GOVERNMENT OF THE REPUBLIC OF SLOVENIA
CENTRE FOR INFORMATICS

DECREE
ON CONDITIONS FOR ELECTRONIC COMMERCE AND ELECTRONIC SIGNING

1. General provisions

Article 1

This decree determines:

- criteria, used for assessment of the compliance with requirements for the operation of the certification service providers, who issue qualified certificates, and contains,
- detailed provisions of internal rules of such certification service providers,
- signature creation and verification of the advanced electronic signatures,
- period of validity of qualified certificates,
- detailed conditions regarding use of secure time stamps
- type and use of marks of the accredited certification service providers,
- conditions for electronic commerce in public administration.

Article 2

Irrespective of the provisions of the other articles of this Decree, hardware, software and the procedures comply with criteria and conditions according to this Decree, if they are in accordance with standards, criteria or conditions, commonly recognized in the European Union and published in the Official Journal of the European Communities.

2. Protection of the infrastructure of the certification service provider in general

Article 3

Premises of the certification service provider and the infrastructure shall be, in accordance with the rules of the profession, properly electronically and physically protected from unauthorized entries.

Article 4

(1) Certification service provider shall implement regular security controls of its infrastructure every working day, or every day, in case he provides his services 24 hours a day, 365 days a year. Certification service provider shall keep a record of all his findings and interventions.

(2) These security controls include verifying, whether the infrastructure is safe, whether all the security systems operate without disturbances and whether in the meantime there had been any intrusions or attempts thereof, by unauthorized persons, trying to get the access to certification service provider’s equipment or data.

Article 5

At least two certification service provider's employees shall operate with the signature creation data at the same time. The certification service provider shall for this purpose ensure that nobody has all the necessary data and tools by himself, with which he could have access to the equipment where the signature creation data of the certification service provider are stored.

Article 6

Certification service provider shall ensure secure storage of at least two backup copies and other media for such transmission of data to prevent a loss of data or use of data by an unauthorized person. Backup copies shall be stored separately form the certification service provider's information system for administration of qualified certificates, on another safe location. Certification service provider shall record the information about the storage of the backup copies.

Article 7

Certification service provider shall use and protect his signature creation data for qualified certificates with reasonable care of an expert and physically and electronically protect them in accordance with the established rules of the profession to prevent physical or electronic breaking in or unauthorized access to these data.

Article 8

Certification service provider shall keep one or few separate records in written, where all the information prescribed with this Decree and other information about the procedures and interventions into infrastructure, which affect the reliability of the operation of the certification service provider, shall be entered. The record shall be accessible and kept for at least 5 years.

Article 9

(1) Certification service provider shall draft special minutes about all the initial authorizations and procedures, used for the establishment of his information system for the administration of qualified certificates. Minutes shall by signed by all the participants in these procedures and permanently stored.

(2) If some changes in the authorizations or important changes of settings of the information system for the administration of qualified certificates, which were

determined when the system was set up, occur later, all the aforementioned changes shall be documented in minutes.

3. Physical protection of infrastructure of the certification service provider

Article 10

Certification service provider shall ensure a proper physical protection of his hardware and supervision of the physical access to his information system for the administration of qualified certificates. He shall promptly enter all the physical accesses to the information system in his record.

Article 11

(1) A contemporary presence of at least two persons, who have a permit for access to the information system, is required for a physical access to the information system of a certification service provider for the administration of qualified certificates.

(2) Entry into premises of the certification service provider, where his information system for the administration of qualified certificates is situated, shall be allowed only to the persons, who discharge their duties and tasks for the certification service provider in these premises. The access shall be in accordance with a written list of persons, who are allowed regularly to enter to individual premises. Persons, to whom a regular entry is not allowed, shall be registered on a special list by persons, who are allowed regularly to enter, and shall be accompanied by such persons all the time.

4. Electronic protection of the infrastructure of certification service provider

Article 12

(1) The information telecommunication infrastructure of a certification service provider, linked to another information telecommunication network, shall be protected with reliable safety mechanisms (system for preventing and detecting of breaking in, fire security and similar), which prevent unauthorized accesses through this network and limit the access to the protocols that are essential for the administration with qualified certificates. All the other protocols shall not be able to access.

(2) If the system is designed in a way that the communication with the system of the certification service provider for the administration of qualified certificates goes through another network, this passage shall be in codes.

Article 13

Information system of the certification service provider for the administration of qualified certificates shall be composed only by hardware and software, required for the administration of qualified certificates.

Article 14

After the validity of the signature creation data of the certification service provider, which are not crucial for the verification of data retroactively, expires, the certification service provider shall safely and reliably destroy all the copies.

Article 15

Information of the certification service provider, which could affect the reliability and safety of the operation of the certification service provider, shall not leave the system uncontrolled in a way that could threaten the operation in accordance with the effective regulations and internal rules of the certification service provider. After they have been used, the means of communication shall be removed and then safely and reliably destroyed.

Article 16

(1) Information system of the certification service provider for the administration of qualified certificates shall have incorporated sufficient security mechanisms, which prevent the abuse by the employees and enable a clear division of the tasks from the scope of the Article 21 of this Decree.

