### Certification Practice Statement for Qualified Certification Services

<table>
<thead>
<tr>
<th>Position</th>
<th>Name, Surname</th>
<th>Data</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEO</td>
<td>Vania Ganeva</td>
<td>01.07.2017</td>
<td></td>
</tr>
<tr>
<td>Coordinated by</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Representative of the management on ISMS</td>
<td>Dimitar Brankov</td>
<td>01.07.2017</td>
<td></td>
</tr>
<tr>
<td>Prepared by</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator PKI</td>
<td>Emil Dautov</td>
<td>01.07.2017</td>
<td></td>
</tr>
</tbody>
</table>

Date of document registration: 01.07.2017

The original is stored at: A representative of the management in ISMS

**Form type and №**

<table>
<thead>
<tr>
<th>Original</th>
<th>Controlled copy</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

Uncontrolled copy and multiplication is not allowed! All rights reserved!  
© Copyright. All Rights reserved!
CONTENTS

1. INTRODUCTION ........................................................................................................... 7
  1.1. REVIEW ................................................................................................................... 7
  1.2. NAME AND DOCUMENT IDENTIFICATION .......................................................... 8
  1.3. Participants in the infrastructure of SEP Bulgaria ................................................ 9
  1.3.1. Certification authorities ........................................................................................ 9
  1.3.1.1. Root certification authority (eSign Sep Root CA) .............................................. 9
  1.3.1.2. Operational certification authority (eSign Sep QES CA) .................................. 9
  1.3.2. Registration authority .......................................................................................... 10
  1.3.3. Users .................................................................................................................. 10
  1.3.3.1. Signature .......................................................................................................... 10
  1.3.3.2. Creator of the seal ............................................................................................ 11
  1.3.3.3. Relying parties .................................................................................................. 11
  1.3.4. Other participants ............................................................................................... 11
  1.3.4.1. Validation authority .......................................................................................... 11
  1.4. Qualified Certificates usage ...................................................................................... 12
  1.4.1. Types of Qualified certificates and recomended range of applicability ............ 12
  1.4.2. Usage ................................................................................................................ 12
  1.5. Practice management in Qualified certificate service providing ................................ 13
  2. Responsibility for publication and repository .......................................................... 13
  2.1. Repository .............................................................................................................. 13
  2.2. Information, published by SEP Bulgaria ................................................................. 13
  2.3. Frequency of publication ....................................................................................... 14
  2.4. Access to publications ............................................................................................ 14
  3. Identity identification and authentication ................................................................. 14
  3.1. Names .................................................................................................................... 15
  3.1.1. Type of names ..................................................................................................... 15
  3.1.2. Necessity for distinguished names ..................................................................... 15
  3.1.3. User anonymity ................................................................................................ 15
  3.1.4. Rules for different names interpretation ............................................................. 16
  3.1.5. Uniqueness of the names .................................................................................... 16
  3.1.6. Recognition, authentication and role of the trademark. Dispute Resolution Procedure. .................................................................................................................................... 16
  3.2. Initial registration .................................................................................................. 16
  3.2.1. PERSONAL KEY POSSESSION VERIFICATION ........................................... 17
  3.2.2. Establishing the identity of a legal entity ............................................................. 17
  3.2.3. VERIFICATION OF THE IDENTITY OF A PHYSICAL PERSON IN ASSOCIATION WITH A LEGAL PERSON ................................................................. 18
  3.2.4. ESTABLISHING THE IDENTITY OF A NATURAL ENTITY ..................................... 18
  3.2.5. INITIAL IDENTIFICATION AND AUTHENTICATION OF THE PERSON FOR AN ELECTRONIC REGISTRATION ........................................... 19
  3.2.6. SPECIAL ATTRIBUTES .................................................................................... 19
  3.2.7. UNCONFIRMED INFORMATION ...................................................................... 19
  3.2.8. Verification by the certifying authority ................................................................ 20
  3.2.9. CRITERIA OF CONFORMITY .......................................................................... 20
  3.3. IDENTIFICATION AND IDENTITY VERIFICATION FOR A QUALIFIED CERTIFICATE RENEWAL ............................................................. 20
  3.4. IDENTIFICATION AND IDENTITY VERIFICATION FOR A QUALIFIED CERTIFICATE SUSPENSION ............................................................... 21
  3.5. IDENTIFICATION AND IDENTITY VERIFICATION FOR A QUALIFIED CERTIFICATE TERMINATION .............................................................. 22
  3.6. IDENTIFICATION AND IDENTITY VERIFICATION AFTER TERMINATION OF A QUALIFIED CERTIFICATE .......................................................... 22
  4. OPERATIONAL REQUIREMENTS .............................................................................. 22
  4.1. REQUEST SUBMISSION FOR A QUALIFIED CERTIFICATE ISSUANCE .......... 23
  4.1.1. WHO CAN SUBMIT A REQUEST FOR A QUALIFIED CERTIFICATE? ........... 23
  4.1.2. PROCESSING OF THE REQUEST FOR A QUALIFIED CERTIFICATE ISSUANCE AND THE RELATED OBLIGATIONS ............................................................... 23
  4.1.2.1. USER CERTIFICATES ....................................................................................... 23
  4.1.2.2. CERTIFICATE AUTHORITY AND REGISTRATION AUTHORITY CERTIFICATES ................................................................. 24
  4.1.2.3. REQUEST FOR REGISTRATION OF USERS OF QUALIFIED CERTIFICATION SERVICES ............................................................. 24
4.1.2.4. Qualified Certificate Renewal (Renewal), Generation of a new key pair (re-key) and a qualified certificate change

4.1.2.5. Request for a Certificate Suspension and Termination

4.2. Request Processing

4.2.1. Identification and Identity Verification

4.2.2. Acceptance or Rejection of a Request

4.2.2.1. Request Processing by the Registration Authority

4.2.2.2. Request Submission to the Certification Authority for a qualified certificate issuance

4.2.3. Waiting for the qualified certificate issuance

4.2.4. Certification Authority allows the processing of the data

4.3. Qualified certificate issuance

4.3.1. Processing

4.3.2. Provision of Information

4.4. Qualified Certificate Acceptance

4.4.1. Confirmation of Acceptance of a Qualified Certificate

4.4.2. Publication of a Qualified Certificate

4.4.3. Information for Other Parties

4.5. Usage of a Qualified Certificate and of a Key Pair

4.5.1. By users

4.5.2. By Relying Parties

4.6. Renewal of a Qualified Certificate (Renewal)

4.7. Issuance of a Qualified Certificate with Generation of a New Key Pair (re-key)

4.7.1. Circumstances under which a qualified certificate is issued by generating a new key pair (re-key)

4.7.2. Who can request a Key Pair Update?

4.7.3. Re-key and Request Processing

4.7.4. Information for the User

4.7.5. Confirmation of Acceptance of a New Certificate

4.7.6. Publication of a New Qualified Certificate

4.7.7. Information for the Relying Parties

4.8. Change in the Qualified Certificate

4.8.1. Circumstances for a change in the qualified certificate

4.8.2. Who can request a change in the qualified certificate?

4.8.3. Request Processing

4.8.4. Information for the User

4.8.5. Confirmation of Acceptance of a New Qualified Certificate

4.8.6. Publication of a New Qualified Certificate

4.8.7. Information for the Relying Parties

4.9. Suspension and Revocation of a Qualified Certificate

4.9.1. Reasons for Revocation of a Qualified Certificate

4.9.2. Who can request revocation of a qualified certificate?

4.9.3. Procedure for Revocation of a Qualified Certificate

4.9.3.1. Procedure for Revocation of a Qualified Certificate

4.9.3.2. Procedure for Revocation of a Qualified Certificate of a CA or a RA

4.9.4. Grace Period of Revocation of a Qualified Certificate

4.9.5. Time Limit for Processing the Request for Revocation

4.9.6. Checking the Certificate Revocation List (CRL)

4.9.7. Frequency of Issuing the Certificate Revocation List (CRL)

4.9.8. Maximum Delay of Publication of the CRL

4.9.9. Online Certificate Status Checking

4.9.10. Requirements for Online Certificate Status Checking

4.9.11. Specific Requirements Regarding the Breach of the Key Security

4.9.12. Reasons for Suspension of a Qualified Certificate

4.9.13. Who can request a suspension of a qualified certificate?


4.9.15. Grace Period of a Suspension of a Qualified Certificate

4.9.16. Resuming the validity of a suspended certificate

4.9.17. Procedure for resuming the validity of a qualified certificate
4.10. CHECKING THE CURRENT STATUS OF A QUALIFIED CERTIFICATE ................................................................. 37
4.10.1. CHARACTERISTICS ........................................................................................................................................ 37
4.10.2. ADDITIONAL FUNCTIONS .......................................................................................................................... 37
4.11. TERMINATION OF A QUALIFIED CERTIFICATION SERVICES CONTRACT BY A USER ........................................ 38
4.12. PRIVATE KEY (ESCROW) .................................................................................................................................. 38
4.1. CONTROL OVER THE PHYSICAL AND ORGANIZATIONAL SECURITY .............................................................. 38
5. 1. CONTROL OF THE PHYSICAL CONTROL ........................................................................................................... 38
5. 1.1. PREMISES AND STRUCTURE OF THE PREMISES ............................................................................................ 38
5. 1.2. PHYSICAL ACCESS ........................................................................................................................................ 38
5. 1.3. ELECTRICAL POWER AND AIR-CONDITIONING .............................................................................................. 39
5. 1.4. FLOODING ....................................................................................................................................................... 39
5. 1.5. FIRE PREVENTION AND FIRE PROTECTION ..................................................................................................... 39
5. 1.6. DATA MEDIA STORAGE .................................................................................................................................. 39
5. 1.7. WASTE DISPOSAL ........................................................................................................................................... 40
5. 1.8. LIFETIME OF TECHNICAL COMPONENTS ....................................................................................................... 40
5. 2. ORGANIZATIONAL CONTROL ............................................................................................................................ 40
5. 2.1. TRUSTED ROLES ................................................................................................................................................ 40
5. 2.1.1. TRUSTED ROLES SEP BULGARIA .................................................................................................................. 40
5. 2.1.2. REQUIREMENTS FOR THE DIVISION OF RESPONSIBILITIES ................................................................. 41
5. 2.1.3. IDENTIFICATION AND AUTHENTICATION CERTIFICATION FOR EACH ROLE ............................................ 41
5. 3. CONTROL OVER THE PERSONNEL .................................................................................................................... 41
5. 3.1. REQUIRED QUALIFICATIONS FOR THE PERSONNEL ..................................................................................... 41
5. 3.2. INSPECTION PROCEDURES FOR THE PERSONNEL ....................................................................................... 42
5. 3.3. PERSONNEL TRAINING REQUIREMENTS OF SEP BULGARIA ....................................................................... 42
5. 3.4. TRAINING FREQUENCY AND REQUIREMENTS FOR EMPLOYEES’ SKILLS UPGRADING ............................. 42
5. 3.5. CHANGE OF JOB ............................................................................................................................................... 42
5. 3.6. SANCTIONS FOR UNAUTHORIZED ACTIONS ................................................................................................ 42
5. 3.7. CONTRACT WITH THE EMPLOYEE ................................................................................................................ 43
5. 3.8. DOCUMENTATION MADE AVAILABLE TO THE PERSONNEL ................................................................. 43
5. 4. 3 EVENT RECORDS AND LOGS MAINTENANCE ............................................................................................... 43
5. 4.1. RECORD TYPES ................................................................................................................................................ 43
5. 4.2. FREQUENCY OF RECORDS CREATING ........................................................................................................... 44
5. 4.3. PERIOD OF RECORD STORAGE ........................................................................................................................ 44
5. 4.4. RECORD PROTECTION ..................................................................................................................................... 44
5. 4.5. KEEPING BACKUP COPIES OF EVENTS RECORDS .......................................................................................... 45
5. 4.6. NOTIFICATION SYSTEM AFTER RECORDS ANALYSIS .................................................................................. 45
5. 4.7. VULNERABILITY AND ASSESSMENT ................................................................................................................ 45
5. 5. ARCHIVING .......................................................................................................................................................... 45
5. 5.1. TYPES OR ARCHIVES ....................................................................................................................................... 45
5. 5.2. PERIOD OF ARCHIVES STORAGE ....................................................................................................................... 46
5. 5.3. PROTECTION OF ARCHIVAL INFORMATION .................................................................................................. 46
5. 5.4. RECOVERY OF ARCHIVED INFORMATION ..................................................................................................... 46
5. 5.5. REQUIREMENTS FOR THE ARCHIVING TIME RECORDING ....................................................................... 46
5. 5.6. ARCHIVING STORAGE ...................................................................................................................................... 46
5. 5.7. ARCHIVAL INFORMATION ACCESS AND VERIFICATION PROCEDURES ......................................................... 46
5. 6. TSP’S KEY CHANGE ............................................................................................................................................ 47
5. 7. COMPROMISE OF KEYS AND RECOVERY AFTER ACCIDENTS ........................................................................... 47
5. 7.1. ACTIONS IN CASE OF ACCIDENTS ..................................................................................................................... 47
5. 7.2. INCIDENTS, RELATED TO FAILURES IN HARDWARE, SOFTWARE AND/OR DATA ........................................ 48
5. 7.3. COMPROMISE OR SUSPENSION FOR COMPROMISE OF PRIVATE KEY OF THE CERTIFICATION AUTHORITY .... 48
5. 7.4. BUSINESS CONTINUITY AND POST- DISASTER RECOVERY ......................................................................... 48
5. 8. CESSION OF ACTIONS OF SEP BULGARIA ......................................................................................................... 49
5. 8.1. REQUIREMENTS RELATING TO THE TRANSITION TO THE CESSION OF THE TSP ....................................... 49
5. 8.2. TRANSFER OF ACTIVITIES TO ANOTHER TSP OF QUALIFIED CERTIFICATION SERVICES ....................... 50
5. 8.3. WITHDRAWAL OF SEP BULGARIA’S QUALIFIED STATUS OR THE QUALIFIED STATUS OF THE TRUST SERVICE ...... 50
6.  MANAGEMENT AND CONTROL OF TECHNICAL SECURITY .................................................................................. 50
6. 1. KEY PAIR GENERATION AND INSTALLATION ................................................................................................ 50
6.1.1. GENERATION OF A KEY PAIR FOR A CERTIFICATION AUTHORITY .................................................................................. 51
6.1.2. GENERATION OF A KEY PAIR FOR SIGNATORY/CREATOR .................................................................................... 51
6.1.3. DELIVERY OF THE PRIVATE KEY TO THE USER ........................................................................................................ 51
6.1.4. DELIVERY OF A PUBLIC KEY BY USER TO THE TSP .................................................................................................. 51
6.1.5. DELIVERY OF TSP’S PUBLIC KEY TO THE RELYING PARTIES .................................................................................... 52
6.1.6. LENGTH OF KEYS ........................................................................................................................................................... 52
6.1.7. PARAMETERS OF THE PUBLIC KEYS ............................................................................................................................... 52
6.1.8. KEY USAGE ........................................................................................................................................................................ 52
6.2. PROTECTION OF PRIVATE KEY AND CONTROL OVER THE CRYPTOGRAPHIC MODULE .................................................. 52
6.2.1. CRYPTOGRAPHIC MODULES STANDARDS ..................................................................................................................... 52
6.2.2. CONTROL OVER THE USAGE AND STORAGE OF PRIVATE KEY .................................................................................. 53
6.2.3. PRIVATE KEY (ESCROW) .................................................................................................................................................. 53
6.2.4. PRIVATE KEY STORAGE ................................................................................................................................................... 53
6.2.5. PRIVATE KEY ARCHIVING .............................................................................................................................................. 53
6.2.6. TRANSFER OF THE PRIVATE KEY IN A CRYPTOGRAPHIC MODULE .............................................................................. 54
6.2.7. PRIVATE KEY STORAGE IN A CRYPTOGRAPHIC MODULE .............................................................................................. 54
6.2.8. PRIVATE KEY ACTIVATION METHOD ............................................................................................................................... 54
6.2.9. PRIVATE KEY DEACTIVATION METHOD ............................................................................................................................ 54
6.2.10. PRIVATE KEY DESTRUCTION METHOD ........................................................................................................................ 54
6.2.11. EVALUATION OF THE CRYPTOGRAPHIC MODULE .................................................................................................... 54
6.3. OTHER ASPECTS OF THE KEY PAIR MANAGEMENT .......................................................................................................... 54
6.3.1. PUBLIC KEY ARCHIVING ................................................................................................................................................ 55
6.3.2. VALIDITY PERIOD OF A QUALIFIED CERTIFICATE AND USAGE OF KEYS ......................................................................... 55
6.4. ACTIVATION DATA ................................................................................................................................................................. 55
6.4.1. GENERATION AND INSTALLATION OF ACTIVATION DATA ............................................................................................ 55
6.4.2. ACTIVATION DATA PROTECTION .................................................................................................................................. 56
6.4.3. OTHER ASPECTS OF ACTIVATION DATA ......................................................................................................................... 56
6.5. COMPUTER SYSTEMS SECURITY ........................................................................................................................................... 56
6.5.1. DEGREE OF COMPUTER SECURITY ................................................................................................................................ 56
6.6. IT SYSTEM’S LIFECYCLE SECURITY .................................................................................................................................. 56
6.6.1. DEVELOPMENT CONTROLS OF THE IT SYSTEM .............................................................................................................. 56
6.6.2. CONTROLS FOR THE IT SYSTEM SECURITY MANAGEMENT ........................................................................................... 57
6.6.3. IT SYSTEM SECURITY LIFECYCLE ASSESSMENT ............................................................................................................... 57
6.7. NETWORK SECURITY ................................................................................................................................................................. 57
7. PROFILES OF QUALIFIED CERTIFICATES, CRL AND OF OCSP ............................................................................................ 57
7.1. PROFILE OF QUALIFIED CERTIFICATES ............................................................................................................................. 57
7.1.1. VERSION ............................................................................................................................................................................. 58
7.1.2. ELIGIBLE EXTENSIONS IN THE FORMAT OF QUALIFIED CERTIFICATES ........................................................................ 58
7.1.3. IDENTIFIERS OF ELECTRONIC SIGNATURE/SEAL ALGORITHMS ................................................................................ 58
7.1.4. NAMING FORMS ............................................................................................................................................................... 58
7.1.5. RESTRICTIONS ON NAMES ............................................................................................................................................. 59
7.1.6. POLICY IDENTIFIER ........................................................................................................................................................ 59
7.1.7. EXTENSION IDENTIFIER ............................................................................................................................................... 59
7.1.8. DESIGNATION OF THE QUALIFIED CERTIFICATE ....................................................................................................... 59
7.1.9. USING AN IDENTIFIER FOR AN EXTENSION OF THE “CRITICAL” KEY ........................................................................ 59
7.2. PROFILE OF THE LIST OF CANCELLED AND INTERRUPTED CERTIFICATES (CRL) ................................................................. 59
7.2.1. VERSION ............................................................................................................................................................................. 59
7.2.2. FORMAT ............................................................................................................................................................................. 60
7.2.3. BASIC ATTRIBUTES OF THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL) .................................................. 60
7.2.4. ADDITIONAL ATTRIBUTES TO THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL) .................................. 60
7.2.5. FORMAT OF AN ELEMENT FROM THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL) .................................. 60
7.2.5.1. ATTRIBUTES OF AN ELEMENT IN THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL) .................................. 60
7.2.5.2. INDICATIONS OF THE REASON FOR A CERTIFICATE’S CANCELLATION/REVOCATION ............................................. 60
7.3. PROFILE OF A RESPONSE FOR ONLINE VERIFICATION OF A CERTIFICATE STATUS (OCSP) ...................................................... 60
8. CHECKING AND CONTROL OF TSP’S ACTIVITY ...................................................................................................................... 61
8.1. AUDIT FREQUENCY ............................................................................................................................................................... 61
8.2. QUALIFICATION OF THE AUDITORS .................................................................................................................................. 61
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.</td>
<td>RELATIONSHIP OF VERIFIERS WITH TSP</td>
<td>61</td>
</tr>
<tr>
<td>8.4.</td>
<td>AUDIT SCOPE</td>
<td>61</td>
</tr>
<tr>
<td>8.5.</td>
<td>ACTIONS TAKEN AS A RESULT OF THE AUDIT CONDUCTED</td>
<td>62</td>
</tr>
<tr>
<td>8.6.</td>
<td>AUDIT RESULTS STORAGE</td>
<td>62</td>
</tr>
<tr>
<td>9.</td>
<td>OTHER BUSINESS CONDITIONS AND LEGAL ASPECTS</td>
<td>62</td>
</tr>
<tr>
<td>9.1.</td>
<td>PRICES AND FEES</td>
<td>62</td>
</tr>
<tr>
<td>9.1.1.</td>
<td>FEES</td>
<td>62</td>
</tr>
<tr>
<td>9.1.2.</td>
<td>FEES FOR CERTIFICATION, CRYPTOGRAPHIC, INFORMATION AND CONSULTANCY SERVICES</td>
<td>63</td>
</tr>
<tr>
<td>9.1.3.</td>
<td>INVOICING</td>
<td>63</td>
</tr>
<tr>
<td>9.1.4.</td>
<td>RETURN OF CERTIFICATE AND RECOVERY OF PAYMENT</td>
<td>63</td>
</tr>
<tr>
<td>9.1.5.</td>
<td>FREE SERVICES</td>
<td>63</td>
</tr>
<tr>
<td>9.2.</td>
<td>FINANCIAL RESPONSIBILITIES</td>
<td>64</td>
</tr>
<tr>
<td>9.2.1.</td>
<td>INSURANCE OF ACTIVITIES</td>
<td>64</td>
</tr>
<tr>
<td>9.2.2.</td>
<td>INSURANCE COVERAGE</td>
<td>64</td>
</tr>
<tr>
<td>9.3.</td>
<td>CONFIDENTIALITY OF BUSINESS INFORMATION</td>
<td>64</td>
</tr>
<tr>
<td>9.3.1.</td>
<td>SCOPE OF CONFIDENTIAL INFORMATION</td>
<td>64</td>
</tr>
<tr>
<td>9.3.2.</td>
<td>NON-CONFIDENTIAL INFORMATION</td>
<td>65</td>
</tr>
<tr>
<td>9.3.3.</td>
<td>PROTECTION OF CONFIDENTIAL INFORMATION</td>
<td>65</td>
</tr>
<tr>
<td>9.4.</td>
<td>PRIVACY OF PERSONAL DATA</td>
<td>65</td>
</tr>
<tr>
<td>9.4.1.</td>
<td>PRIVACY STATEMENT</td>
<td>65</td>
</tr>
<tr>
<td>9.4.2.</td>
<td>INFORMATION TREATED AS PERSONAL</td>
<td>66</td>
</tr>
<tr>
<td>9.4.3.</td>
<td>INFORMATION THAT IS NOT CONSIDERED PERSONAL</td>
<td>66</td>
</tr>
<tr>
<td>9.4.4.</td>
<td>RESPONSIBILITY FOR THE PROTECTION OF PERSONAL DATA</td>
<td>66</td>
</tr>
<tr>
<td>9.4.5.</td>
<td>CONSENT FOR THE USE OF PERSONAL DATA</td>
<td>66</td>
</tr>
<tr>
<td>9.4.6.</td>
<td>OTHER CIRCUMSTANCES FOR DISCLOSURE OF INFORMATION</td>
<td>66</td>
</tr>
<tr>
<td>9.5.</td>
<td>INTELLECTUAL PROPERTY RIGHTS</td>
<td>66</td>
</tr>
<tr>
<td>9.5.1.</td>
<td>RIGHT TO OWNERSHIP OF DATA IN QUALIFIED CERTIFICATES</td>
<td>66</td>
</tr>
<tr>
<td>9.5.2.</td>
<td>RIGHT TO OWNERSHIP OF NAMES AND TRADEMARKS</td>
<td>67</td>
</tr>
<tr>
<td>9.5.3.</td>
<td>Right of ownership of a key pair</td>
<td>67</td>
</tr>
<tr>
<td>9.6.</td>
<td>GENERAL CONDITIONS</td>
<td>67</td>
</tr>
<tr>
<td>9.6.1.</td>
<td>Liabilities, responsibilities and guarantees of SEP Bulgaria</td>
<td>67</td>
</tr>
<tr>
<td>9.6.2.</td>
<td>Liabilities, Responsibilities and Guarantees of the Registration Authority</td>
<td>68</td>
</tr>
<tr>
<td>9.6.3.</td>
<td>Obligations of the Users</td>
<td>69</td>
</tr>
<tr>
<td>9.6.4.</td>
<td>Due care of the relying party</td>
<td>70</td>
</tr>
<tr>
<td>9.6.5.</td>
<td>Obligations of other parties</td>
<td>70</td>
</tr>
<tr>
<td>9.6.5.1.</td>
<td>Obligations of the qualified certification validation authority</td>
<td>70</td>
</tr>
<tr>
<td>9.6.5.2.</td>
<td>Obligations of the Qualified operational certification authority for qualified electronic signature/seal s</td>
<td>70</td>
</tr>
<tr>
<td>9.6.5.3.</td>
<td>Obligations of SEP Bulgaria regarding the public registers/ the repository</td>
<td>71</td>
</tr>
<tr>
<td>9.7.</td>
<td>Liability waiver</td>
<td>71</td>
</tr>
<tr>
<td>9.8.</td>
<td>Liability limitations</td>
<td>71</td>
</tr>
<tr>
<td>9.9.</td>
<td>Responsibility of the signature owner/creator</td>
<td>72</td>
</tr>
<tr>
<td>9.9.1.</td>
<td>Signatory/Creator's responsibility towards SEP Bulgaria</td>
<td>72</td>
</tr>
<tr>
<td>9.10.</td>
<td>Terms and termination of the Practice of provision of qualified trust services</td>
<td>72</td>
</tr>
<tr>
<td>9.10.1.</td>
<td>Terms</td>
<td>72</td>
</tr>
<tr>
<td>9.10.2.</td>
<td>Termination</td>
<td>72</td>
</tr>
<tr>
<td>9.10.3.</td>
<td>Termination effect and survival</td>
<td>72</td>
</tr>
<tr>
<td>9.11.</td>
<td>Notification and communication between the parties</td>
<td>73</td>
</tr>
<tr>
<td>9.12.</td>
<td>Amendments to the Practice of provision of qualified trust services</td>
<td>73</td>
</tr>
<tr>
<td>9.13.</td>
<td>Dispute resolution</td>
<td>73</td>
</tr>
<tr>
<td>9.15.</td>
<td>Compliance with the applicable law</td>
<td>73</td>
</tr>
<tr>
<td>9.16.</td>
<td>Other provisions</td>
<td>73</td>
</tr>
<tr>
<td>9.17.</td>
<td>Used Terms and Abbreviations</td>
<td>74</td>
</tr>
<tr>
<td>9.17.1.</td>
<td>Appendix 1: Terms and Abbreviations</td>
<td>74</td>
</tr>
<tr>
<td>9.17.2.</td>
<td>Appendix 2: Terms and Abbreviations in English</td>
<td>75</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

"System for Electronic Payments Bulgaria/SEP Bulgaria" JSC (SEP Bulgaria) 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 Lozenetz, R.D., Lozenetz, 1 Zlatovrakh str.
Contact telephone: 070018283. Internet address: http://www.eSign.bg/

The company conducts public functions under the meaning of the Law on Electronic Document and Certification Services. SEP Bulgaria is a TSP of qualified certification services. It provides to clients qualified certification services and products with high degree of security against remuneration. The TSP provides its services both on the territory of the Republic of Bulgaria and in all member-states of the European Union.

eSign is a trade mark for certification services of "System for Electronic Payments Bulgaria/SEP Bulgaria" JSC. eSign serves for confirming identity when participating in electronic exchanges, such as Web-based applications, signing electronic documents and/or contracts, e-mails, bank transactions. eSign certification services ensures your access to e-services provided by the administrative authorities of the State and local management, access to online banking, high level of security in your Internet communication, the ability to encrypt documents, which can be used to implement various internal projects.

1.1. REVIEW

"Certification Practice Statement" (Certification Practice Statement/CPS) of SEP Bulgaria JSC is a public document and is available to all interested parties. This document, as well as all documents of a public nature, are available in electronic form on the SEP Bulgaria web site. It can be changed at any time by the TSP and every new edit shall be communicated to the people concerned, by publishing it on the website of SEP Bulgaria.

