Pursuant to Article 31, paragraph 3 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (Official Gazette of the RS, No. 94/17) and Article 42, paragraph 1, Article 43, paragraph 3 of the Law on Government (Official Gazette of the RS, No. 55/05, 71/05 – corrigendum, 101/07, 65/08, 16/11, 68/12 – CC, 72/12, 7/14 – CC, 44/14 and 30/18 – other law),

The Government has passed

REGULATION

on requirements for the provision of qualified trust services

I. INTRODUCTORY PROVISIONS

Scope of the Regulation

Article 1

This Regulation shall regulate requirements for provision of qualified trust services.

All the terms used in this Regulation in masculine gender shall include the same terms in feminine gender.

Carrying out of qualified trust services in compliance with regulations, standards and recommendations

Article 2

A qualified trust service provider (hereinafter: the service provider) shall perform the qualified trust services in compliance with the requirements from the ETSI EN 319 401 standard "Electronic Signatures and Infrastructures (ETSI); General Policy Requirements For Trust Service Providers" (hereinafter: EN 319 401) including the requirements from other standards that are directly and indirectly referred to in that standard, as well as in compliance with other standards, documents and recommendations pertaining to the provision of qualified trust services, determined by this Regulation and other regulations passed on the basis of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (hereinafter: the Law).

Agreement on provision of qualified trust services

Article 3

At the request of the user, an agreement shall be concluded between the service provider and the service user, concerning provision of qualified trust service.

Contents of the service provider's acts

Article 4

In the acts referred to in Article 31, paragraph 2 of the Law, the service provider shall, among other things, specify:

1) the general conditions of service provision;

2) the services' provision policies;

3) the practice statement for service provision and

4) the information security policies.

General conditions of service provision

Article 5

In compliance with Article 31, paragraph 2, item 1) of the Law, in accordance with the requirements of the EN 319 401 standard pertaining to the document referred to in section "6.2 Terms and Conditions", the service provider shall adopt the General Conditions of service provision (hereinafter: the General Conditions) which shall be made available to all the service users and relying parties.

The General Conditions shall, among other things, lay down applicable services' provision policies and shall specify the following for each policy:

1) the obligations of the service user;

2) information for the relying parties;

3) limitations on the use of the service;

4) limitations of liability, including the limitation of liability for damage incurred through the use of the service exceeding the indicated limitations;

5) the period of time during which the event logs related to the provision of the service are retained in the event logbook;

6) the legal framework applicable to service provision;

7) the method of dealing with complaints and dispute resolution;

8) the manner in which it has been assessed that the service provision is conformant with the service provision policy;

9) contact information of the service provider;

10) guaranteed level of service availability;

11) requirements for technical support to the service user.

The service users should be precisely informed of the General Conditions prior to concluding the service agreement.

The relying parties should be informed of the General Conditions in the manner suitable for and applicable to the service in question.

The service provider shall ensure that the General Conditions are publicly accessible on their

website, in such a manner that the simple and continuous accessibility thereof is ensured.

Service provision policy and practice statement for the provision of services

Article 6

The service provision policy shall specify the rules for provision of qualified trust service.

Within one qualified trust service referred to in Article 41, paragraph 2 of the Law, the service provider may have one or multiple service provision policies which shall be adjusted to individual target groups of service users and/or adjusted to specific requirements relating to security.

The practice statement shall define the operating procedures and other conditions with the aim of complying with the requirements laid down in the service provision policy, and in accordance with the requirement of the EN 319 401 standard from section "6.1 Trust Service Practice statement".

The practice statement for the provision of qualified trust services should be publicly accessible within the acts that are clearly posted on the website of the service provider.

The form and the contents of the service provision policies and practice statement may be additionally regulated by the provisions of this and other regulations governing provision of individual trust services.

Information security

Article 7

Provisions on the protection measures from the Regulation on more detailed regulation of the protection measures of information and communications systems of special importance (Official Gazette of the RS, No. 94/16) pertaining to the operator of ICT system of special importance shall apply *mutatis mutandis* to the service providers.

By means of the act laying down the information security policy, the service providers should comply with the requirements from the EN 319-401 standard pertaining to information security, as well as provide for the application of the measures referred to in paragraph 1 of this Article.

