GOVERNMENT OF THE REPUBLIC OF SLOVENIA
CENTRE FOR INFORMATICS

ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT

LJUBLJANA, JUNE 2000

INTRODUCTION
Marin Silic

The Act of the electronic commerce and electronic signature regulates a new field of the operation of the economic subjects, citizens and state organs. This field has not been regulated until now, but it is becoming more and more important because of the fast technological development. A lack of its legal regulation could in the first place represent, which I would particularly like to emphasize, a significant obstacle within the development of the electronic commerce of the business sector and thus within the development of the Republic of Slovenia in general.

Electronic commerce includes the use of all kinds of information and communication technology in the business processes among the trade, production and service-providing organizations, providers of information, state and public administration and consumers.

It changes the ways of creating products and services and their interference from the producers to the consumers. Additional stimulation for the development of the electronic commerce is given, besides internet, also by the liberalization of the telecommunication. Electronic commerce offers a variety of benefits: faster disclosure of the most advantageous provider of the desired product or service in an optional location in the world at the optional time; more affordable business transactions in connection with marketing, design, production, flow of orders and transport. Therefore possibilities are opening for an interactive communication also among the customers, who have never been in a business or similar relationship. New business possibilities are available, thus creating new ways for increasing of productiveness and decreasing of costs and new ways to approach the customers.

Electronic commerce thus offers to the Republic of Slovenia an opportunity for a faster economic development and an equal competition with much bigger countries to its economy. Namely it is precisely in the electronic world, where the size is losing its significance.

That is why we had to ensure as fast as possible a safe judicial environment for the electronic commerce in domestic and international operation. With a new regulation we removed all the obstacles for the electronic commerce, represented by legislative standards, designed and adopted in the time of exclusively classical operation on paper. Thus all the provisions of Slovenian regulations, which regulate written form of documents, submission of originals, signed documents and similar things, are not a problem any more. At the same time it was necessary to restore a safe environment for verifying the authenticity of the electronically created, stored, sent, received or otherwise processed data. Among the more exacting problems that we regulated there was surely the problem of signature and thus ensuring of the legal effect of the data in an electronic form.

Electronic signatures enable the recipient of the electronic data to verify the source of the data. Thus the recipient himself verifies the authenticity of the source of the data. He verifies also, whether the data are integral and unaltered and thus protects their inalterability. The verification of the authenticity and inalterability of the data does not ensure nevertheless positively the identity of the signatory, who creates electronic

signatures. The recipient thus demands more reliable information about the identity of the signatory. Such information can be given by the signatory himself by providing sufficient proofs to the recipient. The identity of the signatory can also be confirmed by a third party (i. e. a person or an institution, which have confidence by both parties).

The need for a reliable and predictable judicial environment for the electronic commerce caused the demands also elsewhere in the world. In the European Union the European Commission in its report "European initiative in the electronic commerce" from April 1997 wrote that the electronic commerce is essential to increase safety and confidence in the open networks. The Governmental Declaration form Bonn also defined the electronic signature as the key item of the electronic commerce.

Also on wider international level there are many activities and debates in progress. The Commission of the United Nations International Trade Law (UNCITRAL) adopted the Model law on the electronic commerce in 1996 and it is preparing Unified rules for the electronic signature creation. The Organization for Economic Cooperation and Development (OECD) is also dealing with this field since 1997, when it adopted Directives for the Cryptographic Policy. Also other international organization, including the World Trade Organization (WTO), are dealing with the same questions. That is why the adoption of the relevant legislation is indispensable in the Republic of Slovenia for its integration into the world information society.

Besides the general demands, the Act for the enforcement of the electronic commerce had to meet other two requirements. First, it had to take into account the world experiences and decisions in this field. The electronic commerce does not consider at all the state borders and must thus be regulated in an unified way not only on the European, but also on international level. The second requirement derived from the sole nature of the electronic commerce as the commerce that is based on rapid technological development. The development of the information communication technology is extremely fast and bring revolutionary novelties almost on regular bases. Therefore the purpose of a good legislation in this field must not be to follow the technological development, but to remain technologically neutral.

The Act of the electronic commerce and electronic signature wants, it the time if its validity, to achieve various goals, amongst which we will mention only the most important ones. With hte Act the Government wants to encourage and in no way to obstruct fast technological development of the electronic commerce and to remove normative obstacles for the electronic commerce with a special emphasis on equalizing the safe electronic forms with the classical paper form (requirement for the written form) and equalizing of safe and reliable electronic signatures with the autographic signature. The new Act provides clear and predictable rules for the exchange of the electronic messages, and rules for the use of the electronic signature and operation of the certification service providers of the electronic signatures. The new Act insured also that the Slovenian legal framework of the electronic commerce and electronic signature is adjusted with the relevant foreign, mostly European and international legal framework, and thus to ensure an international recognition of the electronic signatures.