The Certification Practice Statement of SEP Bulgaria describes the general requirements for provision of qualified certification services. The document contains rules and procedures which should be complied with when issuing and managing the effect of qualified certificates for electronic signatures and seals.

This document, in conjunction with a User Agreement, forms the contractual relationship between SEP Bulgaria and the respective user, within which the latter is entitled to use the qualified certification services provided by SEP Bulgaria. The practice has the nature of the General Terms and is binding for SEP Bulgaria and for the respective user - after signing the specific contract for the provision of qualified certification services. This document specifies the rights and obligations of the Public Key Infrastructure (PKI) of the TSP participants in the use of certification services provided by SEP Bulgaria.

This document contains a description of:
1. Scope and feasibility of the qualified certification services offered by SEP Bulgaria;
2. The technology for issuing and managing qualified certificates for electronic signatures and electronic seal s;
3. The form, timing and validity of the qualified certificates issued for electronic signatures and electronic seal s;
4. The necessary documents for acceptance and verification of requests for the provision of qualified certification services;
5. Documents and data stored by the TSP in the provision of Qualified Certification Services;
6. Supported algorithms for electronic signatures and electronic seal s and data protection;
7. The obligations and responsibilities of all parties involved in the issuance and management of qualified certificates for electronic signatures and electronic seal s;
8. The rules and procedures that are performed by the TSP when issuing qualified certificates for electronic signatures and electronic seal s;
9. The Rules and Procedures Performed by the TSP upon Suspension, Termination, and Resumption of Qualified Electronic Signature and Electronic Seal Certificates.

The contents and structure of this document are in compliance with the following standards and standardization documents:
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
• ETSI EN 319 410: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service TSPs;
• ETSI EN 319 411-1 v1.1.1: Policy and security requirements for Trust Service TSPs issuing certificates General requirements;
• ETSI EN 319 411-2 v2.1.1: Policy and security requirements for Trust Service TSPs issuing certificates Requirements for trust service TSPs issuing EU qualified certificates;
• 319 412-1 v1.1.1: Certificate Profiles Overview and common data structures;
• 319 412-2 v2.1.1: Certificate Profile for certificates issued to natural persons;
• 319 412-3 v1.1.1: Certificate Profiles Certificate profile for certificates issued to legal persons;
• 319 412-4 v1.1.1: Certificate Profiles Certificate profile for web site certificates issued to organisations;
• 319 412-5 v2.1.1: Certificate Profiles QCStatements;

Qualified certification services are provided in compliance with the Integrated Management System applied by SEP Bulgaria, which includes the requirements of ISO: 9001: 2009 and ISO / IEC 27001: 2013, Regulation (EC) No 910/2014 and the applicable legislation in the Republic of Bulgaria.

1.2. Name and document identification

The full name of this document is “Qualified Certification Practice Statement” by “System for Electronic Payments Bulgaria/SEP Bulgaria” JSC (SEP Bulgaria) and is publically accessible in electronic version on the website of SEP Bulgaria: http://www.eSign.bg/En/useful/documents/.

The practice is assigned a unique Object Identifier (OID) 1.3.6.1.4.1.30299.2.3

The practice fulfills the general requirements for authentication policies set forth in ETSI EN 411: NCP + for QCP-1-qscd and NCP + for QCP-n-qscd,
NCP for QCP-n and NCP for QCP-1.

In order to provide trusted parties with easy access to information on the terms and conditions for the issuance of Qualified Electronic Signatures and Electronic Seal certificates, SEP Bulgaria includes the following OIDs in the Qualified Certificates issued:

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Object Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>eSign Sep Root CA</td>
<td>1.3.6.1.4.1.30299.3</td>
</tr>
<tr>
<td>eSign Sep QES CA</td>
<td>1.3.6.1.4.1.30299.3.1</td>
</tr>
<tr>
<td>disputes</td>
<td>1.3.6.1.4.1.30299.3.1.1</td>
</tr>
<tr>
<td>eSign Sep TSA</td>
<td>1.3.6.1.4.1.30299.3.1.2</td>
</tr>
<tr>
<td>eSign QES Natural</td>
<td>1.3.6.1.4.1.30299.3.1.3</td>
</tr>
<tr>
<td>eSign QES Delegated</td>
<td>1.3.6.1.4.1.30299.3.1.4</td>
</tr>
<tr>
<td>eSign QES Seal</td>
<td>1.3.6.1.4.1.30299.3.1.5</td>
</tr>
</tbody>
</table>

The policy includes:
1. A description of the conditions that the TSP complies with and observes when issuing Qualified Certificates, as well as the applicability of these Certificates considering the security level and limitations during their use;
2. A set of specific procedures which are complied with during the process of issuing and maintaining qualified certificates, requirements during identification, conditions and necessary levels of security during creation of the electronic signature and seal and storage of the private keys;
3. Applicability and degree of trust in the applied information in the Qualified Certificates.
1.3. Participants in the infrastructure of SEP Bulgaria

The Practice is a common regulatory document for all participants in the process of providing qualified certification services by SEP Bulgaria. This document describes the process of certification service provision and the interaction between the registration authority, the certification authority (CA), users and relying parties.

The Practice is also a leading document when conducting inspections of the TSP’s activities, in particular concerning the activities of the certifying authority - eSign Sep Root CA and the Registration Authority - on the one hand, and on the other - the relations with the Signatory / Creator, entered In Qualified Electronic Signature and Electronic Print Certificates, with Trustworthy Parties.

SEP Bulgaria provides qualified certification services to all legal and natural persons, adopting the rules and procedures described in this document. The application of these rules and procedures is intended to ensure the declared levels of security in the provision of qualified certification services.

The requirements and rules described in the Practice apply to:
1. Certification Bodies;
2. Registration authorities;
3. Users;
4. Relying countries;
5. Other participants.

1.3.1. Certification authorities

SEP Bulgaria provides qualified certification services through a hierarchy of certifying authorities and a network of registering authorities by issuing and managing qualified certificates for electronic signature and electronic seal.

SEP Bulgaria as a qualified TSP, publish information on the status of qualified certificates for electronic signature and electronic seal, and make it available to relying parties for the purpose of verification of electronic signatures and seals.

1.3.1.1. Root certification authority (eSign Sep Root CA)

eSign Sep Root CA issues a basic electronic signature of itself and operational electronic signatures of other certifying bodies belonging to the hierarchy of Certification Authorities of SEP Bulgaria. This electronic signature does not include an OID (policy identifier) for the policy for issuing and managing electronic signatures. The absence of a policy identifier should be interpreted as a lack of policy constraints against which the certifying authority - eSign Sep Root CA - issues certificates.

eSign Sep Root CA is the starting point of trust for all users of Certification Services of SEP Bulgaria. This means that the certification path for each issued electronic signature and seal in the TSP’s hierarchy starts with the electronic signature of the certifying authority - eSign Sep Root CA.

1.3.1.2. Operational certification authority (eSign Sep QES CA)

eSign Sep QES CA issues user-qualified certificates in accordance with the Practice and Policy for Qualified Certification Services.

The operational certifying authority of SEP Bulgaria fulfills the following specific obligations:
1. Accepts an electronic request for Qualified Certificates or Qualified Certification Services;
2. Issue a Qualified Certificate and provide Qualified Certification Service on the basis of the requests after identification of the applicants;
3. Publishes and maintains issued Qualified Certificates in accordance with the procedures described in the SEP Bulgaria Policy and Practice;
4. Accepts and executes a request for cancellation of a Qualified Certification Service in accordance with the procedures set forth in the SEP Bulgaria Policy and Practice;
5. Issues Certificate Revocation List (CRL);
6. Publishes issued CRL (CRL);
7. Stores the records (logs) on the process of issuing electronic signatures / seals to be audited;
8. Other activities and services related to the activities of SEP Bulgaria.
SEP Bulgaria reserves the right to expand or change its infrastructure with another hierarchy by the 1.3.1.2. Operational Certification Authority.

### 1.3.2. Registration authority

Registration authorities (RA) are part of SEP Bulgaria's infrastructure as a qualified TSP. RAs represent SEP Bulgaria in contact with users and operate according to the rights delegated to them by the certifying authority in terms of identity verification, respectively the identity of the Signatory / Creator and the registration of requests for the issue or management of qualified certificates for electronic signature / seal.

The Supplier issues qualified electronic signature / seal certificates after verification of the identity, respectively the identity of the applicants for qualified certification services. In this regard, SEP Bulgaria provides its services through a network of Registration Authorities, which have the following functions:

1. Accept, verify, approve or reject requests for qualified certificates for electronic signature / seal;
2. Accept, verify, approve or reject requests for the management of Qualified Electronic Signature / Seal Certificates;
3. Participate in all stages of identification of applicants, Signatory and Creator of Qualified Certification Services and identity verification, respectively of their identity;
4. Conclude contracts for the provision of Qualified Certificates (on issuance, maintenance and management of certificates) with the Signatory on behalf of SEP Bulgaria;
5. Perform other activities related to the provision of Qualified Certification Services described in TSP's policies, practices and procedures.

The registration authorities act on behalf of SEP Bulgaria, in accordance with its policies, practices and procedures. RA accepts, verifies and approves or rejects requests for issuance, modification, renewal, suspension / resumption and termination of qualified certificates for electronic signatures / seals.

When checking the identity, or the identity of the Signatory / Creator, the operators of the RAs directly or indirectly identify the persons to whom qualified certificates will be issued using identification methods giving the same degree of security as for physical identification.

SEP Bulgaria concludes a contract with the RA (in the cases when the specific RA is a unit outside the legal organization of SEP Bulgaria), by virtue of which the activities described above are carried out, the Practice and the Policies of the TSP are part of this contract.

Any person may act as the TSP's RAs after having stated this and fulfilling the conditions arising from SEP Bulgaria's Regulatory Documents. The list of RAs that are authorized by SEP Bulgaria is public and is available on the SEP Bulgaria website.

### 1.3.3. Users

Any natural or legal person that has a written contract with SEP Bulgaria is a user of a qualified certification service provided by SEP Bulgaria.

Where practicable, the certification services provided and the products used to provide these services are also available to disabled persons.

#### 1.3.3.1. Signature

The signatory is a natural person who creates an electronic signature.

A Signatory may also be a natural person who is authorized by a legal person to sign electronic statements in accordance with the authority granted to him on behalf of the legal person. The Qualified Certificate also indicates the person who represents the Accountant.

The signatory of the electronic signature can assign the servicing of the tokens for creating qualified electronic signatures to a third party, under the condition that appropriate mechanisms and procedures were implemented, which guarantee that the signatory has sole control on using the data, related to creation of their electronic signature, and that when using the token the conditions regarding the qualified electronic signature were executed.

Only the signatory of the qualified certificate has the right to access the private key for signing electronic statements, through which they create an elaborate or qualified electronic signature.
1.3.3.2. Creator of the seal

The creator of a seal is a legal entity, which creates an electronic signature. The creator can seal electronic objects, regardless of their nature (software, pictures, music, movies, books, architectural projects, database, deSign, etc.), with which they manifest that they are the legitimate source of this electronic object and that the object is with intact integrity. The electronic seal does not guarantee rights on the electronic object (copyright or other). The creator is stipulated in the issued qualified certificate for electronic seal as Creator. Only the Creator in their capacity as User of the qualified certificate, is entitled to access to the private key for sealing electronic statements, through which they create an elaborate or qualified electronic seal.

1.3.3.3. Relying parties

Relying party means a natural person or legal entity who relies on the certification service. In essence, the Relying Party receives documents signed with an electronic signature / seal by taking action, trusting in the qualified certificate for the relevant electronic signature / seal. The trustee is responsible for verifying the validity of the Qualified Electronic Signature / Seal Certificate.

Relying parties shall assess whether the type of qualified electronic signature / seal certificate and the guarantees associated with it are sufficient for the purposes for which it is used. The relying parties should have knowledge and skills regarding the use of the qualified certificate and to trust the certified circumstances in them, considering only the applicable Policy, especially regarding the security level during inspection of the identity of the Signatories and the identity of the Creators of these qualified certificates, as well as regarding the use limitations included in the certificate.

The relying parties have permanent access to the registers of SEP Bulgaria, for inspection of the validity of the qualified certificates, for establishing the electronic identity of the Signatories/Creators, or of other circumstances and data, included in the certificates or these registers. The relying parties established outside the territory of the Republic of Bulgaria can rely on reliable, secure, easy and comfortable qualified validation of the qualified electronic signatures and electronic seals in an automated manner, the certificates for which were issued by SEP Bulgaria.

1.3.4. Other participants

1.3.4.1. Validation authority

The certified certificate in the infrastructure of SEP Bulgaria, used to signing the signature / seal validation request is eSign OCSP. Used to validate customized signatures / seal s and issued by an operational certification authority (eSign Sep QES CA).

The Qualified Validation Service for Electronic Signatures and Electronic Seals is provided by SEP Bulgaria as a Qualified Certification Services TSP. In the process of validation of the qualified electronic signature / seal eSign OCSP of the SEP Bulgaria confirms the validity of the qualified electronic signature / seal, provided that:
1. The signature certificate at the time of signing / seal ing was a qualified electronic signature / seal certificate that complies with the requirements of Regulation (EU) 910/2014;
2. The Qualified Certificate issued by the TSP was valid at the time of signing / seal ing;
3. The signature / seal validation data corresponds to the data provided by the relying party;
4. The unique set of data representing the Signatory / Creator of the electronic signature / seal in the certificate is duly submitted to the relying party;
5. If an alias was used at the time of signing / seal ing, this is clearly indicated to the relying party;
6. The electronic signature / seal is created by an electronic signature / print creation device;
7. The integrity of the signed / seal ed data is not jeopardized;
8. The requirements of this document have been fulfilled at the time of signing / seal ing.
The validated SEP Bulgaria's Qualified Electronic Signature / Printing System provides the relying party with the correct outcome of the validation process and allows it to detect any security issues.

When each relying party accepts a qualified certificate, it can request real-time inspection of the status of the certificates through an OCSP server (On-line Certificate Status Protocol).

The real-time inspection of the status of a qualified certificate is not an obligatory function for the relying parties, but the TSP recommends using this service. In order to achieve greater security when using electronic signatures/seals, it is recommended to integrate the service in the process of creation or approving electronically signed/seal documents.

### 1.4. Qualified Certificates usage

Qualified Electronic Signature / Seal Certificate means an electronic signature / seal certificate issued by a qualified certification service TSP and meeting the requirements set out in Regulation (EU) 910/2014.

Qualified certificates allow individuals to prove their identity when participating in electronic transactions. They can be used when it is necessary to protect an exchange of electronic information.

Qualified Public Key Certificate is signed / seal ed by the TSP Electronic Document containing certain requisites certifying the relationship between the Signatory / Creator and his public key corresponding to the private key with which the Signatory / Creator has created the electronic signature / seal and serves to verify the Signature / seal in electronic documents and objects.

Qualified certificates issued by SEP Bulgaria can be used to process secure information (including authentication) of a high level of trust. Users must be aware of the requirements for issuing Qualified Certificates and should specify the application scope before the Registration Authority. When incorrect information is provided by users, they are held accountable.

#### 1.4.1. Types of Qualified certificates and recommended range of applicability

User Qualified Certificates issued by eSign Sep QES CA in the SEP Bulgaria infrastructure are:

1. **eSign QES Natural** - Issued to an individual (Signatory). It has the character of a qualified certificate for qualified electronic signature. It can be used to identify and establish identity when accessing Internet applications, secure communications and electronically signing documents of any type.

2. **eSign QES Delegated**
   a) Issued to a legal entity, but with a Signatory, an individual related to an organization, acting as its legal or contractual agent. It has the character of a qualified certificate for qualified electronic signature. It can be used to identify and establish identity when accessing Internet applications, secure communications and electronically signing documents of any type. Where a qualified electronic seal is required for a transaction by a legal person, the qualified electronic signature of the authorized representative of the legal entity should be treated as equivalent.
   b) Issued to individuals (Signatory) and used to validate the consent / identity and professional membership of a person performing a personal or a freelance job in participating in electronic exchange as web-based applications, Signing electronic documents and / or contracts, banking transactions and making statements within the meaning of EDESA.

3. **eSign QES Seal** - Issued to a legal entity (Creator). It has the character of a sophisticated electronic seal, which is created by a device for creating a qualified electronic seal and is based on a qualified certificate for electronic printing.

Qualified certificates for individuals and legal entities issued in accordance with this document may be used within a range of applicability corresponding to the intended purpose approved by SEP Bulgaria.

Qualified certificates for individuals and legal entities are used to establish personal and professional e-entity in applications that require the highest level of security - web-based applications for e-commerce, electronic signing of documents, electronic signing of contracts, bank transactions, keeping Correspondence and statements made by and to state and local government bodies within the meaning of Regulation (EU) No 910/2014 and national legislation.

#### 1.4.2. Usage

Qualified Certificates of SEP Bulgaria cannot be used in a manner inconsistent with their stated purpose.

Certificates issued and provided to SEP Bulgaria users may be used to:

1. Establishing the identity and identity of a natural person or an individual related to an organization in its capacity as legal or contractual agent;
2. Proof that an electronic document or other information object has been issued by a legal person, ensuring the reliable origin and integrity of the document. The information object, by means of an electronic seal, accompanied by a qualified electronic seal certificate issued by SEP Bulgaria;
3. Signing, encryption and decryption of electronic data such as electronic documents, databases, information objects, e-mail, etc.;
4. Checking signed data, such as documents, recommended e-mail, and others;
5. Encryption and decryption of data and exchange of keys used for encryption;
6. Other.
Information on the applications that can use the qualified certificates issued by SEP Bulgaria is published on the TSP's website on the Internet.

1.5. Practice management in Qualified certificate service providing

Each version of the Qualified Certification Service Practice is effective (current status) until the new version approval and publication. Each new version is developed by SEP Bulgaria employees and, after approval by the Executive Director of the TSP, is published.
Any change to the Practice shall take effect within 7 (seven) days of its publication on the SEP Bulgaria website. Changes in the Practice are binding on all users who, at the time the changes came into effect, use Qualified Certification Services provided by SEP Bulgaria and do not declare their termination in the manner provided for in this document.
Each user has the right to request the termination of the qualified certification services provided by SEP Bulgaria with an explicit written notice within 7 (seven) days of the entry into force of the changes in the Practice. The latter shall not apply where the changes result from the applicable legislation, by an act of a competent authority or provide for more favorable consumer clauses.
Users are obliged to comply only with the valid version of the Practice at the time of using the services of SEP Bulgaria.

2. Responsibility for publication and repository

2.1. Repository

The SEP Bulgaria Public Register is a repository where current and previous versions of electronic documents are located. It contains PKI / Public Key Infrastructure Certificates and User Authentication Certificates. The repository is managed and controlled by the TSP. For this reason, SEP Bulgaria is committed to:
1. Ensure that all certificates published in the repository belong to the users mentioned in the certificates or to the users who are authorized representatives;
2. Ensure that the certificates of certification bodies are published;
3. Publishes the current "Qualified certification services policy", "Practice in providing qualified certification services", forms of documents for users and agreements between the parties;
4. Provides access to information about the status of certificates by publishing the CRL, OCSP;
5. Ensure permanent access to information in the repository for certifying authorities, registrants, users and relying parties;
6. Publish other information promptly and in accordance with the deadlines specified in this document;
7. Provides safe and controlled access to information in the repository.
All users have unlimited access to all the information in the repository. Relying parties have restrictions, but they are common and only concerning the user certificates.

2.2. Information, published by SEP Bulgaria

The public register is available at: https://www.eSign.bg/bg/usages/public-registry/.
SEP Bulgaria, as a qualified TSP, leads a public electronic register in which it publishes the certificates of the certifying authorities from its hierarchy, the qualified certificates for electronic signature and sealing and the information required by the parties using the qualified certification services.
The information published by SEP Bulgaria consists of the following documents:
1. List of qualified certificates for electronic signature / seal from its hierarchy;
2. List of qualified certificates for electronic signature / seal issued;
3. Certificate Revocation List (CRL);
4. Previous and up-to-date versions of the documents regulating the TSP's activity;
5. Practice and Policies;
6. Instructions describing how to use electronic signature / seal;
7. Tariff for the services provided by SEP Bulgaria;
8. Other information that can be modified and modified in real time;
9. Reports of audits carried out by an authorized institution;
10. Additional information, such as messages and notifications.

2.3. Frequency of publication

SEP Bulgaria maintains the information in the public register by updating it with the following periodicity:
1. Policy on Providing Qualified Certification Services and Practice in Providing Qualified Certification Services is subject to immediate publication upon each update;
2. Operating certificates - whenever new certificates are issued;
3. An update of the Public Register of the issued certificates shall be carried out automatically and immediately after the publication of each newly issued valid certificate;
4. An update of the current CRL is automatically made no more than 3 (three) hours or immediately after a valid certificate has been suspended / resumed. In all CRLs, SEP Bulgaria specifies the time for the next edition. The effective period of validity of the published updated list is specified in it unless an update is made;
5. Reports of audits carried out by an Authorized Authority - whenever SEP Bulgaria receives them;
6. Additional information - for each occurrence

2.4. Access to publications

SEP Bulgaria offers directory services for the information stored in the repository (electronic registry), providing HTTP/HTTPS-based access.
All storage information published by SEP Bulgaria is publicly available. Access to this information is not limited to SEP Bulgaria, except at the request of the Signatory / Creator and only in respect of a validly issued Qualified Certificate.
The information published in SEP Bulgaria's repository is available on a permanent basis (24/7/365), except in the event of events beyond the control of the TSP.
The TSP shall provide free access to all the basic and operational certificates of its active Certification Authorities as well as free access to all non-active ones for a period of at least 10 (ten) years after these certificates expire.
SEP Bulgaria has taken measures, logical and physical mechanisms to protect against unauthorized addition, removal and modification of the information posted in the repository. Data entry is only performed by duly empowered employees.

3. Identity identification and authentication

This part of the Practice presents the general rules for the verification of the identity of the users applied by SEP Bulgaria for the issue of qualified certificates. The rules are based on certain types of information that is included in the certificates. This ensures that the information included is accurate and reliable at the time of issuing a qualified certificate. Data verification is mandatory at the registration stage of the user and at SEP Bulgaria's request for all qualified certification services.
The TSP, through its Registration Authority:
1. Accepts requests for issuance of qualified certificates;
2. Performs a check to establish the identity of the Signatory, respectively the identity of the Creator and specific data about them with eligible means;
3. Approves after successful verification or rejects registered requests;
4. Sends a request to the certifying authority to issue the requested certificate.
The Registration Authority collects and receives the necessary identification information and verification of the Signatory/Creator's identity.
The identification and authentication of the Signatory / Creator after registration and prior to the issuance of a qualified certificate requires his / her presence or presence in person by an authorized representative of the person submitting a request to the Registration Authority.
The Supplier ensures that physical and legal persons are properly identified, that their identity is verified and that requests for qualified certificates issuance are fully, accurately duly verified and approved, including the full name/title and legal status of the natural person/legal person concerned and the relationship between the verified data and the natural/legal person.

3.1. Names

The qualified certificates have a format in conformity to X.509 standard. The Registration Authorities shall verify and ensure that the names in the request for certificate issuance comply with the X.509 standard.

The “Subject” field on the certificate contains the Signatory/Creator’s Author’s name. The name and other distinguishing signs of the Signatory/Creator’s in the corresponding fields for each type of certificate are in accordance with DN (Distinguished Name) formed according to X.500 and X.520 standard.

In order to ensure easy electronic communication with the Signatory / Creator, SEP Bulgaria includes in the content of the certificate an electronic address in accordance with RFC822.

The names of the directories where the Qualified Certificates, the Discontinued and Discontinued Certificates List, Practice, and Qualified Certification Services Policies are in compliance with RFC1738 and the LDAP Protocol Name Scheme - RFC 1778.

SEP Bulgaria operative certificates contain in the “Subject” field and the “Issuer” field a DN attribute that forms its unique name. A detailed specification of the certificates issued by SEP Bulgaria is contained in the next sections of this document.

3.1.1. Type of names

The name requirements in the issued certificates are as specified in Recommendation ITU-T X.509 or IETF RFC 5280 and ETSI EN 319 412. The names may be in accordance with the Domain Name Service (DNS) described in RFC 2247. This way allows subscribers to use two types of names: DN and DNS at the same time.

In order to provide an easier way for electronic communication with the user, an alternative name (nickname) may also be used. The TSP may issue a qualified certificate using a “nickname” to name the user only after the necessary identity information has been gathered for the same and it has been successfully identified. The name may also contain the user e-mail address which is to be in conformity to recommendation RFC 822.

3.1.2. Necessity for distinguished names

Qualified Certificates issued by SEP Bulgaria contain unique names with a generally understandable semantics allowing the identification of the Distributor Name and the Subject Distinguished Name.

The names included in the Distinguished Name (DN) of the user have their meaning in Bulgarian or in another foreign language. The DN structure is approved by the registrant and depends on the type of certificate and the user. DN consists of the following areas (the descriptions are in accordance with RFC 3280 and X.520):

1. field C - BG,
2. field ST - area,
3. field L - city,
4. field CU - name of the individual or organization,
5. field O - name of the institution that the person represents,
6. field OU - the name of the organizational unit,
7. field E - email address of the subscriber,
Field D - additional description of the person.

The DN must be verified by an operator of the registration authority and approved by the certifying authority.

3.1.3. User anonymity

SEP Bulgaria does not publish certificates and other credentials to ensure user data anonymity (e.g., CIN).
3.1.4. Rules for different names interpretation

The interpretations of the fields provided in the certificates issued by SEP Bulgaria are in accordance with the user profile certificates described in Part 7 of this document.

The TSP includes in the Qualified User Certificates the Electronic Identification Information of the Signatory / Creator that has been successfully verified and confirmed by the Registration Authority on the basis of the Identity and Identity of the Owner / Creator.

In all Certificates where the Signatory is entered, the Common Name (CN) field contains the name of the individual with whom it is commonly indicated in his / her activity.

In the professional certificate, the unique name attribute (DN) also contains information about the identity of the person that the Account Signatory represents.

3.1.5. Uniqueness of the names

To ensure the uniqueness of the issued Qualified Certificates, SEP Bulgaria assigns a unique sixteen-digit serial number ("SerialNumber") to the TSP's domain for each issued certificate. The combination of "Issuer" and "SerialNumber" fields ensures the uniqueness of the issued certificate in the public domain.

The "Subject" field on the certificate is formed by Signatory / Creator information provided online or on paper by the person requesting or by an authorized representative when registering an initial application for a certificate and which is verified by the registrant based on Documents, video identification and checks in primary government registers.

The vendor guarantees the uniqueness of the "DN" of the Signatory / Creator in the SEP Bulgaria domain, by adding a requisite that guarantees such uniqueness.

Signatory / Creator with a unique "DN" in the SEP Bulgaria domain may have more than one issued valid Qualified Certificates.

3.1.6. Recognition, authentication and role of the trademark. Dispute Resolution Procedure

Consumers are not entitled to request the issuance of qualified certificates using names that are subject to copyright or related rights of third parties, or to violate any other proprietary or non-proprietary rights. The holders of such rights shall certify this right by submitting the relevant due document to the RA in the process of submitting a request for issuance of the respective qualified certificate. SEP Bulgaria is not responsible when the names used in the issued certificates violate foreign rights on a trade name, trademark, domains, copyrights, etc. Users are liable to the TSP for any damage suffered by the latter in connection with breaches of the requirements of this document.

SEP Bulgaria checks whether the user has the right to use the name given in the registration request but does not play the role of arbitrator to resolve disputes.

In the event of disputes regarding the provision of qualified certification services by SEP Bulgaria, the interested parties file complaints in writing to the CEO of SEP Bulgaria at the following address:

* System for Electronic Payments Bulgaria/SEP Bulgaria* JSC (SEP Bulgaria)
1, Zlatovrah Str
1164, Sofia

Complaints from users of SEP Bulgaria are also submitted electronically to eSign@sep.bg.

For this purpose, the consumer should duly sign his complaint with a valid electronic signature / seal. Only complaints duly signed shall be deemed to have been received.

Within 30 (thirty) days of receipt, the complaint shall be considered and the complainant shall be sent a written response from the Executive Director.

3.2. Initial registration

The user's initial registration is made when he first applies for registration in SEP Bulgaria.

Registration includes a number of procedures that allow the identification of data to be collected before a qualified user certificate is issued. Confirmation of such data requires personal contact (face to face) with a representative of the Registration Authority, notary or other authorized person confirming his / her identity / identity.