Human resources

Article 8

In compliance with Article 31, paragraph 1, item 1) of the Law, and in accordance with the requirements of the EN 319 401 standard pertaining to the human resources, the service provider shall ensure the necessary human resources and the preconditions related thereto.

Liability insurance against damage incurred through provision of qualified trust service

Article 9

In compliance with Article 31, paragraph 1, item 2) of the Law and according to the requirements from the EN 319 401 standard pertaining to insurance from liability, the service providers shall ensure financial resources for insurance from liability against damage incurred through provision of qualified trust services.

The insurance method as well as the adequate amount of financial means must be clearly indicated in the General Conditions and/or in the service provision policy and conformant with the prescribed lowest insurance amount from the by-law passed on the basis of Article 32 of the Law.

Use of secure devices and products

Article 10

The service providers shall be obliged to use secure devices and products that are protected from unauthorized alterations in such a manner as to guarantee technical safety and reliability of the processes supported by them, to use secure systems for preservation of data entrusted to them and to apply measures against data forgery and theft, all in compliance with the requirements from section 7 of the EN 319 401 standard, as well as with the requirements of the standards the application of which is prescribed for individual types of trust services.

The service providers shall, prior to starting performing qualified trust services, as well as periodically, during operational work, perform risk analyses to identify critical services requiring the use of secure devices and products and high security levels.

Keeping of relevant information

Article 11

The service providers shall keep the information referred to in Article 31, paragraph 1, item 6) of the Law, including data on user registration and information concerning significant events relating to the operational work of the service provider, as well as to management of keys and certificates, in compliance with the requirements referred to in section 7.10 of the EN 319 401 standard.

Termination plan of the service provider

Article 12

The termination plan of the service provider referred to in Article 31, paragraph 1, item 8) of the Law shall be passed and updated by the service provider in compliance with the requirements referred to in section 7.12 of the EN 319 401 standard, and bearing in mind the necessity to comply with the requirements referred to in Article 36 of the Law in cases of issuing of qualified electronic certificates.

II. ISSUING OF QUALIFIED ELECTRONIC CERTIFICATES

Qualified electronic certificate

Article 13

Provisions of this Regulation pertaining to issuing of qualified electronic certificates shall

apply to issuing of qualified certificates for electronic signature, issuing of qualified certificates for electronic seal and to issuing of qualified certificates for website authentication.

Application of ETSI EN 319 411-2 standard

Article 14

The qualified electronic certificate issuance service shall be performed in compliance with the requirements from the ETSI EN 319 411-2 standard "Electronic Signatures and Infrastructures (ETSI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates" (hereinafter: EN 319 411-2), including the requirements from other standards that are directly and indirectly referred to in that standard, relevant international standards and recommendations and/or other standards, documents and recommendations pertaining to provision of qualified electronic certificate issuance service, as determined by this Regulation.

Application of policy indicators in EN 319 411-2 standard

Article 15

When applying the EN 319 411-2 standard during issuing qualified electronic certificates intended for qualified electronic signature, the certificate issuance policy indicator "[QCP-n-qscd]" shall be taken into account.

When applying the EN 319 411-2 standard during issuing qualified electronic certificates intended for qualified electronic seal, the certificate issuance policy indicator "[QCP-l-qscd]" shall be taken into account.

When applying the EN 319 411-2 standard during issuing qualified electronic certificates intended for website authentication, the certificate issuance policy indicator "[QCP-l-w]" shall be taken into account.

Certificate issuance policy and practice statement for certificate issuing

Article 16

Policy of provision of qualified electronic certificate issuance service (hereinafter: the certificate issuance policy) shall define requirements that the qualified electronic certificate issuance service should comply with, while the practice statement for the provision of qualified electronic certificate issuance service (hereinafter: practice statement for certificate issuing) shall define the operational procedure to comply with those requirements, i.e. the manner in which the qualified electronic certificate issuer (hereinafter: certificate issuer) fulfils the technical, organizational and procedural requirements of business determined in the certificate issuance policy.

The certificate issuance policy shall be defined independently from the specific operational environment of the certificate issuer, while the practice statement for certificate issuing shall provide a detailed description of the organizational structure, operating procedures, as well as the physical and computer environment of the certificate issuer.