The adoption of the Act thus gives to the Slovenian economy and state administration an important competitive advantage, because Slovenia with a modern legal framework is

placed among the first ten European countries, which have, accordingly to the new rules of the EU, regulated the electronic commerce and opened with the relevant legislation a way into a new, technologically supported millenium.

BRIEF EXPLANATIONS TO THE ACT

Gorazd Perenic

Introduction

The Act of the electronic commerce and electronic signature regulates certain legal questions, imposed by fast technological development and accelerated introduction of the electronic commerce into the business and public sector. The essential purpose of the legislator was legally equalize, where it is possible and reasonable, the electronic form of operation with the earlier classical paper operation, and, under special conditions recognize to the electronic signature the same validity as the autographic signature has in the paper world. Thus the Act has suppressed a variety of legal obstacles for the electronic commerce and enabled, together with recently adopted modern legislation, even faster intr oduction of the electronic commerce.

The Act is entirely adjusted with the provisions United Nations' Commission or the International Trade Law's (UNCITRAL) Model Law of the electronic commerce and with the provisions of the primary European legislation. It assumes also all the provisions of the Directive 1999/93/EC of the European parliament and EU Council from 13. December 1999 concerning common framework of the Community framework for electronic signatures.

Principles

The Act of the electronic commerce and electronic signature is based on modern principles: the principle of the non-discrimination of the electronic form, the principle of openness, the principle of the contractual freedom of the parties, the principle of duality, the principle of protection of personal data and protection of the consumers and the principle of international recognition.

The principle of the non-discrimination of the electronic form means, that the paper form and the electronic form are reasonably equalized, thus the courts and state organs within the evaluation of the evidence can not refuse the evidence solely on the grounds of its electronic form.

The principle of the openness or technological neutrality ensures, that the Act does not refer only to one kind of technology or just to current solutions, but it remains general and thus useful for a longer time term and new technologies. Along with the fast and various technological development goes also the principle of duality, which allows the use of different technological solutions with different reliability and thus different legal consequences of the use of such solutions.

The principle of the contractual freedom of the parties enables the parties to agree and regulate their relationships differently. Therefore t he Act explicitly provides that it is not valid for the closed systems, where the parties regulate in advance with a contract all the essential characteristics of the operation of the system. Thus contractual parties within the electronic commerce in the c losed systems are not bound only by the solutions, foreseen by law.

Because of the technological complexity of the solutions for the electronic commerce, also the principle of the protection of personal data and protection of the consumers are important. The principle of the protection of personal data follows the newest rules, enforced in Slovenia and European Union concerning the protection of personal data which are even more exposed in the electronic world. The principle of the protection of the consumers protects an average consumer, for whom - without a lot of technological knowledge - is more difficult to implement his rights in the complicated electronic commerce, and imposes to the service-providers a special care for the consumer.

The principle of international recognition enables a simple mutual recognition of the electronic documents and signatures and thus enables a simple integration of the Slovenian economy into the international economy. International recognition of the legal effect of the data and signatures in an electronic form is very important, because the electronic commerce does at all not take into account the state borders or borders between individual legal systems.

Electronic commerce

The Act is divided into five chapters. In the first chapter the Act defines the field, which it regulates: the electronic commerce and the use of data in the electronic form and electronic signature in the legal transactions and determines the meaning of individual expressions, used in the Act. As the similar legislation, also the Act of the electronic commerce and electronic signature allows the freedom of the clients to regulate their relationship within the creation, sending, receiving storing and otherwise processing the electronic messages, unless otherwise provided by law.

Electronic signature

In the third chapter the Act regulates more extensively the electronic signature and the operation of the certification service providers, who represent an inevitable condition for the use of the electronic signatures. The Act is entirely relying on the European and world orientations and uses a so-called dual approach. Namely, it allows the operation of the certification service providers without previous permission and also does not imply special conditions for their operation, but it enables the operation of the certification service providers under very various conditions providing of different services of verification, which gives them different legal effect regarding their reliability. A part of t hese rules is also a provision of obligatory and voluntary supervision. The first is done by the Agency for the telecommunications, or until its foundation, the Government Center for Informatics within the so-called voluntary accreditation scheme.

The Act provides only general conditions for the operation of the certification service providers and electronic signature creation. the more detailed requirements are – on an explicit legal authorization – with a special provision provided by the Government of the Republic of Slovenia. The Act in itself in its fourth chapter incriminates certain conducts as criminal offences and thereof provides the sanctions.

ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT

I. GENERAL PROVISIONS

Article 1

(1) This act regulates electronic commerce, which includes commerce in the electronic form on distance by the use of information and communication technology and use of electronic signature in legal affairs, including electronic commerce in judicial, administrative and ot her similar procedures, unless provided otherwise by law.

(2) Unless otherwise agreed, the provisions of this act, except the provisions of article 4 in 14, do not apply to closed systems, which are entirely based on contracts among the established number of contracting parties.