The registration for requesting qualified certification services can also be found on the SEP Bulgaria website.
3.2.1. PERSONAL KEY POSSESSION VERIFICATION

If a person controls a private key and wants a qualified certificate, the TSP must make sure that the public key provided for authentication matches the private key held by the person. Checking to hold a private key is done through a procedure to prove possession of a private key. The procedure confirms that the Public Key of the Signatory/Creator matches the private key and is under his / her exclusive control.

For issuance or continuation of a qualified certificate, SEP Bulgaria needs to receive an electronic request in PKCS #10 format. The specification of this certificate request format requires the request to be signed by the Signatory/Creator holding the private key.

SEP Bulgaria checks the validity of the electronic signature / seal accompanying the request. Establishing the validity of the electronic signature / seal provided is sufficient reason to believe that the Signatory/Creator has submitted an electronic request and has the private key that is technically fit and corresponds to the public key contained in the request.

The TSP may provide the Signatory/Creator service locally or by remotely generating the key pair.

The pair of keys corresponding to the Qualified Certificate issued by the TSP must be generated in an electronic signature / print creation device.

The control of access to the private key is kept only by the Signatory/Creator.

3.2.2. Establishing the identity of a legal entity

The establishment of the identity of a Bulgarian legal person (Author) shall be carried out by a representative of the Registration Authority, by verification at the relevant registers by given UIC, respectively BULSTAT under the procedure of the Electronic Government Act. The following documents shall be submitted for Bulgarian legal entities who are not traders, as well as for foreign legal persons for which cannot be perform automated inspection:

1. Identity document of the applicant (original and certified copy, with the copy remaining with RA);
2. Document for judicial registration of the legal person (original and copy certified by the legal entity, the copy remaining with the RA) - insofar as it is applicable in view of the type of the legal person;
3. Document for registration by identification number (BULSTAT / UIC) (original and copy certified by the legal entity, with the copy remaining with PO) - insofar as it is applicable in view of the type of the legal person;
4. A certificate on the current status of the legal person, issued within one month from the date of filing the application for certification services (original and copy certified by the legal entity, with the copy remaining with the RA);
6. Notarized power of attorney of the applicant for certification services by the legal entity.

Where a legal person is his authorized representative, the authentication of the information contained in the submitted documents shall be effected by:

1. "true to the original" authentication and handwritten signature on the documents before an employee of the registering authority in the case of personal transmission of the documents;
2. Notary certification of the documents, which are sent by mail to the registering body;
3. Signing of the attached electronic formats of the documents with a valid certificate for qualified electronic signature / seal;

Authentication of a legal entity has two purposes. The first objective is to prove that the legal entity exists during the review of the application. The second objective is to prove that the representative who applied for a certificate has been authorized by the legal person to represent it.

Employer of the registering body can check the registration through all accessible public services in accordance with the Bulgarian legislation.

If the identity verification is successful, a RA operator shall process the data of the legal entity and the related certification service activities:

1. Offers a contract for qualified certification services signed on behalf of the TSP and keeps all documents submitted to the contract;
2. Confirms the request for issuance and sends an electronic application for issuance of a certificate to the Operational Certification Body of the TSP;
3. Record the issued QSCD / Secure Signature Creation Device certificate and transmit it to the Holder or the authorized person.

After verification of the data provided and a contract for a qualified certification service, the person who submitted the request is included as a user of the services of SEP Bulgaria.
3.2.3. VERIFICATION OF THE IDENTITY OF A PHYSICAL PERSON IN ASSOCIATION WITH A LEGAL PERSON

The registration authority requires the submission of appropriate documents that clearly and without any doubt confirm the identity of the legal entity specified in the relevant request for the issuance of a qualified certificate and the identity of the natural person authorized to represent the legal entity. The certificate will be entered as the Holder the individual.

Documents include:
1. Name of the Account Holder;
2. Identity card of the Account Holder - identity card, international passport or other identity document;
3. National identification number, if any;
4. Contact details - mobile phone, e-mail and address;
5. A certificate on the current status of the legal person, issued within one month from the date of filing the application for certification services (original and copy certified by the legal entity, with the copy remaining with the RA);
6. A document on the template of the TSP to explicitly authorize the Holder with representative authority from the legal entity, if the reason for the representative authority does not follow from the law (original remaining with the RA);
7. A notary certified power of attorney of the applicant for certification services, in the event that the legal person authorizes a representative other than the Holder, to claim qualified certification services.
9. Document for judicial registration of the legal entity (original and copy certified by the legal entity, with the copy remaining with the RA) - insofar as it is applicable in view of the type of the legal person;
10. Document for registration by identification number (BULSTAT / UIC) (original and legalized by the legal entity, the copy shall remain with the RA) - insofar as it is applicable in view of the type of the legal entity.

The RA can verify the necessary data for identification of the legal entity on its own, using public registers, and this right does not remove the obligation of the persons to submit the above mentioned documents.

If the identity verification is successful, a RA operator shall process the data of the legal entity and the related certification service activities:

After successful verification of the Holder's identity, the authorized operator in the Registration Authority:
1. Offers a contract for qualified certification services signed on behalf of the TSP and keeps all documents submitted to the contract;
2. Confirms the request for issuance of a qualified certificate and sends an electronic application for issuance of a certificate to the Operational Certification Body of the TSP;
3. Record the issued certificate of a QSCD / Secure Signature Creation Device and transmit it to the holder or the authorized person.

After verification of the data provided and a contract for a qualified certification service, the person submitting a request is included as a user of the services of SEP Bulgaria.

3.2.4. ESTABLISHING THE IDENTITY OF A NATURAL ENTITY

The identification and verification of the identity of the natural person (Signatory) is carried out by a representative of the Registration Authority. Identification can also be done automated by remote verification.

An identity document is required to be produced for identifying and verifying the identity of the natural person.

In order to identify and verify the identity of an individual, he / she is required to produce an identity document.

The natural person who requests the issuance or management of a qualified certificate shall complete and transmit to SEP Bulgaria documents in accordance with the policy of the TSP for the issue and management of qualified certificates. Facial data can include mobile phone number, email address, home address, and more. The physical person confirms the authenticity of the data by:
1. A handwritten signature on the documents before an employee of the registering authority in the case of personal transmission of the documents;
2. Notary certification of the documents, which are sent by mail to the registering body;

SEP Bulgaria verifies the authenticity of the information in the completed documents, with all legally permitted funds in the respective public registers.

The list of required documents for an individual for issuing and managing a qualified certificate is made up of:
1. Identity card of the holder (original and copy certified by the holder, the copy remaining with the RA);
2. A power of attorney notarized on a template of the Certified TSP's Certified Service TSP, in case the Holder authorizes his / her representative to request certification services;

3. Extensive proof proving the affiliation of the person identified as a legal entity to the relevant professional / branch organization (where the certification services requested are for the use of a qualified certificate of the SEP Qualified Profession type (original and copy certified by the holder, the copy remaining In RA).

After successful verification of the identity of the holder, the authorized operator in the registration authority:
1. Proposes a contract for qualified certification services signed on behalf of the TSP and keeps all documents submitted to the contract;
2. Confirms the request for issuance of a qualified certificate and sends an electronic application for issuance of a certificate to the Operational Certification Body of the TSP;
3. Record the issued certificate of a QSCD / Secure Signature Creation Device and transmit it to the holder or the authorized person.

The RA can verify the necessary identification data of the holder himself using public registers, and this right does not remove the obligation of the persons to provide the above mentioned documents.

### 3.2.5. Initial Identification and Authentication of the Person for an Electronic Registration

Registration includes the provision of data to the applicant for qualified certification services in an electronic manner that allow SEP Bulgaria to identify it. The registration data includes:

1. Three names and / or alias;
2. Personal data for the applicant;
3. Valid email address to be used later for communication with the applicant.

The information provided during the initial registration is stored by SEP Bulgaria and can be used in accepting requests for qualified certification services from the TSP.

Upon validation of the collected data, the person may proceed to the next steps of requesting qualified certification services. Together with the request, the user should electronically send the necessary documents to establish the Holder / Creator's identity / identity, as well as the other required documents mentioned above.

In the event that the registered applicant does not hold a validly qualified certificate issued by the TSP, the submission of the request and the supporting documents in this case shall be made to the registering body in the order provided in the document. If the verification is successful, the operator of the registrant proceeds to the processing of the data and related activities for the provision of qualified certification services.

After successful verification of the person's identity, the authorized operator in the Registration Authority:
1. Offers a contract for qualified certification services signed on behalf of the TSP and keeps all documents submitted to the contract;
2. Confirms the application for the issuance of a qualified certificate and sends an electronic application for issuance of a certificate to the Operational Certification Body of the TSP;
3. Record the issued certificate of an Electronic Signature Creation Device (QSCD / Secure Signature Creation Device) and transmit it to the Holder or the Authorized Person.

After verification of the data provided and a contract for a qualified certification service, the person who submitted the request is included as a user of the services of SEP Bulgaria.

### 3.2.6. Special Attributes

The TSP may include special attributes associated with the Signatory/Creator in the issued certificate if the Qualified Certificate is issued for a specific policy purpose.

This information is subject to verification by the registrant.

### 3.2.7. Unconfirmed Information

Any information beyond the compulsory verified is unconfirmed information. The TSP may include in the issued certificate and unconfirmed information for the Signatory/Creator that is not subject to verification by the Registration Authority. In this case, SEP Bulgaria shall bear no responsibility for this information.
Unverified information may be, but is not limited to:
• Email address for correspondence;
• Identifiers specific to the Holder / Creator.
Unconfirmed official information is included in the content of the certificate on the basis of a declaration by the requesting Holder / Creator.

3.2.8. Verification by the certifying authority

After successful identification and verification by the registrant of the conditions for the issue or management of a qualified certificate, a representative of the registering authority shall confirm the data to the certifying authority. The Certifying Authority shall immediately publish the issued certificate in the Public Register / Repository of the issued Certificates or, respectively, in the CRL.
In SEP Bulgaria, only the operating certifying authority that issued a qualified electronic signature / seal certificate may terminate this certificate.

3.2.9. CRITERIA OF CONFORMITY

Qualified certificates issued by SEP Bulgaria meet the requirements of Regulation (EU) 910/2014 and are recognized in the European Union. Given the cross-border interoperability of the qualified electronic signatures and seals formats introduced by Regulation (EC) 910/2014, the qualified certificates do not exceed the mandatory requirements laid down in this Regulation. At national level Qualified Certificates include specific data, such as Personal Identification Number and other specific data at the request of a user, but SEP Bulgaria ensures that they do not hinder cross-border interoperability and the recognition of Qualified Certificates and Electronic Signatures / Seals in the European Community.

3.3. IDENTIFICATION AND IDENTITY VERIFICATION FOR A QUALIFIED CERTIFICATE RENEWAL

Renewal of a validly qualified certificate is the issue of a new certificate requested before the expiry of the validity of the valid certificate. Renewed only valid Qualified Certificates that have not been terminated and the information contained therein has not been changed.
SEP Bulgaria may renew a valid Qualified Certificate which has not been terminated within its term of validity in two ways:
1. Keeping the generated pair of keys for the current certificate (Renewal);
2. Generating a new key pair (Re-key).
The Qualified Certificate is renewed for the same asymmetric Renewal of the current Holder / Creator's Certificate if the Signatory/Creator information in the renewal certificate is identical to that in the current Certificate. Only the validity period in the renewed certificate becomes different from the current one.
SEP Bulgaria allows repeated renewal of the qualified certificate by retaining the current Renewal Key, but recommends that this practice be limited in order to reduce the risk of compromising the private key.

SEP Bulgaria will renew a current Owner / Creator's Certificate with a new Re-key only if he / she submits a request to the registrant and declares that there has been no change in the certified information in the current Qualified Certificate. The renewed certificate has a different public key and a new validity period, and the verified Signatory/Creator information is retained.
Upon renewal, the current Qualified Certificate shall not be terminated and shall remain valid within its period of validity. For authentication and authentication of the Signatory/Creator of the Qualified Certificate, which is renewed, their personal presence in the TSP's registration body is not required.
In the event of changes to the Signatory/Creator of Qualified Certificate information, the current certificate is not renewed. The TSP issues a new Qualified Certificate following initial authentication and authentication and terminates the current Qualified Certificate immediately.
The renewal of a certificate of a certifying authority of SEP Bulgaria is not allowed in cases requiring replacement of the certificate. The practice always recommends that a new certificate be issued to the certifying authority.

The TSP may renew a Qualified Electronic Signature / Seal Certificate within 30 days prior to its expiration and up to 30 days after expiration of its validity by Renewal and Re-key. For this purpose, it is required that there be no change to the "DN" of the certificate and that it has been issued to an electronic signature creation device (SSCD). Where a certificate is issued after the expiration of its validity period, the renewal request To be submitted to the registration authority.

On receipt of a request for renewal of a qualified certificate, the Contractor shall, through the appropriate registrant:
1. Carries out the relevant identification / authentication of the person;
2. The registration authority handles the request in accordance with the requirements of this document;
3. Concludes a contract for qualified certification services (if the relevant contract is tied to a specific certificate);
4. Issue an invoice for a paid price;
5. An operator of the registering authority shall submit an electronic application to the certification authority’s server for the issuance of a qualified certificate;
6. If the procedure is successful, the server generates the certificate and signs it using a hardware cryptomodule. The new certificate has a new serial number and term of validity. The generated certificate is stored in the certification authority’s database and is published in the public electronic register (repository);
7. The certifying authority prepares a response containing the generated renewed certificate and submits it to the customer through the registration authority or electronically.

The Signatory/Creator may object if the issued renewal certificate issued contains errors or incompleteness within 3 (three) days of its publication in the public electronic register of the TSP. In this case, the TSP issues a new certificate at no extra cost, except in cases where the errors are due to the provision of untrue data by the Signatory/Creator or the Authorized Person. In the event that the Signatory/Creator or Authorized Person does not object within the above mentioned time limit, it is considered that the content of the issued renewal certificate was accepted.

### 3.4. IDENTIFICATION AND IDENTITY VERIFICATION FOR A QUALIFIED CERTIFICATE SUSPENSION

Suspension of validity of qualified certificates is established operational practice of SEP Bulgaria and differs from termination in that it leads to temporary loss of validity of a certificate. For reasons of legal certainty, the vendor always makes clear the status of the certificate's suspension. SEP Bulgaria assumes responsibility to clearly mark the status of the certificate and, in the event that its validity is suspended, the exact suspension period.

SEP Bulgaria is obliged, through the registration body, to suspend the validity of a valid certificate upon request for suspension, but not for more than 24 hours.

The TSP, through the Registration Authority, does not authenticate and certify the Signatory/Creator and immediately stops the operation of the certificate.

The TSP, through the registration authority, automatically resumes the suspended certificate after the expiration of the 24-hour period.

The time in the systems associated with stopping and terminating certificates is synchronized to UTC at least once every 24 hours.

Suspending a qualified certificate is to temporarily include the certificate on the CRL. For the time of suspension of the certificate, the latter is considered invalid and all electronic signatures / seals associated with it are invalid.

Suspension of a qualified certificate is made in the following cases:
1. Upon request to the TSP by the Signatory/Creator or a person authorized by him / her, without the TSP being obliged to ascertain his / her identity or representative authority;
2. At the request of a person for whom it is apparent from the circumstances that he or she may be aware of security breaches of the private key, such as a representative, partner, employee, family member, etc.;
3. At the request of the supervisory authority.

On receipt of a request for suspension of a Qualified Certificate, the TSP processes it in the following order:
1. A representative of the registering authority processes the request in the manner provided for in this document;
2. A representative of the registrant shall submit an electronic application to the certifying authority to suspend the certificate by the procedure provided for in this document;
3. The certifying authority shall verify the validity of the certificate whose suspension is requested and the correlation between the data in the request and the particulars entered in the certificate;
4. The Certifying Authority suspends the certificate by including it on the CRL with the reason for termination;
5. The Certifying Authority shall immediately notify the Owner or the authorized person of the suspension of the validity of the certificate.
3.5. Identification and Identity Verification for a Qualified Certificate Termination

When SEP Bulgaria, through the registrant terminates the validity of a qualified certificate, the TSP records this in its own database with certificates and publishes the revoked status of the certificate in a timely manner, but in any case within 24 hours of receipt of the request. Cancellation becomes effective as soon as it is published on the CRL.

The request for termination is filed as follows:
1. On behalf of the Signatory/Creator or a person authorized to do so;
2. At the request of bodies specified in the act.

The information contained in the request for termination is as follows:
1. Information about the suspended certificate;
2. The full name of the Holder;
3. The full name of the Creator;
4. Full name of the person authorized to represent the Signatory/Creator upon requesting the service;
5. Signatory/Creator IDs: PIN, FDI, UIC, BULSTAT;
6. Permanent address / registered office and address of management of the legal person;
7. Permanent / business address of the Titleholder;
8. Reason for termination.

On receipt of a request for termination of a Qualified Certificate, the TSP processes it in the following order:
1. The operator of the registering body carries out identification / authentication of the Signatory/Creator or the authorized person;
2. An operator of the registering authority processes the request in accordance with the procedure provided for in this document;
3. The Certifying Authority processes the request in the manner provided for in this document;
4. The Certifying Authority publishes information on the termination of the CRL certificate together with information on the reason for termination;
5. The certifying authority sends an acknowledgment of termination of the certificate to the applicant for the termination request;
6. The Certifying Authority shall immediately notify the Signatory/Creator or the authorized representative of the legal entity to terminate the certificate.

The TSP, through the Registration Authority, shall terminate the certificate only after successful identification and authentication of the Signatory/Creator and a specified reason for termination. Otherwise, the certificate will resume within 24 hours.

SEP Bulgaria provides each relying party with information on the suspension of the validity of the qualified certificates issued by it. This information is made available at any time and even after the validity of the certificate.

3.6. Identification and Identity Verification after Termination of a Qualified Certificate

The policy and practice of providing qualified certification services to SEP Bulgaria does not allow the renewal of a qualified certificate through Renewal or Re-key after its termination.

The Signatory/Creator or Authorized Representative of the legal entity of a suspended certificate may request the issuance of a new certificate.

The TSP, through the Registration Authority, performs initial identification, authentication of the Signatory/Creator if he / she requests a new certificate.

4. Operational Requirements

SEP Bulgaria, through the registrant, within the framework of a Qualified Certification Services Agreement, provides the following operating procedures for Qualified Certification Services applicable to Qualified Electronic Signatures / Seals:
1. Registration of a request for a qualified certificate;
2. Processing a request for a qualified certificate;
3. Issuance of a qualified certificate;
4. Transmission of a qualified certificate issued;
5. Using a pair of keys and a qualified certificate;
6. Renewal of the Qualified Certificate by Renewal;
7. Renewal of a qualified certificate through Re-key;
8. Suspension / resumption of a qualified certificate;
9. Termination of a qualified certificate;
10. Qualified certificate status.

The TSP, through the Registration Authority, allows the Signatory/Creator to terminate the Qualified Certification Services Agreement between them.

### 4.1. REQUEST SUBMISSION FOR A QUALIFIED CERTIFICATE ISSUANCE

Submission of a qualified certificate is a process whereby the user submits to a Registration Authority of SEP Bulgaria, in writing or in electronic form, a request for issuance of a qualified certificate according to the policy of issuance of the respective certificate.

The request may be made personally by the TitleSignatory/Creator or an authorized representative of the legal entity.

The user registers a request to issue a qualified certificate online or through an operator at the TSP Registration Authority.

In online mode, requests are submitted through network protocols such as HTTP, HTTPS, S / MIME or TCP / IP.

The information contained in the request is as follows:

1. The full name of the Holder, as well as his nickname, if one is required to enter the Holder in the relevant certificate;
2. The full name of the Creator;
3. Full name of the person authorized to represent the Signatory/Creator upon requesting the service;
4. Signatory/Creator IDs: PIN, FDI, UIC, BULSTAT;
5. Permanent address / registered office and registered office of the Holder;
6. Permanent / official address of the Creator;
7. Type of Qualified Certificate for Electronic Signature / Seal;
8. E-mail address of the Holder for the purpose of using the certificate;
9. Additional information needed to obtain the requested type of electronic signature / seal certificate;
10. Details of the Representative Power of the Holder - type, number and date of the document certifying the representative authority, individualizing the marks of the body that issued the document.
11. Data and information on the person's affiliation to the respective branch / professional organization.

Together with the provision of the above information, the person requesting the issuance of a qualified certificate shall also submit the following statements regarding:

1. completeness, correctness and accuracy of the data submitted with the request;
2. Preservation and processing of the personal data contained in the request;
3. Existence or lack of desire to restrict public access to the requested certificate.

### 4.1.1. WHO CAN SUBMIT A REQUEST FOR A QUALIFIED CERTIFICATE?

Any person belonging to one of the following categories may apply for the issuance of a qualified certificate:

1. A natural person who is or will be the user of a qualified certificate;
2. Authorized representative of a legal entity or an institution;
3. Authorized representative of the Certification Authority of SEP Bulgaria;
4. Authorized representative of the registering authority.

### 4.1.2. PROCESSING OF THE REQUEST FOR A QUALIFIED CERTIFICATE ISSUANCE AND THE RELATED OBLIGATIONS

#### 4.1.2.1. USER CERTIFICATES

All users of Qualified Certificates (including Certification Entities) and all end users must accept the obligations and warranties set forth in the Qualified Certification or Qualified Certification Services Agreement. Each user of a qualified certificate goes through a registration process that requires the following:

1. Submission of a qualified certificate containing true and accurate information. The request may include additional, unverifiable information, part of which is certified, and another part facilitates the contact of the TSP with the Holder / Creator;
2. Generate a pair of cryptographic keys or perform the generating activity itself. The pair of cryptographic keys must be generated in an electronic signature / print creation device meeting the security level requirements of Signature / Sealing Regulation (EU) 910/2014;
3. The electronic format of the request for the issue of a qualified certificate with the information to be included in the certificate is a structure signed with the private key of the generated key pair in an electronic signature / print creation device;
4. In cases where necessary, the registering authority shall provide the Signatory/Creator or a person authorized by him / her in a protected form of information / code for access to the private key in an electronic signature / seal creation device;
5. Approved requests for issuance and management of a qualified certificate shall be signed by the TSP.

4.1.2.2. Certificate Authority and Registration Authority Certificates

Registration authorities that provide qualified services for or under the control of SEP Bulgaria and are not in the organizational structure of the TSP (external registration authorities) must first enter into an agreement with SEP Bulgaria. In addition to the rights and obligations of both parties, the agreement must also include information on the identity of the persons involved in the registration body and their authorization to represent both parties during the performance of the contract. The persons authorized to carry out this activity should determine the type and purpose of the certificates before issuing them.

The keys and certificates of the certifying authority can only be generated at a key ceremony involving only persons authorized to carry out this activity.

4.1.2.3. Request for Registration of Users of Qualified Certification Services

The request for registration of users of Qualified Certification Services is filed with the registrant by natural, legal or a person authorized by him / her in a protected form of information / code for access to the private key in an electronic signature / seal creation device;

5. Additional information requested to be included in the certificate as well as an admissible unconfirmed one;
6. Signing a Qualified Certification Services Agreement and agreeing to the terms and conditions of the Policy and Practice for the provision of Qualified Certification Services by SEP Bulgaria.

Depending on the content of the certificate and its type, some of the data listed above may be absent.

If the pair of cryptographic keys is generated by the Holder / Creator, the Registration Authority should check the submitted electronic registration request and the security level requirements of the electronic signature / print creation device.

After authentication and authentication of the person applying for a qualified certificate and receiving confirmation from the Registration Authority, the application for registration is sent to the Certification Authority for issuing a certificate.

4.1.2.4. Qualified Certificate Renewal (Renewal), Generation of a New Key Pair (Re-key) and a Qualified Certificate Change

The Signatory/Creator or Authorized Person may request the renewal of a qualified certificate, subject to the time limits, requirements and renewal conditions.

The renewal of a Qualified Certificate keeps the Signatory/Creator or Authorized Person information from the current certificate, and the validity period is changed in the renewed certificate.

Renewal of a qualified certificate that has not been terminated during its period of validity may be accomplished in two ways:
- the generated pair of keys for the current certificate (Renewal) is retained;
- A new pair of keys (Re-key) is generated.

The renewal of a qualified certificate is preceded by the registration of a renewal application before the registration authority or online.
When the Qualified Certificate has expired and the renewal request is subject to the specified time limits and renewal identification requirements, the Signatory/Creator or Authorized Person should personally visit the SEP Bulgaria Registration Authority. The Signatory/Creator or Authorized Person may repeatedly renew a Qualified Electronic Signature / Seal Certificate. SEP Bulgaria does not recommend the repeated renewal of a qualified certificate through Renewal in order to reduce the risk of compromising the private key.

The TSP does not allow the use of a pair of electronic signature / seal keys for a period longer than 3 (three) years. SEP Bulgaria recommends that the Signatory/Creator or Authorized Person renews his / her Qualified Certificate via Re-key.

The Registration Authority will renew a Qualified Electronic Signature / Print Certificate by Renewal subject to the following conditions:
1. The certificate has not been terminated during its period of validity;
2. The Signatory/Creator or Authorized Person declares that there is no change in the Certified Information in his / her current Certificate;
3. A request for renewal of a qualified certificate shall be made within 30 days before the expiry of the period of validity of the certificate;
4. Strictly performs the authentication and authentication of the user and the specified time limits upon renewal.

The Registration Authority will renew a Qualified Electronic Signature / Print Certificate by Re-key under the following conditions:
1. The certificate has not been terminated within its term of validity;
2. The Signatory/Creator or Authorized Person declares that there is no change in the Certified Information in his / her current certificate;
3. A request for renewal is made up to 30 days before or after expiry of the validity of the certificate;
4. Strictly performs the authentication and authentication of the user and the specified time limits upon renewal.
In all cases where there is a change in the certified information for the Signatory/Creator or authorized person of the current certificate, the latter is not subject to renewal, and SEP Bulgaria issues a new qualified certificate.

Request for renewal of a qualified certificate through Renewal or Re-key must contain at least the following:
1. The unique name of the Signatory/Creator or Authorized Person;
2. Type of Qualified Certificate / Purpose;
3. The authentication policy identifier on the basis of which the certificate is issued;
4. A public key (which was previously used in the event of a renewal or change of a certificate or the new public key in the case of a Re-key) to be authenticated.
Some or all of the data contained in the request for renewal of a qualified certificate can be authenticated by electronic signature / seal ing provided that the subscriber has a valid private signing / printing key at the time .
The TSP does not allow a change in the profile of Qualified Electronic Signature / Seal Certificates.

4.1.2.5. REQUEST FOR A CERTIFICATE SUSPENSION AND TERMINATION

Request for suspension and termination of a qualified certificate shall be filed by the Signatory/Creator or an authorized person on site at the Registration Authority or electronically.
At the time of suspension and termination of a qualified certificate, the registering body shall notify the consumer of this fact (for example by e-mail).

SEP Bulgaria shall terminate a certificate issued by:
1. Death or incapacitation of the Signatory/Creator with the termination of the representative authority of the Creator;
2. Termination of the Representative Power of the Holder against the Creator;
3. Identification of false data when issuing the certificate;
4. Subsequently, false information has been verified;
5. Upon change of already certified information of the Holder / Creator;
6. Compromise of the private key;
7. Delay in payment of due remuneration;
8. Request for Termination by the Signatory/Creator after the TSP has ascertained their identity and the representative authority of the Creator.

The TSP shall immediately revoke the validity of a certificate issued in each of the above circumstances.

The TSP terminates the certificates he / she issued if he ceases his activity without transferring it to another TSP.

The TSP may suspend and terminate an attestation certificate from the infrastructure if there are reasonable grounds for doubting the private key of that authority.
Upon termination of the certificate of the operational certifying authority for issuance and maintenance of qualified certificates for electronic signature / seal, the validity of all certificates issued by him / her and valid certificates shall be terminated.

Only the operating certifying authority that has issued a qualified electronic signature / seal certificate may terminate this certificate.

If the termination is a result of an operator error or a consequence of compromising an operational private key of SEP Bulgaria, the TSP will issue an equivalent consumer certificate at its own expense.

Termination and Suspension Management Services are available 24 hours a day, 7 days a week.

In the event of system failure, services, or other factors beyond the control of the certifying authority, SEP Bulgaria shall do its utmost to ensure that the service is not missing for a period longer than the maximum period of time, which in this case is 3 three hours.

The time in the systems associated with stopping and terminating certificates is synchronized to UTC at least once every 24 hours.

