

ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT (ZEPEP-UPB1) (Official consolidated text)

On basis of article 153 of the National Assembly of **Slovenia** Rules of Procedure the National Assembly of the Republic of **Slovenia** approved on its session on the 21. of May the Official consolidated text of the **Act** on **electronic commerce** and **electronic signature** comprising the:

- **Act** on **electronic commerce** and **electronic signature** – ZEPEP (Official Journal of RS, no. 57/2000 from 23. 6. 2000),
- Organization and Competence of Ministries **Act** –ZODPM-C (Official Journal of RS, no. 30/2001 from 26. 4. 2001) and
- **Act** Amending the **Electronic Commerce** and **Electronic Signature Act** – ZEPEP-A (Official Journal of RS, no. 25/2004 from 19. 3. 2004).

No. 043-03/00-2/3

Ljubljana, the 21. of May 2004

ZEPEP

First chapter

GENERAL PROVISIONS

Article 1

(1) This **Act** governs **electronic commerce**, which covers **commerce** in **electronic** form with the use of information and communications technology and the use of **electronic** signatures in legal transactions, which also includes **electronic commerce** in judicial, administrative and other similar procedures, unless otherwise stipulated by law.

(2) Unless otherwise agreed, the provisions of this **Act**, with the exception of the provisions of Articles 4 and 14, shall not apply to closed systems fully arranged by contracts among a known number of contracting parties.

Article 2

Individual terms used in this **Act** shall have the following meanings:

1. **data in electronic form** are data designed, stored, sent, received or exchangeable electronically;
2. **electronic message** is a series of data sent or received electronically and in particular includes **electronic** data exchange and **electronic** mail;
3. **electronic signature** is a series of data in **electronic** form that is contained in, added to or logically connected to other data and that is intended for verification of the presence of such data and identification of the signatory;
4. a **secure electronic signature** is an **electronic signature** that meets the following requirements:

- that it is linked exclusively to the signatory;
- that it is possible reliably to determine the signatory from it;
- that it is created using means of secure **electronic** signing under the exclusive control of the signatory;
- that it is linked to the data to which it refers such that all subsequent changes to such data or links thereto are evident;

5. **time stamp** is an electronically signed declaration by the certification authority confirming the contents of the data to which it refers at the time stated, while a secure time stamp is an electronically signed declaration by the certification authority that meets the conditions from the previous point of this Article;

6. **the sender of an electronic message** is the person who sent the **electronic** message or on whose behalf and in accordance with whose wishes the message was sent; the mediator of an **electronic** message shall not be considered as the sender of such **electronic** message;

7. **the addressee of an electronic message** is the person for whom the sender intended the **electronic** message;

8. **the recipient of an electronic message** is the person who received the **electronic** message; the mediator of an **electronic** message shall not be considered as the recipient of such **electronic** message;

9. **the mediator of an electronic message** is a person who sends, receives or stores an **electronic** message for another person or provides other services relating to an **electronic** message;

10. **signatory** is a person who creates an **electronic signature**, or on whose behalf and in accordance with whose wishes an **electronic signature** is created;

11. **information system** is software, hardware, and communications and other equipment that operates independently or in a network and that is intended for the collection, processing, distribution, use and other processing of data in **electronic** form;

12. **data for electronic signing** are unique data, such as codes or private encryption keys that a signatory uses to form an **electronic signature**;

13. **means of electronic signing** is software or hardware that a signatory uses to form an **electronic signature**;

14. **means of secure electronic signing** is means of **electronic** signing that meets the requirements from Article 37 of this **Act**;

15. **electronic signature verification data** are unique data, such as codes or public encryption keys, used for verification of an **electronic signature**;

16. **means of electronic signature verification** is software or hardware used to verify an **electronic signature**;

17. **equipment for electronic signing** is hardware or software, or specific components thereof, used by a certification authority for services relating to **electronic** signing or used for the formation or verification of **electronic** signatures;

18. **certificate** is a certificate in **electronic** form that links **electronic signature** verification data to a specific person (holder of the certificate) and that confirms his or her identity;

19. **qualified certificate** is a certificate from the previous point that meets the requirements from Article 28 of this **Act** and that is issued by a certification authority operating in accordance with the requirements from Articles 29 to 36 of this **Act**;

20. **certification authority** is a natural person or legal entity that issues certificates or provides other services relating to verification or **electronic** signatures;

21. **Information society service** is a service usually provided for remuneration remotely using **electronic** means at the individual request of the recipient of the service, where:

remotely means that the service is provided without the parties being present simultaneously;

using **electronic** means means that the service is initially sent to and received at the destination using **electronic** equipment for the processing (including digital compression) and storage of data, and is sent, transferred and received in full by wire, radio, optical means or other electromagnetic means;

at the individual request of the recipient of the service means that the service is provided by the transfer of data at an individual request.