Article 2

For the purpose of this act:

1. electronic data means data, which are formed or stored in an electronic way;
2. electronic message means an array of data, which are sent or received in an electronic way, which includes particularly electronic data interchange and electronic mail;
3. electronic signature means an array of data in an electronic form, included, attached to or logically associated with other data and serves as a method of authentication of these data and identification of a signatory;

4. advanced electronic signature means an electronic signature, which meets the following requirements:
- that it is uniquely linked to the signatory;
- that it is reliably capable of identifying the signatory;
- that it is created using secure signature creation device that the signatory can maintain under his sole control;
- that it is linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and the signature are detectable;

5. time stamp means an electronically signed certificate of the certification service provider confirming the contents of the specific data at alleged time;
6. sender of an electronic message means a person by whom or on whose behalf the electronic message was sent; an intermediary shall not be deemed to be the sender of the electronic message;
7. addressee of an electronic message means a person to whom the sender intended the electronic message;
8. recipient of an electronic message means a person who received the electronic message; an intermediary shall not be deemed to be recipient of the electronic message;

9. intermediary of an electronic message means a person who for another person sends, receives and stores electronic messages or provides other services relating to electronic messages;
10. signatory means a person by whom, or on whose behalf, an electronic signature is created;
11. information system means a system used for forming, sending, receiving, storing or otherwise processing electronic data;
12. signature creation data means unique data, such as codes or private cryptographic keys, used by the signatory to create an electronic signature;
13. signature creation device means configured software or hardware, used by the signato ry to create an electronic signature;
14. secure signature creation device means a signature creation device which meets the requirements laid down in Article 37 of this Act;
15. signature verification data means unique data such as codes or public cryptog raphic keys, used for the purpose of verifying an electronic signature;
16. signature verification device means configured software or hardware, used for the purpose of verifying an electronic signature;
17. electronic signature product means configured ha rdware or software, or relevant components thereof, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures;
18. certificate means a certificate in an electronic form, which links signature verification data to a person (certificate holder) and confirms the identity of that person;
19. qualified certificate means a certificate which meets the requirements laid dow n in Article 28 of this Act and is issued by the certificate service provider who fulfils the requirements laid down in Articles 29 to 36 of this Act;
20. certification service provider shall mean a natural or legal person, who issues certificates or provides other services related to certification service or electronic signatures.

Article 3

Persons shall be free to agree on matters regarding creating, sending, receiving, storing or other processing of electronic messages in a different manner than it is stated in this act, unless this conflicts with individual provisions of this act or their meaning.

Article 4

Legal effectiveness and admissibility as evidence shall not be denied to the data in the electronic form solely on the grounds that they are in the electronic form.

II. ELECTRONIC COMMERCE

Section 1 - Electronic message

Article 5

(1) It is assumed that an electronic message originates from a sender if:
- it is sent by the sender, or;
- it is sent by a person authorised by the sender, or;

- it is sent by an information system, programmed by the sender himself, or programmed by an order of the sender to operate automatically, or;
- the recipient established the origin of a message by application of procedure or technology, which was previously agreed upon between the sender and the recipient.

(2) Previous paragraph does not apply:
- as of the time when the recipient has both received notice from the sender that the electronic message is not that of the sender, and had reasonable time to act accordingly or;
- if the recipient knew or should or should have known, had it exercised reasonable care or used any agreed technology and procedure, that the electronic message was not that of the sender.

Article 6

The recipient is entitled to regard each electronic me ssage received as a separate electronic message and to act on that assumption, except to the extent that the electronic message was duplicated and the recipient knew or should have known, had it exercised reasonable care or used any agreed technology and procedure.

Article 7

(1) Where the sender has previously or at the time of sending the electronic message or within the electronic message requested or agreed with the recipient upon the acknowledgement of the receipt of the message and stated that the electronic message is conditional on receipt of the acknowledgement, the electronic message is treated as though it has never been sent, until the sender receives the acknowledgement on the receipt.

(2) Where the sender does not state that the electronic message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the sender may give notice to the recipient stating th at no acknowledgement of the receipt has been received and specifying a reasonable time by which the acknowledgement must be received. If the acknowledgement is not received within the time specified, upon previous notice to the recipient, may the sender t reat the electronic message as though it had never been sent.

(3) Where the sender has not agreed with the recipient on a particular form of the acknowledgement of the receipt of the electronic message, an acknowledgement may be given by any confirmation by the recipient, automated or otherwise, or any conduct of the recipient, sufficient to indicate to the sender that the electronic message has been received.

Article 8

Where the sender receives the recipient’s acknowledgement of the receipt, it is presumed that the related electronic message was received by the recipient. That presumption does

not imply that the electronic message sent corresponds to the electronic message received.

Article 9

Unless otherwise agreed, the dispatch of the electronic message occurs when it enters an information system outside the control of the sender or the person who sent the electronic message on behalf of the sender.

Article 10

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

(2) Unless otherwise agreed and regardless of the provisions of the previous paragraph, if the recipient has designated an information system for the purpose of receiving electronic messages, receipt occurs at the time when the electronic message enters the designated information system, or, if the electronic message is sent to an information system other than the designated information system, at the time when the electronic message is retrieved by the recipient.