**4.2. REQUEST PROCESSING**

SEP Bulgaria accepts requests online and on site at the registering authority. In case the documents are sent by post, a notary certification of the signatures is necessary.

An online submission is made using the TSP's website at: http://www.eSign.bg/en/deSign-products/electronic-privacy-policy-policy/#Applications. The user who has visited the site appropriately completes (in accordance with the instructions on this site) an appropriate application form and sends it to the registrant online. Requests for Qualified Certification Services are processed manually. Electronic protocols such as HTTPS, S / MIMME, or TCP / IP are used to send requests electronically via SEP Bulgaria's website.

When submitting a request to a registration body, a Signatory/Creator or an authorized person is required. In case of authorization, documents proving authenticity are required.

The information provided during the initial registration is stored by SEP Bulgaria and can be used when accepting Certification Services requests from the TSP.

Upon validation of the collected data, the person may proceed to the next steps of requesting qualified certification services.

**4.2.1. IDENTIFICATION AND IDENTITY VERIFICATION**

The authentication and authentication activities of the users of SEP Bulgaria shall be carried out by the registrant in accordance with the conditions specified in paragraph 1.3.2.

**4.2.2. ACCEPTANCE OR REJECTION OF A REQUEST**

**4.2.2.1. REQUEST PROCESSING BY THE REGISTRATION AUTHORITY**

Any request submitted electronically or on paper to the registering authority shall be processed as follows:

1. The registration authority receives the request of the Signatory/Creator or Authorized Person (in hard copy or in electronic format);
2. The registration authority shall verify that the person has paid a fee for the examination of the application for a qualified certificate, provided that the payment is provided in the SEP Bulgaria price list. In the absence of such a fee, the request shall be rejected;
3. The registering authority verifies the data specified in the request, such as the person's personal data (procedure described in paragraphs 3.2.2 to 3.2.5), and checks for the possession of a private key (3.2.1);
4. In the event of a positive check, the registrant shall confirm the request;
5. If the original app contains incorrect information, it is rejected or corrected;
6. A certificate shall be issued as a result of the confirmation;
7. The registration authority may also check other data not specified in the request but required by SEP Bulgaria. When providing Qualified Certification Services, the TSP verifies the power of representation of the persons holding the representation or authorized by the Holder or the Creator respectively, before taking action to perform the requested services. The representation is verified on the basis of official documents provided by the Holder / Creator, from which the fact and the volume of the representative power is obvious. The TSP may collect the necessary data to confirm the representation, where the latter is based on a statutory provision, from publicly available registers.
SEP Bulgaria is not responsible, does not verify the legal entity’s right to use the personal data of the Account Holder. The legal person is responsible for the misuse of the personal data of the Account Holder. The legal entity is required to declare the right to use, store and submit the personal data to the Holder.

### 4.2.2.2. REQUEST SUBMISSION TO THE CERTIFICATION AUTHORITY FOR A QUALIFIED CERTIFICATE ISSUANCE

SEP Bulgaria may refuse to issue a qualified certificate to any person without any obligation or liability if the user points out incorrect data in the certificate application. If, following a refusal to issue a certificate, damage is suffered for the user, the certifying authority must immediately refund the user the fee for the certificate (if the consumer has paid it).

Refusal to issue a qualified certificate may occur:
1. The Signatory/Creator has not submitted the required documents for the issuance of a qualified certificate;
2. The consumer can not prove the existence of an explicit representative authority regarding the performance of the factual and legal acts for the supply of a certificate;
3. If there are doubts that incorrect data and / or untrue or falsified documents were used in conducting the certification procedure;
4. A pre-agreed limit for the number of issued Certificates of a particular Signatory/Creator has been reached;
5. If there are other grounds for refusal regulated by current legislation.
6. If the user can not prove his / her rights to the proposed DN;
7. The consumer did not pay for the issuance of a certificate, provided that the payment is provided in the SEP Bulgaria price list; Information about the refusal to issue the certificate and the reasons for it shall be communicated to the consumer. The person refused to issue a qualified certificate may file a complaint within 3 (three) days in the manner provided for in this document. Candidates whose applications have been rejected subsequently may again apply for a qualified certificate.

### 4.2.3. WAITING FOR THE QUALIFIED CERTIFICATE ISSUANCE

The registration authority of SEP Bulgaria immediately, in the presence of the user - Signatory/Creator or a person authorized by him / her, performs all the functions of checking the request for issuance of a qualified certificate. After verifying the necessary documents, the TSP validates the information provided.

The Certification Body of the TSP shall issue a Qualified Certificate immediately upon approval by the registrant of the electronic request for issue.

SEP Bulgaria ensures that upon receipt of a request for issuance or management of a certificate, the registrant will examine the request and the issuance of the certificate immediately and, in special cases, no later than 3 (three) days from the day of filing . This period depends mainly on the type of qualified certificate, the completeness of the request submitted and the technological time for coordination of the service between the administrative structures of the TSP and the time between the TSP and the consumer.

### 4.2.4. CERTIFICATION AUTHORITY ALLOWS THE PROCESSING OF THE DATA

The SEP Bulgaria Certification Authority electronically identifies the registration body that has validated the electronic request for the issuance of a qualified electronic signature / seal certificate.

The Certifying Authority generates the required certificate according to the selected account, signs it with the electronic signature of the TSP and immediately publishes it in its Public Register (Storage).

### 4.3. QUALIFIED CERTIFICATE ISSUANCE

### 4.3.1. PROCESSING

Upon receipt of a request for a qualified certificate and its processing, the certifying authority issues a qualified certificate. All certificates are issued online. The issuing procedure is as follows:
1. Any request for the issue of a qualified certificate shall be recorded and verified by the registrant;
2. Only persons performing trusted roles shall have access to the operational activities of the registering authority. Account usage protects multi-level operations and allows secure processing of a qualified certificate request, including the creation of an appropriately formatted certificate application form by the certifying authority;
3. The processed and formatted certificate request is sent to the Qualified Certificate Issuance server according to the selected profile;
4. The Certifying Authority generates the required certificate, signs it with the electronic signature of the TSP and immediately publishes it in its Public Register;
5. The Certifying Authority prepares a response containing the issued certificate and provides it to the consumer.

### 4.3.2. Provision of Information

An authorized representative of the registration authority of SEP Bulgaria shall immediately notify the Signatory/Creator or the person authorized by the Creator for the issued and published certificate. Authorized representative of the registration authority of SEP Bulgaria shall send to the Signatory/Creator an electronic notification by email with information about the Holder's name, the type of the electronic signature / seal issued, the unique serial number of the Qualified Certificate and its period of validity.

The TSP shall deliver the certificate issued to the Holder / Creator, respectively to the person authorized by him, through the registration body;

The authorized operator of the registration authority records the certificate of an electronic signature / print creation device where the pair of cryptographic keys for that certificate was generated.

### 4.4. Qualified Certificate Acceptance

#### 4.4.1. Confirmation of Acceptance of a Qualified Certificate

Upon receiving a Qualified Certificate, the user commits to verify its content, especially for the accuracy of the data and the availability of a public key corresponding to the private key it owns. If the certificate has any errors that can not be accepted by the user, the certificate must be terminated immediately.

The Signatory/Creator may object if the issued Qualified Certificate contains errors or incompleteness within 3 (three) days of its publication in the Register. SEP Bulgaria removes them by issuing a new certificate without payment of remuneration unless they are due to the provision of untrue data. In the absence of an objection, the content of the certificate is deemed to have been accepted.

The rules in this section apply to both the issue of a certificate and the renewal of a certificate. After a Qualified Certificate acceptance procedure, it is assumed that the user has been thoroughly acquainted with the certification procedures described in this document.

By accepting the Qualified Certificate, the User accepts the Practice and the Policy in the presence of Qualified Certification Services and agrees to comply with the agreement reached with SEP Bulgaria.

#### 4.4.2. Publication of a Qualified Certificate

Each issued and accepted certificate shall be published immediately in the SEP Public Register / Storage Facility.

#### 4.4.3. Information for Other Parties

Following the immediate publication of the certificate issued in the Public Register of the issued certificates, it becomes available to all interested parties.

### 4.5. Usage of a Qualified Certificate and of a Key Pair

#### 4.5.1. By Users
Users must use the private keys and their respective certificates:
1. In accordance with their intended purpose as specified in this Practice and in accordance with the content of the certificate (fields keyUsage, EnhancedKeyUsage);
2. In accordance with the Certification Services Agreement between the consumer and SEP Bulgaria;
3. Only for the duration of their validity, except for the purpose of decryption of documents and verification of electronic signature / seal;
4. When the certificate is suspended, the user must not use the private key to create an electronic signature / seal.
The private key corresponding to the authenticated public key is controlled by the Account Holder. Responsibility for using the private key is the Holder.

4.5.2. BY RELYING PARTIES

The responsibility of the relying parties upon receipt of a document signed with an electronic signature / seal is to verify that the public key of the Qualified Certificate that corresponds to the Private Key of the Signatory/Creator used in electronic signature / printing is not published in the CRL. The relying party should make the online check in the current current CRL or OCSP. The final decision on the acceptance of the certificate shall be taken by the relying party. The TSP is not responsible for the actions of the relying party for failure to meet the above requirements.

Relying parties, including operators at the registering authority, must use the public keys and their respective certificates:
1. In accordance with their intended purpose as specified in this Practice and in accordance with the contents and attributes of the certificate itself;
2. Only after checking their status and checking the electronic signature of the certifying authority that issued the certificate;
3. Until the validity of a key is revoked;
4. When the certificate is suspended, the relying party must not accept the public key.

4.6. RENEWAL OF A QUALIFIED CERTIFICATE (RENEWAL)

Renewal of a qualified certificate means replacing a valid certificate with a new one without changing the existing information in it, except for a new serial number and a new validity period. Renewal is only performed within the validity period of a current certificate. It must be preceded by the registration of a renewal application in an appropriate form accepted and approved by an operator in a registration authority, verified identity and correctness of the request made.

4.7. ISSUANCE OF A QUALIFIED CERTIFICATE WITH GENERATION OF A NEW KEY PAIR (RE-KEY)

A new pair of keys is generated by SEP Bulgaria, in cases where an already registered user requests to generate a new key pair or a new user requests to generate a pair of keys. The generation of a new pair of keys is accompanied by the issue of a new qualified certificate confirming ownership of the newly created key pair.
Issuing and renewing with Re-key should be interpreted as follows:
1. The issuance of a new key pair is not associated with any valid certificates and is used by users to obtain a certificate of any kind;
2. Re-key refers to a specific valid certificate specified in the request. As a result, the new certificate includes the same content, the only differences being: a new serial number, a new public key, a new term of validity, and a new electronic signature / seal.
SEP Bulgaria shall pre-notify users by e-mail at least 10 days before the expiration of the validity of the issued certificate whenever possible.
The procedure for issuing a qualified certificate with the generation of a new key pair may also be applied to the certifying authority and to the registration authority.

4.7.1. CIRCUMSTANCES UNDER WHICH A QUALIFIED CERTIFICATE IS ISSUED BY GENERATING A NEW KEY PAIR (RE-KEY)

A consumer renewal application submitted to SEP Bulgaria may only be applied if:
1. The user is the same;
2. The certificate is valid at the time of submission of the request and has not been canceled before;
3. The user requires additional certification of the same type or of a different type, but only within the policy for authentication of the valid qualified certificate;
4. There is no valid certificate issued under the policy of authentication defined in this Practice.

4.7.2. WHO CAN REQUEST A KEY PAIR UPDATE?

The request to issue a qualified certificate with the generation of a new key pair (Re-key) is made only by the Signatory/Creator or a person authorized by him / her.

4.7.3. Re-key and request processing

Renewal of an electronic signature / seal certificate with Re-key is preceded by the registration of a renewal request before the Signatory Authority of the TSP. The request for renewal of a qualified certificate, by electronic application, shall be certified with an electronic signature / seal corresponding to the current Holder / Creator's certificate or a person authorized by him / her. In the event that the certificate that is renewed has expired, the Signatory/Creator or a person authorized by him / her has to visit the TSP's own registration body personally. An authorized operator of the registrant strictly follows the requirements for identification and identity identification and the renewal conditions.

After successful identification and verification of renewal conditions, the registrant confirms the renewal request to the SEP Bulgaria Operational Certification Authority. After the successful electronic authentication of the registration body, through the authorized operator, the operational certifying authority executes the confirmed request for renewal of the certificate. In the event of failure to identify and verify the renewal conditions, the registrant shall reject the application for renewal of the certificate and shall immediately inform the consumer of the reason. In this case, the user with a rejected renewal request may request the issuance of a new electronic signature / seal certificate.

4.7.4. INFORMATION FOR THE USER

An Authorized Representative of the SEP Registration Authority Bulgaria shall immediately notify the Signatory/Creator or a person authorized by him / her for the renewed and published certificate. In cases where the request is submitted electronically, the TSP sends electronically (by e-mail) information on the new qualified certificate: the name of the user, the type of qualified certificate, the unique serial number and the period of validity of the renewed certificate. The e-mail address from which the new qualified certificate can be removed is also sent. When the user submits his request in situ to the registering authority, the Signatory/Creator or person authorized by him / her shall receive the renewed qualified certificate through an authorized operator of the registrant. An operator records it on an electronic signature / print creation device in which the pair of cryptographic keys for the Qualified Certificate.

4.7.5. CONFIRMATION OF ACCEPTANCE OF A NEW CERTIFICATE

Upon receiving a new Qualified Certificate, the user commits to verify its content, especially for the accuracy of the data and the availability of a public key corresponding to the private key it owns. If the certificate has any errors that can not be accepted by the user, the certificate must be terminated immediately. The Signatory/Creator or person authorized by him / her may object if the issued certificate contains errors or incompleteness within 3 (three days) of its publication in the register. SEP Bulgaria removes them by issuing a new certificate without payment of remuneration unless they are due to the provision of untrue data. In the absence of objection, the content of the Qualified Certificate is deemed to have been accepted.
4.7.6. Publication of a new qualified certificate

SEP Bulgaria, through the Operational Certification Authority, shall immediately publish the renewed certificate in the Public Register / Storage Facility.

4.7.7. Information for the relying parties

Following the immediate publication of a qualified certificate issued in the Public Register of the issued certificates, it becomes available to all interested parties.

4.8. Change in the qualified certificate

4.8.1. Circumstances for a change in the qualified certificate

Changing a qualified certificate means changing the content of the data in a previously issued and published Qualified Electronic Signature / Seal Certificate. Upon changing a qualified certificate, a new pair of keys is required to be generated. The change is treated in the same way as issuing a new qualified certificate.

SEP Bulgaria does not allow a change in the profile of qualified electronic signature / seal certificates.

4.8.2. Who can request a change in the qualified certificate?

Signatory/Creator or person authorized by him / her may request change of a qualified certificate provided that the requirements and renewal conditions described in this document are met.

4.8.3. Request processing

The change of qualified electronic signature / seal certificate shall be preceded by the submission of a request for change by the Signatory/Creator or a person authorized by him / her with the registration authority of SEP Bulgaria.

The request for change, by electronic application, shall be certified by an electronic signature / seal of the Signatory/Creator corresponding to a validly qualified certificate.

In the event that the certificate that changes is expired, the Signatory/Creator or a person authorized by him / her must visit the TSP’s own registration body personally. The registration authority strictly follows the requirements for identification and identification and the conditions for changing a qualified certificate.

After successful identification and verification of the conditions for change, the registering authority shall acknowledge the request to the Operator Certification Body of the TSP.

After successful electronic authentication of the authorized operator of the registering authority to the operating certifying authority, the latter shall execute the confirmed request for change of the qualified certificate.

In the event of failure to identify and verify the conditions for change, the registrant shall reject the request and shall immediately inform the consumer of the reason. In this case, the user with a rejected request for change may request the issuance of a new Qualified Electronic Signature / Seal Certificate.

4.8.4. Information for the user

An authorized employee of the registration authority of SEP Bulgaria shall immediately notify the Signatory/Creator or a person authorized by him / her for the changed and published qualified certificate.

The TSP sends to the Signatory/Creator an electronic notice (email) with the name of the Holder / Creator, the type of qualified electronic signature / seal certificate, the unique serial number and the term of validity of the changed certificate. The user also receives an electronic link from which he can download the changed qualified certificate.
When the Signatory/Creator or person authorized by him / herself visits the registration authority, the user receives the new certificate on the spot. An Authorized Officer of the Registration Authority shall record the new qualified certificate of a signature / print creation device in which the pair of cryptographic keys for the certificate.

4.8.5. CONFIRMATION OF ACCEPTANCE OF A NEW QUALIFIED CERTIFICATE

Upon receipt of the changed qualified certificate, the user commits to verify its content, especially the accuracy of the data and the availability of a public key corresponding to the private key it owns. If the certificate has any errors that can not be accepted by the user, the certificate must be terminated immediately.

The Signatory/Creator or person authorized by him / her may object if the issued certificate contains errors or incompleteness within 3 (three days) of its publication in the register. SEP Bulgaria removes them by issuing a new qualified certificate without payment of remuneration unless they are due to the provision of untrue data. In the absence of objection, the content of the certificate is deemed to have been accepted.

4.8.6. PUBLICATION OF A NEW QUALIFIED CERTIFICATE

SEP Bulgaria, through the Operational Certification Authority, shall immediately publish the changed qualified certificate/seal in the Public Register / Repository.

4.8.7. INFORMATION FOR THE Relying Parties

The public key in the Qualified Certificate corresponding to the Private Key held by the Holder is publicly available to all Trustworthy parties.

Each trustee, including an operator in a registration body, should use the public key and the Holder / Creator's certificate in accordance with the policy stated in the certificate.

Relying parties must use the public key only after checking the status of the certificate and checking the TSP’s electronic signature.

It is of particular importance that relying parties do not use the public key after termination of the certificate or at a time when it is suspended.

4.9. SUSPENSION AND REVOCATION OF A QUALIFIED CERTIFICATE

Suspension and termination of the validity of a qualified certificate is established operational practice of SEP Bulgaria. They are only performed during the period of validity of the certificate. Suspensions cause temporary suspension of the certificate. Termination leads to irrevocable suspension of the certificate and is an irreversible process.

If the certificate is terminated after the initial activation, it loses its validity from the moment of termination and its status can not be restored under any circumstances.

If the Contractor suspends or terminates a certificate, he registers this change in his certificate database and publishes the revoked status of the certificate in a timely manner, but in any event within 24 (twenty four) hours of receipt of the request.

Suspension or termination shall become effective as soon as it is published in the Public Register. They are always clearly marked with the exact date and time of status change in the Certificate revocation list (CRL) and in the Online Certificate Status Protocol (OCSP).

Upon termination of the certificate of the operating certifying body for issuance and maintenance of qualified certificates for electronic signatures / seal s, the validity of all issued and valid certificates shall be terminated.

Only the operating certifying authority that has issued a qualified electronic signature / seal certificate may terminate this certificate. If the termination is a result of an operator error or a consequence of compromising an Operational Private Key of the TSP that led to the termination of the validity of the certificate of the Operational Certification Body, the TSP shall issue an equivalent qualified certificate on its own account.

Suspension and termination management services for a qualified certificate are available 24 hours a day, 7 days a week.

In the event of system failure, services, or other factors beyond the control of the certifying authority, SEP Bulgaria shall do its utmost to ensure that the service is not missing for a period longer than the maximum period of time, which in this case is 3 three hours.
SER Bulgaria shall provide all relying parties with information on the validity or not of the qualified certificates issued by it. This information is made available at any time and even after the validity of the certificate in an automated, reliable way. The time in systems related to suspension and certificate termination is synchronized to UTC at least once every 24 hours.

### 4.9.1. Reasons for Revocation of a Qualified Certificate

The main reason for terminating a Qualified User Certificate is the loss of this certificate or even a suspicion of such loss. Circumstances exist when the private key owned by the user is outside its scope of security when there is a material breach of the Owner’s / Creator’s obligations described in the contract between him and the TSP or the requirements of policy and practice in the provision of qualified certification services are not met by the user.

SEP Bulgaria shall terminate a qualified certificate issued by it if the following situation arises:

1. where the information entered in the certificate has changed;
2. When there is suspicion that the private key associated with the public key contained in the certificate is compromised (unauthorized access to the private key has occurred or there is reason to suspect such access, loss of a private key, or the suspected reason to suspect For such a loss, theft of a private key or the presence of a reason to suspect such a theft, accidental deletion of a private key);
3. The consumer decides to terminate the contract with SEP Bulgaria;
4. Death or imprisonment of the Holder / Creator, with termination of a legal entity;
5. Termination of the Representative Power of the Owner with respect to the legal entity;
6. When the user does not meet the requirements of the authentication policy adopted;
7. If the certifying authority ceases its activity;
8. If the user owes outstanding fees for the provision of qualified certification services;
9. When the reliability and security of the private key of the certifying authority is violated;
10. When a user who is an employee of an organization terminates his contract of employment and does not return the used cryptographic card (or device) on which the certificate and the corresponding private key are stored;
11. Other circumstances related to non-compliance with the requirements of the Practice when providing qualified certification services.

A certificate belonging to the certifying authority may be terminated by its issuing authority. Such termination may occur in the following situation:

a) Where the certifying authority has reason to believe that the information in the certificate issued is false;
b) Where the private key of the certifying authority or its information system is violated in a manner affecting the credibility of the certificates issued by that authority;
c) When the Certifying Authority has materially breached an obligation arising from this Practice when providing Qualified Certification Services.

### 4.9.2. Who Can Request Revocation of a Qualified Certificate?

The following entities may apply for the termination of a qualified certificate:

1. A user who is the owner of a certificate;
2. Authorized representative of the certifying authority (in the case of SEP Bulgaria this role is reserved for the security administrator);
3. A legal person who, as an employer, terminates the employment contract of his or her employee terminates the certificate of the Titleholder, who is subordinate to him. In this case, the employer shall immediately inform his subordinate;
4. Where the operator of the registrant has doubts as to the reliability of the information provided by the consumer.

Where a legal person requests a certificate to be terminated by a person authorized by it, the certifying authority must:

- Checks whether the user is authorized to request the termination;
- Notifies the Holder to terminate or initiate a termination procedure;

A request for termination of a qualified certificate may be filed with the registrant on paper and online. When a user submits on paper, the request for termination must appear in person at the registering authority. In cases where an online termination is requested, the request is required to be signed with a current electronic signature / seal. In each case, the certificate is suspended temporarily but in no more than 48 hours. Subsequently, a personal appearance at the Registration Authority is required to clarify the case and confirm the request for termination of the Qualified Certificate.
4.9.3. PROCEDURE FOR REVOCATION OF A QUALIFIED CERTIFICATE

4.9.3.1. PROCEDURE FOR REVOCATION OF A QUALIFIED CERTIFICATE

SEP Bulgaria has no commitment to the Signatory/Creator in relation to the provision of Qualified Certificate Management services after the Contract concluded between them has been terminated or expired. The user of Qualified Certification Services of SEP Bulgaria may at any time terminate the Certification Services used by him. Upon request for termination of the use of certification services, SEP Bulgaria shall terminate the contractual relations with the Signatory/Creator and terminate the issued Qualified Certificates in which the Signatory/Creator is entered. SEP Bulgaria shall not indemnify the Account Signatory/Creator upon termination of the use of Qualified Certification Services upon his / her request. Termination of a qualified end-user certificate is preceded by a request for termination before the registration authority of SEP Bulgaria. A request for termination of a certificate may be registered electronically only when the Signatory/Creator has (another) valid and available for use Qualified Electronic Signature / Seal Certificate. Otherwise, an on-site request is made to an authorized operator with the registering authority. Upon request for termination, the registrant shall register the request and initiate a verification procedure. Evidence of termination of a qualified certificate shall be submitted to the registering body. After reviewing the evidence, the registrant shall decide whether to continue the termination or refuse the request for termination of the certificate to the consumer. The registration body shall prepare and send a request to the certifying authority to authorize the termination procedure. Any request for termination of a certificate must contain irrefutable proof of confirmation of termination. All motives for termination must be validated (signed electronically or signed by hand).

The procedure for terminating a qualified certificate is as follows:
1. The authorized operator of the registration authority shall, without identifying the user, suspend the certificate for not more than 24 hours.
2. The registration authority strictly follows the requirements for identification and authentication of the Signatory/Creator or a person authorized by him and the reasons for termination. In all cases, the Signatory/Creator or a person authorized by him / her must personally visit the SEP Bulgaria registration authority for subsequent verification of the identity or identity of the user.
3. Upon successful authentication of the Signatory/Creator or a person authorized by him / her, the registering body shall, through the authorized operator, submit a processed application to the operating certifying authority to terminate the certificate. Upon confirmation by the certifying authority, the request for termination of the certificate is executed.
4. In the event of failure to identify and verify the conditions for termination, the registering authority shall reject the request for termination of the certificate and immediately notify the Signatory/Creator or a person authorized by him / her, of the reasons for doing so.
5. A user with a rejected request for termination of a qualified certificate may file a new request for termination of the certificate after removing the stated reasons for the refusal.
6. Upon termination of the certificate, the TSP shall, through its operating certifying authority, immediately publish the suspended certificate on the CRL by issuing a new CRL.
7. After termination of the Qualified Certificate, the TSP shall notify the Signatory/Creator of the canceled certificate. Terminated Holder / Creator’s Certificate is not subject to resumption or renewal. Access to the termination request and the system sampling documentation from the termination of a qualified certificate are performed by authorized personnel of SEP Bulgaria. If a certificate is stored on an electronic cryptographic card, upon termination of the Qualified Certificate, the card may be physically destroyed or securely deleted. This operation must be performed by the cardholder. SEP Bulgaria recommends that the cardholder keeps it in a way that prevents it from being stolen, unauthorized, or physically destroyed, and deleting the private key.

4.9.3.2. PROCEDURE FOR REVOCATION OF A QUALIFIED CERTIFICATE OF A CERTIFICATION AUTHORITY OR A REGISTRATION AUTHORITY

A certificate belonging to a certifying authority or to a registration authority may be terminated by the authority which issued it. In this case, authorized entities of the Authority submit a request directly to SEP Bulgaria. SEP Bulgaria may also submit a request for termination of a certificate of a certifying body or of a registration authority. (See paragraph 4.9.2)
4.9.4. Grace Period of Revocation of a Qualified Certificate

Before suspending the validity of a validated certificate, SEP Bulgaria, through its registration body, suspends the validity of the certificate for a maximum of 24 hours grace period. Within this period, the TSP processes the request for termination of the Qualified Certificate:
1. Performs all authentication and authentication checks on the user who submitted the request;
2. Identify the reasons for the termination of the certificate;
3. In case of unconfirmed reasons or after expiration of the grace period, SEP Bulgaria shall resume the validity of the certificate;
4. The TSP allows the certificate to be resumed before the expiration of the grace period only at the explicit request of the Signatory/Creator or a person authorized by him/her.

Information on terminated certificates is stored in a database of SEP Bulgaria. Suspended certificates are published on the CRL within the required technological time, but for no longer than 3 hours.

Operators of suspended certificates by the certifying authority or the registrant as well as the end users concerned shall be automatically informed of such termination.

4.9.5. Time Limit for Processing the Request for Revocation

A request for termination of a qualified certificate is processed by SEP Bulgaria without undue delay.

4.9.6. Checking the Certificate Revocation List (CRL)

The responsibility of the relying parties to obtain an electronic signature signed by electronic signature / seal is to verify that the public key of the certificate corresponding to the Holder / Creator's private key used in electronic signature / printing is not published in the CRL. The trusted party should check online, via the Current CRL or by checking the current status of the certificate in real time via the OCSP Validation Authority – eSign OCSP.

If the audited qualified certificate (or public key, respectively) is included in the CRL, the relying party should reject the electronic document associated with the qualified certificate if the reason for inclusion in the CRL is one of the following:

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unspecified</td>
<td>There is no reason to include the certificate in CRL</td>
</tr>
<tr>
<td>keyCompromise</td>
<td>Security of the private key has been compromised</td>
</tr>
<tr>
<td>caCompromised</td>
<td>The security of the MA's key has been compromised</td>
</tr>
<tr>
<td>cessationOfOperation</td>
<td>The ground for issuing the certificate no longer exists</td>
</tr>
<tr>
<td>certificateHold</td>
<td>Certificate is suspended</td>
</tr>
<tr>
<td>affiliationChanged</td>
<td>Modified are the data entered in the certificate</td>
</tr>
<tr>
<td>Superseded</td>
<td>The certificate has been replaced by another certificate</td>
</tr>
</tbody>
</table>

For reference, it is necessary to download the CRL from the TSP’s site and install it in the Trust Party application. The e-mail address from which the CRL can be downloaded is given in each certificate issued.