Requirements that the policy and the practice statement should comply with

Article 17

The certificate issuance policy and the practice statement for certificate issuing must be brought in line with the provisions of the Law, provisions of the regulations passed on the basis of the Law, as well as the requirements from the standards the application of which is prescribed by these regulations.

The certificate issuance policy should comply with the requirements from the EN 319 411-2 standard, including the requirements from other standards that are directly and indirectly referred to in that standard, and which pertain to the certificate policy.

The practice statement for certificate issuing should comply with the requirements from the EN 319 411-2 standard, including the requirements from other standards that are directly and indirectly referred to in that standard, and which pertain to the certification practice statement.

Provisions of the certificate issuance policy, as well as provisions of the practice statement for certificate issuing should be structured in compliance with the RFC 3647 standard "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".

Services included in the certificate issuing service

Article 18

The certificate issuer shall be obliged to provide certificate issuing services that shall include the following services:

1) user registration;

2) creation of qualified electronic certificates;

3) distribution of qualified electronic certificates to the users;

4) management of the life-time (such as renewal, suspension, revocation) of the qualified electronic certificates;

5) provision of reliable and publicly available service for verification of the revocation status of the qualified electronic certificates.

The certificate issuer may, in addition to the services referred to in paragraph 1 of this Article, prepare, deliver or make available to the user the devices for electronic signature and/or seal creation and other secure devices where provided so in the certificate issuance policy.

Internal rules

Article 19

The certificate issuer shall additionally determine special internal rules of operation and

protection of the certificate issuing system (hereinafter: the internal rules) which shall include and describe in detail the procedures and measures to be applied during issuing and handling of the qualified electronic certificates.

The internal rules may not be public and may comprise the business secret of the certificate issuer.

Contents of the internal rules

Article 20

The internal rules shall comprise detailed provisions on:

1) the system of physical access control in individual rooms of the certificate issuer;

2) the system of logical access control to computer resources of the certificate issuer;

3) the system for safekeeping of the private key of the certificate issuer;

4) the system of distributed responsibility during activation of private key of the certificate issuer;

5) emergency procedures and actions (e.g., fires, floods, earthquakes, other adverse weather conditions, malicious intrusions in the rooms or information system of the certificate issuer).

Actions in cases of serious incidents

Article 21

The certificate issuer shall ensure that in cases of disasters the operational work is restored as soon as possible, and in compliance with the certificate issuance policy and practice statement for certificate issuing.

In cases where their own asymmetric private key is compromised, the certificate issuer shall:

1) cease to issue qualified electronic certificates;

2) notify all the users and other interested parties of the compromise of the private key;

3) publicise information that the qualified electronic certificates issued, as well as information on the revocation status of the qualified electronic certificates, is no longer valid;

4) revoke all the qualified electronic certificates issued immediately and within 24 hours at the latest in compliance with the Law.

Records of certificates issued

Article 22

The certificate issuer shall maintain updated, accurate and secure records of the qualified electronic certificates issued.

The certificate issuer shall maintain updated and secure records of invalid (revoked and suspended) qualified electronic certificates and must, for each certificate that they issued, make information on the validity thereof publicly accessible through the service for verification of revocation status of the electronic certificates.

Determining the time of issuance of the certificate

Article 23

For reliable determining of the time of issuance and revocation of the qualified electronic certificates, the certificate issuer must provide the source of accurate time that is synchronized with the source of reference time determined by the Ministry in charge of information society (hereinafter: the Ministry) and published on the website of the Ministry.

The exact time of issuance of the qualified electronic certificates shall be integrated by the certificate issuer in the qualified electronic certificate issued.

The exact time of issuance and revocation of qualified electronic certificates shall be kept by the certificate issuer in the records of issued and revoked certificates referred to in Article 22 of this Regulation.

User registration

Article 24

Prior to issuing a qualified electronic certificate, the issuer of qualified electronic certificates shall perform user registration within which they shall reliably determine the identity of the users to which qualified electronic certificates are issued, as well as a verification of all other information that will be included in the certificate in compliance with Article 33 of the Law.

The registration procedures referred to in paragraph 1 of this Article shall be performed by the authorized officer of the qualified electronic certificate issuer or of the registration body at a remote registration location established by the certificate issuer for the needs of user registration.

