESSIBILITY

SEP Bulgaria applies the following measures in order to provide accessibility of the service:

1. computer system reservation;
2. internet connection reservation;
3. use of uninterruptible power supplies.

This Policy is publicly accessible on the website of the Provider:

http://www.eSign.bg

## 11. PROCEDURES OF ESIGN SEP TSA

### 11.1. MANAGEMENT OF THE LIFECYCLE OF THE KEY PAIR

### 11.1.1 GENERATING A KEY PAIR OF ESIGN SEP TSA

The requirements for the used algorithms and the length of the signing private key of eSign Sep TSA are complied with the technical specification ETSI TS 119 312.

Generating the signing key of eSign Sep TSA is made in a cryptographic module (HSM) with security level FIPS 140-2, level 3. The generated key pair of RSA keys is 2048 bits.

Generating the signing key of eSign Sep TSA is made in a physically protected environment by persons with trusted roles. Access is two-stage by at least two authorized persons.

### 11.1.2 DISTRIBUTION OF THE PUBLIC KEY OF ESIGN SEP TSA

The certificate of the eSign Sep TSA together with the corresponding public key is published on the web page of the Provider : https://www.eSign.bg

### 11.1.3 RE-ISSUING THE PRIVATE KEY OF ESIGN SEP TSA

The life-time of the private key of eSign Sep TSA cannot be longer than the period of time, through which the selected algorithm or key length satisfy the purpose for which they were approved for use. The validity period of the certificate of eSign Sep TSA is 5 years. After expiration of this period, the validity term of the certificate is prolonged for another period of 5 years. After this period, a new key pair is generated, and its private key is stored in the crypto-module (HSM), and the public key is certified by issuing a new certificate to eSign Sep TSA. The key pair with expired validity term is stored as follows:

1. private key – stored for a period of 10 years;
2. public key – stored for a period of 10 years.

All used algorithms are inspected once a year or when changes occur. In case the algorithm is compromised or becomes inappropriate, a regeneration of all affected keys is initiated.

### 11.1.4 TERMINATION OF THE PRIVATE KEY OF ESIGN SEP TSA

After expiration of the validity term of the private key of eSign Sep TSA, it is destroyed in a way that it cannot be restored.

### 11.1.5 PROTECTION OF THE PRIVATE KEY OF ESIGN SEP TSA

The private key of eSign Sep TSA is generated and stored in HSM corresponding to standard FIPS 140-2, level 3.

The archived copies of the private key of eSign Sep TSA are stored in a special safe.

The storage of a copy of the key is made in order to retrieve it in the event of natural disaster or crash of the system. Storage of the key is periodically inspected by the auditor of SEP Bulgaria. The storage method is described in procedures from the internal documentation of SEP Bulgaria.

### 11.2. MANAGEMENT OF THE LIFECYCLE OF THE SIGNING CRYPTOGRAPHIC EQUIPMENT

During transportation and storage, the used cryptographic module is inspected by trusted personnel with double control. The module is expected for damages:

1. on security stickers;
2. of the module box (scratches, indentations);
3. on the pack.

The following measures are applied:

1. the installation, activation and creation of a spare copy of the signing private key of eSign Sep TSA in the HSM is executed only by trusted personnel with two-stage control in a physically protected environment;
2. in case of scrappage of the cryptographic module, the private keys contained in it will be deleted and destructed in compliance with the recommendation of the producer.

### 11.3. TIME-STAMPING

The server software of eSign Sep TSA implements the technical specification ETSI TS 101 861 v.1.3.1 and the international recommendation IETF RFC 3161.

The system software of eSign Sep TSA maintains communication with the clients of the service for protocol Time-Stamp Certification: TCP/IP, HTTP/HTTPS.

### 11.4. ELECTRONIC TIME-STAMPING TOKEN, TST

Every electronic time-stamp token (TST) issued by SEP Bulgaria includes a unique identifier of the policy of. eSign Sep TSA

The request/reply profile of eSign Sep TSA is in compliance with the technical specifications described above and includes the following attributes/parameters.

| eSign Sep TSA | | |
|---|---|---|
| Version | V3 | |
| Signature algorithm | sha256RSA | |
| Signature hash algorithm | sha256 | |
| Issuer | CN | eSign Sep QES CA |
| | OU | SEP Bulgaria JSC Qualified QES Authority |
| | 2.5.4.97 (organizationIdentifier) | NTRBG-131107204 |