The final decision on the validity of the qualified certificate is taken by the relying party. The TSP is not responsible for the actions of the relying party for failure to meet the above requirements.

4.9.7. Frequency of Issuing the Certificate Revocation List (CRL)

SEP Bulgaria, through its operational certifying authority, shall immediately publish in the repository a new, up-to-date CRL, whenever a valid certificate issued by that authority ceases.

The TSP, through its operational certification authority, updates its CRL at every 2 weeks if there is no suspension or cessation of certification during that period.

The validity period of 2 weeks applies to each new updated CRL of the operating certifying authority.
4.9.8. Maximum delay of publication of the CRL

Each CRL is published without undue delay as soon as it is created (usually automatic within a few minutes).

4.9.9. Online certificate status checking

SEP Bulgaria provides a qualified real-time status verification service on the basis of the OCSP certificate verification protocol described in RFC 2560. The use of OCSP enables information on the status of certificates to be obtained without requiring a check in the CRL and List of Suspended Certificates (CRLs). The OCSP service delivery model is based on the "Inquiry - Response" process. The responses received from the OCSP server providing the service are as follows:

<table>
<thead>
<tr>
<th>Answer</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>good</td>
<td>The certificate is valid</td>
</tr>
<tr>
<td>revoked</td>
<td>The certificate has been terminated</td>
</tr>
<tr>
<td>unknown</td>
<td>The status of the certificate is not set or the certificate is not issued by the respective MA.</td>
</tr>
</tbody>
</table>

The OCSP service generates a database-based response. The OCSP response is valid for 7 days. To maintain proper system performance, OCSP responses are cached for a predetermined time (typically not more than a few hours). Validation service is available 24 hours a day 7 days a week. In case of accidents and natural disasters, SEP Bulgaria takes immediate measures to recover the validation services first.

4.9.10. Requirements for online certificate status checking

The Qualified Service for Checking the Status of Real Time Certificates Provided by the TSP is available at: http://www.eSign.bg/bg/usages/validation-of-tests/.

Relying parties should check the published information in the repository related to the certificates they want to rely on. SEP Bulgaria is not responsible for damages and consequences of non-compliance with these requirements.

4.9.11. Specific requirements regarding the breach of the key security

В случай на нарушаване на сигурността на частния ключ (неговото разкриване) на удостоверяващия орган или други субекти, опериращи в рамките СЕП България, Доставчикът незабавно информира доверяващите се страни.

4.9.12. Reasons for suspension of a qualified certificate

In the event of security breach of the private key (its disclosure) by the certifying authority or other entities operating within SEP Bulgaria, the TSP shall immediately inform the Trust Parties.

4.9.13. Who can request a suspension of a qualified certificate?

SEP Bulgaria shall suspend the issue of a validly qualified certificate if:
1. A request was made by the Signatory/Creator or a person authorized by him / her, without having to verify his / her identity or representative authority;
2. A request has been made by a person who, in the circumstances, is aware that he may know of security breaches of the private key;
3. Request from the Communications Regulation Commission (CRC).

Suspension of a qualified certificate is preceded by the registration of a request for suspension before the registration authority.
1. A request for suspension of a certificate may be registered electronically or submitted on paper to an authorized operator in the registration authority of SEP Bulgaria.
2. The request for suspension of a certificate shall be electronically certified by an electronic signature / seal corresponding to the Holder / Creator's valid certificate.
3. The authorized operator of the registration authority shall immediately suspend the certificate without identifying the user. Suspension of the certificate shall be effected by its temporary entry in the List of Suspended and Suspended Certificates (CRL).
4. After successful authentication of the authorized operator's identity at the registration authority before the operating certifying authority, the latter shall execute the certified request for suspension of the certificate.
5. The registration authority can not reject a suspension request.
6. Following the suspension of the certificate, the TSP shall immediately publish the suspended certificate through its Operational Certifying Authority on the CRL by issuing a new list.
7. After termination of the certificate, the TSP shall immediately notify the Signatory/Creator of the suspended Qualified Certificate.

4.9.15. Grace Period of a Suspension of a Qualified Certificate

SEP Bulgaria shall suspend the validity of a qualified electronic signature / seal certificate for up to 24 hours from receipt of the request for suspension.
SEP Bulgaria temporarily suspends the validity of a certificate before its termination within 24 hours.

4.9.16. Resuming the Validity of a Suspended Certificate

SEP Bulgaria resumes the suspended certificate:
1. Within 24 hours of its suspension;
2. After the suspension period has expired (24 hours) and no request for resumption has been received;
3. Once the reason for stopping before the end of the braking period expires;
4. At the request of the Owner / Creator, after clarifying the reasons for the requested suspension;
Upon renewal of the certificate, the latter is considered to be valid.

4.9.17. Procedure for Resuming the Validity of a Qualified Certificate

The signatory authority resumes a suspended certificate once it has received a resume request from the Signatory/Creator and after a successful authentication and authentication check.
The registration authority immediately resumes a suspended certificate after the statutory suspension period has expired (24 hours).
In all cases, the resume procedure removes the suspended certificate from the current CRL and publishes a new list.

4.10. Checking the Current Status of a Qualified Certificate

4.10.1. Characteristics

Information on the status of certificates issued by SEP Bulgaria can be obtained on the CRL, published on the SEP Bulgaria website and through the OCSP Online Certificate Verification Protocol.
Authentication services for status verification of Qualified Certificates are available in 24/7/365 mode (continuously operating).

4.10.2. Additional Functions
The Online Certificate Verification Online Certificate Verification Service (OCSP) is available for all types of Qualified Certificates as well as for all Trustworthy Parties. The OCSP service is mandatory for all operational certifying bodies issued by SEP Bulgaria.

### 4.11. Termination of a Qualified Certification Services Contract by a User

The contract for qualified certification services between SEP Bulgaria and users is terminated:

1. After the expiration of the last issued Qualified Certificate and the user has not taken any action to update his / her certificate;
2. When the Qualified Certificate has been terminated and the User has not taken action to issue another certificate.

### 4.12. Private Key (Escrow)

The private keys of the Certification Authority of SEP Bulgaria or the users that are included in the Certification Authority of the TSP are not subject to an escrow.

### 5. Control Over the Physical and Organizational Security

This part of the Practice for the provision of qualified certification services describes the general rules regarding the control of the physical and organizational security as well as the activities of the personnel employed in SEP Bulgaria. Security requirements and procedures are being considered at the time of key generation, authentication and authentication of users, issuance of qualified certificates and their management, auditing of the TSP and archiving.

#### 5.1. Control of the Physical Control

The measures taken in relation to the TSP's physical protection are an element of the Information Security System developed and implemented in SEP Bulgaria, which complies with the requirements of ISO / IEC 27001: 2013 and ISO / IEC 19011: 2011. Measures related to the physical protection of information data, technological systems, premises and related support systems are aimed at preventing:

1. Unauthorized access, damage and interference in working conditions;
2. Loss, damage or compromise of resources;
3. Compromise or theft of information or means of processing the information.

SEP Bulgaria provides physical protection and access control of premises where critical components are installed in its infrastructure, registers, repositories and registration authorities. Infrastructure of the TSP is physically and logically distinct and is not used in other activities that the TSP performs.

#### 5.1.1. Premises and Structure of the Premises

SEP Bulgaria has a specially designed and equipped room with the highest degree of physical access control, which houses the certification bodies of the TSP and all the central components of the infrastructure.

#### 5.1.2. Physical Access

The physical security of certificate issuing and management systems is consistent with the requirements of international standards and recommendations.

The building is guarded by 24 (twenty four) hours of physical security. A technical system was developed to monitor the site and the protected areas. The surrounding area and premises are under 24 hours of video surveillance.

Depending on the activities carried out in the relevant premises, some of them are publicly accessible and access to others is controlled or only possible for authorized employees. All employees and visitors wear a badge with information about the physical access zone and access mode.
The protected areas are equipped with physical control and monitoring systems and fire alarm and fire extinguishing systems. Only authorized employees of SEP Bulgaria have access to these areas. Entry and exit from areas and movement in the premises of the zones are monitored and recorded by an access control system. Accompanying persons can only pass after confirmation from an authorized employee.

For the equipment in the protected and isolated premises of the TSP, physical integrity is ensured. There is two-factor access control. Every access to critical infrastructure premises is documented in special journals.

Physical protection of the premises where the TSP and the registering body are located are made of solid and stable construction with strong doors and locks.

All systems are inspected periodically.

Employees of SEP Bulgaria staff strictly adhere to the developed internal procedures for access to the various restricted areas.

In SEP Bulgaria the offices of the registration bodies are separated and separated from the other premises. They are equipped with a technique for safe storage of data and documents. Access to these areas is monitored and limited to authorized persons related to the activity of the registration body (operators of the registrant, system administrators) and their clients.

### 5.1.3. Electrical Power and Air-Conditioning

When the main power supply fails, the systems switch to backup power. In case of short interruptions and fluctuations, uninterruptible power supply (UPS) is used. If the interruption is continuous, a generator is included.

All work rooms are ventilated and air-conditioned. Ventilation is designed and executed in such a way that the physical security of the object is not compromised.

The critical equipment cabinet is powered by an independent UPS system and shielded from external interventions. Air conditioning in an isolated room maintains constant air temperature for normal operation of the process system.

An external electrical supply from a diesel unit is maintained, which is reserved. In the event of a mains power failure, the system switches to an emergency power source (UPS and / or power). The work environment in the field of computer systems is monitored continuously and independently of other work areas.

The ventilation system is specially designed for such classrooms and does not compromise the physical and electromagnetic protection of this room as well as the normal operation of the installed computer components.

The registration authority is connected to the emergency power system of the TSP’s building.

### 5.1.4. Flooding

Measures have been taken to prevent flooding of the premises of SEP Bulgaria. A procedure for responding to problems related to a natural disaster or an industrial accident is implemented.

Moisture sensors in the premises with computer systems as well as in the entire building of the TSP are equipped with sensors for reading the moisture level. These sensors are integrated into the security system of the SEP Bulgaria building. The Security and the Contractor’s employees are instructed and obliged, in case of potential dangers, to immediately notify the relevant services, the security administrator and the system administrator.

### 5.1.5. Fire Prevention and Fire Protection

Measures were taken to detect and fire a fire in the premises used for the operation of SEP Bulgaria. A fire action procedure is in place. All rooms, depending on their type, are equipped with fire extinguishers in accordance with the regulations. In the sheltered premises and archives there is an automatic extinguishing system that switches itself on fire detection automatically.

The Critical Infrastructure Security Room is located in the building, with: sound and light fire alarm system, active fire alarm system with gas and stop gas button under complicated circumstances and evacuation. In the event of a fire, disconnection of the supply of the electric power to the equipment and extinguishing of the fire with gas is provided.

### 5.1.6. Data Media Storage
Depending on the sensitivity of the information stored on the media, archival and backup media are stored in fireboxes located in sheltered premises. Access to safes is provided by two keys held by authorized persons. Copies of this information shall be stored under the same conditions outside the main premises.

There is a system of physical and logical protection in the TSP's archive. SEP Bulgaria has taken serious steps against accidental or deliberate damage to data carriers.

Registration authorities are required to keep and store up-to-date information, including paper-based user documents, in safes. The storage period of the archive is 10 (ten) years and starts from receiving the information and concluding a contract with the consumer.

### 5.1.7. Waste Disposal

The TSP has established a procedure for destroying information and waste disposal. Paper and electronic media with sensitive data after expiration of the storage period shall be appropriately destroyed in such a way that it is not possible to know the information that was on them.

Cryptographic keys information and PIN / PUK numbers used for their storage are fragmented with appropriate devices. This applies to carriers that do not allow the permanent deletion of stored data and its reuse.

In certain cases, information from portable media is destroyed by deleting or formatting the device without recovery.

### 5.1.8. Lifetime of Technical Components

The lifetime of the physical elements in the composition of all critical components of SEP Bulgaria's infrastructure is complied with according to the manufacturer's prescribed operating requirements and after the intended operating period, they are decommissioned.

### 5.2. Organizational Control

This part of a Qualified Certification Service Practice presents a list of trusted roles that can be identified by SEP Bulgaria's staff. Also, this part describes the responsibilities and duties associated with each particular role.

All security procedures for issuing, administering and using Qualified Electronic Signature / Seal Certificates are performed by Trusted SEP Bulgaria Trusted Personnel.

The TSP maintains a sufficient number of Qualified Employees who, at all times, carry out their activities to ensure compliance with applicable laws and internal rules and regulations of the Company.

#### 5.2.1. Trusted Roles

SEP Bulgaria maintains trusted staff and develops job descriptions in line with the requirements of Regulation (EC) No 910/2014. A detailed distribution of the functions and responsibilities of the staff is outlined in the SEP Bulgaria internal documents: job descriptions, establishment plan and corresponding internal operational procedures.

The allocation of functions is done in such a way as to minimize the risk of compromise, leakage of confidential information or the occurrence of a conflict of interest.

#### 5.2.1.1. Trusted Roles - SEP Bulgaria

SEP Bulgaria maintains qualified employees of positions that ensure the fulfillment of its duties at all times in carrying out the activity of issuing, maintaining and managing qualified certificates in accordance with the regulations.

The contractor provides its own staff with some of its activities under SE Regulation (EU) No 910/2014, and SEP Bulgaria can also attract outsiders.

SEP Bulgaria has developed job descriptions for each of the trusted staff roles as follows:

1. Security Administrator - Full Responsibility in the Management and Implementation of System Security Procedures; Develops Security Policy; Take measures for technical protection of data and systems; Defines operational security measures; Performs...
direct control over compliance with the security requirements of the information systems by monitoring compliance with security procedures when installing, configuring, maintaining and modifying information systems or the network.
2. System Administrator - Responsible for installing, configuring and maintaining reliable service management systems: recovering the system as needed; Performing reconfiguration of devices and systems for the realization of new services or solutions; Monitoring the technical and software state of the servers and reporting irregularities;
3. System Operator - is directly responsible for the operation of the reliable technology systems of the TSP and for the backup of the system: creation and management of certificates for qualified electronic signature / printing, including the creation of a pair of keys - private and public for a qualified Electronic signature / seal; Using efficient technologies to ensure day-to-day operation of the system; Testing and checking for fail-safe operation and system security; Compliance with the technical requirements for work with the devices and in the event of a technical failure to notify the relevant officials;
4. System auditor - Storage, archiving and management of event logs (in particular for checking their integrity) when performing internal audits: Responding to the effectiveness of the internal audit; For the verification of compliance with Regulation (EC) № 910/2014; Responsibility on the activity of all registration bodies operating within SEP Bulgaria.

5.2.1.2. REQUIREMENTS FOR THE DIVISION OF RESPONSIBILITIES

The trusted activities of the Contractor's staff are performed by different individuals.

5.2.1.3. IDENTIFICATION AND AUTHENTICATION CERTIFICATION FOR EACH ROLE

Staff of SEP Bulgaria is subject to authentication and authentication in the following situations:
1. When included in a list of persons with restricted access to buildings of SEP Bulgaria;
2. When included in a list of persons with physical access to SEP Bulgaria's technological system and network resources;
3. Authorization to perform an assigned role;
4. Creating and assigning an account and password to the TSP's information system;

Any authorization to perform a particular role requires:
1. the role to be unique and directly related to the individual;
2. not be shared with another person;
3. be limited to the function resulting from the role and performed by a particular person. The role is implemented through the provision of software, a technological system and access to the SEP Bulgaria operating system. Proper role execution requires direct control of the job.

Operations performed in SEP Bulgaria, which require access to shared network resources, are protected by mechanisms introduced for strong authentication and encryption of transmitted data.

5.3. CONTROL OVER THE PERSONNEL

The staff of SEP Bulgaria consists of highly qualified employees. Trusted persons have the necessary professional background and experience to ensure that security requirements and technical security assessment standards are respected. Professional knowledge of information systems, cryptography and public key infrastructure enables employees with trusted roles to perform their duties properly.

Employees of SEP Bulgaria periodically take courses for further training, which corresponds to the contemporary requirements in the areas of activity of the TSP.

5.3.1. REQUIRED QUALIFICATIONS FOR THE PERSONNEL

The TSP shall ensure that the person who performs the trusted role of the certifying authority or of the registration authority system meets at least the following requirements for taking up the post:
1. has at least completed secondary education (unless otherwise required for the post);
2. Signed a work contract or other civil contract describing its role in the system and the respective responsibilities;
3. The necessary preparation has been carried out, relating to the scope of the duties and the tasks for his / her position;
4. Has been trained in the field of personal data protection;
5. Signed an agreement containing a clause on the protection of sensitive (from a security point of view of SEP Bulgaria) security and confidentiality of consumer data;
6. Does not perform tasks that may lead to a conflict of interest with the certifying authority and the registrant.

### 5.3.2. Inspection Procedures for the Personnel

Any new SEP Bulgaria employee who performs a trusted role is inspected by the TSP.
1. To confirm previous employment;
2. Checking personal recommendations;
3. Confirm the highest or the most appropriate educational level;
4. To check a criminal record;
5. Check your ID card.

In the case where the requested information is not available (for example, due to a law in force), SEP Bulgaria uses other techniques that allow information to be obtained.

SEP Bulgaria may reject an application relating to the performance of a trusted role or take action against a person who is already employed and performs a trusted role if it is established that:

a) has been deceived by an applicant or employee with respect to the data requested above;
b) received highly unfavorable or not very reliable recommendations from previous employers;
c) has received information about the applicant for a criminal past or has been convicted by an official with a valid and valid court decision.

In the event of any of the above cases, further steps shall be taken in accordance with the safety procedures of SEP Bulgaria and the applicable law.

### 5.3.3. Personnel Training Requirements of SEP Bulgaria

Staff who perform the functions and tasks arising from their employment in SEP Bulgaria or employment in the registration body (in the presence of an external registration authority) must undergo the following training:
1. Practice in the provision of qualified certification services by SEP Bulgaria;
2. Policy in the provision of qualified certification services by SEP Bulgaria;
3. Provisions, procedures and documentation related to the role played;
4. Security technologies and security procedures used by the certifying authority and the registering authority;
5. System software of the certifying authority and the registrant;
6. Responsibilities arising from roles and tasks performed in the system;
7. Procedures executed in the event of a system failure or interruption of the activities of the certifying authority.

### 5.3.4. Training Frequency and Requirements for Employees’ Skills Upgrading

Staff training is repeated:
1. The need to refresh and consolidate the knowledge and skills related to the fulfillment of the duties for the occupied position;
2. Over specified periods of time;
3. In case of substantial changes in the regulatory documents;
4. If a critical situation or incident is needed.

### 5.3.5. Change of Job

The practice of providing qualified certification services from SEP Bulgaria does not imply any requirements in this area.

### 5.3.6. Sanctions for Unauthorized Actions
In case of non-fulfillment of the duties for the respective position, SEP Bulgaria imposes disciplinary sanctions depending on the type and amount of the violation and in compliance with the applicable labor legislation.

In case of detection or suspicion of unauthorized access, the system administrator together with the security administrator or only the system administrator (employee of the Registration Authority, in the presence of an external Registration Authority) may terminate the access of the perpetrator to SEP Bulgaria or the system of the registering body. Further disciplinary action shall be consulted with the TSP's management.

### 5.3.7. Contract with the Employee

Persons or consultants (such as software developers or consultants) may enter into a contract to perform trusted roles in SEP Bulgaria. In such cases, they meet the same requirements applicable to employees assigned to SEP Bulgaria.

Under a contract, individuals or consultants are subject to the same verification procedure as the Contractor's employees.

### 5.3.8. Documentation Made Available to the Personnel

The management of SEP Bulgaria and the management of the registration body (in the case of an external registration authority) must provide their employees with access to the following documents:

1. Authentication policies;
2. Certification Practices;
3. Templates of requests, statements and declarations;
4. Extracts from documents corresponding to the role performed, including all urgent procedures;
5. Internal procedures and documentation for the respective position;
6. Procedures and controls related to information security;
7. User manuals for system software of MA and RO.

### 5.4. Event Records and Logs Maintenance

For effective control of activities and staff, SEP Bulgaria records all activities that have a significant impact on security.

For the effective management and operation of SEP Bulgaria, all events that have a significant impact on the security and reliability of the technology system, personnel and user control and the security impact of the qualified certification services provided are recorded.

Any party related in some way with the provision of certification services records the information and manages it adequately. Information records compile event logs and are stored in a way that enables authorized persons to access this information (for example, in resolving disputes between countries or detecting attempts to breach the security of SEP Bulgaria). Recorded events are copied and archived. Backups are stored in safes.

It is imperative that each group or team involved in the provision of qualified certification services maintains records of their activities and is responsible for their management in accordance with their position and duties.

Generating journal entries automatically. If this is not possible, events are recorded on paper. All records - automatic and on paper - are provided when conducting inspections of the activities of SEP Bulgaria.

The SEP Bulgaria Audit Team performs regular checks on compliance with the established mechanisms, controls and procedures in accordance with Practice in the provision of Qualified Certification Services, Regulation (EU) No 910/2014 and current national legislation. The audit team assesses the effectiveness of existing security procedures.

### 5.4.1. Record Types

SEP Bulgaria creates records for each activity within its infrastructure. Archival records can be encrypted and stored on media to prevent change or forgery.

All logs generated by the software components of SEP Bulgaria's information system are retained. Entries are divided into the following categories:

1. System records - contain information about system events;
2. Error records - contain protocol and application level error information;
3. Surveillance records - contain information related to qualified certification services, such as filing requests for qualified certificates, acceptance of certificates, issuance of certificates and lists of suspended and discontinued certificates. The above logs are common to any component installed on application servers or workstations. The size of the logs is predetermined and sufficient capacity is provided for normal operation of the systems. When you reach a certain size, new logs are created. Old ones are archived and deleted from operating systems.

Each entry, whether on paper or automatically generated, contains the following information:

a) Type of event;

b) Event identifier;

c) Date and time of the event;

d) Identifier or other data that allows the person responsible for the event to be identified;

e) A decision that corresponds to a successful or wrong operation.

Records can be:

(a) Alarms from firewalls and network sensors;

(b) Operations corresponding to registration, authentication / issuance, change of keys and renewal, termination, suspension / resumption and other services provided by the MA;

(c) Any change of hardware or software;

(d) Physical visit to the protected perimeters and disturbance of the protected perimeters;

(e) Change of PINs, passwords and personnel access rights;

(f) Successful and unsuccessful attempts to access the TSP's databases;

(g) Generation of keys for MAs and other infrastructure elements for the delivery of qualified certification services;

(h) Any request received in electronic form.

(i) All correspondence in electronic form between the TSP and the other participants in the certification process;

(j) History of archive copies of logs, systems, and databases.

Access to the logs has only the administrator and the persons performing verification of the TSP's activity. Records of old and up-to-date versions of Practice in the provision of Qualified Certification Services and Policy in Providing Qualified Certification Services are kept; Request templates, queries, work instructions, and more.

5.4.2. Frequency of records creating

Electronic journal information is generated automatically. In order to identify possible illegal activities, the security administrator, system administrators and the auditor shall analyze the information at least once within one business day.

The Security Administrator has the obligation to review and assess the accuracy and completeness of the registered events and check the compliance with the security procedures of SEP Bulgaria. Entries in the event log are reviewed in detail at least once a month. Each event is subject to explanation and is described in a log of events. The event log review process also includes checking for its falsification or change.

5.4.3. Period of record storage

Logs are stored on hard disks of information systems until a certain amount is reached. During this time they are available online for all authorized persons.

Upon reaching a certain size, the logs are archived. Archives are kept for at least 10 (ten) years.

5.4.4. Record protection

The log files are encrypted during archiving, with the backup key under the exclusive control of the security administrator. The log files can only be viewed by authorized persons and persons for whom the review and analysis of these files is a direct obligation. Access to log files is configured in a way that allows:

1. Only Authorized Inspecting Persons and Servant's employees may have the right to view the files;

2. Only the security administrator has the right to archive and delete files containing registered events;

3. Detection of any violation of data integrity and ensuring that each record is authentic (not falsified).
SEP Bulgaria applies the procedures for the protection of registered events in such a way that even after the logs are archived, it is impossible to delete records before the archive maintenance period expires.

5.4.5. KEEPING BACKUP COPIES OF EVENTS RECORDS

SEP Bulgaria monthly archives event logs and records for their review, analysis and statistics activities, exposed threats and measures. The archives are kept securely in an office of SEP Bulgaria with limited access. Archived copies that are in electronic form have a certified time of their creation.

The SEP Bulgaria Security Procedures require event logs to be backed up in accordance with a valid schedule, but not less than 4 times per year.

5.4.6. NOTIFICATION SYSTEM AFTER RECORDS ANALYSIS

SEP Bulgaria has developed a procedure for analyzing system event logs that allows you to review current events and automatically notify threats or security breakthroughs. In the case of activities that have an impact on system security, the security administrator and the system administrator are automatically notified. In other cases, the notification is directed only to the system administrator.

When critical information is transmitted to authorized persons, from the point of view of system security, situations are envisaged where the transfer is done through other, appropriately secured means of communication, such as mobile phone, e-mail.

Competent authorities have an obligation to take appropriate measures to prevent the detected threat.

5.4.7. VULNERABILITY AND ASSESSMENT

SEP Bulgaria as a qualified TSP and all persons providing qualified certification services on its behalf and on its behalf periodically assess vulnerabilities by analyzing internal procedures, applications and information systems.

SEP Bulgaria classifies and maintains registers of all assets in accordance with the requirements of ISO / IEC 27001: 2013. According to the "Security Policy" of SEP Bulgaria, an analysis of the vulnerability assessment of all internal procedures, applications and information systems is carried out. Analytical requirements may also be determined by an external institution authorized to audit SEP Bulgaria.

The risk analysis shall be carried out at least once a year. The decision to proceed with the analysis is done by the Executive Director.

The Security Administrator is responsible for conducting internal audits. It controls the security records in the logs, the correct archiving of the backups, the activities performed in case of threats and the compliance with the present Practice.

5.5. ARCHIVING

All data and files related to the registration of Qualified Certification Services users and the security of the systems, the information provided by the Holder / Creator, the issued Qualified Certificates, the CRLs generated, the keys used by the PO and all correspondence between SPE Bulgaria and the Owner / Creator, Or their authorized representatives are archived. Documents and data used to identify the Signatory/Creator and identity verification, respectively the identity of the Holder / Creator, are archived.

Documents presented in paper form, whenever possible, shall be converted into electronic format and archived.

SEP Bulgaria maintains electronic and paper archives. The archive is kept for 10 (ten) years.

Information about significant events is archived in electronic form periodically.

The TSP stores the archive in a format that allows playback and recovery.

5.5.1. TYPES OR ARCHIVES

SEP Bulgaria manages two kinds of archives: paper and electronic.

The following data is archived:

1. The information from the inspections and evaluations of the logical and physical protection of the MA and the RA and the public electronic register;
2. Database with the users of certification services;
3. Database of certificates;
4. Generated CRLs;
5. History of managing the keys of the MA of the TSP;
6. History of user keys, generation, delivery, destruction of archive copies after they are provided to the user;
7. Internal and external correspondence, in paper or electronic form, between SEP Bulgaria and the users of qualified certification services and PO;
8. Documents and data used in the identity verification process, respectively the Holder / Creator's identity

5.5.2. Period of archives storage

Archived data (paper and electronic) is kept for a minimum of 10 years. Upon expiration of this storage period, the archived data can be destroyed. Destruction of keys and certificates shall be subject to appropriate procedures.

5.5.3. Protection of archival information

SEP Bulgaria maintains resources and takes measures to maintain the integrity and accessibility of archive data. The measures include the following basic rules:
1. Only authorized persons in trusted positions have the right of access to the archives;
2. The archive is protected from modification by signing the records with an electronic signature / seal and the data being archived on single-entry media;
3. Maintain more than one copy of different, physically remote locations to protect against destruction of the archive;
4. To protect the archive from damage due to aging of the media on which it was recorded, the archive is periodically transferred to new media and the old ones are destroyed. Periodically replacing the bearers of the daily archives;
5. The format of the data and media to which a record of a record is stored or transferred shall be changed as necessary to protect against inability to use due to changes in technology, algorithms, data formats, and backup hardware;
6. Tools are maintained to access archives created in the past.