(3) Provisions of the previous paragraph apply notwithstanding that the place where the information system is located may be different from the place where the electronic message is deemed to be received after this act.

Article 11

(1) Unless otherwise agreed, an electronic message is deemed to be dispatched from the place where the sender has his place of business or his permanent residence at the time of sending of the electronic message, and is deemed to be received at the place where the recipient has place of business or his permanent residence at the time of the receipt.

(2) If the sender or the recipient does not have a permanent residence, an electronic message is deemed to be dispatched, after the previous paragraph, from the place or received at the place of his habitual residence at the time of sending or receiving of the electronic message.

Section 2 – Electronic data

Article 12

(1) Where the law or any other provision requires that certain documents, records or data be retained, that requirement is met by retaining electronic data, provided that the following requirements are met:

- if the information, contained in an electronic document or record is accessible so as to be usable for subsequent reference; and
- if the information is retained on the format, in which it was generated, sent or received, or in a format which represents accurately the information generated, sent or received;

and

- if such information is retained as to enable the identification of the origin and destination of an electronic message and the place and time when it was sent or received; and
- if such technology and procedures are used as to prevent in a sufficient manner any change or deletion of data, which would not be easily ascertained, or to reliably assure the inalterabilit y of the message.

(2) An obligation to retain documents, records or information in accordance with the previous paragraph does not extend to any information the sole purpose of which is to enable the electronic message to be sent or received (communication da ta).

(3) Where the law or any other regulation requires that certain data are to be presented or retained in the original form, that requirement is met by the message in the electronic form, provided that the conditions set forth in paragraph (1) of this arti cle are met.

(4) The provisions of this article shall not apply to the data, for which this act prescribes more rigorous or special requirements on the retention.

Article 13

(1) Where the law or any other regulation requires information to be in writing, that requirement is met by an electronic message, if the information contained therein is accessible so as to be usable for subsequent reference.

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

1. contracts regulating property and other rights and other rights on immovable things;
2. contracts regulating testaments;
3. contracts regulating property relationships between spouses;
4. contracts of disposal of property belonging to persons who have been dispossessed of legal capacity;
5. contracts of tradition and divis ion of property inter vivos;
6. contracts of life-subsistence and agreements of waiver of heirship prior to inheritance;
7. contracts of donations and contracts of donations mortis causa;
8. contracts of sale with the retention of ownership;
9. other legal acts, which shall be, according to legal provisions, made in a form of a notarial note.

III. ELECTRONIC SIGNATURE

Section 1 – General provisions

Article 14

Electronic signature shall not be denied legal effectiveness or admissibility as evidence solely on the grounds of its electronic form or not being based on a qualified certificate or a certificate issued by an accredited certification service provider or not being created by a secure signature creation device.

Article 15

Advanced electronic signature, verified with qualified certificate, is equal to autographic signature in relation to data in electronic form, and has therefore equal legal effectiveness and admissibility as evidence.

Article 16

Persons, who store the documents, which are electronically signed with the use of signature creation data and signature creation devices, shall store complementary signature verification data and signature verification devices for as long as the documents are stored.

Article 17

The use of signature creation data or signature creation devices without the knowledge of the signatory or the holder of a certificate, which refers to these data or devices, is prohibited.

Section 2 – Certificates and certification service providers, who issue them

Article 18

(1) Certification service provider does not require a special permit for performing his activity.

(2) Certification service provider must report the beginning of performing the activity to the ministry, competent for economy (hereafter: ministry) at least eight days before the beginning. At the beginning of performing the activity or at the change of the activity, certification service provider has to inform the ministry about his internal rules regarding the signature creation and verification and about his procedures and infrastructure.

(3) Certification service provider, who provides services of advanced electronic signature creation, must in his own internal rules take into consideration the security requirements defined with this act and the regulations issued on the basis of this act.

(4) Certification service provider must fulfil the requirements from his internal rules so as at the beginning as continuously all the time of performing the activity.

Article 19

(1) Certification service provider must inform promptly the ministry about all circumstances, which obstruct and prevent him from performing the activity in accordance with current regulations or his internal rules.

(2) Certification service provider must inform promptly the ministry about possible beginning of bankruptcy or compulsory settlement.

Article 20

(1) Certification service provider must revoke the certificate laid down in item 18 of Article 2 in time of its validity in accordance with his internal rules, which regulate revocations of the certificates, however always promptly:
- if the revocation is demanded by the certificate holder or his trustee; or
- when the certification service provider finds out that the certificate holder has lost his legal capacity, passed away, ceased to exist or that the circumstances, which have a n essential influence on the validity of the certificate, have changed; or
- if data in the certificate are false or the certificate was issued on the basis of false data; or
- if signature verification data or the information system of the certification servi ce provider were threatened in a way, that influences on the reliability of the certificate; or
- if signature creation data or the information system of the certificate holder were threatened in a way, that influences on the reliability of the electronic si gnature creation; or
- if the certification service provider ceases with the activity or he has been prohibited to operate and it his activity has not been taken over by another certification service provider; or
- upon receiving an order from the competent c ourt, magistrate or an administrative body for the revocation.