| | | |
|---|---|---|
| | O | Sep Bulgaria JSC |
| | C | BG |
| Validity | 5 years | |
| Subject | CN | Common Name |
| | *2.5.4.97 (organizationIdentifier) | Идентификатор за юридическо лице<br>NTRYY-xxxxxxxxx /национален идентификационен код/<br>VATYY-xxxxxxxxx /Данъчен номер/<br>YY – код на държава |
| | O | Organization |
| | L | Locality |
| | C | Country |
| Public key | RSA 2048 bits | |
| Authority Information Access | [1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://www.esign.bg/bg/services/public-register/eSign_Sep_QES_CA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.esign.bg/ocsp | |
| Certificate Policies (Non Critical) | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.30299.3.1.2<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>https://www.esign.bg/bg/useful/documents/ | |
| CRL Distribution Points (Non Critical) | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://crl.sep.bg/eSignSepQESCA.crl | |
| Basic Constraints (Critical) | Subject Type=End Entity<br>Path Length Constraint=None | |
| Key Usage (Critical) | Digital Signature (80) | |
| Enhanced Key Usage (Critical) | Time Stamping (1.3.6.1.5.5.7.3.8) | |

### 11.5. SYNCHRONIZATION OF THE CLOCK WITH UNIVERSAL COORDINATED TIME

SEP Bulgaria guarantees that it provides physical and informational security of the technological system for prevention of unauthorized operations, directed to lack of calibration of the clock or its physical damaging.

eSign Sep TSA uses hardware and source of exactly calibrated time with high degree of exactness. Synchronization of UTC with the source of time is automatic, based on NTP protocol, after establishing difference between the source and time in the system.

In case there is a problem in the hardware during and until its change with a spare one, time servers based in the internet are used as a source of exact time. Synchronization is on the basis of two time sources, through NTP protocol.

SEP Bulgaria has audits, which allow discovering every difference between the clock and time, included in the electronic TST.

## 11.6. MANAGEMENT AND ACTIVITY

### 11.6.1 RISK EVALUATION

SEP Bulgaria regularly performs risk assessment in order to provide quality and reliability of the provided services. The security audits defined in the security concept of the Provider are controlled quarterly in order to provide control effectiveness.

Description of the procedures and plans for achieving continuity and security of the Provider's activities are described in the CPS by SEP Bulgaria.

All systems included in issuing the qualified electronic time-stamps provide high degree of reliability.

The technological system is located in a physically protected environment, minimizing the risk of natural disasters.

In case the private key of eSign Sep TSA is compromised, the affected HSM is immediately isolated from the network, and corrective measures are taken:

1. notifying the security administrator in order to undertake further actions;
2. initiation of security audit of the rest of the HSM – integrity audit and journal analysis;
3. notifying the relying parties which are affected by the compromising;
4. initiation of substitution procedure.

### 11.6.2 SECURITY MANAGEMENT

In SEP Bulgaria is implemented information security policy. All employees are obliged to comply with the norms of this policy. The Information security policy is reviewed on a regular basis and in case there were problems.

All issues related to the security management are described in the CPS.

### 11.6.3 OPERATIONAL SECURITY

The characteristics of the personnel and the trusted roles of the Provider are in compliance with the CPS.

SEP Bulgaria supports qualified employees on positions which provide execution of their obligations at any moment during conducting the activities on issuing electronic time-stamp certificates, in compliance with the legislation.

### 11.6.4 PHYSICAL SECURITY

eSign Sep TSA performed by different security levels of the physical and logical access to the technological system a secure and reliable conducting of operations.

SEP Bulgaria provides:

1. network and services monitoring;
2. separation of the obligations;
3. separation of network segments;
4. protected physical environment;
5. provision of computer systems.

In case an employee who is responsible for Time-Stamp Certification activities, changes their role or leaves the company, all belonging carriers related to the security are returned or invalidated.

The physical control and access control are in compliance with CPS.

### 11.6.5 NETWORK SECURITY

Based on risk assessment, the network infrastructure is divided to zones, considering the functional, logical and physical relation between trusted systems and services. SEP Bulgaria restricts the access and communications to such level, which is necessary for the normal work of the certification services. Connections and services related to the certification services are deactivated. The established rule for access is reviewed periodically.

All elements of the critical infrastructure are kept in a protected environment.

An administrative network was developed, which is separated by the network for operational purposes. The systems used for administration cannot be used for non-administrative activities.

The test and exploitation platform is separated by other environments which have no relation to the work operations.

Communication between remote trusted systems is made only through secure channels, which are logically separated by the other communication channels and provide identification of their end points. Data protection on the channel is provided, against disclosure or modification.

Internet connection is reserved.

The private IP addresses for access are also regularly scanned for liabilities, and then a report is prepared.

Test for system penetration is conducted in the following cases: after the initial setting of the systems and after infrastructural or upgrades of applications and changes. After finishing the test, a report is prepared.

### 11.6.6 ACTIVITY MANAGEMENT

SEP Bulgaria has protected all systems in compliance with the security policy.

SEP Bulgaria has implemented policies providing timely application of security patches (patch/software corrections).

The security is made in every new developed system analysis of the requirements regarding, during the design and functionality planning stage.