5.5.4. Recovery of archived information

It is essential for the proper functioning of SEP Bulgaria that it is possible for the backups to be fully restored (for example, after a system crash).
Detailed procedures for archiving, copying, and recovering the system after an accident are described in the Inside TSP technical documentation. This documentation is only available to authorized personnel and inspection bodies.

5.5.5. Requirements for the archiving time recording

The archival data is secured by certifying the exact time of signing.

5.5.6. Archiving storage

The system for collecting archive data is an internal system for SEP Bulgaria. An exception to this rule is the archives collected by the registrant.
The archive information (on paper and electronic media) is properly kept in a special safe in a room with a high degree of physical protection.

5.5.7. Archival information access and verification procedures
Access to the archive is only available to authorized employees of SEP Bulgaria after successful authentication and confirmation of the access rights. The data is periodically checked and compared to the original data to verify the integrity of the archived information. This activity is performed under the supervision of a security administrator, keeping records for each stage of the procedure. The results of the check shall be recorded in the relevant event logs. If damage or alterations to the original data are detected, the damage will be removed as quickly as possible, according to the internal procedures and rules in SEP Bulgaria.

5.6. TSP’S KEY CHANGE

The TSP may change the key corresponding to the issued operational certificate only by issuing a new certificate or renewing the current one with the "Re-Key". The private key of a certifying authority may be changed in case of:

- expiration of the validity of the accompanying certificate;
- introducing new services from SEP Bulgaria, which impose changes to the characteristics of the private key (for example, security-related changes and the requirement for new applicable cryptographic combinations).

Upon change of the private key of the Certification Authority of SEP Bulgaria, the following rules are observed:
1. The Certifying Authority, whose key is to sign User Qualified Certificates and whose key will be changed, shall suspend the issuance of certificates 60 (sixty) days before the moment the remaining period of validity of the private key is equal to the period of validity of the latter A certificate issued;
2. The Certifying Authority with whose private key is signed the CRL and whose private key will be changed continues to publish lists signed with the old private key until the expiration date of the latter Published certificate.

5.7. COMPROMISE OF KEYS AND RECOVERY AFTER ACCIDENTS

This part of a Qualified Certification Service Practice describes the procedures performed by SEP Bulgaria in case of accidents (including natural disasters) in order to restore customer service. These procedures are carried out in accordance with the "Disaster Recovery Plan" adopted by SEP Bulgaria. In the event of an accident or threat of occurrence of an accident, procedures have been developed to deal with these unusual situations and restore the normal work of the TSP. In the case of possible accidents, an analysis of the availability of the critical resources needed to restore the system is made. Current estimates of recovery costs are made. There are procedures for breakdowns with information technology and for accidents with business processes. For example, in IT, there are requirements for storing system hardware resources, system data storage requirements, and for storing specific (non-standard) hardware resources, distribution of workstations, the Internet, intranet, and n.

This plan is tested once a year and is subject to training by SEP Bulgaria employees.

SEP Bulgaria's disaster recovery plan was set up to ensure full recovery of all SEP Bulgaria functions within one week of a crisis affecting the main structures. The TSP tests his equipment in his structure to maintain the functions of the certifying authority and the registrant after a significant crisis that would stop the operation of the whole structure. The results of these checks serve for evaluation and planning activities. The aim is to restore the activity of the SEP Bulgaria structure as soon as possible, for example after a major crisis.

5.7.1. ACTIONS IN CASE OF ACCIDENTS

Security breaches of information systems are reported immediately after they have been detected by the security administrator responsible for their removal. Employees of SEP Bulgaria have the rights and obligations to make proposals and accordingly to report security suspected violations. Software faults are reported to the Security Administrator. Archival data containing information on requests for the issuance, management and termination of certificates as well as the records of all certificates issued in the database are kept in a secure and reliable place and available to the TSP upon request by the authorized persons in case of occurrence of an accident.

For Emergency Action SEP Bulgaria has developed a "Emergency Plan", which is checked once a year.
The TSP must be able to detect any possible incident. After analyzing what has happened, the goal is to prevent future incidents based on system mistakes or service and technology failures. To do this, the TSP monitors all systems and services uninterrupted (24x7 / 365) and also has a telephone for information and help on their website where users can report incidents or faulty services. The plan indicates the approximate time to detect any kind of incidents. SEP Bulgaria ensures that any potential incident can be detected. The TSP is able to distinguish a real incident from a false alarm. Serious accidents are reported to the Executive Director. The plan indicates approximate time for notification and confirmation. Defines roles and responsibilities. Gives an assessment of the type of incident, appropriate reaction time and follow-up action. Events are recorded. The causes of the incident are documented and how it has affected the performance of the work. Record the measures taken (response time and time to restore the service or system, etc.). Improvements are being offered. This plan specifies what kind of archiving is performed, at what intervals, where to store the information, and so on.

5.7.2. INCIDENTS, RELATED TO FAILURES IN HARDWARE, SOFTWARE AND/OR DATA

All the hardware, software and / or data theft is transmitted to the security administrator acting in accordance with internal procedures developed by SEP Bulgaria. These procedures are related to situation analysis, investigation of the incident, measures to minimize the consequences and to prevent such incidents in the future. In the event of hardware, software or data crashes, the TSP notifies users, restores the infrastructure components and, as a priority, resumes access to the Public Register and the CRL. In such cases, SEP Bulgaria has developed an Incident Management Plan. The TSP has a plan to manage all incidents that affect the proper functioning of the public key infrastructure. This plan is in line with the Business Plan, Continuity Plan and Disaster Recovery Plan.

5.7.3. COMPROMISE OR SUSPICION FOR COMPROMISE OF PRIVATE KEY OF THE CERTIFICATION AUTHORITY

The TSP takes maximum care within its capabilities and resources to minimize the risk of compromising the keys of its certifying bodies as a result of natural disasters or accidents. In the event of a compromise or suspicion of compromising a private key of a certifying authority of SEP Bulgaria, the following actions shall be taken:
1. The certificate of the operating certifying authority shall be terminated immediately;
2. The Certifying Authority generates a new key pair and a new certificate;
3. All users of Qualified Certificates shall be informed of what has happened immediately by means of the media (information on the TSP's website) and e-mail;
4. All relying parties are informed;
5. The certificate corresponding to the compromised key shall be placed on the CRL, together with an appropriate reason for termination;
6. All user certificates issued by the certificate corresponding to the compromised private key shall be terminated and recorded on the List of Suspended and Suspended Certificates, indicating the appropriate reason for their termination;
7. New qualified certificates shall be issued to the affected users;
8. New user certificates are issued at the TSP’s expense (users do not owe a fee);
9. Immediate analysis is carried out and report on the cause of the compromise.

These operations are carried out in accordance with the plan developed by the TSP for security incidents. This plan is being developed by a team of SEP Bulgaria headed by the security administrator and approved by the CEO of SEP Bulgaria.

5.7.4. BUSINESS CONTINUITY AND POST- DISASTER RECOVERY

SEP Bulgaria has developed a "Business Continuity Plan" for the occurrence of accidents, such as major system or network interruptions. This document draws attention to the preparation and processes to ensure that the TSP's business is maintained. The goal is to achieve continuity in the company's business and protect the business when large interruptions to normal business operations are available.

The security policy implemented by SEP Bulgaria takes into account the following threats, affecting the continuity of the services provided:
1. Physical destruction of SEP Bulgaria's systems, including network resources - this threat involves destruction of any, most often casual nature;
2. Software and application malfunction, missing / inaccessible data - these malfunctions are caused by malfunctions of operating systems and user applications as a result of malicious codes;
3. Loss of important network services - loss of power and physical disconnection of cables;
4. Damage to used hardware.
5. Compromise part of the network used by SEP Bulgaria to provide its services.

In order to prevent or limit the losses from the above threats, the security policy of SEP Bulgaria takes the following steps:

a) All users and relying parties should be informed as soon as possible and in a manner best suited to the situation;
b) Regularly create and archive copies of all components of the TSP's infrastructure that are stored in a well-protected and safe place;
c) A database backup is periodically created, which includes all submitted requests, issued, renewed and terminated certificates. Back up copies are archived and stored in a secure and safe place;
d) Periodically back up each server;
e) TSP’s private keys are separated according to security and secret sharing procedures. They are held by trusted persons in a safe and secure place;
f) Replacement of resources shall take place in a way that allows the retrieval of the most recent data.

System recovery procedures following failures are tested on each component of the TSP's technology system at least once a year. These tests are part of the internal audit.
Software update is only possible after intensive testing in a test environment and in strict compliance with the TSP's procedures. Any change in the system requires consent and acceptance by the security administrator.

For each system recovery after a disaster, the security administrator or system administrator shall perform the following:
(a) Modify all previously used passwords;
(b) Remove all rights to access system resources;
(c) Modify all codes and PIN numbers associated with physical access to the system's facilities and components;
(d) If recovery from the accident involves reinstalling the operating system and supporting software, all IP addresses in the system and its subnets change;
(e) Reviewing and analyzing the causes of disasters.

5.8. CESSION OF ACTIONS OF SEP BULGARIA

SEP Bulgaria informs the supervisory body and the clients about its intention to terminate the activity within the statutory deadlines, performing during this period a procedure aimed at minimizing the interruptions in the activity of the users and the relying parties.

5.8.1. REQUIREMENTS RELATING TO THE TRANSITION TO THE CESSION OF THE TSP

Before the certifying authority terminates its services, it is required to:
1. Notify the supervisory authority of its intention to terminate its services in the event of an action for declaring the company bankrupt, declaring the company invalid or otherwise requesting termination or winding-up proceedings. The notification should be made 4 (four) months before the agreed date of termination;
2. Notify (at least 4 months before) their users of the decision to terminate the services they provide;
3. Change the status of your certificates;
4. Cancel all user certificates within the stated period of termination;
5. Notify all their users about termination of services;
6. Makes commercially reasonable efforts to minimize distortion of consumer interests;
7. Compenses consumers. Compensations must be proportional to the remaining period of validity of the certificates;
8. Perform the necessary actions to enable the Supervisory Authority to maintain the CRL.

If the decision to terminate certification services concerns only the registrant (in the case of an external registration authority), it is obliged to:
a) Notify SER Bulgaria of its intention to terminate the registration activity. The notification should be made 4 (four) months before the agreed date of termination;
b) Submit to the TSP the complete documentation related to the users, including the archive and the collected audit data.
5.8.2. Transfer of Activities to Another TSP of Qualified Certification Services

To ensure the continuity of issuance of Qualified Certification Services, the TSP may sign an agreement with another qualified Certification Services TSP. In this case, the TSP:
1. Notifies the supervisory authority of its intention not later than 4 (four) months before the date of termination and transfer of the activity;
2. Make every effort and care to continue the validity of issued user certificates;
3. Notify the supervisory authority and the users in writing that its activity is being undertaken by another qualified qualified TSP as well as his name. The notice is published on the TSP’s website;
4. Notifies users of the conditions of maintenance of the transferred certificates to the receiving TSP;
5. Modify the status of the operating certificates and duly transmit all documentation related to their activity to the receiving TSP, together with all the archives as well as all issued certificates (valid, terminated and suspended);
6. Perform the necessary actions to transfer the information maintenance obligations to the receiving TSP;
7. Transfer the management of end-user certificates already issued to the receiving TSP;
The Receiving TSP assumes the rights and obligations of the Discontinued TSP and continues to manage the active certificates until the end of their action.
The archive of the End-of-Service TSP must be delivered to the TSP accepting the activity.

5.8.3. Withdrawal of SEP Bulagaria’s Qualified Status or the Qualified Status of the Trust Service

In case of cancellation of the qualified status of the TSP or of any of the Certification Services provided by the TSP, the TSP shall perform the following:
1. Notifies the users of the changed status of their services when the changed status enters into force;
2. Change the status of its operational certificates;
3. ceases to issue new qualified certificates but continues to manage the active certificates until the end of their validity;
4. Makes commercially reasonable efforts to minimize the disturbance of consumer interests.

6. Management and Control of Technical Security

This part of Practice in providing Qualified Certification Services describes the procedures for generating and managing cryptographic and related technical requirements.

6.1. Key Pair Generation and Installation

Key cryptographic keys for the TSP Operations Certificates are generated and installed in accordance with the instructions and procedures in this document. Generation is carried out by authorized persons from SEP Bulgaria. To create a signature, a security mechanism with a security profile defined in accordance with technical specifications defining security levels is used.
The TSP uses its private keys only for the purposes of its activities as follows:
• Signs the issued operational certificates of the certification bodies on its infrastructure;
• Signs issued and published CRLs;
• Signs all issued and published Qualified Certificates for Electronic Signature / Printing of Users.
The cryptographic pair of keys (private and public) of the issued electronic signature / seal certificates in the TSP’s infrastructure is generated as follows:
• by the Owner / Creator, with hardware and software under his control but approved by the TSP;
• by an operator of the TSP’s registering body, with hardware and software that is under the control of SEP Bulgaria’s infrastructure.
A digital signature / seal creation device with a security profile in accordance with Regulation (EU) No 910/2014 is always used to generate a pair of keys of a qualified electronic signature / seal certificate.
Only electronic signatures / seals created with a private key of a pair of keys generated in a qualified digital signature / print creation device have the character of a qualified electronic signature / seal.
The Signatory/Creator undertakes to use licensed software to work with an electronic signature / print creation device.
6.1.1. Generation of a Key Pair for a Certification Authority

The TSP generates cryptographic (RSA) pairs of the Base and Operations Certification Bodies using an HSM / Hardware Security Module with FIPS 140-2 Level 3 or above, or CC EAL 4+ or higher respectively. Authorized persons of the TSP's personnel perform the steps of generating, installing and storing the key pairs of the base and operational certification bodies, respectively eSign Sep Root CA and eSign Sep QES CA, according to a documented internal procedure agreed and approved by the SEP Bulgaria management. The procedure is carried out in the presence of the CEO of SEP Bulgaria and a notary. Before generating a base pair of keys, the TSP is prompted to access an HSM / Hardware Security Module by generating independently and independently of each other symmetric keys that are stored on smart cards protected by a Personal Identification Number PIN) to access. Each of the operator maps contains some of the cryptomodule access keys. To manage the Private Keys stored in Cryptomodule, two of three sets with the three roles of operator cards and the corresponding access PIN are required. Private key access codes are independently shared between authorized persons by SEP Bulgaria's staff, in view of the inability to personally activate the access to the respective private key. Established private keys of authentication authorities are kept securely and separately. Separate storage of private keys and individual access control of the private keys stored by the authenticator does not allow these keys to be compromised and / or unregulated reproduced outside the vendor.

6.1.2. Generation of a Key Pair for Signatory/Creator

The key pair of the Holder/creator of the qualified certificate for electronic signature/seal is generated only in an approved device TSP for creating an electronic signature/seal, checked for security and for successful work in the interfaces of the infrastructure of SEP Bulgaria's infrastructure. When the key pair is generated at the TSP, an electronic signature / print creation device is always in use. The private key of the generated key pair can not be output from the device. The control of the private key is through an access code. The Holder uses the private key to create a signature / seal by entering the device access code for creating a qualified electronic signature / print.

6.1.3. Delivery of the Private Key to the User

In the event that the Signatory/Creator or Authorized Entity explicitly states that the pair of keys is to be generated by the TSP, this is done in a secure and reliable manner and then the TSP provides the Signatory/Creator with access to an electronic signature / SSCD), subject to the order provided by the Certification Services Policy. Upon initial issuance of a certificate on an electronic signature / printing device before generating a pair of keys, the device is initialized and the following access codes are created: User ("User") and Administrative ("SO"). Codes are also created for personally accessing the private key and unblocking a blocked device. The initial user and administrative code for accessing and unblocking the device is provided to the Signatory/Creator or his person authorized in a sealed, opaque paper envelope. The Signatory/Creator is obliged to change his / her original user access code to the device using the software provided with it. SEP Bulgaria recommends the Signatory/Creator to periodically change his user code. In case of a certain number of unsuccessful attempts to enter a correct access code to the Owner / Creator's private key, access to it is blocked. In such cases, the Signatory/Creator must use the appropriate unblocking code provided.

6.1.4. Delivery of a Public Key by User to the TSP

It is executed only by the Signatory/Creator in which a pair of keys is generated and which should deliver its public key to the TSP for the purposes of the Qualified Certificate Issuance process. The Signatory/Creator delivers the public key of the generated key pair through the Signal Authority of the TSP via an electronic form requesting the PKCS # 10 format. The request contains a public key and has been signed electronically with the
corresponding private key. By checking the authenticity of the SEP signature, Bulgaria can also establish the authenticity of the public key that is sent.

6.1.5. Delivery of TSP’s public key to the relying parties

The public keys of the TSP are contained in the certificates of the Certification Authority of SEP Bulgaria in X.509 v.3 format. The certificates are published and available in the public register / store of SEP Bulgaria at: http://www.eSign.bg. Each Relying Party builds trust with the TSP by accepting and loading into the systems under its control the Operator's Certificates of the TSP.

6.1.6. Length of keys

The length of the base switch of ESign Sep Root CA is 4096 bits, with a combination of asymmetric and hash algorithms: sha2-with-RSA.

The length of the eSign Sep QES CA key pair of keys is 4096 bits, with a combination of asymmetric and hash algorithms: sha2-with-RSA.

The length of the SEP OCSP key pair of keys is 2048 bits, with a combination of asymmetric and hash algorithms: sha2-with-RSA.

6.1.7. Parameters of the public keys

The public key parameters are specified in the certificate that the TSP issues for this public key corresponding to the private key that is generated and stored in an electronic signature / print creation device. The Signatory/Creator of a key pair is responsible for verifying the quality of the generated private key parameters. It is required to verify the ability of the key to encrypt and decrypt, including creating an electronic signature and performing a check.

The environment used to generate and store the key components of SEP Bulgaria’s infrastructure is HSM with certified security level FIPS 140-2 Level 3 and CC EAL 4+, which meets the regulatory requirements. Devices for creating a qualified electronic signature / seal and the provided environment for generating and storing the Holder / Creator’s Keys are CC EAL 4+ and FIPS 140-2 Level 3.

6.1.8. Key usage

Parameters for using the key pair, specifically the private key, are contained in the certificate issued by the TSP using the keyUsage and extended keyUsage attributes that meet the X.509 v3 standard. The use of each attribute in the specified areas is consistent with RFC 5280.

6.2. Protection of private key and control over the cryptographic module

Each user, Certification Authority Operator and Registrar operator, creates and stores a private key using a secure system for its security. The Certification Authority generates a pair of keys upon request from the user and transmits them to a protected form by notifying them of the rules for storing and protecting their private key.

The private keys of the Certification Authority of SEP Bulgaria are stored in secure cryptographic modules that meet the regulatory requirements of Regulation (EU) No 910/2014. The installed cryptographic modules have the highest level of security, as required by international standards.

6.2.1. Cryptographic modules standards

The main components of the SEP Bulgaria eSign Sep OCSP infrastructure, eSign Sep QES CA and eSign Sep Root CA uses a FIPS 140-2 Level 3 Certified Security Module (HSM) that meets regulatory requirements. The device for qualified electronic signature creation, where the private key of the Signatory/Creator is generated and stored is with security level CC EAL 4 +/FIPS 140-1 Level 2 or higher.
6.2.2. Control over the usage and storage of private key

The private keys of the Certification Authorities of SEP Bulgaria are stored and used only in the HSM / Hardware Security Module and are accessible through access codes divided into several parts known to authorized persons by the TSP’s staff. The Base Certification Authority of the TSP is in Offline Mode. Simultaneously with the generation of a pair of keys of the authentication body, the procedure for storing the private key (or the pair of keys) is carried out in accordance with an established internal procedure. To manage the Private Keys stored in the Cryptomodule Private Key, two of three sets of three smart card roles and the appropriate Personal Identification Numbers (PIN) are required. Key archive is made initially - after all keys are created, and subsequently after some of them are regenerated. Archiving Private Security Keys (HSMS) with FIPS 140-2 Level 3 security level is performed on a device with the same level of security. Two of the three cryptosystem (HSM) access cards are required to make a key archive. Archiving takes place in a protected environment. After the Backup is created, it is placed in a safe at a remote location with the necessary security measures.

The Owner / Creator's private key is only used in an electronic signature / print creation device (as required by Regulation (EU) No 910/2014) and is accessible through a personal access code. Simultaneously with generating a pair of Keys / Creator keys, a private key is stored in an electronic signature / print creation device. The TSP does not in any way store or archive a private key of Signatory/Creator to create an electronic signature / seal, regardless of where the pair is generated.

6.2.3. Private key (escrow)

The private keys of the Certification Authority of SEP Bulgaria and of the users included in the Certification Authority of the TSP are not subject to escrow.

6.2.4. Private key storage

The Certifying Authority’s private keys are stored in separated parts on separate tokens with safety profile CC EAL 4+ or higher, whereas the access to each device is controlled with an access code by the relevant authorized person from the TSP’s personnel.

The separate storage of the Certifying Authority’s private keys on several tokens and the personal control over the access to these devices prevents the keys from being compromised or being subjected to unauthorized reproduction outside the TSP. The reproduction of the TSP private keys on a reserve crypto module after a defect on the operational one is made only in the presence of at least two authorized persons, each of which controls the access to his device.

SEP Bulgaria does not store copies of the private keys of the operators of the registering body. The TSP does not create copies of the private keys of the users. The owner / creator private key is only stored on a qualified digital signature / printing device and can not be played on another device. Upon defecting the qualified digital signature / printing device, the user must replace it and request the issuance of a new qualified certificate.

6.2.5. Private key archiving

The private key of the certifying authority used to create qualified electronic signatures / seal s shall be archived for at least 10 years after its expiry or after its termination. The same requirement applies to the authentication of the public key corresponding to the private key after expiration of its validity or after its termination. The expired or terminated TSP’s certificates must be electronically available for at least 10 years. SEP Bulgaria does not create archive copies of the private keys of the registering body and the private keys of the users.
6.2.6. TRANSFER OF THE PRIVATE KEY IN A CRYPTOGRAPHIC MODULE

Transferring a private key into a cryptographic module is done in the following cases:
1. For security, in the case of backups of private keys stored in a cryptographic module (e.g., in the case of a compromise or a malfunction of the cryptographic module);
2. When it is necessary to transfer the private key from the operative cryptomodule to another cryptomodule (in the event of an operational cryptomodule failure or destruction if necessary).

The private key transfer in the cryptomodule is a critical operation. Such an operation requires appropriate measures and procedures to prevent the disclosure of the private key or its change and counterfeiting during the execution of the operation.

The private key transfer in a cryptographic module requires the key to be restored from the cards of two of the three authorized employees in the presence of the Executive Director and a notary.

6.2.7. PRIVATE KEY STORAGE IN A CRYPTOGRAPHIC MODULE

Depending on the cryptographic module used, the private keys of the Certification Authority of SEP Bulgaria are stored in encrypted or unencrypted form. Regardless of the private key storage format, it is not available to unauthorized persons outside of the cryptographic module.

6.2.8. PRIVATE KEY ACTIVATION METHOD

The private key of the TSP is activated by a shared system access code, the individual parts of which are known to more than one authorized person in SEP Bulgaria. Only in the presence of these faces is access to the slot in the cryptographic module (HSM) enabled and the private key is activated after entering all parts of the access code.

The Private Holder / Creator Private Key is enabled by entering the user ID to access the location where the key is stored securely or by another means of identification with the same or higher security level.

6.2.9. PRIVATE KEY DEACTIVATION METHOD

A private key of a certification authority of SEP Bulgaria located in a cryptographic module (HSM) is deactivated by terminating the logical access to that key. Deactivation requires resetting the cryptographic module memory. This terminates the ability to access and use the private key. Any disabling of a private key is recorded in a log.

Private Holder / Creator key is deactivated by terminating logical access to the device to create a qualified electronic signature / seal or by physical destruction. This will permanently disable the access and use of the private key.

6.2.10. PRIVATE KEY DESTRUCTION METHOD

A private key of a certifying authority in a cryptographic module (HSM) is destroyed by deleting the key or slot. If necessary, the recovery media stored in the archive is also deleted. Any destruction of a private key is recorded in a log.

The owner / creator private key is destroyed by deleting it from the qualified digital signature / printing device or by physically destroying the device.

6.2.11. EVALUATION OF THE CRYPTOGRAPHIC MODULE

SEP Bulgaria uses a reliable cryptographic system (Hardware Security Module/HSM), certified for security level FIPS 140-2 Level 3.

6.3. OTHER ASPECTS OF THE KEY PAIR MANAGEMENT

The requirements described in this part of the “Practice in providing qualified certification services” are applied to the procedures for public keys archiving and the procedures describing the validity terms of the user keys and the certifying authority keys.
6.3.1. PUBLIC KEY ARCHIVING

The public keys of the certifying bodies are contained in the issued SEP Bulgaria Operational Certificates and are kept in an internal register. Public keys are accessible to trusted parties and users by posting certificates in the repository on the TSP's website.

The public keys of the certifying bodies shall be archived and stored for at least 10 years after the expiry of the period of validity or the termination of the relevant certificates. The purpose of archiving the public key is to enable an electronic signature / seal check after the certificate has been removed from the public register of valid certificates. This is extremely important in the case of checking the status of the certificate.

Public Keys of Owners / Creators are contained in the certificates issued for them that are published in a public register on the TSP's site and stored in a repository. Public Keys of Owners / Creators are stored and periodically archived in the repository.

Any public key archive or any logical and physical destruction of a public key is recorded in a log.

6.3.2. VALIDITY PERIOD OF A QUALIFIED CERTIFICATE AND USAGE OF KEYS

The period of use of public keys is determined by the value of the field in its certificate describing the validity of the public key. The certificates validity and their corresponding private keys may be shortened in case of certificates' termination.

Maximum periods of use of qualified certificates:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>eSign Sep Root CA</td>
<td>20 (twenty) years</td>
</tr>
<tr>
<td>eSign Sep QES CA</td>
<td>10 (ten) years</td>
</tr>
<tr>
<td>eSign Sep OCSP</td>
<td>10 (ten) years</td>
</tr>
<tr>
<td>eSign Sep TSA</td>
<td>10 (ten) years</td>
</tr>
<tr>
<td>eSign QES Natural</td>
<td>3 (three) years</td>
</tr>
<tr>
<td>eSign QES Delegated</td>
<td>3 (three) years</td>
</tr>
<tr>
<td>eSign QESeal</td>
<td>3 (three) years</td>
</tr>
</tbody>
</table>

When a signing key is used after its certificate's expiration, the signature is invalid.

Six months before the expiry of a Certification Authority’s qualified certificate, the TSP shall issue a new qualified certificate and generate a new key pair. The certificate shall be made public in accordance with the procedures described in this document.

6.4. ACTIVATION DATA

When the user is personally present at the Registration Authority, the private key activation data is used mainly by an operator of the Registration Authority. Users use authentication and access control to their private key.

In cases where the Signatory/Creator generates a key pair for a qualified certificate, they themselves create and manage the activation data.

6.4.1. GENERATION AND INSTALLATION OF ACTIVATION DATA

Activation data are used in the initial issuance of a certificate, on a signature/seal creation device, before a key pair generation. In this case, the device is initialized and access codes are created: User (“User”) and Administrative (“SO”). These codes allow personal access to the private key in the device and, if necessary, to unblock it.

The codes for access and unblocking the device for qualified electronic signature/seal creation is provided to the Signatory/Creator or a person authorized thereby in a sealed, opaque paper envelope.

The Signatory is obliged to change the initial User access code through the software provided with the device.

The TSP recommends the Signatory/Creator to periodically change its User access code to the device for the creation of the qualified electronic signature/seal.

The Signatory/Creator should use the Administrative access code to unblock a blocked device.
6.4.2. ACTIVATION DATA PROTECTION

The Signatory/Creator is obliged to store and keep from compromising the access codes to the qualified electronic signature/seal creation device. Users should know that upon several unsuccessful attempts to access the device, it is blocked (locked). In such cases, the user must use the provided Administrative access code to unblock the device. The TSP recommends the device activation data never to be stored together with the device itself.

6.4.3. OTHER ASPECTS OF ACTIVATION DATA

Activation data must always be kept in a single copy. The personal identification number (PIN) for the access must be periodically changed. Activation data can be archived.