Information society services include in particular the services of the sale of goods or services, access to data or advertising on the World Wide Web, and services providing access to communications networks, data transfer or storage of the recipient's data on a communications network. Radio and television broadcasting services are not information society services under this **Act**;

22. **information society service provider** is a natural person or legal entity that provides services from the previous point of this **Act**.

Article 3

Persons may arrange their relations in the creation, sending, receipt, storage or other processing or **electronic** messages otherwise than as stipulated in this **Act** if not otherwise specified by individual provisions of this **Act** or the sense thereof.

Article 4

Data in **electronic** form may not be declared invalid or lacking in evidential value solely because they are in **electronic** form.

Second chapter

ELECTRONIC COMMERCE

Section 1

Electronic message

Article 5

(1) An **electronic** message shall be deemed to originate from the sender:

- if he sends it himself, or
- if it is sent by a person authorised by the sender, or
- if it is sent by an information system operated by the sender himself or by another person under his instructions so that it operates automatically, or
- if the addressee uses to verify the origin of the message a technology and procedure agreed in advance for this purpose between the recipient and the sender.

(2) The provisions of the previous paragraph shall not apply:

- if the sender informed the recipient that the **electronic** message is not his and the recipient had time to **act** accordingly, or
- if the recipient knew or should have known if he had acted with due diligence, or if he had used the agreed technology and procedure, that the **electronic** message was not the sender's.

Article 6

The recipient shall be entitled to treat each **electronic** message received as an individual message, and to **act** accordingly, except where the **electronic** message was duplicated and the recipient knew or should have known this if he had acted with due diligence, or if he had used the agreed technology and procedure.

Article 7

(1) If the sender requested on or before sending an **electronic** message, or in the **electronic** message itself, or agreed with the recipient, that receipt of the message be confirmed, and stated that the **electronic** message was conditional on confirmation of receipt, the **electronic** message shall be considered not to have been sent until the sender receives confirmation of receipt.

(2) If the sender fails to state that the **electronic** message is conditional on confirmation of receipt, and does not receive confirmation of receipt within the specified or agreed interval, or if such is not stipulated or agreed within a reasonable interval, the sender may inform the recipient that he has not received confirmation of receipt and may stipulate a reasonable interval within which he must receive confirmation of receipt. If he still does not receive confirmation of receipt within such interval after prior notification to the recipient, the **electronic** message shall be considered not to have been sent.

(3) If the sender fails to agree with the recipient on the form of confirmation of receipt of an **electronic** message, any automatic or other confirmation by the recipient, or any behaviour by the recipient that is sufficient for the sender to know or be able to know that the **electronic** message was received, shall be considered as confirmation.

Article 8

If the sender receives from the recipient confirmation of receipt of the **electronic** message, the addressee shall be considered to have received such **electronic** message, but the **electronic** message sent shall not be deemed to be identical to the message received.

Article 9

Unless otherwise agreed, an **electronic** message shall be deemed to have been dispatched when it enters an information system beyond the control of the sender or the person who sent the **electronic** message on behalf and in accordance with the wishes of the sender.

Article 10

(1) Unless otherwise agreed, the time of receipt of the **electronic** message shall be the time when the **electronic** message enters the recipient's information system.

(2) Unless otherwise agreed, and irrespective of the provisions of the previous paragraph, the time of receipt of an **electronic** message, if the recipient specifically stipulated an information system for receipt of **electronic** messages, shall be the time when the **electronic** message enters such information system, or if the **electronic** message was sent to another information system, the time when the recipient collected the **electronic** message.

(3) The provisions of the previous paragraph shall also apply if the information system is located in another place, which under this **Act** shall be considered as the place of receipt of the **electronic** message.

Article 11

(1) Unless otherwise agreed, the place where the sender has his registered office or permanent residence at the time of sending shall be considered as the place from which the **electronic** message was sent, while the place where the recipient has his registered office or permanent residence at the time of receipt shall be considered as the place of receipt of the **electronic** message.

(2) If the sender or recipient has no permanent residence, his residence at the time of sending or receipt of the **electronic** message shall be considered as the place from which the **electronic** message was sent or received.

Section 2

Data in **electronic** form

Article 12

(1) Where the law or other regulation stipulates that certain documents, records or data are to be stored, they may be stored in **electronic** form:

- if the data contained in an **electronic** document or record are accessible and suitable for later use, and

- if the data are stored in the form in which they were formed, sent or received, or in another form that authentically represents the data formed, sent or received, and

- if it is possible to determine from the stored **electronic** message where it originates from, to whom it was sent and the time and place of its sending or receipt, and

- if the technology and procedures used prevent to a satisfactory extent subsequent changes to or deletion of data, which could not be readily determined, or if there exists a reliable assurance that the message has not been altered.

(2) The obligation to store documents, records or data from the previous paragraph shall not apply to data the sole purpose of which is to enable the **electronic** message to be sent or received (communications data).

(3) Where the law or other regulation stipulates that certain data shall be submitted or stored in their original form, an **electronic** form of the message shall be considered adequate if it complies with the conditions from the first paragraph of this Article.