(2) Certification service provider must in his internal rules define when and in what way a notification about an issuance or a revocation of the certificate will be given.

(3) Irrespective of internal rules, a certification service provider must always inform promptly the certificate holder about the revoked certificate and deliver the information about the revocation to every person that demands it, or publish them if he keeps a register on revoked certificates.

Article 21

The ministry must promptly ensure the revocation of the certificates of the certification service provider if he ceases to operate or he is prohibited to operate and his activity has not been taken over by another certification s ervice provider, if the certification service provider does not revoke the certificate.

Article 22

(1) The certificate holder must keep signature creation data and signature creation devices with reasonable care and use them in accordance with the requirement s of this act and regulations issued on the basis of this act and must prevent unauthorised access to these data and devices.

(2) The certificate holder must demand the revocation of his certificate if his signature creation data or his information system we re lost or threatened in a way, which influences on the reliability of the electronic signature creation, or if a possibility of abuse exists or if data stated in the certificate have been changed.

Article 23

If the certificate includes information about a third person, who is not a certificate holder, this person is also entitled to demand a revocation of the certificate.

Article 24

(1) As between the certificate holder and certification service provider, the revocation is effective from the moment of revocation. As between certification service provider and any other person, the revocation is effective from the time it is published or, if the revocation is not published, from the moment that the other person is informed about it.

(2) Revocation of the certificate shall include the time when the revocation took place.

(3) Revocation is valid from the moment it took place onward. A retroactive revocation is not permitted.

Article 25

Provisions regulating certificate and qualified certificate shall mutatis mutandi s apply to the time stamp and services concerning it.

Article 26

Certification service provider must keep the documentation about the security measures in accordance with this act and the regulations, issued on the basis of this act, and about all the issued and revoked certificates in such a manner, that the information will be accessible at any time and its authenticity and inalterability can be verified at all times but at least five years from the particular event or action.

Article 27

(1) The certification service provider must previously notify the ministry and the certificate holders that received his certificates, of the cessation of his activity, and ensure that all his rights and obligations concerning the certificates, issued by him, are taken over by another certification service provider or are revoked.

(2) Certification service provider must forward all of his documentation to another certification service provider, who will take over all of his rights and obligations concerning the issued certific ates, or to the ministry, if there is no such certification service provider.

Section 3 – Qualified certificates and certification service providers, who issue them

Article 28

(1) Qualified certificate must contain:
- an indication that it is issued as a qualified certificate;
- name or firm and State of permanent residence or of place of business;
- name and pseudonym of the signatory respectively or name and pseudonym of the information system respectively, alleging the certificate holder, under whose control it is, with a compulsory statement that it is a pseudonym;
- specific data of the certificate holder, required for the purpose for which the certificate is intended;
- signature verification data, which correspond to signature creation data under the control of the certificate holder;
- an indication of the beginning and the end of the period of validity of the certificate;
- identification code of the certificate;
- safe electronic signature of the certification service provider, who issued the certificate;
- eventual limitations on the scope of the use of the certificate;
- eventual limitations on the value of transactions, for which the certificate can be used.

(2) Unless otherwise agreed, a certificate must not include any other data.

Article 29

Certification service provider, who issues qualified certificates, must ensure to provide services concerning electronic signature with reasonable professional care.

Article 30

(1) Certification service provider, who issues qualified certificates, must ensure the management of a register of revoked certificates, which must contain in particular the identification code of the revoked certificate, so that it can be precisely identified. The register must not contain the information about the reasons for the revocation or any other data, which are not contained in the certificate, except the date and time of the revocation. The register must have a safe electronic signature and the signature must be verified with a qualified certificate with at least the same reliability as the certificates, revoked in the register.

(2) Certification service provider must ensure a possibility of a prompt and safe revocation of the qualified certificate, and also a possibility, that the time when the qualified certificate was issued or revoked, can be precisely determined.

(3) Certification service provider, who issues qualified certificates, must upon the cessation of his activity ensure that another certification service provider, who issues qualified certificates, keeps the revoked qualified certificates in his own register.

(4) If certification service provider does not ensure a continuation of the revocation service, the ministry shall ensure at his expenses that the service is taken over by another certification service provider.

Article 31

Certification service provider, who issues qualified certificates, must with help of an official personal identity document - with a photograph for natural persons or with officially verified documents for legal persons - reliably ascertain the identity and other important characteristics of the person, who requires a certificate.

Article 32

(1) Certification service provider, who issues qualified certificates, must, to ensure implementation of all the provisions of this act, employ personnel who possess the expert knowledge, experience and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic commerce technology and familiarity with proper security procedures.

(2) Personnel must apply administrative a nd management procedures, which are adequate to recognised standards.