6.5. COMPUTER SYSTEMS SECURITY

SEP Bulgaria only uses reliable and secure hardware and software that are part of the TSP’s computer system. The computer systems, which operate all critical components of SEP Bulgaria's infrastructure, are equipped and configured with means of locally protecting access to software and information data. The TSP uses information security management procedures for all SEP Bulgaria infrastructure in accordance with generally accepted international practice. The computer systems realize the following controls:
1. Required operating system authentication and system application;
2. Keeping a journal on the actions of the operators;
3. The access to the systems is only performed by duly empowered employees of SEP Bulgaria;
4. Cryptographic control to protect exchanges and databases.
For greater reliability and security of the systems used, the technical and cryptographic security of their processes, the TSP performs a number of tests and inspections of the technical equipment and the used technologies. Tests and checks of computer systems are performed according to a security assessment methodology (regarding: processor status - consumption, load, use, storage status, memory status - basic, padding in-out, storage status, Load balancing). They are performed both periodically and with any change affecting the security of the infrastructure. For security management of computer systems in SEP, Bulgaria takes into account the requirements of ISO / IEC 27001: 2013.

6.5.1. DEGREE OF COMPUTER SECURITY

The degree of security of the systems used in the SEP Bulgaria infrastructure complies with the regulatory requirements for the performance of the TSP's activities and is determined by the SEP Bulgaria Security Policy document.

6.6. IT SYSTEM’S LIFECYCLE SECURITY

6.6.1. DEVELOPMENT CONTROLS OF THE IT SYSTEM

The software applications used in SEP Bulgaria's technological system have been developed and implemented by highly qualified specialists. Before the introduction of new applications, they pass through the test period. The tests are made on separate systems, independent of those in regular operation. All hardware changes are monitored and registered. When purchasing new technical equipment, it is supplied with the necessary operating procedures and instructions for use. The technological security of the system is guaranteed as follows:
- Technological equipment is delivered in a way that allows its tracking. An estimate of the route from the initial point to the location of its installation is made;
- Delivery and replacement of technological equipment is done only with original hardware. The change is done by trusted and trained staff

6.6.2. CONTROLS FOR THE IT SYSTEM SECURITY MANAGEMENT

The purpose of the security management control is to supervise the functionality of the technology system and ensure that it functions properly and in accordance with the supplied production configuration.
The current configuration of SEP Bulgaria's technological system, as well as all changes and updates of the system, are recorded and performed under control. The controls allow continuous checks of the technological system integrity, timely updating, and troubleshooting.

6.6.3. IT SYSTEM SECURITY LIFECYCLE ASSESSMENT

The “Practice in the provision of qualified certification services” does not imply any requirements in this area.

6.7. NETWORK SECURITY

In SEP Bulgaria's infrastructure, modern technical means of information exchange and protection are used to ensure the network security of the systems against external interventions and threats.
Servers and critical technology of SEP Bulgaria are connected to an internal LAN.
The remote access to the network infrastructure (PKI) is performed by a specially installed and configured VPN server which accepts authentication through a special name and password, issued for this purpose to authorized persons involved in the issuance of electronic signature/seal and infrastructure administration (Public Key infrastructure/PKI).
The computer system of the TSP is protected against denial of service in case of attacks. Security control has been developed on the basis of a firewall and filtering the traffic of routers and proxy services. Attempts to penetrate the system are monitored through the built IDS / IPS system. All Intrusion or Potential Penetration Alarms, as well as Denial of Access attacks, are sent to the system administrator for analysis.
Attempts for unauthorized access to the system are documented by the Intrusion Prevention System (IPS).
A detailed description of the SEP Bulgaria's network configuration and the TSP's remedies are provided in the technical documentation of the infrastructure. This documentation has "internal" status and is accessible only to authorized persons.

7. PROFILES OF QUALIFIED CERTIFICATES, CRL AND OF OCSP

The profiles of the user qualified certificates and of the List of cancelled and revoked certificates (CRL) correspond to the format described in the ITU-T X.509 v.3 standard. A certificate of the X.509 v.3 type is a set of data which unequivocally certifies the public key belonging to the author of the qualified electronic signature/seal. The OCSP profile complies with RFC 2560,

7.1. PROFILE OF QUALIFIED CERTIFICATES

In accordance with X.509 v.3 standard, the electronic certificate is a sequence of the following fields:
1. Version: version of the certificate (X.509 v.3);
2. SerialNumber: unique identification code of the certificate;
3. SignatureAlgorithm: identifier of the algorithm for the electronic signature creation;
Issuer: distinguished name of the certificate issuer (DN);
Validity: validity period, described by the date and time of the certificate issuance (notBefore) to the date and time of certificate's expiry (notBefore) (universal coordinated time, presented in Zulu format);
6. Subject: distinguished name (DN) of the Signatory/Creator, subject to entry in the certificate;
7. SubjectPublicKeyInfo: identifier of the key;
8. SignatureAlgorithm: identifier of the algorithm used by the issuing certifying authority to sign the certificate in accordance with RFC 5280;
9. SignatureValue: the electronic signature of the certificate. (Calculated on all fields in the main field: version, serialNumber, signature, issuer, validity, subject, subjectPublicKeyInfo, using signatureAlgorithm).

7.1.1. VERSION

All certificates issued by SEP Bulgaria are in compliance with version 3 (X.509 v.3).

7.1.2. ELIGIBLE EXTENSIONS IN THE FORMAT OF QUALIFIED CERTIFICATES

The values of the extensions are created in accordance with the RFC 5280 recommendation. The function of each extension is determined by the standard value of the respective object identifier (IDENTIFIER):
1. Subject Key Identifier - formed as a hash value of the Public Key of the Signatory/Creator;
2. Authority Key Identifier - formed as a hash value of the public key of the Operator Certification Authority of the TSP;
3. Issuer Alternative Name - contains a URL string as an alternate name for the TSP;
4. Basic Constraints - Specifies the type of certificate and has the value "End entity" in the user certificate;
5. Certificate Policy - Identifies the Qualified Qualified Enabled Qualified Signature / Printing Qualification Policy Identifier;
6. Key Usage - defines the purposes for which the certificate key can be used. This imposes restrictions on the checks that can be made through the public key of the certificate. This extension allows you to distinguish the use of different keys. Possible values are:
   • digitalSignature: for checking electronic signature / printing;
   • nonRepudiation: to ensure the fact of electronic signature / printing;
   • keyEncipherment: for secure key exchange;
   • dataEncipherment: for encryption of data;
   • keyCertSign: to verify electronic signature / certificate printing;
   • cRLSign: to check the electronic signature of CRL;
   • The Key Usage extension is critical.
7. Enhanced Key Usage - Defines the applications for which the certificate key can be used. This extension specifies one or more areas in addition to the Key Usage field for acceptable use of the certificate. These areas should be interpreted as a limitation on acceptable use. There is one or a combination of several of the following:
   • serverAuth: for TLS WWW server authentication. Compatible with digitalSignature, keyEncipherment or keyAgreement;
   • clientAuth: for TLS WWW authentication for a client. Compatibility with digitalSignature and / or keyAgreement;
   • codeSigning: for signing executable code most commonly distributed over the Internet DigitalSignature Compatibility;
   • emailProtection: to protect E-mail. Compatibility digitalSignature, nonRepudiation, and / or (keyEncipherment or keyAgreement);
   • timeSeal: attaches hash to an object at a specific time. Compatibility with digitalSignature and / or nonRepudiation;
   • OCSPSigning: Signing of OCSP Response Compatibility with digitalSignature and / or nonRepudiation;
   • This extension is not critical. With both the Key Usage and Enhanced Key Usage extensions, the two extensions are handled by the app individually and the certificate is used for purposes that are compatible with both extensions. Otherwise, it is not used for any purpose.
8. CRL Distribution Point - contains a link to the current CRL of the Operator Certification Body of the TSP;
9. Authority Information Access - contains the URL of the OCSP certificate server;
10. Qualified Statements - the attribute contains an indication that the certificate is qualified and indicates whether the private key is generated and stored on an electronic signature creation device (QSCD).

7.1.3. IDENTIFIERS OF ELECTRONIC SIGNATURE/SEAL ALGORITHMS

The "Signature algorithm" attribute identifies the algorithms (cryptographic mechanisms) that are used. In SEP Bulgaria, a relevant combination of asymmetric and hash algorithms is used: sha256-with-RSA and sha384-with-RSA.

7.1.4. NAMING FORMS
The naming forms are described in the “Types of names” part of this document.

**7.1.5. RESTRICTIONS ON NAMES**

The types of restrictions on the names are described in the “Types of names” part of this document.

**7.1.6. POLICY IDENTIFIER**

A qualified certificate issued in accordance with the SEP Bulgaria Policy, which fits into the attribute “Certificate Policy” of the certificate.

**7.1.7. EXTENSION IDENTIFIER**

This identifier (“Extensions”) provides a specific information related to the service. For its use at this stage the Practice sets no restrictions.

<table>
<thead>
<tr>
<th>Certification Authorities</th>
<th>Policy object Identifiers (O.I.D.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eSign Sep Root CA</td>
<td>1.3.6.1.4.1.30299.3</td>
</tr>
<tr>
<td>eSign Sep QES CA</td>
<td>1.3.6.1.4.1.30299.3.1</td>
</tr>
<tr>
<td><strong>End user certificate profiles</strong></td>
<td><strong>Policy object Identifiers (O.I.D.)</strong></td>
</tr>
<tr>
<td>eSign Sep OCSP</td>
<td>1.3.6.1.4.1.30299.3.1.1</td>
</tr>
<tr>
<td>eSign Sep TSA</td>
<td>1.3.6.1.4.1.30299.3.1.2</td>
</tr>
<tr>
<td>eSign QES Natural</td>
<td>1.3.6.1.4.1.30299.3.1.3</td>
</tr>
<tr>
<td>eSign QES Delegated</td>
<td>1.3.6.1.4.1.30299.3.1.4</td>
</tr>
<tr>
<td>eSign QESeal</td>
<td>1.3.6.1.4.1.30299.3.1.5</td>
</tr>
</tbody>
</table>

**7.1.8. DESIGNATION OF THE QUALIFIED CERTIFICATE**

SEP Bulgaria, in the qualified certificate with profile under the X.509 v.3 standard, uses the “Qualified Statements” attribute with identifier: “esi4-qcStatement-1” (OID=0.4.0.1862.1.1).

SEP Bulgaria, in the qualified certificate for qualified electronic signature with profile under the X.509 v.3 standard, uses the “Qualified Statements” attribute with identifiers: “esi4-qcStatement-1” (OID = 0.4.0.1862.1.1) and “esi4-qcStatement-4” (OID=0.4.0.1862.1.4).

**7.1.9. USING AN IDENTIFIER FOR AN EXTENSION OF THE “CRITICAL” KEY**

In practice there is no requirement to use the „CRITICAL CERTIFICATE EXTENSIONS“.

**7.2. PROFILE OF THE LIST OF CANCELLED AND INTERRUPTED CERTIFICATES (CRL)**

**7.2.1. VERSION**

SEP Bulgaria, through its Certification Authority issues, publishes and maintains Lists of cancelled and revoked certificates (CRL) in the X.509 v.2 format. The version is entered in the issued CRL.
7.2.2. FORMAT

SEP Bulgaria issues, publishes and maintains a list of cancelled and revoked certificates (CRL), whose format is consistent with the requirements of the international recommendation RFC 5280. The SEP Bulgaria Certification authority issues, publishes and maintains separate full lists (CRL-s) recording therein only cancelled certificates issued by the relevant Certification authority.

7.2.3. BASIC ATTRIBUTES OF THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL)

1. Version – version of the list of cancelled and revoked certificates (CRL);
2. Issuer Name – name of the List issuer (Certification authority);
3. Effective Date/This update – date and time of the List (CRL) issuance;
4. Next Update - time of the CRL validity. After that time, the Certifying authority shall immediately issue a new list. During the period of validity, in the event of cancellation/revocation of a certificate, the Certifying authority automatically issues a new CRL;
5. Signature algorithm – identifier of the algorithm for creation of an electronic signature of the CRL;

7.2.4. ADDITIONAL ATTRIBUTES TO THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL)

“Authority Key Identifier” – identifier of the Certifying authority, issuing and signing the List of cancelled and revoked certificates (CRL), contains the meaning of “subjectKeyIdentifier” from the certificate of the Certifying authority.

7.2.5. FORMAT OF AN ELEMENT FROM THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL)

The list of cancelled and revoked certificates (CRL) of the Certifying authority contains elements of all cancelled certificates. These elements are constant in the List.
The List of cancelled and revoked certificates (CRL) of the Certifying authority contains an element for each certificate cancelled by the Certifying authority. This element is temporary in the list until the certificate resumption.

7.2.5.1. ATTRIBUTES OF AN ELEMENT IN THE LIST OF CANCELLED AND REVOKED CERTIFICATES (CRL)

1. Serial number - serial number of a cancelled certificate;
2. Revocation date - time of the certificate cancellation/revocation;
3. CRL Reason Code - code identifying the reason for cancellation/revocation.

7.2.5.2. INDICATIONS OF THE REASON FOR A CERTIFICATE’S CANCELLATION/REVOCATION

1. keyCompromise - compromised private key of a Signatory/Creator;
2. ACompromise - compromised private key of the SEP Bulgaria operational Certification Authority;
3. affiliationChange - changed status of the Signatory to another person – change in the representative power, withdrawal of representative powers, termination of employment, etc.;
4. superseded - the certificate has been superseded by another one;
5. certificateHold - the certificate is temporarily suspended

7.3. PROFILE OF A RESPONSE FOR ONLINE VERIFICATION OF A CERTIFICATE STATUS (OCSP/ONLINE CERTIFICATE STATUS PROTOCOL)

SEP OCSP Validation Authority of SEP Bulgaria operates and provides the qualified online verification service for real-time certificate status in accordance with the internationally approved IETF RFC 6960 recommendation.
The reply contains information on the status of the inspected electronic signature/seal certificate, the validity period of the reply and has a testimonial character. The OCSP server which issues confirmations about the state of the qualified certificates has a specially generated key pair, issued especially for that purpose.

8. CHECKING AND CONTROL OF TSP’S ACTIVITY

The inspections carried out in SEP Bulgaria aim to control the Practice in providing certified certification services to what extent it is compatible with the integrated management system that includes the requirements of IEC 27001: 2013, Regulation (EC) No 910/2014 and internal management decisions And measures. Verification by the TSP applies to all certification bodies belonging to the underlying certification authority, the registrant, and other elements of the public key infrastructure, such as an OCSP server. SEP Bulgaria periodically performs full or partial inspections of individual activities and / or infrastructure units for the provision of qualified certification services.

SEP Bulgaria is audited at least once every 24 months by a Conformity Assessment Body. The purpose of the audit is to confirm that the Qualified Certification Services TSP and the Qualified Certification Services provided by it meet the requirements set out in Regulation (EU) No 910/2014. The TSP shall submit the relevant compliance assessment report to the supervisory authority within 3 (three) working days after receiving it.

The Authority may at any time carry out an audit or request the Conformity Assessment Body to assess the compliance of the TSP.

8.1. AUDIT FREQUENCY

The SEP Bulgaria management appoints periodic checks on the current activity compliance with the established Certificate Policy and Certification Practice Statement regarding the operation of SEP. The SEP Bulgaria's management carries out constant operational control for the accurate execution of the instructions at work given by SEP Bulgaria's personnel.

8.2. QUALIFICATION OF THE AUDITORS

External audit is conducted by an accredited and independent of SEP Bulgaria Conformity assessment body. Auditor accreditation and competence system are specified in Regulation (EC) No 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 and is regulated by ISO/IEC 17065:2012: Conformity assessment - Requirements for bodies certifying products, processes and services. External inspection by a supervisory body is carried out at any time by authorized employees of the Supervisory body - the Communications Regulation Commission.

The internal audit is performed by SEP Bulgaria employees with the necessary experience and qualification. For the purposes of auditing, SEP Bulgaria has hired and authorized employees who possess the necessary technical knowledge related to public key infrastructure, with the reliable and secure operation of the technology system, information security, as well as the presence of a large practical experience in auditing.

8.3. RELATIONSHIP OF VERIFIERS WITH TSP

Verifiers must be independent, not directly or indirectly related to, and have no conflict of interest with the TSP. The relations between the TSP and an external verifier are governed by a contract.

8.4. AUDIT SCOPE

The inspection by the Supervisory body covers the statutory requirements for the activities of the TSP according to the applicable legislation in the sector of qualified certification services.

The audit by the Conformity Assessment Body covers the entire the TSP operation for the provision of qualified certification services and implementation of all standards and standardization documents related to Regulation (EU) No 910/2014:
8.5. ACTIONS TAKEN AS A RESULT OF THE AUDIT CONDUCTED

The reports of internal and external audits are submitted to SEP Bulgaria.
The report of the Conformity Assessment Body shall be submitted to the Supervisory Authority within 3 (three) days of its handing over to the SEP Bulgaria management.
Based on the assessments made in the report, SEP Bulgaria Management shall outline measures and deadlines to remedy the identified gaps and inconsistencies.
SEP Bulgaria personnel undertakes specific actions for their removal within the specified deadlines.

8.6. AUDIT RESULTS STORAGE

The results of the performed internal and external audits are properly kept in the TSP archive.
The certification document received by the Conformity Assessment Body may be posted on the TSP’s website.

9. OTHER BUSINESS CONDITIONS AND LEGAL ASPECTS

9.1. PRICES AND FEES

SEP Bulgaria maintains a webpage "Prices": http://www.eSign.bg/bg/facts/.
The TSP has the right to unilaterally change the Tariff at any time during the term of Contract, and shall notify the Signature Owner/Creator of a seal by publishing the changes on its website.
The change shall be effective for the Signature Owner/Creator of a seal on the day following the day of publication.
Within 5 (five) days from the date of the change, and as far as an increase in the price has occurred, the Signature Owner/Creator of a seal is entitled to unilaterally terminate the Contract by giving a written notice to TSP, as from the date of expiry of the last certificate. In this case, the contract is deemed to have been canceled as of the date of the change and the remuneration paid under the contract for the use of the services shall not be refundable. In the absence of a notice of termination, it is considered that the Signature Owner/Creator of a seal agrees to the change.
The change in the remunerations may not affect remunerations already paid.

9.1.1. FEES

The contract value may include one or more of the following fees:
1. fee for the issuance and maintenance of a qualified certificate;
2. fee for renewal of a qualified certificate;
3. fee for consultations and technological assistance made at the request of the Signature Owner/Creator of a seal;
4. price for equipment purchased or leased by SEP Bulgaria;
5. fee for personalization of physical media;
6. other fees for qualified certification services provided.

Fees and amounts payable shall be paid to TSP in the amounts, according to the Tariff of Qualified Certification, Information, Cryptographic and Consultancy Services provided by SEP Bulgaria and within deadlines in manner as specified in the Contract and its annexes thereto.
As far as there is an agreed advance or subscription fee for the use of a service, it is shall not be refundable if the Signature Owner/Creator of a seal has not consumed the service provided during the relevant period to which the advance or subscription fee relates.
The price does not include the amounts accrued by telecommunications companies in connection with their services used by the Signature Owner/Creator of a seal for the purposes of the services provided by the TSP. These shall be payable entirely by the Signature Owner/Creator of a seal to the relevant telecommunications company. The TSP shall not be held liable and responsible for the payment of these amounts.

All costs and fees for the transfer of the amounts due on the account of the TSP are at the expense of the User.

9.1.2. FEES FOR CERTIFICATION, CRYPTOGRAPHIC, INFORMATION AND CONSULTANCY SERVICES

For the services to provide and use Qualified Certificates and related services, a due amount shall be paid when requesting the service. In the other cases, the payment shall be made within 1 week of receipt of the invoice or according to the contract concluded.

The services related to the provision of technological assistance and consultancy for the construction and maintenance of an infrastructure and information security solutions shall be charged on a „man-hour“ basis and shall be paid on the basis of a bilaterally signed protocol for the work performed. The prices of the hourly rate in the annexed Tariff are valid within the established working time. When working outside the established working time, the prices shall be increased by an appropriate percentage, according to the Tariff.

The service “Issuance of Qualified Electronic Time-seal s” at an agreed service level shall be paid according to the contractual terms.

The cost of equipment purchased or leased by the TSP shall be negotiated and shall be due under the terms of the contract. The legal relationship between the TSP and the Signature Owner/Creator of a seal shall be governed by the general rules of the Sale contract, respectively the Lease contract.

In case of delay of payments after the agreed term, the User shall owe to the TSP the statutory interest for the period until the final payment of the amounts due.

The use of documents published on the website of the TSP is free of charge. For recording and delivery of these documents on a physical medium, the cost of this medium and the courier charges shall be paid.

9.1.3. INVOICING

The TSP shall issue an invoice to the User for services provided. Failure to receive an invoice does not relieve the User from its obligation to pay the due fees within the agreed deadlines.

All amounts due under the Contract shall be paid by the User in cash or by bank transfer. Payment by bank transfer shall be deemed to be made after the bank account of the Supplier is credited with the full amount due.

All bank commissions, fees and expenses in connection with the bank transfers shall be borne by the User.

9.1.4. RETURN OF CERTIFICATE AND RECOVERY OF PAYMENT

A Signature Owner/Creator of a seal can object to the inaccuracy or incompleteness in the contents of a certificate within 3 days after its publication in the Public Register.

If the cause of the false content of the certificate lies with the Registration Authority, the TSP shall terminate the certificate and shall issue a new one free of charge, with a correct content, or shall recover the payment made for the terminated certificate with the false content.

If the cause of the false content of the certificate is incorrect presentation of data by the Signature Owner/Creator of a seal, the TSP shall terminate the certificate and shall not recover the payment made. The TSP may issue a new certificate with correct content, to the User’s expense.

The User may refuse to accept a qualified certificate issued with true content. In this case, the TSP shall terminate it immediately, without recovering the payment made.

9.1.5. FREE SERVICES

The TSP shall provide free registration and information services related to the use of the Public Register/storage, as follows:

1. check-up of the status of a certificate in real time;
2. download a current Certificate Revocation List (CRL) and access to CRL archive;
3. download the operating certificates of the Suppier;
4. download the public documents of the Suppier;
5. other services

9.2. FINANCIAL RESPONSIBILITIES

The financial liability of any person involved in the activity of providing and using a Qualified Certification Service shall be indicated by mutual agreement.
SEP Bulgaria is financially responsible for users of certification services that rely on its business.
The TSP’s financial liability only applies if the damage is caused by SEP Bulgaria or the parties with which it has entered into an agreement.
If SEP Bulgaria acknowledges and agrees that damages have occurred, it shall undertake to pay the damages. The maximum payment limit may not exceed the amount of the damages.

9.2.1. INSURANCE OF ACTIVITIES

SEP Bulgaria shall take out a compulsory insurance of its activity as a TSP of qualified certification services.
The compulsory insurance shall be for a continuous period and shall be renewed annually.
The subject of the insurance is the liability of the TSP to perform its activities according to the requirements of the national legislation.
The compulsory insurance covers the responsibility of the TSP to Signature Owners/Creators of a seal, respectively the “Relying Parties”, for material and non-material damages caused up to the limits defined by the national legislation.
Upon occurrence of an event that may allow making a claim covered by the insurance, the person concerned must notify the TSP and the insurer in writing within 7 days after becoming aware of the event.

9.2.2. INSURANCE COVERAGE

The insurance coverage for any non-material and/or material damage suffered by a Signature Owner/Creator of a seal shall not exceed the amount established by the national legislation.
The insurance shall not cover cases of waiver of responsibility, in particular for damages caused by:
1. non-compliance of a Signature Owner/Creator of a seal;
2. compromise or loss of private key of a Signature Owner/Creator of a seal due to the failure to exercise the due care to protect the key during use;
3. non-compliance with requirements to verify the validity of the electronic signature/seal and the Qualified Certificate by a Relying Party
4. force majeure and other circumstances beyond the control of the Suppier.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

SEP Bulgaria ensures that the collection, processing and storage of information during its activity as a TSP of qualified certification services is in accordance with the national legislation.
SEP Bulgaria ensures that the Relying parties have access only to the information that is publicly available in the Public Register/repository.

9.3.1. SCOPE OF CONFIDENTIAL INFORMATION

SEP Bulgaria accepts as confidential the information contained in or relating to:
1. The Signature Owner/Creator, except the published data in the certificate;
2. Contract for Qualified Certification Services;
3. The reason for suspension or termination of qualified certificates, beyond the published information about the status of the certificate;
4. Correspondence related to the activity of SEP Bulgaria as a qualified TSP of certification services;
5. The official keys of SEP Bulgaria;
6. Archives for requests for issuance, suspension, revocation and termination of qualified certificates;
7. Archives of Transactions;
8. Records of external and internal controls and reports;
9. Disaster recovery plans and contingencies.
Confidential information is collected by the TSP only to the extent necessary for the purposes of issuing and maintaining the certificates.
The confidential information may not be disclosed to third parties without the explicit consent of the Signature Owner/Creator of a seal, except in cases where the TSP is required by law.
The TSP may collect additional information that is also not included in the certificates but is used for the purpose of qualitative maintenance of qualified certification services.
Confidential information is kept on-site, access restricted to persons from the Contractor's personnel authorized to operate with the data and disclosed only with the explicit consent of the Signature Owner/Creator, except in cases where the TSP is obliged by law.

9.3.2. NON-CONFIDENTIAL INFORMATION

Non-confidential is any information contained in the Public Registry/repository regarding the Qualified Certificates issued, as well as in the published up-to-date Certificate Revocation List (CRL) and in the archive copies of this list.
The following information in the repository is available to the public:
2. a template of Contract between SEP Bulgaria and the users;
3. price list of services provided by SEP Bulgaria
4. user guidelines;
5. Contact addresses with the Registration Authority and the Certification Authority;
6. user certificates (only after user approval);
7. Certificate Revocation List (CRL);
8. excepts from reports (certification document) from the Conformity Assessment Body or other authorized body (as detailed as possible).
The published reports shall inform the public about:
• the scope of the audit;
• the overall assessment for the audit;
• the degree of implementation of the recommendations.

9.3.3. PROTECTION OF CONFIDENTIAL INFORMATION

The TSP and the Signature Owner/Creator of a seal are not allowed to disseminate or allow dissemination of information made known to them during or in connection with their obligations under the Contract, including payments, without the prior written permission of the other Party.

9.4. PRIVACY OF PERSONAL DATA

SEP Bulgaria is registered as an administrator of personal data in accordance with the Law for Protection of Personal Data (LPPD).
As a Personal Data Administrator, the TSP strictly respects the confidentiality and non-dissemination requirements of the personal data of the Signature Owner/Creator of a seal that have come to his knowledge as Qualified Certification Services TSP.

9.4.1. PRIVACY STATEMENT
Personal data provided to SEP Bulgaria are stored and processed in accordance with the Law for Protection of Personal Data. SEP Bulgaria collects a quantity of information in proportion to its intended purpose and use. Each user gives consent for the processing of their personal data. This consent is made by signing the Certification Services Contract. Personal data is only used in connection with the provision of the certification services. Personal data is protected in accordance with the confidentiality rules contained in SEP Bulgaria security policy.

9.4.2. INFORMATION TREATED AS PERSONAL

Any user information that is not publicly available through the content of the issued certificates, the repository, or online by the Certificate Revocation List (CRL) shall be treated as personal.

9.4.3. INFORMATION THAT IS NOT CONSIDERED PERSONAL

All the information disclosed in the certificates is considered to be non-personal, unless expressly provided otherwise in the Law for Protection of Personal Data.

9.4.4. RESPONSIBILITY FOR THE PROTECTION OF PERSONAL DATA

SEP Bulgaria and the Registration Authority, which receive confidential information, guarantee the protection of personal data to the users. SEP Bulgaria does not allow compromise and disclosure of personal data to third parties. Providing access to personal information is only in accordance with the requirements of the Law for Protection of Personal Data.

9.4.5. CONSENT FOR THE USE OF PERSONAL DATA

Unless otherwise specified in the “Certification Practice Statement for Qualified Certification Services”, the applicable privacy rules (except in the case of an agreement) require that personal data shall not be used without the consent of the Signature Owner/Creator of a seal.

9.4.6. OTHER CIRCUMSTANCES FOR DISCLOSURE OF INFORMATION

The Certification Practice Statement for Qualified Certification Services does not indicate any other circumstances in this regard.