(4) The provisions of this Article shall not apply to data for which this **Act** stipulates stricter or special conditions of storage.

Article 13

(1) Where the law or other regulation stipulates a written form, an **electronic** form shall be considered equivalent to the written form if the data in **electronic** form are accessible and appropriate for later use.

(2) The provisions of the previous paragraph shall not apply to:

1. legal transactions transferring ownership rights to real estate or establishing other material rights to real estate;

2. testamentary transactions;

3. contracts arranging property relations between spouses;

4. contracts disposing of the assets of persons declared legally incapacitated;

5. contracts on the handover and distribution of assets for life;

6. endowment contracts and agreements on renunciation of inheritance;

7. promises of gifts and gift contracts in the event of death;

8. purchase contracts with retained ownership rights;

9. other legal transactions which the law stipulates must be concluded in the form of a notarised record.

Section 3

Responsibility of information society service providers

Article 13a – General provisions on responsibility of information society service providers

(1) No special licence is required for the provision of information society services.

(2) Information society service providers shall be responsible for the data they transmit or store in accordance with the provisions of this section, unless otherwise stipulated by the regulations governing their responsibilities in the area of taxes, protection of personal data, protection of competition, the legal profession, notaries public and games of chance.

(3) Information society service providers may not be required to undertake general monitoring or protection of data in **electronic** form that they transmit or store, and may not be subjected to imposition of measures requiring them to actively investigate the facts or circumstances indicating the illegality of individual activities or data.

(4) Information society service providers from this section shall be obliged to **act** with the due diligence of a good professional in ensuring the security of operation of their information systems and the transmission of data in **electronic** form.

(5) The Government of the Republic of **Slovenia** shall, at the suggestion of the minister responsible for the information society, determine a contractor for tasks of ensuring the security of operation of information systems and transmission of data in **electronic** form (hereinafter: contractor of tasks). Information society service providers shall be obliged to inform the contractor of tasks of activities and data that endanger the security of operation of information systems, and to cooperate with him. The contractor of tasks shall collect information on activities and tasks that endanger the security of operation of information systems and of data in **electronic** form, inform the public, cooperate with bodies to ensure the security of operation of information systems and the transmission of data in **electronic** form of other countries, warn of threats to security and propose solutions for their removal. The method of implementation of tasks shall be determined in greater detail by the Government of the Republic of **Slovenia** in the **act** appointing the contractor of tasks.

Article 13b – Excluded transmission

(1) Where part of the information society service is the transmission of data in **electronic** form in a communications network provided by the recipient of the service, or the provision of access to a communications network, the service provider shall not be responsible for the data transmitted, provided that:

- he does not initiate the transmission of data;
- he does not choose the addressee of the data transmitted; and
- he does not select or alter the contents of the data transmitted.

(2) Transmission and the provision of access from the first paragraph of this Article shall include automatic, intermediate and transient storage of transmitted data in **electronic** form, if this is intended solely for their transmission in the communications network and if the data are not stored for longer than normally required for their transmission.

Article 13c – Caching

Where part of an information society service is the transmission in a communications network of data in **electronic** form provided by the recipient of the service, the service provider shall not be responsible for automatic, intermediate and temporary storage of such data where such storage is intended solely for the efficient transmission of data to other recipients of the service upon their request, provided that:

- he does not modify the contents of the data;

- he acts in accordance with the conditions for access to the data;
- he acts in accordance with the conditions on updating of data specified in generally recognised and used industry standards;
- his actions do not interfere with the lawful use of technologies for the acquisition of information on the use of data specified in generally recognised and used industrial standards; and
- without delay he removes or prevents access to data he has stored immediately on becoming aware of the fact that the initial source of such data has been removed from the network, or access to it has been disabled, or that a judicial or administrative body has ordered such removal or disablement.

Article 13d – Hosting

(1) Where part of an information society service is the storage of data provided by a recipient of the service, the service provider shall not be liable for data stored at the request of the recipient of the service, provided that:

1. he does not know that it involves unlawful activity or data, and is not aware of the facts or circumstances from which the unlawfulness is apparent with regard to compensation claims, or
2. immediately he learns or becomes aware of the unlawfulness, he removes or disables access to such data without delay.

(2) The first paragraph of this Article shall not apply in instances where the recipient of the service was acting under the authorisation or control of the service provider.

Third chapter

ELECTRONIC SIGNATURE

Section 1

General provisions

Article 14

Electronic signatures may not be declared invalid or lacking in evidential value solely due to their **electronic** form, or because they are not based on a qualified certificate or certificate of an accredited certification authority or because they are not formed with means for secure **electronic** signing.

Article 15

Secure **electronic** signatures certified by a qualified certificate shall with regard to data in **electronic** form be equivalent to an autographic **signature**, and shall have the same validity and evidential value.

Article 16

Persons storing documents electronically signed using data and means for signing shall be obliged to store complementary data and means for verifying **electronic** signatures for as long as they store the documents.