(3) The Government of the Republic of Slovenia prescribes with a governmental regulation the kind and the degree of the professional education, years of experience and eventual additional q ualifications required to meet the requirements form the paragraph (1).

Article 33

(1) Certification service provider must use trustworthy systems and products, which are protected against modification and ensure the technical and cryptographic security of the process supported by them.

(2) Certification service provider must take security measures against forgery of certificates, and, in cases where he generates signature creation data, guarantee confidentiality of the data during the whole process of generatin g these data.

(3) Certification service provider must not store the signature creation data of the certificate holder.

(4) Certification service provider must, to store the certificates, use trustworthy systems, which enable a simple detection of alterat ions and at the same time enable:

1. that only authorised persons can make new entries and changes;
2. that information can be checked for authenticity;
3. that certificates are publicly available only if the certification service provider has previously obtained a consent from the certificate holder;
4. that any technical changes compromising the security requirements are apparent to the operator.

(5) The Government of the Republic of Slovenia prescribes with an governmental regulation the more exact criteria to meet the requirements from this article.

Article 34

Certification service provider, who issues qualified certificates, must ensure the risk of liability for damages. The lowest amount of the insurance is prescribed by the regulation by the Government of the Republic of Slovenia.

Article 35

(1) Certification service provider, who issues qualified certificates, must store all relevant information concerning qualified certificates, in particular for the purpose of providing evidence of certification for the purposes of judicial, administrative and other proceedings, for as long as the data, signed with the electronic signature to which the qualified signature is referred, will be stored, but at least for five years from the issuance of the certificate.

(2) The important information of the qualified certificates are deemed in particular the information about how to establish the identity of a certificate holder, about the time and the way of issuing the certificate, the cause, the time and the way of an eventual revocation of the certificate, the time of validity of the certificate and about all the messages, referring to the validity of the certificate, exchanged between the certification service provider and the certificate holder.

(3) The information from the paragraphs (1) and (2) may be recorded electronically.

Article 36

(1) Certification service provider, who issues qualified certificates, must before entering into contractual relationship with a person requiring a certificate, notify that person of all important circumstances regarding the use of the certificate.

(2) Notification shall include:

1. a precise summary of valid regulations and internal rules and other conditions regarding the use of the certificate;
2. information on eventual limitations on the use of the certificate;
3. information on existence of a voluntary accreditation;
4. information on the procedures for complaints and dispute settlements;
5. information on the measures of the certificate holder, necessary for the security of signature creation and for the verification of the electronic signatures and information on the appropriate technology;
6. admonition that the data, which are already electronically signed, will have to be electronically signed again before the security of the existing electronic signature is diminished with time.

(3) Such notification must be written in a readily understandable language and in writing on durable means of communication.

(4) Relevant parts of this notification must be available on request to third persons relying on the certificate.

Section 4 – Technical requirements for secure signature creation

Article 37

(1) Secure signature creation devices must, by the use of appropriate procedures and infrastructure ensure that:

1. the signature creation data used for signature creation are unique and their secrecy is reasonably assured;
2. the signature creation data cannot, in reasonable time and by reasonable means, be derived from the signature verification data, and the electronic signature is effectively protected against forgery using currently available technology;
3. the signatory can reliably protect his signature creation data from unauthorised access.

(2) Secure signature creation devices must not alter the signed data or prevent the data to be presented to the signatory prior to the signature process.

(3) The Government of the Republic of Slovenia prescribes with a governmental regulation more exact criteria to meet the requirements concerning secure signature creation devices from this article.

Article 38

(1) During the advanced signature verification process must be ensured with the use of appropriate procedures that

1. the data used for verifying the electronic signature correspond to the data displayed to the verifier;
2. the signature is reliably verified and the result of the verification and identity of the certificate holder is correctly displayed to the verifier;
3. the verifier can reliably establish the contents of the signed data;
4. the authenticity and validity of the certificate required at the time of signature verification are verified;
5. the use of a pseudonym is clearly indicated;
6. any security-relevant changes can be detected.

(2) The Government of the Republic of Slovenia prescribes with a governmental regulation more exact criteria to meet the requirements concerning the procedures and infrastructure from the previous paragraph.

Section 5 – Liability of the certification service providers

Article 39

(1) By issuing a qualified certificate, the certification service provider is liable to any person, who reasonably relies on the qualified certificate, for:

- accuracy of all data in the qualified certificate as from the time it was issued and that the certificate contains all the data, prescribed for a qualified certificate;
- assurance that at the time of the issuance of the certificate, the certificate holder identified in the certificate held the signature creation data corresponding to the signature verification data, given or identified in the certificate;
- assurance that the signature creation data and the signature verification data together function in a complementary manner in cases where the certification service provider generates them both;
- immediate revocation of the certificate, if there is a reason for such action, and notification of the certificate revocation;
- implementation of the requirements of this act and the regulations issued on the basis of this act regarding advanced electronic signatures and qualified certificates.