The registered body, within the meaning of this Regulation, shall be an organizational unit of the certificate issuer or another legal person that is authorized by the certificate issuer to perform the user registration tasks and/or a relevant organisational unit of such legal person.

Asymmetric cryptographic keys

Article 25

Information for electronic signature and/or seal creation and data for electronic signature and/or seal validation shall be technically realized as an asymmetric pair of cryptographic keys comprising of an asymmetric private and asymmetric public key, where the asymmetric private key shall present data for electronic signature and/or seal creation, and the asymmetric public key shall present data for electronic signature and/or seal validation.

Requirements for user registration procedure

Article 26

During user registration, the certificate issuer shall be obliged to ensure:

1) that prior to establishing a contractual relation with the user, they publicly inform the user in a clear and comprehensible language of all the relevant requirements regarding the use of qualified electronic certificates;

2) that, in case that the user is identified as a natural person, they determine and check the identity of the user based on the document serving for identification based on the law, and specifically:

(1) by the physical presence, and based on the identity card, travel document, foreign travel document for foreigners or identity card for foreigners, or

(2) remotely, by using a public document serving as the means for identification in compliance with the law;

3) that, in case that the user is identified as a legal person:

(1) in compliance with item 2) of this paragraph the identity of the authorized person of the user requesting that the qualified electronic certificate is issued in the name of the user is determined and verified;

(2) check the authorisation based on the act of the user authorising the authorized person to request that the qualified electronic certificate is issued in the name of the user;

(3) that the information on the user as a legal person is checked based on inspection of data of the Business Registers Agency or based on the act of the competent authority on registration of the legal person;

4) that, in case that the user is identified as a natural person that is a member of a legal person or an organisation, following the procedure referred to in item 2) of this paragraph, the affiliation thus stated is checked based on:

(1) proof that the user is authorized by such legal person or organisation for acquiring the qualified electronic certificate in which the affiliation to the legal person and/or organisation is declared;

(2) inspection of data of the Business Registers Agency or based on the act of the competent authority on registration of the legal person and/or organisation;

5) that, in case that the user is identified by additional specific attributes, such as the designation of the organisational unit or the role in the organisation in which they are employed, accuracy of information presented in such attributes is verified;

6) verification of whether the name of the internet domain included in the qualified electronic certificate has been regularly registered, in case of issuance of a qualified certificate for website authentication;

7) that information included in the qualified electronic certificate is trustworthy and accurate;

8) that accurate and trustworthy information on the physical address or other attributes describing how the user can be contacted is acquired from the user;

9) preservation of all pieces of information used for verification of identity of the user and of the documentation used for identification, as well as any limitations on the validity thereof;

10) that a contract is concluded with the user, which should particularly include:

(1) the obligations of the user,

(2) the obligations of the user pertaining to the use of the qualified device for electronic signature and/or seal creation, in case that such a device is issued to the user,

(3) the obligation of the certificate issuer to preserve the data used in user registration and all pieces of information on the life-time of the issued qualified electronic certificate of the user. Such information shall be forwarded to the third parties under conditions defined in the relevant certificate issuance policy,

(4) requirements for publication of the certificate,

(5) confirmation that the information included in the certificate is correct;

11) the contract referred to in item 10) of this paragraph shall be kept within the time limit referred to in Article 45 of the Law;

12) except when issuing qualified certificates for website authentication, to, in case where the asymmetric pair of user's kays has not been generated by the body issuing the qualified electronic certificates, the process of generating the application for qualified electronic certificate completely ensures that the user possesses the asymmetric private key that is a mathematical one, based on an asymmetric cryptographic algorithm, linked to the public key presented for certification. In such a case, the user must ensure that the asymmetric pair of keys is generated exclusively in a qualified device for creation of electronic signatures and/or seals;

13) that the provisions of regulations in force regulating protection of personal data are complied with.