Article 17

The use of data for **electronic** signing without the knowledge of the signatory or holder of the certificate to which such data refers shall be prohibited.

Section 2

Certificates and the certification authorities that issue them

Article 18

- (1) Certification authorities shall not require special licences to perform their activities.
- (2) Certification authorities shall be obliged to report commencement of activities to the ministry responsible for the economy (hereinafter: ministry) at least eight days prior to commencement. At the start of performance of activities or on modification of activities, the certification authority shall be obliged to inform the ministry of their internal rules regarding **electronic** signing and verification, and of their procedures and infrastructure.
- (3) Certification authorities providing secure **electronic** signing services shall be obliged in their internal rules to respect the security requirements stipulated by this **Act** and implementing regulations issued pursuant thereto.
- (4) Certification authorities shall be obliged to comply with the requirements from their internal rules both on commencement and throughout the duration of performance of activities.

Article 19

- (1) Certification authorities shall be obliged without delay to inform the ministry of all circumstances that hinder or prevent the implementation of activities in accordance with valid regulations or their own internal rules.
- (2) Certification authorities shall be obliged without delay to inform the ministry of the commencement of bankruptcy or compulsory settlement procedures.

Article 20

- (1) Certification authorities shall be obliged to revoke certificates from point 18 of Article 2 of this **Act** during their validity in accordance with their internal rules governing revocation of certificates, however always without delay:
 - if revocation of the certificate is requested by the holder of the certificate or an authorised person thereof, or
 - when the certification authority learns that the holder of the certificate has been declared legally incapacitated, has died or has ceased to exist, or that circumstances that fundamentally influence its validity have changed, or
 - if data on the certificate are incorrect, or if the certificate was issued on the basis of incorrect data, or

- if the data for verification of the **electronic signature** or the information system of the certification authority were endangered in a manner that affects the reliability of the certificate, or
- if the data for **electronic** signing or the information system of the holder of the certificate were endangered in a manner that affects the reliability of formation of the **electronic signature**, and the certification authority has been informed thereof, or
- if the certification authority ceases to operate or is prohibited from operating and his activities are not taken over by another certification authority, or
- if revocation is ordered by a competent court, misdemeanours judge or administrative body.

(2) In their internal rules, certification authorities shall be obliged to stipulate when and in what manner notification shall be issued on the issuing or revocation of certificates.

(3) Irrespective of their internal rules, certification authorities shall be obliged always without delay to inform holders of revoked certificates. Data on the revocation must be transmitted to all persons requesting them, or must be published if the certification authority maintains a register of revoked certificates.

Article 21

The ministry shall be obliged without delay to ensure the revocation of certificates of a certification authority if the certification authority ceases operations or if his operation is prohibited and his activities are not taken over by another certification authority if the certification authority fails to revoke the certificates.

Article 22

(1) Holders of certificates shall be obliged to store data for **electronic** signing with due diligence, and to use them in accordance with the requirements of this **Act** and implementing regulations issued pursuant thereto, and to prevent unauthorised access to such data.

(2) Holders of certificates shall be obliged to request revocation of their certificates if the data for **electronic** signing or the information system of the holder of the certificate were lost or endangered in a manner that affects the reliability of formation of the **electronic signature**, or if there is a risk of abuse, or if the data stated on the certificate have changed.

Article 23

If the certificate contains data on a third person that is not the holder of the certificate, such person shall also be entitled to request revocation of the certificate for the reasons stipulated in the second paragraph of the previous Article.

Article 24

(1) Revocation of the certificate shall take effect between the holder of the certificate and the certification authority from the moment of revocation. Revocation of the certificate between third parties and the certification authority shall take effect from the moment of publication or, if the revocation was not published, from the moment when the third party learned of the revocation.

(2) Revocation of the certificate must state the time of revocation.

(3) Revocation shall always apply from the moment of revocation on. Retroactive revocation shall be prohibited.

Article 25

The provisions governing certificates shall apply *mutatis mutandis* to time stamps and related services, while the provisions governing qualified certificates shall apply to secure time stamps and related services.

Article 26

Certification authorities must keep documentation on security measures in accordance with this **Act** and regulations issued pursuant thereto and on all certificates issued and revoked such that their data shall always be accessible and their authenticity and constancy always verifiable, for at least five years from the individual event or action.

Article 27

(1) Prior to ceasing operations, certification authorities shall be obliged without delay to inform the ministry and holders of certificates issued by them thereof, and to ensure that all their rights and responsibilities with regard to issued certificates are taken on by another certification authority, or that they revoke valid certificates.

(2) Certification authorities shall be obliged to submit all documentation that they have hitherto kept to the other certification authority taking on the rights and responsibilities of the previous certification authority with regard to certificates issued, or to the ministry, if there is no such certification authority.