When new versions are released, procedures for control of changes are applied, including in case of urgent changes in the software.

The integrity of the systems and information of eSign Sep TSA are protected from viruses, malicious code and unauthorized software.

Handling external carriers in SEP Bulgaria are made in a secure manner in order to protect them from damage, theft or aging.

Procedures for all trusted and administrative roles related to provision of certification services were implemented.

The requirements to the capacity of computer systems are monitored, in order to provide sufficient quantity of calculation capacity and disk space.

### 11.6.7 SYSTEM ACCESS MANAGEMENT

SEP Bulgaria provides monitoring on the access to computer systems and user requests regarding:

1. unusual system activities showing potential violation of the security, including breach in the network of SEP Bulgaria and reporting through the alarm system;
2. starting and shutting off log functions;
3. availability and using services in the network of SEP Bulgaria.

After every security breach or loss of integrity, which have significant influence on the provided trusted service, as well as on the managed personal data, SEP Bulgaria communicates it to the Supervisory Authority. After establishing a critical security breach, the Supervisory Authority is notified within 24 hours.

### 11.6.8 SECURE ENVIRONMENT

The operational environment for storage of the private key of the eSign Sep TSA and for electronic signing of electronic TST, supplied to the users, is the HSM with certified with security level FIPS 140-2 Level 3.

Documents relate to the environment security are mostly internal documentation of SEP Bulgaria and are periodically reviewed by the auditor.

## 11.7. COMPROMISING THE PRIVATE KEY OF ESIGN SEP TSA

SEP Bulgaria takes maximum care within its abilities and resources, to minimize the risk of compromising the private key of the eSign Sep TSA as a result of human mistake, natural disasters or emergencies.

In case of compromising or doubt for compromising a private key of eSign Sep TSA, the following actions are taken:

1. immediately terminates the certificate of eSign Sep TSA;
2. eSign Sep QES CA generates new key pair and new certificate;
3. all users and relying parties are informed for the events immediately with information of the web page of SEP Bulgaria;
4. the certificate corresponding to the compromised key is put in the CRL, together with the appropriate reason for termination;
5. immediate analysis is performed and a report for the reason for compromising is prepared.

These operations are performed in compliance with the plan, developed by SEP Bulgaria for security accidents.

### 11.8. TERMINATION OF THE ACTIVITY OF ESIGN SEP TSA

SEP Bulgaria applies its procedures from the CPS in case of termination of eSign Sep TSA.

### 11.9. COMPLIANCE WITH LEGAL REQUIREMENTS

For all matters which are not settled in the CPS the provisions of Regulation 910/EU and the applicable legislation are applied.
All requirements for provision of qualified electronic time-stamps, arising from this document are in compliance with the requirements of the standards and standardization documents of ETSI, arising from the provisions of Regulation (EU) № 910/2014.

### 11.10. RECORD OF EVENTS

SEP Bulgaria records and keeps accessible all information related to issued or received data, for the corresponding period of time. These records are stored even after termination of the service. Every evidence for the condition of the technological system and information data is recorded in a secure and reliable manner.
SEP Bulgaria provides:

1. records related to the activity of the service can be provided to the competent authorities for the purposes of court proceedings, in case evidence for its correct functioning is needed;
2. records of all events related to the lifespan of the keys and certificates of eSign Sep TSA is maintained;
3. records of all events related to synchronization of the clock of eSign Sep TSA with the coordinated universal time (UTC) are maintained. This includes information related to the normal recalibration or synchronization of the clocks, used for provision of qualified electronic time-stamps ;
4. records for all events after establishing loss of synchronization;
5. all events are recorded in a manner which makes them hard for deletion.
6. journals for events are kept for at least 3 months;
7. the journal for the issued qualification time-stamps is kept for at least 10 years;
8. confidentiality and integrity of the current and archived records, related to the activity of the services in accordance with the good practices.

### 11.11. SCHEME OF ORGANIZATION

SEP Bulgaria maintains internal documents for the correct work of eSign Sep TSA, describing the operational control related to:

1. personnel security;
2. access control;
3. risk assessment;
4. etc.

These internal documents are analysed by an independent Authority for evaluation of the compliance in accordance with the requirements of technical specification ETSI TS 119 421.

"SYSTEM FOR ELECTRONIC PAYMENTS BULGARIA/SEP BULGARIA" JSC (SEP Bulgaria / Provider) is a legal entity, registered in the Commercial Register to the Registry Agency with UIC 131107204, with seat and management address:
Sofia city, 1164, region Lozenez, R.D. „ Lozenez", 1 Zlatovrah str..
Contact telephone: 070018283. Internet address: http://www.eSign.bg/

| Record changes | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Page** | | | | | | | | | | | | | | | | | | | | |
| **Valid amendment** | | | | | | | | | | | | | | | | | | | | |