Additional requirements for the contract in cases of certificates for electronic signature and seal

Article 27

In cases of issuing of qualified certificates for electronic signatures or seals, the contract referred to in Article 26, paragraph 1, item 10) of this Regulation shall, within setting out the obligations of the user referred to in Article 26, paragraph 1, item 10), subitem (1) of this Regulation, must include the obligations of the user to:

1) deliver accurate and complete information to the certificate issuer in accordance with the registration procedure defined in the certificate issuance policy in compliance with this Regulation;

2) use exclusively their own asymmetric private key for creating the qualified electronic signature and/or seal in compliance with the contract;

3) prevent unauthorized access to their private key;

4) in cases where the user generates the pair of asymmetric keys on their own:

(1) use the qualified device for electronic signature and/or seal creation that has been entered in the Register of qualified devices for creation of electronic signatures and electronic seals,

(2) use the prescribed length of the key and the algorithm in compliance with the regulations passed on the basis of the Law,

(3) ensure that their own private key is possessed by them only;

5) immediately notify the certificate issuer if prior to the expiry of the certificate validity indicated in the certificate itself:

(1) the user's private key is lost, stolen or reasonable doubt arises that it is compromised,

(2) ceases control over the use of the user's private key due to the reasons related to compromised activation data (PIN code or a password) for the device for qualified electronic signature creation or due to other reasons,

(3) they determine falsity or modification of the contents of the qualified electronic certificate;

6) discontinue the use of their own private key where there is reasonable doubt that the key is compromised or regarding control over activation data for the device for qualified electronic signature creation.

Issuing of qualified electronic certificates to previously registered users

Article 28

A user that has a valid qualified electronic certificate for electronic signature or seal may request that a new qualified electronic certificate for electronic signature and/or seal is issued to them by the same service provider without a repeated registration (hereinafter: certificate re-issuing) where provided so in the certificate issuance policy applied.

The certificate issuance policy referred to in paragraph 1 shall regulate the issues of certificate re-issuing in compliance with the requirements from the ETSI EN 319 411-1. standard "Electronic Signatures and Infrastructures (ETSI)", section 6.3.6 "Certificate renewal".

The certificate re-issuing application shall be signed by the user by using the qualified electronic signature and/or seal based on the certificate referred to in paragraph 1 of this Article.

Provisions of Article 26 of this Regulation shall be applied *mutatis mutandis* during

certificate re-issuing, where the repeated user identification referred to in Article 26, paragraph 1, item 2) of this Regulation and/or identification of the authorized person referred to in Article 26, paragraph 1, item 3), subitem (1) of this Regulation shall not be required if the user, i.e. authorized person data has not changed.

Human resources employed by the certificate issuer

Article 29

The certificate issuer shall provide the necessary human resources, and the preconditions related thereto, and in addition to the requirements referred to in Article 8 of this Regulation, they should particularly provide:

1) that the employees with the certificate issuer mandatorily possess the expert knowledge and the necessary qualifications for the services offered by the certificate issuer, as well as for relevant business functions, and specifically:

(1) at least two employees with college or university education in the field of information and communications technologies and at least three years of professional experience in the field of maintenance and security of information systems and passed at least one of the following exams: CompTIA Security+, ISC2 CISSP or SANS GSEC, as well as that the employees regularly, and at least once a year, attend training courses and seminars with the aim of refreshing their knowledge of new security threats and current security procedures,

(2) at least two employees with university education and five years of professional experience in the field of information systems and passed at least one of the following exams: ISC2 CISSP examination or SANS GSEC, as well as that the employees regularly, and at least once a year, attend training courses and seminars with the aim of refreshing their knowledge of the new security threats and current security procedures;

2) the security roles and functions, as specified in the certificate issuance policy and in the practice statement for certificate issuing, must be documented and specified in detail, inclusive of the descriptions of each post with the certificate issuer. The business functions on the highest level of confidentiality, on which the security of issuing of the qualified electronic certificates is dependent the most, must be identified separately and clearly;

3) the employed and hired persons with the certificate issuer must have descriptions of jobs defined from the aspect of segregation of duties and privileges. In the descriptions of jobs, difference must be made between the general tasks and the specific functions of the issuer of qualified electronic certificates. It is recommended that the descriptions of jobs additionally include the definitions of requirements for specific skills and experiences required from the employees;

4) the employees in management structure of the issuer of qualified electronic certificates must possess expertise in public key infrastructure and electronic signature technology, be well acquainted with the security procedures for employees with the responsibilities in the domain of security, as well as possess adequate experiences in application of secure information systems and risk assessment;

5) all employees with the certificate issuer with security functions shall be free from conflict of interest that may prejudice the impartiality of operations involved in issuing of qualified electronic certificates;