Section 3

Qualified certificates and certification authorities issuing them

Article 28

(1) The following must be determinable from a qualified certificate:

- statement that it is a qualified certificate;
 - name or title and country of permanent residence or registered office of the certification authority;
 - name or pseudonym of the holder of the certificate, with a mandatory statement that it is a pseudonym;
 - additional data on the holder of the certificate prescribed for the purpose for which the certificate is to be used, which may not conflict with the purpose of use of the pseudonym;
 - data for verification of the **electronic signature** matching the data for **electronic** signing under the control of the holder of the certificate;
- start and end of validity of the certificate;
- identification code of the certificate;

- secure **electronic signature** of the certification authority issuing the certificate;
- possible restrictions relating to the use of the certificate;
- possible restrictions regarding the transaction values for which the certificate may be used.

(2) Unless otherwise agreed, certificates may not contain data protected by a special law.

(3) Qualified certificates issued for the purposes of personal documents shall contain in addition to the data from the first paragraph of this Article also a personal identification code which may to this end be referred to or linked to the central population register. The Government of the Republic of **Slovenia** shall determine in greater detail the method for determining personal identification codes, establishment and maintenance of the register of personal identification codes and the conditions and method for referring or linking to the central population register in accordance with regulations governing the protection of personal data.

Article 29

Certification authorities issuing qualified certificates shall be obliged to provide services relating to **electronic** signing with due diligence.

Article 30

(1) Certification authorities issuing qualified certificates shall be obliged to ensure the maintenance of a register of revoked certificates, which must in particular contain the identification codes of revoked certificates to enable them to be identified precisely. The register may not contain data on the reasons for the revocation or any data not contained in the certificate except the date and time of revocation. The register must be securely electronically signed with the **signature** verified by a qualified certificate with at least the same reliability as certificates revoked in the register.

(2) Certification authorities shall be obliged to provide the possibility of immediate and secure revocation of qualified certificates, as well as the possibility of precise stipulation of the moment of issue and revocation of qualified certificates.

(3) Certification authorities that issue qualified certificates and cease operations shall be obliged to ensure that another certification authority that issues qualified certificates maintains revoked qualified certificates in their register.

(4) If a certification authority that ceases to operate fails to ensure the storage of documentation and the maintenance of revoked qualified certificates by another certification authority, the ministry shall so ensure at the certification authority's expense.

Article 31

Certification authorities issuing qualified certificates shall be obliged with the help of an official personal document with a photograph for natural persons, or officially confirmed documents for legal entities, to reliably establish the identity and other important features of persons requesting certificates.

Article 32

(1) Certification authorities issuing qualified certificates shall be obliged to employ persons with the necessary professional knowledge, experience and skills in the area of the services provided, and particularly in the area of operating and knowledge of the technology of **electronic commerce** and appropriate security procedures to ensure compliance with all the provisions of this **Act**.

(2) Personnel shall be obliged to **act** following administrative and operative procedures and regulations in accordance with established rules of the profession.

(3) The Government of the Republic of **Slovenia** shall by implementing regulations determine the type and level of required professional education, the number of years of experience and possible additional training for compliance with the requirements from the first paragraph of this Article.

Article 33

(1) Certification authorities shall be obliged to use reliable systems and equipment protected against monitoring and that ensure technical and cryptographic security of procedures in which they are used.

(2) Certification authorities shall be obliged to implement security measures against the forging of certificates and in instances where the certification authority forms data for **electronic** signing, to ensure the confidentiality of data throughout the procedure for the formation of such data.

(3) Certification authorities may not store data for the **electronic** signing of a certificate holder.

(4) Certification authorities shall be obliged to use for storage of certificates reliable systems that enable simple detection of modifications and that at the same time ensure:

1. that only authorised persons may input new data and modify existing data;
2. that the authenticity of data can be verified;
3. that certificates are only publicly accessible if the certification authority has obtained the prior consent of the holder of the certificate;
4. that users can simply observe any technical modifications that could endanger compliance with such security requirements.

(5) The Government of the Republic of **Slovenia** shall by implementing regulations prescribe more detailed criteria for compliance with the requirements from this Article.

Article 34

Certification authorities issuing qualified certificates shall be obliged to have liability insurance. The minimum amount of insurance cover shall be prescribed by the Government of the Republic of **Slovenia** by decree.

Article 35

(1) Certification authorities issuing qualified certificates shall be obliged to store all important data on qualified certificates, particularly for the demonstration of verification in judicial, administrative and other procedures, for at least as long as the data signed by **electronic signature** to which the qualified certificate refers are stored, and for no less than five years from the issuing of the certificate.

(2) Important data on qualified certificates shall include in particular data on the method of determining the identity of the holder of the certificate, the time and method of issuing the certificate, the reason, time and method of any possible revocation of the certificate, the validity period of the certificate and all messages that relate to the validity of the certificate exchanged between the certification authority and the holder.

(3) Data from the first and second paragraphs of this Article may be stored in **electronic** form.

Article 36

(1) Certification authorities issuing qualified certificates shall be obliged to notify persons requesting certificates of all important circumstances of use of the certificate prior to issuing the certificate.