(2) Security measures of the information system for the administration of qualified certificates shall ensure a controlled access to information and supervision of the access up to the very individual, namely for all the interventions and functions, which affect the administration of qualified certificates of the certification service provider.

5. Technical requirements, which the certification service provider shall meet

Article 17

Certification service provider shall within his technology and procedures ensure the uniqueness of the signature verification data, which means that he shall enable an unequivocal and safe determination of identity of the holder from the electronic creation data.

Article 18

(1) Software, used by the certification service provider, shall correspond to the worldwide enforced security and technical standards (FIPS 140-1 for cryptographic modules, recommendable EAL5 or at least EAL3 of Common criteria /ISO 15408/, recommendations of the group of experts from the European Electronic Signature Standardization Initiative – EESSI and other).

(2) Software, which generates the signature creation data, shall ensure the smallest possibility of misappropriation of the data by the use of momentarily available technologies.

Article 19

Certification service provider shall ensure confidentiality and singleness of the use of data, used to generate a qualified certificate.

6. Registry service

Article 20

(1) Employees in registry service of the certification service provider shall reliably ascertain the identity of persons, personally and by use of official documents with a photography of the holder, and collect and communicate the data of the persons, necessary for an issue of a qualified certificate by the certification service provider.

(2) Registry service of the certification service provider shall communicate the acquired data of persons to the other services of the certification service provider in accordance with the law that prescribes protection of personal data.

7. Employees of certification service provider

Article 21

(1) Certification service provider shall employ at least three persons with university education; hence at least two persons with university degree in technical or natural science, and at least two persons shall have two years' working experience in the field of the operation of the certification service providers or related fields.

(2) Duties of the employees for performing tasks of certification service provider shall be distributed among several persons, in a way that the employees are prevented from the abuse. The duties shall be determined in a way that the scope of administration of

qualified certificates, the scope of the administration with the information system of the certification service provider and the scope of protection and control are clearly separated.

Article 22

Certification service provider shall employ or have a proper counseling contract with a lawyer with university degree and with the State exam of jurisprudence.

Article 23

(1) All the persons from the previous two Articles shall have special expertise in administration and knowledge of technology, security procedures and legal requirements from the field of electronic commerce and operation of the certification service providers, for which they shall be professionally qualified.

(2) Employees in the registry service shall be qualified for a reliable determination of the identity of persons.

Article 24

(1) Besides their employment, the employees of the certification service provider shall not perform same or similar work as they perform within their employment, for other certification service providers, if the latter are not subordinate certification service providers, and they shall not perform work, which is incompatible with the working duties and responsibilities they have towards the certification service provider.

(2) Irrespective of the provision of the preceding paragraph the employee of the certification service provider can perform independent scientific and pedagogic work, work in cultural, artistic, sports, humanitarian and other similar associations and organizations, and journalistic work.

8. Technical requirements for secure signature creation and verification of advanced signature

Article 25

Each use of secure signature creation data shall require from the signatory a conscious and reliable act for presentation to the secure signature creation device (i.e. entry of password, fingerprint or similar), except when the information system is programmed in advance to react automatically.

Article 26

(1) User shall always verify the electronic signature in accordance with the instructions of the signatory. When the signatory also annexed the certificate of the certification service provider to the signature, the user shall verify the electronic signature also in accordance with the instructions of the certification service provider, who issued the certificate, or the certification service provider, who is superior or acknowledges the certification service provider, who issued the certificate.

(2) By verifying the electronic signature with the help of the certificate of the certification service provider, the user shall always verify the validity of the certificate in accordance with the instructions of the certification service provider, who issued the certificate. The user shall also verify whether the certificate is registered in the register of the revoked certificates, if the certification service provider, who issued the certificate, keeps such register.

(3) Advanced signature verification device shall enable the user to clearly determine, which data were signed and to what extend they were signed. If the signed data are connected to other data or they refer to other data and the user can automatically link to these data, the device shall clearly warn the user in case the data were not acquired with verified electronic signature.

9. Insurance for the risk of liability

Article 27

The lowest insurance sum, with which the certification service provider, who issues qualified certificates, ensures the risk of liability for damages, is of 50,000.000 tolars.

10. Internal rules of certification service providers

Article 28

Internal rules of certification service providers, who issue qualified certificates, shall include a public and a private part. All the essential provisions of internal rules, which affect the relationship among the certification service provider, holders of qualified certificates, issued by him, and third parties, who rely on these certificates, shall be included in the public part of internal rules.

Article 29

In the public part the internal rules shall include at least:

1. provisions about the infrastructure of the certification service provider, which contain basic technical and procedural properties and information about the level of security and reliability of the infrastructure;
2. provisions about the number, structure and qualifications of the employees of the certification service provider;
3. provisions about the requirement of possible subordinate certification service providers, requirement of mutual recognition of the certification service providers;
4. provisions about security requirements and obligations of the holder of qualified certificates and third parties, who rely on qualified certificates;
5. provisions about basic characteristics and content of qualified certificates, issued by the certification service provider;
6. provisions about administration of qualified certificates, which contain above all the provisions about application for an issue and verification of the identity of persons and provisions about issue, extension of validity and revocation of qualified certificates;
7. provisions about the liability of the certification service provider and about the insurance sum;
8. information about the identity of the certification service provider and his infrastructure;
9. provisions about the procedures in case of cessation of the activity of the certification service provider.

