

Important Disclaimer

The English language text below has been provided by the Translation Centre of the Ministry for European Integration for information only; it confers no rights and imposes no obligations separate from those conferred or imposed by the legislation formally adopted and published. Only the latter is authentic.

CROATIAN PARLIAMENT

242

Pursuant to Article 88 of the Constitution of the Republic of Croatia, I hereby issue this

DECISION

ON THE PROCLAMATION OF THE ELECTRONIC SIGNATURE ACT

I hereby proclaim this Electronic Signature Act, which was enacted by the Croatian Parliament at its session held on 17 January 2002

Number: 01-081-02-237/2
Zagreb, 24 January 2002

President
of the Republic of Croatia
Stjepan Mesić (*signed*)

ELECTRONIC SIGNATURE ACT

I. GENERAL PROVISIONS

Article 1

This Act shall govern the right of natural and legal persons to use electronic signatures in administrative, commercial and other operations, and the rights, obligations and responsibilities of natural and legal persons associated with the providing of services to certify electronic signatures, unless specified otherwise by special legislation.

Definition of terms Article 2

Individual terms used in this Act shall have the following definitions:

1. *Electronic signature* – shall mean a set of data in electronic form which are associated or logically connected with other data in electronic form and which serve to identify the signatory and the authenticity of the signed electronic document,
2. *Advanced electronic signature* – shall mean an electronic signature which fully guarantees the identity of the signatory and which complies with the requirements stipulated in Article 4 hereof,
3. *Signatory* – shall mean a person who possesses the means to generate the electronic signature and to sign therewith, and who acts either on his or her own behalf or on behalf of the natural or legal person that he or she represents,
4. *Electronic document* – shall mean a complete set of data which is electronically generated, sent, received or stored on electronic, magnetic, optical or other media. The content of an electronic

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

document shall encompass all forms of written or other text, data, images and drawings, maps, sound, music, speech and computer databases,

5. *Electronic signature development data* – shall mean the unique data, such as the codes or the private encryption key which the signatory uses to generate the electronic signature,

6. *Electronic signature development tools* – shall mean the appropriate computer equipment or software which the signatory uses to generate the electronic signature,

7. *Advanced electronic signature development tools* – shall mean the means used to generate the signature which complies with the requirements contained in Article 9 hereof,

8. *Signature verification data* – shall mean data such as codes or public encryption keys which are used for the purpose of verifying electronic signatures,

9. *Signature verification tools* – shall mean the appropriate computer equipment or software used to apply the data for verification of signatures,

10. *Certificate* – shall mean the confirmation in electronic form which links the data for authentication of the electronic signature with a specific person and confirms the identity of such person

11. *Key certificate* – shall mean a certificate which complies with the requirements stipulated in Article 11 hereof and which is issued by the certification authority that fulfils the conditions from Article 17 hereof,

12. *Certification authority* – shall mean a legal or natural person who issues certificates or provides other services pertaining to electronic signatures,

13. *Electronic signature tools* – shall mean the computer equipment or software or their relevant components which are intended for application by the certification authority to render services pertaining to electronic signatures or which are intended for application in the development or authentication of electronic signatures.

II. ELECTRONIC SIGNATURES AND ADVANCED ELECTRONIC SIGNATURES

Article 3

For the purpose of this Act, an electronic signature shall be a set of data in electronic form which serve to identify the signatory and the authenticity of the signed electronic document.

Article 4

The advanced electronic signature shall, for the purpose of this Act, be an electronic signature which:

1. is exclusively linked to the signatory,
2. ***positively** identifies the signatory,
3. emerges through the utilisation of tools which can be independently managed by the signatory and which are under the signatory's exclusive supervision,
4. contains a direct connection with the data to which it pertains in a manner that renders wholly visible and apparent any alterations to the original data.

Article 5

The advanced electronic signature shall be identical in validity to and shall serve as a replacement for a ***written signature** and imprint of an official seal if it is developed in accordance with the provisions hereof and if it complies with all the other conditions stipulated hereof and all regulations adopted pursuant to this Act.

Article 6

An electronic signature may not be the grounds for ***the invalidity, rejection or contestation of the validity and value of the content of a document*** exclusively due to its electronic form.

By way of derogation, Paragraph (1) hereof shall not apply to:

1. legal proceedings whereby title to real estate is conveyed or other material rights to real estate are established,

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

2. probate hearings,
3. asset-related premarital or marital contracts,
4. encumbrance or alienation of assets which requires the approval of social welfare centres,
5. contracts on the transfer and disposal of assets during the conferring party's lifetime,
6. contracts on lifelong support and agreements pertaining to inheritance,
7. bequest agreements,
8. other legal proceedings which must be compiled in the form of notary public deeds or documents as stipulated by special legislation,
9. other legal proceedings or operations wherein special legislation or regulations adopted pursuant to the law explicitly stipulate the use of *manual signatures* on paper documents or certification of manual signatures*.

Article 7

The provisions from Article 6(1) of this Act shall only apply in cases when the protection of electronic signatures and advanced electronic signatures and the verification of the signatory's identity are implemented with the help of the existing technology by the signatory or the certification authority. The Minister of Economy shall issue regulations which stipulate the measures for the protection of electronic signatures and advanced electronic signatures and the measures to verify the identity of signatories that must be undertaken pursuant to Paragraph (1) hereof.