(2) Notification must contain:

1. a detailed summary of the content of valid regulations and internal rules and other conditions concerning the use of certificates;
2. data on possible restrictions on the use of the certificate;
3. data on the existence of voluntary accreditation;
4. data on procedures for resolving complaints and peaceful resolution of disputes;
5. data on measures by holders of certificates required for the security of **electronic** signing and verification of **electronic** signatures, and on appropriate technologies;
6. warning that electronically signed data may require to be electronically signed again before the security of the existing **electronic signature** is reduced over time;
7. warning that the holder of a qualified certificate shall himself be obliged to report changes to compulsory data of qualified certificates from Article 28 of this **Act**.

(3) Notifications must be expressed in readily understandable language and be in written form.

(4) Appropriate parts of the notification must on request be accessible by third persons relying on the certificate.

Section 4

Technical requirements for secure **electronic** signing

Article 37

(1) Means for secure **electronic** signing must through the use of suitable procedures and infrastructure ensure the following:

1. data for **electronic** signing must be unique and their confidentiality assured;
2. data for **electronic** signing cannot within a reasonable interval and with reasonable means be determined from the data for verification of **electronic** signatures, and **electronic** signatures must be effectively protected against forgery through the use of currently available technology;
3. signatories can reliably protect their data for **electronic** signing against unauthorised access.

(2) Means for secure **electronic** signing may not amend data being signed or prevent presentation of data to the signatory prior to signing.

(3) The Government of the Republic of **Slovenia** shall by implementing regulations prescribe more detailed criteria for compliance with the requirements regarding means for secure **electronic** signing from this Article.

Article 38

(1) During the procedure of verification of secure **electronic** signatures, the following must be ensured through the use of appropriate procedures and infrastructure:

1. data used for verification of **electronic** signatures must be equal to the data shown to the user;
2. the **signature** must be reliably verified and the results of verification and the identity of the signatory correctly shown to the user;
3. users can reliably determine the content of signed data;
4. the authenticity and validity of certificates must be verified during verification of the **signature**;
5. the use of pseudonyms must be clearly marked;
6. all modifications that in any way affect the security of the **electronic signature** must be detected.

(2) The Government of the Republic of **Slovenia** shall by implementing regulation prescribe more detailed criteria for compliance with the requirements regarding procedures and infrastructure from the previous paragraph.

Section 5

Liability of certification authorities

Article 39

(1) Certification authorities shall be liable to each person that justifiably relied on a qualified certificate issued by the certification authority for:

- the accuracy of data in the certificate at the moment of issue of the certificate, and for the certificate containing all the prescribed data for qualified certificates;
- assurance that the holder of the certificate stated on the certificate had at the time of issue of the certificate of the data for **electronic** signing appropriate data for verification of the **electronic signature** stated or marked on the certificate;
- assurance that the data for **electronic** signing and the data for verification of the **electronic signature** complement each other if the certification authority formed both data sets;
- immediate revocation of certificates and publication of the revocation if grounds exist for the revocation;
- compliance with the requirements of this **Act** and implementing regulations issued pursuant thereto with regard to secure **electronic** signatures and qualified certificates.

(2) Certification authorities may on qualified certificates mark the limits of use or the maximum transaction value for a particular certificate, and shall not be liable for the consequences of use of the certificate outside such limits if the restrictions are recognisable by third parties.

(3) Certification authorities shall be liable if they fail to prove that damage arose through no fault of their own.

Section 6

Oversight -> Supervision?

Article 40

1. Inspection oversight of the implementation of the provisions of this **Act** shall be performed by the ministry.

2. Within the context of inspection oversight, the ministry shall:

- verify whether the requirements of the **Act** and implementing regulations issued pursuant thereto have been appropriately transferred into internal rules of certification authorities;

- verify whether certification authorities throughout the performance of activities comply with the requirements from this **Act** and implementing regulations issued pursuant thereto and from their internal rules;

- in instances of the provision of qualified certificates, supervise the use of appropriate procedures and the necessary infrastructure;

- supervise the legality of issuing, storage and revocation of certificates;

- supervise the legality of provision of other services by certification authorities.

3. The ministry shall maintain an **electronic** public register of certification authorities in the Republic of **Slovenia**. The register of certification authorities shall record certification authorities if they comply with the conditions from this **Act**. Foreign certification authorities shall at their request also be recorded in the register of certification authorities if they comply with the conditions from this **Act** for their certificates to be valid in the Republic of **Slovenia**.

4. The register of certification authorities shall be securely electronically signed by the ministry. Data for verification of the qualified certificate of the ministry shall be published on the website of the ministry together with the register of certification authorities.

Article 41

(1) In performing inspection oversight, inspectors shall be entitled:

- to inspect documentation and acts referring to the operation of certification authorities;

- to inspect premises in which verification services are provided and the information technology, infrastructure and other equipment and technical documentation of certification authorities;

- to check the measures and procedures of certification authorities.

(2) Inspectors shall have the right for a maximum of fifteen days to seize documentation if required for protection of evidence or precise determination of irregularities. They shall be obliged to issue confirmation thereof.