Article 30

In the private part the internal rules shall include at least:

1. provisions about the premises of the certification service provider;
2. additional provisions about the employees of the certification service provider, which mostly include the provisions about competences and tasks of individual members of staff, provisions about special authorizations of members of staff, conditions, required from staff and provisions about eventual external co-workers;
3. provisions about physical protection of infrastructure of the certification service provider, which mostly include the provisions about access into the premises of the certification service provider (entry rights, authentication system, etc.); about management of hardware and wastes; and about entering and taking out the equipment and material;
4. provisions about protection of electronic or software system, which mostly include provisions about security settings of servers, use of telecommunication devices and equipment and provisions about registration into system, security copies and similar;

5. provisions about internal supervision, which include mostly operative implementation and following of the events (control of the physical access, control of authorizations, reporting about security problems and similar);
6. provisions about measures in case of unexpected events;
7. provisions about how to keep registers and to draft minutes, including the provisions about the eventual electronic form of records.

Article 31

Public part of internal rules of the certification service providers shall be publicly accessible in the electronic form on internet or on durable means of communication in an electronic or classical form.

11. Period of validity of qualified certificates

Article 32

Period of validity of a qualified certificate shall be five years at the most from the day if its issue.

Article 33

(1) A person, who stores data, signed with the electronic signature, shall ensure at the latest one month before the termination of the period, determined for the validity of the data for the electronic signature by the certification service provider in the public part of internal rules, a renewed electronic signature of such data by all persons, who electronically signed the data the first time, or by notary, or he shall ensure a confirmation of the data with a secure time stamp of the certification service provider. If no period of validity was determined, the above-mentioned measures shall be taken with the day the qualified certificate expires.

(2) Certification service provider shall, by issuing a qualified certificate, warn the certificate holder about the renewed electronic signature from the preceding paragraph.

12. Secure time stamp

Article 34

(1) Secure time stamp shall contain unequivocal and correct information about the date, exact time (at least to the second) and the certification service provider, who created the secure time stamp.

(2) Secure time stamp may be added or annexed to the document and connected with it, but nevertheless the same requirements shall be met as for the advanced electronic signature with a qualified certificate.

Article 35

Certification service provider, who issues secure time stamps, shall use the information system that is synchronized with a source of the exact time.

13. Mark of accredited certification service provider

Article 36

(1) Mark of accredited certification service provider shall be in a form of a circle, with a capital "A" in the middle and with an inscription "AKREDITIRANI OVERITELJ V REPUBLIKI SLOVENIJI" in the Slovene version; and with an inscription "ACCREDITED CERTIFICATION SERVICE IN THE REPUBLIC OF SLOVENIA" in the English version (enclosure no.1), along the whole margin of the circle.

(2) The mark may be used in arbitrary size by preserving the same proportions (enclosure no.1).

Article 37

(1) Accredited certification service provider may use the mark form the preceding Article for his operation on the documents in classical or electronic form.

(2) Certification service provider shall, by operating in Slovene language, always use the Slovene version of the mark, and by operating in other languages he may use the English version of the mark.

14. Electronic commerce in public administration

Article 38

All the information solutions for the electronic commerce in public administration shall, by including the use of the electronic signature, use exclusively the certificates of the certification service provider of the Government Center for Informatics, SIGOVCA, or the certificates of his subordinates or the other certification service providers, confirmed

by him. The Government Center for Informatics shall develop a hierarchically distributed model of confidence.

Article 39

Administration units shall perform tasks connected to registration and determination of the identity of the persons for the use of electronic commerce with the institutions of public administration. An authorization may be released also to other institutions.

Article 40

(1) A commission operates within the Government Center for Informatics as a counseling body for the questions about the use of electronic commerce and signature in public administration, mostly for examination of security, technical and legal requirements and other questions.

(2) On the basis of Electronic Commerce and Electronic Signature Act the commission gives to the Government of the Republic of Slovenia and to the minister, competent for economy, suggestions for adoption of implementing regulations within their competence, and to inspection and accreditation body the recommendations about determination of security and technical criteria for implementation of the supervision of operation of certification service providers.

Article 41

Members of the commission are nominated by the Government of the Republic of Slovenia from among scientific, technical and legal experts in State administration and outside it on a suggestion by the director of the Government Center for Informatics of the Republic of Slovenia.

15. Provisional and final provisions

Article 42

Employees and contractual co-workers of certification service providers, who will begin to operate before January the 1st 2002, shall meet the requirements form Article 23 of this Decree at the latest until the above-mentioned date.

Article 43

This Decree shall enter into force a day after its publication in the Official Journal of the Republic of Slovenia.