(2) Certification service provider may indicate in a qualified certificate limitations of the use or the highest values of transactions of that certificate and is not liable for consequences arising from use of a qualified certificate which exceeds the limitations on it, if the limitations are recognisable to third persons.

(3) Certification service provider is liable for the eventual damage, if he is not able to prove that the damage occurred without his fault.

Section 6 – Supervision

Article 40

(1) Ministry performs the supervision over the implementation of the provisions of this act.

(2) The ministry, within its supervision powers:

- verifies, whether the requirements of this act and regulations issued on the basis of this act are adequately transmitted into internal rules of the certification service providers;
- verifies, whether the certification service provider within his activity at all times fulfils the requirements of this act and regulations issued on the basis of this act and his internal rules;
- supervises the use of appropriate procedures and necessary infrastructure in case of assurance of qualified certificates;

- supervises the legitimacy of issuing, storage and revocations of the certificates;
- supervises the legitimacy of implementation of other services of certification service providers.

(3) The ministry keeps an electronic publi c register of all certification service providers in the Republic of Slovenia. On the request of certification service providers also foreign certification service providers may be registered in the register of all certification service providers, if they fulfil the requirements of this act for the validity of their certificates in the Republic of Slovenia.

(4) The register of certification service providers receives an advanced electronic signature from the ministry. The qualified certificate of the ministry is published in the Official Journal of the Republic of Slovenia.

Article 41

(1) Within his supervision the inspector is in title to:

- inspect the documentation and files, which refer to the operation of certification service providers;
- inspect premises, in which the certification service is performed, information technology, infrastructure and other equipment and technical documentation of the certification service providers;
- control measures and procedures of the certification service provider.

(2) Inspector has the right to confiscate the documentation for up to fifteen days, if it is necessary to secure the evidence or to accurately ascertain the irregularities. In such cases he must issue a receipt about the confiscation.

(3) The inspector is obliged to safeguard the information about the certificates and personal data, obtained within the implementation of his inspection, as an official secret.

(4) The inspector may by an administrative decision:

- prohibit the use of inappropriate procedures and infrastructure;
- in full or in part temporarily suspend the operation of the certification service provider;
- prohibit the operation of the certification service provider, if he fails to fulfil the requirements of this act and the regulations issued of the basis of this act , and if milder measures failed or would fail to succeed;
- order revocation of the certificates, when there is a reason to believe that the certificates were forged;

(5) A complaint, on which the government of Republic of Slovenia will decide, is allowed against the provision from the previous paragraph. The complaint does not suspend the execution of the decree issued under the second indent of the paragraph 4 of this article.

(6) Prohibition of operation shall not influence the validity of previously issued cert ificates.

Section 7 – Voluntary accreditation

Article 42

(1) Certification service providers, who prove that they fulfil all the requirements prescribed with this act and the regulations issued on the basis of this act, may demand that the accreditation body registers them in the register of the accredited certification service providers.

(2) On the request of the accredited certification service providers also foreign certification service providers are registered in the register of accredited certification service providers, if they fulfil the requirements of this act for the validity of their certificates in the Republic of Slovenia.

(3) Certification service providers, registered in the register of the accredited certification service providers (accredited certification service providers) can officiate with the declaration of their accreditment.

(4) Certification service providers, registered in the register of the accredited certification service providers, may indicate this fact in the issued certificates.

Article 43

(1) Accreditation body keeps a public electronic register of its voluntary accredited certification service providers.

(2) Accreditation body gives an advanced electronic signature to the register of the accredited certification service providers. Qual ified certificate of the accreditation body is published in the Official Journal of the Republic of Slovenia.

Article 44

(1) Accreditation body performs the supervision and the official actions over the accredited certification service providers.

(2) Accreditation body:

- issues general recommendations of the operation of the certification service providers and recommendations and standards for the operation of the accredited certification service providers in accordance with the law and the regulations issued o n its basis;
- verifies, whether the requirements of the law and the regulations issued on its basis are adequately transmitted to the internal rules of the accredited certification service providers

- verifies, whether the certification service provider meets the requirements of this act and regulations issued on the basis of this act and his internal rules at all times within his activity;
- controls the use of appropriate procedures and infrastructure with the accredited certification service providers;
- controls the legitimacy of issuing, storage and revocations of the certificates of the accredited certification service providers;
- controls legitimacy of the implementation of other services of the accredited certification service providers.

(3) Accreditation body may recommend:

- a change of the internal rules of the accredited certification service provider;
- cessation of further use of inappropriate procedures and infrastructure to the accredited certification service provider.

(4) In the certification service provider does not follow the recommendations of the accreditation body, he is erased from the register of the accredited certification service providers by the accreditation body with an administrative decision.

(5) Within fifteen days from receiving such administrative decision a complaint is allowed, upon which is decided by the minister, competent for economy.

(6) The minister is obliged to issue an administrative decision on the complaint within thirty days after receiving it. The decision on the complaint is final.

Article 45

The duty of the accreditation body is performed by the Agency for telecommunications.