(3) Inspectors shall be obliged to protect as confidential data on certificates, personal data and data protected under a special law obtained by inspectors in the course of inspection oversight.

(4) Inspectors shall by decision:

- prohibit the use of inappropriate procedures and infrastructure;
- temporarily prohibit the operation of a certification authority, in part or in full;
- prohibit the operation of a certification authority if the certification authority fails to comply with the requirements of this **Act** and regulations issued pursuant thereto, and if less stringent measures have been or would be unsuccessful;
- order the revocation of certificates if it is likely that the certificates were forged.

(5) Appeals shall be permitted against decisions from the previous paragraph and shall be decided on by the Government of the Republic of **Slovenia**. Appeals against decisions from the second indent of the previous paragraph shall not suspend their implementation.

(6) Prohibition of operation shall not affect the validity of previously issued certificates.

Section 7

Voluntary accreditation

Article 42

(1) Certification authorities that demonstrate that they comply with conditions prescribed by this **Act** and implementing regulations issued pursuant thereto for their operation may request that the accreditation body record them in the register of accredited certification authorities.

(2) Foreign certification authorities may also be recorded in the register of accredited certification authorities at their request if they comply with the conditions from this **Act** for the validity of their certificates in the Republic of **Slovenia**.

(3) Certification authorities recorded in the register of accredited certification authorities (accredited certification authorities) may operate with a statement of their accreditation.

(4) Certification authorities recorded in the register of accredited certification authorities may mark this fact in certificates issued.

Article 43

(1) The accreditation body shall maintain a public **electronic** register of certification authorities voluntary accredited with the body.

(2) The accreditation body shall securely electronically sign the register of accredited certification authorities. Data for verification of the qualified certificate of the accreditation body shall be published on the website of the accreditation body together with the register of accredited certification authorities.

Article 44

(1) The accreditation body shall conduct oversight and shall take measures with regard to accredited certification authorities.

(2) The accreditation body shall:

- issue general recommendations for the operation of certification authorities and recommendations and standards for the operation of accredited certification authorities in accordance with this Act and implementing regulations issued pursuant thereto;
- verify whether the requirements of this Act and implementing regulations issued pursuant thereto have been suitably transferred into the internal rules of accredited certification authorities;
- verify whether certification authorities throughout the performance of activities comply with the requirements from this Act and implementing regulations issued pursuant thereto and from their internal rules;
- supervise the use of appropriate procedures and infrastructure by accredited certification authorities;
- supervise the legality of the issuing, storage and revocation of certificates of accredited certification authorities;
- supervise the legality of provision of other services of accredited certification authorities.

(3) The accreditation body may recommend:

- modification of the internal rules of an accredited certification authority;
- that an accredited certification authority cease further use of inappropriate procedures and infrastructure.

(4) If a certification authority fails to respect the recommendations of the accreditation body, the accreditation body shall by decision remove the certification authority from the register of accredited certification authorities.

(5) Appeals shall be permitted against decisions from the previous paragraph within fifteen days of receipt of the decision, and shall be decided by the minister responsible for the information society.

(6) The minister shall be obliged to issue a decision on appeals within thirty days of receipt of the appeal. Decisions on appeals shall be final.

Article 45

(1) The Government of the Republic of Slovenia shall at the proposal of the minister responsible for the information society appoint for the performance of the tasks of the accreditation body a body competent for

the performance of the tasks of the accreditation body, or shall award public authorisation or a concession for the performance of such tasks.

(2) The body from the previous paragraph may not be a certification authority.

Section 8

Validity of foreign certificates

Article 46

(1) Qualified certificates of certification authorities with registered offices in the European Union shall be equivalent to domestic qualified certificates.

(2) Qualified certificates of certification authorities with registered offices in third countries shall be equivalent to domestic certificates:

1. if the certification authority complies with the conditions from Articles 29 to 36 of this Act and is voluntarily accredited in the Republic of Slovenia or a member state of the European Union;
2. if a domestic certification authority that complies with the conditions from Articles 29 to 36 of this Act guarantees such certificates as if they were its own;
3. if so stipulated by bilateral or multilateral agreements between the Republic of Slovenia and other countries or international organisations;
4. if so stipulated by bilateral or multilateral agreements between the European Union and third countries or international organisations.

(3) Certificates of certification authorities with registered offices in the European Union that cannot under this Act be defined as qualified shall be treated equally to domestic certificates in accordance with the provisions of this Act.