6) the security functions with the certificate issuer shall include the following roles:

(1) of the principal security administrator – overall responsibility for administering and implementation of the security functions and procedures, as well as managing the activities on additional improving of the tasks of generation, revocation and suspension of the qualified electronic certificates,

(2) system administrators – authorized responsibility for installation, configuration and maintenance of secure systems of the issuer of qualified electronic certificates of the user registration body, generation of qualified electronic certificates, securing of devices for qualified electronic signature creation for users and management of qualified electronic certificates' revocation,

(3) system operators – responsibility for operation of secure systems of the certificate issuer in current operations on the daily level and authorized responsibility for implementation of system for creation of backup copies and recovery procedures,

(4) system auditors – authorized responsibility for viewing and maintenance of archives and log files of secure systems of the certificate issuer;

7) employees with the certificate issuer must be formally appointed to security functions by the higher management structure competent for security;

8) the certificate issuer must not appoint to security or managerial functions persons with past convictions or those who were sanctioned in any manner in relation to their eligibility for work in functions involving responsibilities. The employees must not have access to security functions before the necessary checks are completed.

Management of own asymmetric keys

Article 30

The certificate issuer shall ensure that the asymmetric keys that they use in their work are generated under strictly controlled and secure conditions and in particular that:

1) generation of asymmetric keys is performed in a physically protected environment by and with the minimum number of authorized employees (two employed persons at the minimum) for the performance of this function and in accordance with the requirements and procedures defined in the practice statement for certificate issuing;

2) generation of asymmetric keys is performed in a device that:

(1) is a trustworthy system according to EAL4 or a higher level, in accordance with the ISO/IEC 15408 standard (parts 1 to 3) "Information technology – Security techniques – Evaluation criteria for IT security" and that it conforms to the requirements from the ISO/IEC 19790:2012 standard "Information technology – Security techniques – Security requirements for cryptographic modules", or

(2) conforms to the requirements from the FIPS PUB 140-2 (2001) standard "Security Requirements for Cryptographic Modules" level 3;

(3) that the backup copies of private keys for electronic signing of qualified electronic certificates have the same or a higher level of security controls compared to the keys used for operational purposes.

Preservation of data

Article 31

The certificate issuer shall ensure:

1) confidentiality and integrity of current and archived records of the qualified electronic certificates;

2) complete and trustworthy archiving of information on qualified electronic certificates in compliance with the certificate issuance policy and practice statement for certificate issuing;

3) that the records relating to the qualified electronic certificates, as well as the registration and other information on the user, are accessible for the needs of legal transactions as evidence of completed certificate issuing;

4) reliable archiving of the exact time of the significant events with the certificate issuer;

5) that information relating to the qualified electronic certificates are preserved over the period of time required for their use in legal transactions related to the certificates used;

6) recording of all the events in such a manner as that they cannot be easily deleted or destroyed (except for the purpose of transmission to the durable storage media) within the period of time of their mandatory preservation;

7) documenting of specific events and data that should be recorded;

8) recording of all the events relating to user registration, including applications for certificate renewal, and in particular:

(1) the type of identification document that was presented by the user and/or authorized person of the legal person,

(2) the information on the user taken from the identification documents,

(3) the place in which copies of application documents and identification acts, including the signed contract with the user are kept,

(4) the specific elements from the contract entered into with the user,

(5) the identity of the officer of the registration body that performed the registration of the user,

(6) information on the method used for validation of identification acts,

(7) the name of certificate issuer that received the registration information and/or the

name of the registration body that sent the information;

9) privacy protection of the user's data;

10) recording of all the events relating to the life-cycle of the keys of the certificate issuer;

11) recording of all the events relating to the life-cycle of the qualified electronic certificates;

12) recording of all the events relating to the life-cycle of the keys managed by the certificate issuer, including the user keys where these were generated by the certificate issuer;

13) recording of all the events relating to the preparation of the qualified devices for electronic signature creation;

14) that all the requests and reports relating to certificate revocation procedure are recorded, including all the relevant activities.