9.5. INTELLECTUAL PROPERTY RIGHTS

The TSP owns and retains all intellectual property rights in databases, electronic pages, trademarks and signs (eSign), electronic signature / seal certificates, and any other documents it develops and maintains. SEP Bulgaria allows the issued certificates without user access to be reproduced and distributed, provided that they are reproduced in full distribution. All trademark, trademark, and trademark rights are retained by the owners of these rights. SEP Bulgaria uses the subject of such rights only for the purpose of providing certification services. Various data included in the Qualified Certificates issued by the TSP or published in the public register / repository are subject to intellectual property rights and other tangible and intangible rights.

The pair of keys corresponding to the certificates issued by the TSP as well as the corresponding classified material shall be subject to the TSP's rights regardless of ownership over the physical media of the keys.

SEP Bulgaria shall retain all intellectual property rights of the data included in the Qualified Certificates.
9.5.2. Right to ownership of names and trademarks

SEP Bulgaria owns a registered trademark consisting of a graphic sign and an inscription which is the following logo:

![Logo](image)

The logo is a registered trademark of SEP Bulgaria and can not be used by other parties without the prior written approval of SEP Bulgaria.

All users reserve the intellectual property right to a trademark, service mark, or trade name contained in each Qualified Certificate issued.

Intellectual property right is the unique name (DN) within each certificate issued to Signature Owners/Creators of a seal.

9.5.3. Right of ownership of a key pair

The user key pair and the connected to the public key qualified certificate issued by SEP Bulgaria, as well as the corresponding classified material, are ownership of SEP Bulgaria, regardless of the ownership of the physical environment in which the keys are stored and protected.

The Certification Authorities are owned by SEP Bulgaria.

9.6. General conditions

This part of Certification practice statement for qualified certification services describes the obligations, guarantees and liability of SEP Bulgaria, the Registration Authority, the users and the relying parties. The rights, obligations and due diligence of the users and the relying parties are settled. The obligations and liability of the users and SEP Bulgaria are settled by contractual agreements. Relationships with relying parties are governed by common delict law. Contracts for the provision of certification services should be concluded in written or electronic form, subject to the provisions of Regulation (EC) No 910/2014 and the applicable legislation in the Republic of Bulgaria.

9.6.1. Liabilities, responsibilities and guarantees of SEP Bulgaria

SEP Bulgaria guarantees that it carries out its activities as:

1. Strictly complies with the terms of this document, the requirements of Regulation (EC) No 910/2014 and the national legislation in the performance of its activity as a TSP of Qualified Certification Services;
2. The services provided do not infringe the copyrights and licensed rights of third parties;
3. Uses technical equipment and technologies that ensure reliability of the systems and the technical and cryptographic security in the process implementation, including also a safe and secure mechanism/device for generating keys and creating an electronic signature/seal in its infrastructure;
4. Issues qualified certificates for electronic signatures/seals after verifying the information provided by means permitted by law;
5. Securely stores and maintains information related to the certificates issued and the operational work of the systems;
6. Complies with the established operating procedures and rules for technical and physical control, in accordance with the Certificate Policy and Certification Practice Statement;
7. Upon request, issues the relevant types of certificates, complying with the terms and procedures in this document, the relevant Policies and generally accepted standards:
   - certification services - X.509, PKCS # 10, PKCS # 7, PKCS # 12;
   - time-sealing - recommendation RFC 3161;
   - verification of the status of a certificate - recommendation RFC 2560;
8. Notifies the Users of the fact of its accreditation, if any;
9. creates an opportunity for immediate suspension and revocation of a qualified certificate;
10. Revokes and suspends certificates under the terms and conditions of the relevant Policy;
11. Immediately informs the interested parties after suspension of a certificate;
12. Provides conditions for precise verification of the time of issuance, suspension, renewal and revocation of certificates;
13. Performs identification and authentication procedures for the Signature Owner/Creator of a seal;
14. Measures against forgery of certificates and for preserving the confidentiality of data disclosed to it in the process of creating the signature;
15. Uses trustworthy systems to store and manage certificates;
16. Ensures that only duly authorized employees have access to make changes to the data, and verify the authenticity and validity of the certificates;
17. Takes immediate action in case of occurrence of technical problems relating to security;
18. Upon expiration of the validity of the Qualified Certificate, revokes its validity;
19. Informs the Signature Owners/Creators of a seal and the Relying Parties of their obligations and due diligence in the use and reliance on the certification services provided by SEP Bulgaria as well as of the proper and safe use of certificates issued and of certification services related thereto;
20. Uses and stores the collected personal and other information solely for the purposes of its activities on providing certification services in accordance with the national legislation;
21. Does not store or copy data to create user private keys;
22. Maintains supporting means that enable it to carry out its activities;
23. Takes out insurance for the time of its activity;
24. Maintains trusted personnel with the necessary expertise, experience and qualification to perform the activity;
25. Maintains a Public Registry/repository in which it publishes the issued Qualified Certificates, an updated Certificate Revocation List (CRL), other circumstances and electronic documents pursuant to this document and the national legislation;
26. Provides anytime access to the Public Register electronically (24/7);
27. Provides protection against any unauthorized changes to the maintained Public Register, as a result of unregulated and unauthorized access or by accident;
28. Immediately publishes in the Public Register the certificates issued and signed;
29. Creates conditions for each Relying Party to check the status of a issued and published certificate in the Public Register of certificates;
30. Performs periodic internal audits of the activity of the Certification Authority and the Registration Authority;
31. Performs external audits by independent auditors and publishes the results of the audit on its site;
32. Uses certified software and hardware in its business as well as secure and reliable technology systems;
33. Maintains on the SEP Bulgaria website a list of Registration Authorities, a list of recommended software and hardware to be used by the users, blanks, forms, standard contract template, etc. documents for the benefit of the users;

The TSP shall be responsible before the Signature Owner for any damages caused by gross negligence or intent:

a) As a result of a failure to meet the requirements of Regulation (EC) No 910/2014 in the performance of its activity on providing qualified certification services;

b) As a result of false or missing data in the Qualified Certificate at the time of its issue;

c) As a result of damages caused in the event that at the time of the issuance of the certificate the person named as Signature Owner/Creator of a seal did not have the private key corresponding to the public key;

d) As a result of the algorithmic discrepancy between the private key and the public key entered in the certificate.

e) As a result of non-compliance with its obligations to issue and manage qualified certificates;

f) As a result of entering false or missing data in the certificates;

g) As a result of any omissions in establishing the identity of the Signature Owner/Creator of a seal.

9.6.2. Liabilities, Responsibilities and Guarantees of the Registration Authority

SEP Bulgaria guarantees that the Registration Authority performs its functions and duties in full compliance with the terms of this document, with the requirements and procedures in the Policy and the issued internal operational instructions.

SEP Bulgaria is responsible for the actions of the Registration Authority in the SEP Bulgaria infrastructure.

SEP Bulgaria guarantees that the Registration Authority:

1. Performs its business while using reliable and secure devices and software;
2. Provides services that are in accordance with national legislation and does not infringe the copyrights and licensed rights of the users;
3. Makes the necessary efforts to perform proper user identification, correctly and accurately inputs the data in the SEP Bulgaria database and updates this information at the time of confirmation of the data;
4. Does not make any deliberate errors or does not insert inaccuracies in the information contained in the certificates;

5. Its services are in accordance with the generally accepted standards: X.509, PKCS #10, PKCS #7, PKCS #12;

6. Its services are provided on the basis of procedures that comply with the recommendations of “Certification Practice Statement”; This applies to:
   - user authentication procedures;
   - verification procedures to prove a private key associated with a public key;
   - procedures for accepting, processing and confirming or rejecting users’ requests for issuance, renewal, suspension and revocation of certificates;
   - procedures for requesting confirmation from a Certification Authority based on already accepted user request for the issuance, renewal, suspension or revocation of a certificate;
   - procedures for creating an archive of the applications collected and data received from the users;
   - procedures for generating user keys;
   - procedures for personalization and issuance of electronic cryptographic cards on which the certificates and the key pair are stored;
   - participate in external and internal audits of SEP Bulgaria.

Each Registration Authority undertakes to:

1. Present to SEP Bulgaria recommendations, especially those resulting from the audits;

2. To ensure protection of personal data in accordance with the Law for Personal Data Protection and the relevant legislation;

3. To keep the private keys of the operators in safe custody in accordance with the security requirements specified in this document;

4. Not to use personal operator keys for purposes other than those specified in this document.

9.6.3. Obligations of the Users

The Signature Owner/Author of a seal, or the person duly authorized by the Author of a seal, identified in the Qualified Certificate, has the following obligations:

1. To become acquainted with and to comply with the terms of the Contract, the Certificate Policy and Certification Practice Statement of SEP Bulgaria, as well as the requirements in the other documents published in the Public Register of SEP Bulgaria;

2. When submitting requests for issuance and management of certificates to provide true, accurate and complete information that SEP Bulgaria requires under the Contract, the legal requirements, the applicable Policies and Practices;

3. To generate cryptographic keys by using a secure method and algorithm in accordance with the requirements of Regulation (EU) No 910/2014 and to use approved by SEP Bulgaria electronic signature creation device/electronic seal creation device;

4. To verify the completeness and the accuracy of the content of the authentication information provided by it in the DN (Distinguished Name) field of the issued certificates. In the event of a discrepancy between the submitted information and the certified content, the user must immediately notify SEP Bulgaria;

5. To discontinue the use of the certificate in case of doubt about loss or compromise of the private key and to file with SEP Bulgaria an application for its suspension;

6. To discontinue the use of the certificate in the presence of obsolete, altered, incorrect and/or false information included in the issued certificate and to file a request for suspension of the certificate;

7. Before using the new certificate, to change the current PIN to access the electronic signature/seal creation device where the private key is stored;

8. To apply due diligence and to take the necessary measures to prevent the private key from compromising, loss, disclosure, modification or other unauthorized action;

9. To use the certificate issued by SEP Bulgaria for lawful purposes only and in accordance with the policy and practice specified therein;

10. To approve the terms and conditions set out in the Contract between him/her and SEP Bulgaria; This approval must be done with a handwritten signature on the Contract;

11. To approve the certificate issued to him/her;

12. Not to disclose the access password for the electronic signature/seal creation device to unauthorized persons;

13. Not to make their private key available to others.
9.6.4. Due care of the relying party

Persons who rely on a qualified electronic signature/seal certificate shall have basic knowledge of the principles of use and applicability of the electronic signature/seal and the services related to the use of a qualified electronic signature/seal certificate. The relying party should take due care, by:

1. Trusting certificates only in terms of the Policy on their purpose and the limitations and conditions under which they were issued;
2. Verifying the status of the certificate in the Public Register/repository maintained by SEP Bulgaria. Verification of the electronic authenticity and integrity of the certificate outside the Public Register or in an outdated Certificate Revocation List (CRL) does not provide for verification of its validity and all damages incurred as a result of actions taken, after making only such an inspection, shall be at the expense of the Relying Party;
3. Verifying the validity of the electronic signature/seal of electronically signed statements, as well as the validity of the electronic signature of SEP Bulgaria along the chain of certificates to the basic certificate;
4. Ensuring that the applications with which the certificate is used, are functionally applicable to the intended purpose, for which it is issued, as well as in view of the level of security specified in the relevant Policy;
5. To verify that the signature/seal, accompanied by the certificate, has not been used for purposes and for value of transactions beyond the limits and purposes entered in the certificate;
6. To make sure that the length of the keys used meets the security requirements of the Relying Party;
7. To make sure that the certificate was valid at the time of creation of the electronic signature/seal.

The verification of the intended purpose of the certificate shall be carried out on the following data contained in the certificate profile:

a) Policy according to which an electronic signature/seal certificate is issued and managed, specified in the “Certificate Policies” field;
b) The intended purpose and the limitations of the validity of the certificate, described in the “Key Usage” and “Extended Key Usage” fields;
c) Signature Owner/Creator of a seal details, specified in the “Subject” field.

SEP Bulgaria shall not be held liable for any damages incurred to the Relying Party resulting from failure to perform due diligence. Any document with a defective or questionable electronic signature/seal should be rejected or possibly subjected to other procedures that make it possible to indicate its validity. Any person who approves such a document shall be responsible for any consequences.

9.6.5. Obligations of other parties

9.6.5.1. Obligations of the qualified certification validation authority

Qualified Validation Authority (“SEP OCSP”) of SEP Bulgaria performs its functions in accordance with the requirements set out in Regulation (EU) No 910/2014. The requirements determine the technical and organizational conditions in the SEP Bulgaria operation, the policies for certifying a qualified certificate, the technical requirements for the Signature/Seal Creation/Verification Devices.

SEP Bulgaria guarantees that:

1. Uses operational and security management procedures that exclude any possibility of manipulating the status of the certificates or the data;
2. Verifies the validity of electronic signatures/seal s used in accordance with the requirements of Regulation (EU) No 910/2014 and with the RFC 2560 Online Certificate Status Protocol (OCSP) recommendation.

9.6.5.2. Obligations of the Qualified operational certification authority for qualified electronic signature/seal s
The obligations of the Qualified Operational Certification Authority for qualified electronic signatures/seals of SEP Bulgaria eSign Sep QES CA, carries out its functions in accordance with the requirements laid down in Regulation (EU) No 910/2014 for determining the technical and organizational conditions in the activities of the TSPs. The requirements relate to the Policies related to the issuance of qualified certificates and the technical requirements for Signature/Seal Creation/Verification Devices. SEP Bulgaria uses operational and security management procedures that preclude any possibility of manipulating the status of the certificates or the data.

**9.6.5.3. Obligations of SEP Bulgaria regarding the public registers/ the repository**

The Public registers are managed and controlled by SEP Bulgaria, as it guarantees that:

1. Publishes and archives qualified certificates of the Qualified Root Certification Authority, Qualified Operational Certification Authority, Qualified Certification Authority for verification of the status of the certificates;
2. Publishes and archives the Certificate Policy and Certification Practice Statement, contracts with the clients, lists of recommended applications and devices, and a list of Registration Authorities, as well as other documents related to its activities;
3. Provides access to qualified certificates only in cases where they are publicly available and as fas as the user has not expressed disagreement, and where the certificate contains a personal identifier – with his or her explicit consent;
4. Gives access to certificate status information by publishing a Certificate Revocation List (CRL), or by Online Certificate Status Protocol (OCSP);
5. Provides non-stop access to the information in the public register for a Certification Authority, Registration Authority, clients and relying parties;
6. Publishes a Certificate Revocation List (CRL) without delay and in accordance with the deadlines specified in this document.

**9.7. Liability waiver**

The liability of SEP Bulgaria is based on the general rules set out in this Certification Practice Statement and is in accordance with the necessary legal acts in force in the Republic of Bulgaria. Disclaimers should be defined in contracts between the users and SEP Bulgaria.

SEP Bulgaria shall not be held liable in cases where the damages incurred are as a result of failure to exercise due diligence, failure to fulfil obligations, or lack of knowledge of the field of the PKI technology (“Public Key Infrastructure”) by the Signature Owners or the Relying Parties.

SEP Bulgaria shall not be held liable also in cases of any damages caused by:

1. The use of a certificate outside the scope of the intended purposes and limitations of its operation stated in it in relation to the purposes of use and limitations on the value of the transactions;
2. Unlawful actions by Signature Owners or the Relying Parties;
3. Providing the way of identifying the signature/seal creation device and access to the private key by the Signature Owner/Creator of a seal to third parties;
4. Incidental events of the nature of force majeure, including malicious actions of third parties (hacking attacks, deprivation of the signature/seal creation device, access to the private key, becoming aware without the Signature Owner's knowledge of the way of identification, etc.);
5. Use of a certificate not issued, or used in accordance with the requirements and procedures of Practice and Policy of SEP Bulgaria;
6. Use of an invalid certificate (certificate that has been suspended or revoked);
7. Not timely action to revoke or suspend a certificate (due to a delay of request by the Signature Owner/Creator of a seal, or for reasons beyond the control of SEP Bulgaria);
8. A compromised private key, corresponding to the public key in the certificate at fault of the the Signature Owner/Creator of a seal;
9. Poor quality and functionality of the software products and hardware devices used by the Signature Owner/Creator of a seal and the Relying Parties.

**9.8. Liability limitations**
SEP Bulgaria restricts the effect of electronic signatures for which it issues certificates for electronic signature / seal to a certain limited property interest. SEP Bulgaria limits its liability to the following limits:

<table>
<thead>
<tr>
<th>Type of qualified certificate</th>
<th>Maximum liability limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>eSign QES Natural</td>
<td>60 000 levs</td>
</tr>
<tr>
<td>eSign QES Delegated</td>
<td>60 000 levs</td>
</tr>
<tr>
<td>eSign QESeal</td>
<td>60 000 levs</td>
</tr>
</tbody>
</table>

These limits of liability are considered to be limitations of the TSP’s liability within the meaning of national laws.

### 9.9. Responsibility of the signature owner/creator

The responsibility of the Signatory/Creator is the result of performing his/her duties. The terms of liability are governed by a contract with SEP Bulgaria.

Signature Signatory/Creator of a seal shall be held liable before SEP Bulgaria and all relying persons, if:

1. In creating the private-public key pair he/she has used an algorithm and electronic signature/seal creation devices that do not meet the requirements of Regulation (EU) No 910/2014;
2. Does not exactly meet the security requirements determined by SEP Bulgaria;
3. Does not request that SEP Bulgaria suspends or revokes the certificate after he/she has become aware that the private key was used improperly or is in danger of unauthorized use;
4. Has made untrue statements to SEP Bulgaria that are also related to the content or the issuance of the qualified certificate;
5. When the certificate is issued with a registered Creator of a seal and a person authorized by him/her, he/she is responsible for the failure of the authorized person to fulfill his/her obligations.

#### 9.9.1. Signatory/Creator's responsibility towards SEP Bulgaria

Signatory/Creator shall be held liable to SEP Bulgaria if he/she or the person authorized by him/her has provided untrue data, respectively, has withheld data relevant to the content or issuance of the certificate, as well as when he/she did not properly store the private key corresponding to the public key specified in the certificate.

### 9.10. Terms and termination of the Practice of provision of qualified trust services

#### 9.10.1. Terms

This Practice shall come into force upon its approval by the Board of Directors of SEP Bulgaria and its publication in the Public Register/Repository of SEP Bulgaria.

The provisions in this document shall be valid until the next version of “Certification Practice Statement for Qualified Certification Services” is issued and published.

#### 9.10.2. Termination

The practice is valid (has an actual status) until the approval and publication of a new version.

Upon termination of the operation of SEP Bulgaria, the validity of the Practice, as well as the provisions contained in this document shall be terminated. TSP shall keep duly and securely all previous versions/revisions of this document.
9.10.3. Termination effect and survival

Upon termination of this document, the Users and the Relying Parties shall remain bound by this document from the point of view of the issued User Qualified Certificates for the remainder of the period of validity of these certificates.

9.11. Notification and communication between the parties

Persons referred to in this Practice can make statements and exchange information by using regular mail, e-mail, fax, telephone, and network protocols (such as TCP/IP, HTTP) etc.

The choice of means can be done depending on the type of the exchanged information.

Information on any breakthrough in the security of the private keys of the Certification Authorities should be posted on the SEP Bulgaria web site, making it available to all stakeholders.

9.12. Amendments to the Practice of provision of qualified trust services

Amendments to the Practice may result from observed errors, updates and suggestions from affected parties. In the event of an invalid clause in this document, the validity of the entire document is retained and the contract with the Signatory/Creator is not violated. The invalid clause is replaced by a lawful norm.

SEP Bulgaria may make revision changes to this document that do not affect the content of the rights and obligations contained therein.

Changes that lead to a new version/revision of the document shall be published on the SEP Bulgaria website.

9.13. Dispute resolution

Subject to disputes may only be the discrepancies or contradictions between persons, parties to the contract with SEP Bulgaria. Disputes or complaints concerning the use of certificates and certification services provided by SEP Bulgaria will be settled through mediation on the basis of information submitted in writing. Requests shall be made in writing at the address SEP Bulgaria:

“System for Electronic Payments Bulgaria/SEP Bulgaria”

Sofia 1164, 1 Zaltovrah str.

Phone: 0700 18283

or electronically on: eSign@sep.bg.

Complaints will be considered by the Legal Department of SEP Bulgaria. The complainant will receive a reply within 5 (five) working days of receiving the complaint. In the event that no resolution of the dispute is found within 30 days of the commencement of the settlement procedure, the dispute shall be brought in the court for settlement.


For all matters not settled in this document the provisions of Regulation (EU) No 910/2014 and the Bulgarian legislation shall apply.

9.15. Compliance with the applicable law

This document has been developed in accordance the provisions of Regulation (EU) No 910/2014 and with the national law.

9.16. Other provisions

The Practice does not specify any other provisions.
### 9.17. Used Terms and Abbreviations

#### 9.17.1. Appendix 1: Terms and Abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation</td>
<td>Validation means the process of verifying and confirming that an electronic signature or a seal is valid</td>
</tr>
<tr>
<td>Validation data</td>
<td>Validation data means data that is used to validate an electronic signature or an electronic seal</td>
</tr>
<tr>
<td>Person identification data</td>
<td>Person identification data means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;</td>
</tr>
<tr>
<td>Electronic signature creation data</td>
<td>Electronic signature creation data means unique data which is used by the signatory to create an electronic signature</td>
</tr>
<tr>
<td>Relying party</td>
<td>Relying party (&quot;Relying Parties&quot;) means a natural or legal person that relies upon an electronic identification or a trust service</td>
</tr>
<tr>
<td>Qualified trust service TSP</td>
<td>Qualified trust service TSP means a trust service TSP who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body</td>
</tr>
<tr>
<td>Electronic document</td>
<td>Electronic document means any content stored in electronic form, in particular text or sound, visual or audio-visual recording</td>
</tr>
<tr>
<td>Electronic seal</td>
<td>Electronic seal means 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. The electronic seal serves as evidence that an electronic document is issued by a legal entity and guarantees the reliable origin and integrity of the document. Except for the verification of the authenticity of a document issued by a legal entity, electronic seals can be used for the verification of the authenticity the digital assets of a legal entity such as a software code or servers.</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>Electronic signature means 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;</td>
</tr>
<tr>
<td>Qualified electronic seal</td>
<td>Qualified electronic seal means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.</td>
</tr>
<tr>
<td>Qualified electronic signature</td>
<td>Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.</td>
</tr>
<tr>
<td>Qualified certificate for electronic signature</td>
<td>Qualified certificate for electronic signature means a certificate for electronic signatures, that is issued by a qualified trust service TSP and meets the requirements according to the Regulation (EU) No 910/2014</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>Practice</td>
<td>Practice in the provision of certification services (Certification Practice Statement) is a document containing rules on the issuance, suspension, renewal and revocation of certificates, the conditions for certificates access.</td>
</tr>
<tr>
<td>Policy</td>
<td>Policy for the provision of certification services (Certificate Policy) is a document describing the policy which the TSP follows when issuing certificates, as well as for all services provided</td>
</tr>
<tr>
<td>Registration Authority</td>
<td>Registration Authority (&quot;RA&quot;) is a separate structure of a TSP which carries out some of the activities or all of the following related to: accepting, checking, approving or rejecting requests and electronic applications for issuance and management of certificates, registering the submitted requests to the Certification Authority for issuing and making changes to the status of certificates, performing the respective identity authentication checks, respectively the identity of the Signature Owners, as well as specific data about them, with the lawful means and in accordance with the Certificate Policy and Certification Practice Statement.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>Author of a seal</td>
<td>Creator of a seal means a legal person who creates an electronic seal.</td>
</tr>
<tr>
<td>Signature Owner</td>
<td>Signature Owner means a natural person who creates an electronic signature.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.</td>
</tr>
<tr>
<td>Certificate for electronic seal</td>
<td>It is issued to legal entities and serves to validate integrity and original of data/documents.</td>
</tr>
<tr>
<td>Certificate for electronic signature</td>
<td>Certificate for electronic signature means 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.</td>
</tr>
<tr>
<td>Trust service</td>
<td>Trust services means electronic services normally provided for remuneration by the Trust Services TSP which consists of: the creation, management, and verification of electronic signatures, electronic seals and certificates related to those services, or the storage of the electronic signatures/seals or the related certificates.</td>
</tr>
<tr>
<td>Certification Authority</td>
<td>Certification Authority (&quot;CA&quot;) is a distinct structure of a TSP that carries out the activities on providing certification services. The Certification Authority has no separate legal personality and all actions and acts performed by its employees are performed in their capacity of employees of SEP Bulgaria within the limits of their powers.</td>
</tr>
<tr>
<td>Electronic seal creation device</td>
<td>Electronic seal creation device means configured software or hardware used to create an electronic seal.</td>
</tr>
<tr>
<td>Qualified electronic seal creation device</td>
<td>Qualified electronic seal creation device means an electronic seal creation device that meets the requirements in Regulation (EU) № 910/2014.</td>
</tr>
<tr>
<td>Qualified electronic signature creation device</td>
<td>Qualified electronic signature creation device means an electronic signature creation device that meets the requirements in Regulation (EU) № 910/2014.</td>
</tr>
<tr>
<td>Advanced electronic seal</td>
<td>Advanced electronic seal means an electronic seal, which meets the 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.</td>
</tr>
<tr>
<td>Advanced electronic signature</td>
<td>Advanced electronic signature means an electronic signature which meets the requirements: 1. it is uniquely linked to the signatory; 2. it is capable of identifying the signatory; 3. it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and 4. it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.</td>
</tr>
<tr>
<td>Legal persons</td>
<td>Legal persons within the meaning of the Treaty on the Functioning of the European Union (TFEU) mean all entities constituted or regulated under the law of a Member State, whatever their legal form.</td>
</tr>
</tbody>
</table>

9.17.2. Appendix 2: Terms and Abbreviations in English

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1 Abstract Syntax Notation One</td>
<td>Abstract Syntax Notation One</td>
</tr>
<tr>
<td>A Actuality</td>
<td>Actuality</td>
</tr>
<tr>
<td>BG Bulgaria</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>C Country</td>
<td>Country</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>CA Certification Authority</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CC Common Criteria</td>
<td>Common Criteria</td>
</tr>
<tr>
<td>CN Common Name</td>
<td>Common Name</td>
</tr>
<tr>
<td>CPS Certification Practice Statement</td>
<td>Certification Practice Statement</td>
</tr>
<tr>
<td>CRL, Certificate Revocation List</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>DSA, Digital Signature Algorithm</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>DN, Distinguished Name</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>E-mail</td>
<td>E-mail</td>
</tr>
<tr>
<td>e-ID</td>
<td>Electronic Identity</td>
</tr>
<tr>
<td>Enhanced key usage</td>
<td>Enhanced key usage</td>
</tr>
<tr>
<td>FIPS, Federal Information Processing</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>HSM, Hardware Security Module</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>ISO, International Standardization</td>
<td>International Standardization Organization</td>
</tr>
<tr>
<td>Organization</td>
<td>Issuer</td>
</tr>
<tr>
<td>IP, Internet Protocol</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>Location</td>
<td>Location</td>
</tr>
<tr>
<td>Number</td>
<td>Number</td>
</tr>
<tr>
<td>O,C, Organization</td>
<td>Organization</td>
</tr>
<tr>
<td>OU, Organization Unit</td>
<td>Organization Unit</td>
</tr>
<tr>
<td>OID, Organization Unit</td>
<td>Organization Unit</td>
</tr>
<tr>
<td>PKCS, Public Key Cryptography Standards</td>
<td>Public Key Cryptography Standards</td>
</tr>
<tr>
<td>PKI, Public Key Infrastructure</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PSE, Personal Security Environment</td>
<td>Personal Security Environment</td>
</tr>
<tr>
<td>RA, Registration Authority</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>RSA, Rivest-Shamir-Adelman</td>
<td>Rivest-Shamir-Adelman</td>
</tr>
<tr>
<td>SSCD, Secure Signature Creation Device</td>
<td>Secure Signature Creation Device</td>
</tr>
<tr>
<td>SHA, Secure Hash Algorithm</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SSL, Secure Socket Layer</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>SMIME, Secure Multipurpose Internet Mail</td>
<td>Secure Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>Extensions</td>
<td></td>
</tr>
<tr>
<td>S Street</td>
<td>Street</td>
</tr>
<tr>
<td>T Title</td>
<td>Title</td>
</tr>
<tr>
<td>Token</td>
<td>Token</td>
</tr>
<tr>
<td>URL, Uniform Resource Locator</td>
<td>Uniform Resource Locator</td>
</tr>
</tbody>
</table>
Regulation 910 / 2014
eIDAS

certification practice statement for qualified certification services

Version – 2.1
01.07.2017

Record changes

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Valid amendment</th>
</tr>
</thead>
</table>