Fourth chapter

PENALTY PROVISIONS

Article 47

(1) A fine of between SIT 500,000 and SIT 5,000,000 shall be imposed for misdemeanours on a certification authority if:

1. it fails reliably to establish the identity or other important features of a person requesting a qualified certificate (Article 31);
2. it issues a qualified certificate that does not contain all the required data or that contains data that it should not contain (Article 28);
3. it fails to revoke a certificate or qualified certificate in instances required by this Act or its internal rules (Articles 20 and 23);

4. it fails to state in a revocation the time of revocation of a certificate or qualified certificate, or revokes a certificate or qualified certificate retroactively (Articles 20 and 24);
5. it fails to inform an applicant for a certificate or qualified certificate of all prescribed data (Article 36);
6. prior to ceasing to operate it fails to inform the ministry and to ensure that responsibility for all valid certificates or qualified certificates is taken on by another certification authority or to revoke them (Article 27);
7. it fails to deliver all documentation to another certification authority or to the ministry (Article 27);
8. it fails to inform the ministry of possible initiation of bankruptcy or compulsory settlement or of other circumstances that prevent it from complying with prescribed requirements (Article 19);
9. it fails to maintain the prescribed documentation (Article 26);
10. it fails to enable an inspector to inspect or seize documentation, or fails to provide the required information and explanations (Article 41);
11. it fails to report the start of performance of activities or to submit internal rules (Article 18);
12. it issues qualified certificate and it fails to maintain or inadequately maintains a register of revoked certificates (Article 30);
13. it issues qualified certificates and fails to perform appropriate security measures to prevent unauthorised collection or copying of data for **electronic** signing by itself or a third party (Article 33);
14. despite prohibition of the performance of activities by the ministry it continues to perform activities (Article 41);
15. without justification it uses the mark of an accredited certification authority (Article 42).

(2) A fine of between SIT 50,000 and SIT 100,000 shall be imposed for misdemeanours on the responsible person of the legal entity or on an individual sole trader that commits misdemeanours from the previous paragraph.

(3) If a certification authority is an individual, the fine imposed for misdemeanours from the first paragraph of this Article shall be between SIT 100,000 and SIT 300,000.

Article 48

A fine of between SIT 50,000 and SIT 150,000 shall be imposed for misdemeanours on the holder of a certificate or the responsible person for legal entities or a sole trader if:

1. it fails to request revocation of a certificate or qualified certificate (Article 22);
2. it uses data for **electronic** signing in contravention of the requirements of this **Act** and implementing regulations issued pursuant thereto (Article 22).

Article 49

A fine of between SIT 50,000 and SIT 150,000 shall be imposed for misdemeanours on an individual who without the knowledge of the signatory or holder of a certificate uses its data for **electronic** signing (Article 17).

Fifth chapter

TRANSITIONAL AND FINAL PROVISIONS

Article 50

(1) The Government of the Republic of **Slovenia** shall issue implementing regulations governing in greater detail:

1. the criteria for determining reliability and for determining compliance with technical requirements from Articles 33, 37 and 38 of this **Act**;
2. professional education, knowledge and experience from Article 32 of this **Act**;
3. the minimum insurance cover held by certification authorities to cover liability;
4. the form, publication and accessibility of internal rules of certification authorities;
5. the duration of validity of qualified certificates, the period for repeat **electronic signature** of previously signed **electronic** data and procedures relating thereto;
6. the area of use, requirements and acceptable deviations in the provision of services relating to secure time stamps;
7. the type and form of marking of accredited certification authorities;
8. technical conditions for **electronic commerce** in the public administration.

(2) The Government of the Republic of **Slovenia** shall issue the implementing regulations from the previous paragraph no later than within sixty days of publication of this **Act** in the *Uradni List* of the Republic of **Slovenia**.

Article 51

The minister responsible for economic affairs may prescribe more precisely the method of implementation of individual provisions of this **Act**.

Article 52

Until the entry into force of an **Act** governing the conditions for **electronic commerce** in the verification of signatures before a notary public or other competent body, the provisions of Article 15 of this **Act** shall not apply to such instances.

Article 53

Point 4 of the second paragraph of Article 46 of this Act shall begin to apply on the date of acceptance of the Republic of Slovenia as a member of the European Union.

Article 54 – deleted considering ZEPEP_A

Article 55

This Act shall enter into force on the sixtieth day after publication in the *Uradni List* of the Republic of Slovenia.

The Act Amending the Electronic Commerce and Electronic Signature Act – ZEPEP-A (Official Journal of RS, no. 25/2004 from 19. 3. 2004) contains the following transitional and final provisions:

TRANSITIONAL AND FINAL PROVISIONS

Article 26

(1) The Government of the Republic of Slovenia shall determine the body from the fifth paragraph of Article 13a no later than three months after the entry into force of this Act.

(2) The Government of the Republic of Slovenia shall issue the regulations from the fourth paragraph of Article 10 of this Act no later than one year after the entry into force of this Act.

Article 27

(1) Fines stipulated by this Act shall, until the start of application of the Misdemeanours Act (*Uradni List* RS 7/03, ZP-1), be imposed in misdemeanours procedures as monetary fines in the bands laid down in Articles 22 to 24 of this Act.

(2) The provisions of this Act governing fines for misdemeanours committed by the responsible person of a sole trader shall apply until the start of application of the Misdemeanours Act (*Uradni List* RS 7/03, ZP-1).

Article 28

This Act shall enter into force on the fifteenth day after publication in the *Uradni List*.