Actions during termination of activity

Article 32

The certificate issuer shall ensure minimum possible damage to the users and other interested parties in case of their termination and continuous preservation of data required in legal procedures as proof of certification service provided, and in particular:

1) prior to cessation of the service of issuing qualified electronic certificates, they shall perform the following activities:

(1) notify all the users and other interested parties of the termination of work,

(2) destroy, or completely prevent the use of, their own asymmetric private keys that were used for the creation of qualified electronic signature for qualified electronic certificates;

2) provide the required financial means for realisation of the requirement referred to in item 1) of this paragraph;

3) in the certificate issuance policy and in the practice statement for certificate issuing, define the termination procedure, which shall include:

(1) notification of interested parties,

(2) any transfer of obligations to other certificate issuers,

(3) revocation procedure for the issued qualified electronic certificates for which the validity term has not expired and the transfer of lists of the revoked certificates to another certificate issuer.

Qualified device provided by the issuer

Article 33

Where the issuer of a qualified certificate for electronic signature or seal provides qualified devices for electronic signature and/or seal creation for the users, they shall do that in a secure manner and shall particularly ensure that:

1) the preparation of the device must be securely controlled by the certificate issuer;

2) the devices must be securely kept and distributed;

3) deactivation and re-activation of the devices must be securely controlled by the certificate issuer;

4) where the devices have associated activation data (a PIN code or a password), the same must be securely prepared and distributed separately from the device. The separate dispatch can be ensured either through the delivery thereof at different times or in a different manner.

Delivery of the qualified device

Article 34

The issuer of qualified certificates for electronic signature that is delivering the qualified devices for electronic signature creation to the users must guarantee confidentiality of activation data (PIN code, password), following their integration therein.

The person authorized by the certificate issuer referred to in paragraph 1 of this Article shall personally deliver the qualified device for electronic signature creation to the users and shall then take from the user a confirmation of delivery in written form bearing own signature or in electronic form inclusive of the qualified electronic signature of the user in question.

The qualified electronic certificate issued must not include the possibility of verification or the option of availability to any third parties upon user's permission until the user to which the certificate is issued has confirmed the receipt of the qualified device for electronic signature creation and relevant activation data.

III. MANAGING OF QUALIFIED DEVICES FOR ELECTRONIC SIGNATURE AND/OR SEAL CREATION

Basic provisions on qualified device management service

Article 35

The management service of the qualified device for electronic signature and/or seal creation can be performed only by the issuer of qualified electronic certificates as an additional service for the users to which qualified electronic certificates have been issued.

When issuing the qualified electronic certificate referred to in paragraph 1 of this Article, the certificate issuer shall generate an asymmetric pair of keys and provide a qualified device for electronic signature and/or seal creation that shall be made accessible to the user through the management service of the qualified device for electronic signature and/or seal creation.

The qualified device for electronic signature and/or seal creation referred to in paragraph 2 of this Article must be entered in the Register of qualified devices for electronic signatures and electronic seals creation as a device that has been envisaged to be used through the

management service of the qualified device for electronic signature and/or seal creation.

Policy and practice statement for the provision of management service of the qualified device

Article 36

The service provision policy for the management service of the electronic signature and/or seal creation device shall be an integral part of the relevant certificate issuance policy.

The practice statement for the provision of management service of the electronic signature and/or seal creation device shall be an integral part of the relevant practice statement for certificate issuing.

User's sole control over the asymmetric private key

Article 37

The management service of the qualified device for electronic signature and/or seal creation must be based on the service provision policy, practice statement for service provision, internal rules and the technical solution which are ensuring that the user has sole control over their own asymmetric private key, as well as that signing and/or sealing by using such asymmetric private key can be carried out solely under control of the user possessing such private key.

Authentication criteria

Article 38

The electronic identification scheme conforming to the criteria for the electronic identification scheme of the medium assurance level shall be used for user authentication when using the electronic signature and/or seal creation device management service.

In cases where the electronic identification scheme referred to in paragraph 1 of this Article is entrusted to a third person in a part thereof or in its entirety, the relevant electronic identification service must be registered for the medium or high assurance level in compliance with the Law.

IV. TRANSITIONAL AND FINAL PROVISIONS

Article 39

This Regulation shall enter into force on the eighth day from the date of its publication in the "Official Gazette of the Republic of Serbia".

05 number 110-3793/2018-1

In Belgrade, on May 10, 2018

The Government

The Prime Minister,

Ana Brnabić, own signature