Section 8 – Validity of foreign certificates

Article 46

(1) Qualified certificates of the certification service provider with a place of business originating from European Union are equal to domestic qualified certificates.

(2) Qualified certificates of the certification service providers with a place of business originating from the third countries are equal to domestic qualified certificates:

1. if the certification service provider fulfils the requirements laid down in Articles 29 to 36 of this Act and is voluntarily accredited in the Republic of Slovenia or in one of the European Union Member States;
2. if the domestic certification service provider, who fulfils the requirements, laid down in Articles 29 to 36 of this Act, guarantees for such certificates as if they were his own;
3. if it is provided by a bilateral or multilateral agreement among the Republic of Slovenia and other countries or international organisations;
4. if it is provided by a bilateral or multilateral agreement among European and other

countries or international organisations.

IV. PENAL PROVISIONS

Article 47

(1) Monetary penalty of 500.000 tolars to 5.000.000 tolars for minor offence is imposed on the certification service provider if he:

1. does not certainly ascertain the identity or other meaningful characteristics of the person, who requests the qualified certificate (Article 31);
2. issues a qualified certificate, which does not contain all the re quested data or contains the data, which it should not contain (Article 28);
3. does not revoke the certificate or qualified certificate in cases, where it is requested by law or his internal rules (Articles 20 and 23);
4. within the revocation does not indicate the time of the revocation of the certificate or the qualified certificate or if he revokes it retroactively(Articles 20 and 24);
5. does not inform the petitioner of the certificate or qualified certificate about all the obligatory information(Article 36);
6. does not inform the ministry before the cessation of his operation and does not ensure that the concern for all the valid certificates or qualified certificates is taken over by another certification service provider, or that the certificates are revoked (Article 27);
7. does not hand over all the documentation to another certification service provider or to the ministry (Article 27);
8. does not inform the ministry about the possible beginning of bankruptcy or compulsory settlement or other circumstances, which prevent him from implementing the provided requirements (article 19);
9. does not keep the prescribed documentation (article 26);
10. does not enable an insight or confiscation of his documentation to the inspector or does not hand the necessary information and explication (article 41);
11. does not report the beginning of performing the activity or does not present the internal rules (article 18);
12. issues qualified certificates and does not keep or deficiently keeps a register of revoked certificates (Article 30);
13. issues qualified certificates and does not execute adequate security measures to prevent unauthorised collecting or copying of signature creation data from his part or by a third person (Article 33);
14. performs his activity in spite of interdiction by the mini stry (Article 41);
15. unjustifiably uses the characterisation of the accredited certification service provider (Article 42).

(2) If the certification service provider is a legal person, a monetary penalty of 50.000 to 100.000 is imposed also on the responsible person of the legal person for minor offence according to the previous paragraph of this article.

Article 48

Monetary penalty of 50.000 to 150.000 tolars for minor offence is imposed on the certificate holder or, in case of a legal person, his responsib le person, if he:

1. does not demand a revocation of the certificate or qualified certificate (Article 22);
2. uses signature creation data and signature creation devices in a manner that is violating the requirements of this act and the regulations issued on the basis of this act (article 22);

Article 49

Monetary penalty of 50.000 tolars to 150.000 tolars for minor offence is imposed on the individual who without knowledge of the signatory or a certificate holder abuses of his signature creation data or signa ture creation devices (article 17).

V. TRANSITIONAL AND FINAL PROVISIONS

Article 50

(1) The Government of the Republic of Slovenia issues an governmental regulation to regulate:

1. measures for the assessment of reliability and for the assessment of implement ation of technical requirements laid down in Articles 33., 37. and 38;

2. professional education, knowledge and experiences from the Article 32;

3. a minimal amount, which a certification service provider shall have at disposal for the defrayal of responsibili ty;

4. the form, publication and the accessibility of the internal rules of the certification service providers;

5. period of validity of the qualified certificates, the period after which a new electronic signature should be given to already electronically s igned data and the relevant procedure;

6. scope of use, requirements and admissible deviations at performing services concerning secure time stamps;

7. type and form of characterisation of the accredited certification service provider;

8. technical conditions f or the electronic commerce in public administration.

(2) The Government of the Republic of Slovenia issues implementing regulations laid down in the first paragraph of this Article in sixty days at the latest after this act is published in the Official Journa l of the Republic of Slovenia.

Article 51

Minister competent for economy may regulate more precisely the way of the implementation of individual provisions of this act.

Article 52

Until the adoption of an act that will regulate the conditions for the e lectronic commerce concerning the verification of a signature by notaries or other competent body, the provision from the article 15 does not apply for such cases.

Article 53

The item 4. of the second paragraph of Article 46 of this act enters into force on the day of the admission of the Republic of Slovenia into a full membership of the European Union.

Article 54

Until the Agency for telecommunications does not take over the duties after this act, duties from its competence after this act are performed by Government Centre for Informatics.

Article 55

This act shall enter into force on the 60 th day after its publication in the Official Journal of the Republic of Slovenia.