Article 8

Electronic signatures shall be generated by electronic signature development tools. Advanced electronic signatures shall be generated by advanced electronic signature development tools.

Article 9

The advanced electronic signature development tools shall comply with the following requirements:

1. the advanced electronic signature development data only appears once, and their security is ensured,
2. the advanced electronic signature development data may not reoccur, and the signature is protected from forgery in the use of existing and available technology,
3. *the advanced electronic signature development data can fully protect the signatory against its use by others.*

Upon the generation of the advanced electronic signature, advanced electronic signature development tools shall not enable the *alteration of electronic signature development data* nor prevent the signatory from viewing these data prior to the process of generating the electronic signature.

III. CERTIFICATES AND CERTIFICATION AUTHORITIES

Article 10

For the purpose of this Act, a certificate shall be any electronic confirmation whereby the identity of the signatory may be authenticated in procedures of exchange of electronic documents.

Article 11

For the purpose of this Act, a key certificate shall be any electronic confirmation whereby a certification authority verifies an advanced electronic signature.

The key certificate from Paragraph (1) hereof shall contain:

1. a designation which indicates that it is a key certificate,
2. an identifying set of data on the person issuing the certificate (personal name; name of father or mother; nickname, if one exists; date of birth; place of residence or sojourn; designation of legal person and headquarters, if the certificate is issued by a legal person),

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

3. an identifying set of data on the signatory (personal name; name of father or mother; nickname, if one exists; date of birth; place of residence or sojourn).
 4. data for the authentication of the electronic signature which correspond to the electronic signature development data controlled by the signatory,
 5. data on the duration of validity of the certificate,
 6. an identifying designation of the issued certificate (numerical or other designation, and date of issue),
 7. the advanced electronic signature of the certification authority issuing the certificate,
 8. limitations pertaining to the use of the certificate, if any exist,
 9. limitations to the value of the transaction for which the certificate is issued, if any exist.
- The certification authority issuing key certificates shall be obliged to insure against risks for liability for damages which emerge in the rendering of certification services (compulsory liability insurance). The Minister of Economy shall issue regulations to establish the lowest insurance rate from Paragraph (3) hereof.

Article 12

The certification authority may provide certification services if it possesses:

1. the appropriate organisational solutions which guarantee the quality of rendering certification services,
2. the appropriate financial and material means which secure the long-term rendering of certification services and the coverage of possible damages, compensation associated with insurance, and similar contingencies,
3. qualified personnel able to execute the appropriate technical and expert operations involved in the rendering of certification services, maintenance of signatory registers and safeguarding of confidential data,
4. the appropriate technical and programming framework which supports international standards for the rendering of certification services,
5. the system of physical protection for devices, equipment and data,
6. the security solutions to protect against unauthorised access and damage to information.

The Minister of Economy shall issue regulations to stipulate the type, content and methods for submitting documentation on the fulfilment of the conditions from Paragraph (1) hereof.

Article 13

Certification authorities shall not be required to obtain a special licence for providing services.

Article 14

The Ministry of Economy (hereinafter: the Ministry) shall have jurisdiction over the maintenance of records on certification authorities.

Article 15

The certification authority shall be obliged to report to the Ministry on the commencement of providing certification services not less than eight days before the commencement of operations.

Together with the report from Paragraph (1) hereof or in cases of changes in the rendering of services, the certification authority shall submit to the Ministry the documentation which delineates the internal operating rules pertaining to the generation and authentication of electronic signatures and data on internal structure, as well as documentation which testifies to the fulfilment of the conditions from Article 12 of this Act.

Article 16

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

The Ministry shall enter the certification authorities into the Directory of Certification Authorities in the Republic of Croatia (hereinafter: the Directory) immediately after the certification authority submits the report whereby the Ministry is informed of the commencement of rendering services.

Entry into the Directory shall not be subject to administrative court proceedings.

The Minister of Economy shall issue regulations that stipulate the content of the Directory, the methods for maintaining the Directory, and the forms to apply for entry into the Directory and to report changes to be entered.

Article 17

Over and above the conditions stipulated in Article 12 hereof, the certification authority which issues key certificates must additionally fulfil the following conditions:

1. proven ability to securely provide certification services,
2. secured operating conditions to maintain a secure and updated signatory register and implement secure and immediate discontinuation or revocation of certification services at the request of the signatory,
3. secure accurate establishment of the date and time (hour and minute) of issuing or revoking confirmations,
4. secure authentication—in an appropriate manner and in accordance with valid legislation—of the identity and, if necessary, any additional features of the person for whom the certificate is issued,
5. a staff with specialist knowledge and the experience necessary to render certification services, particularly with abilities at the managerial level, professionalism in the application of electronic signature technology and the corresponding security procedures, together with the application of the corresponding administrative and managerial procedures which comply with generally accepted standards,
6. reliable systems and products which are protected from modification and which ensure technical and cryptographic operational security,
7. reliable measures against forgery, and in cases wherein electronic signature data is generated, assurance of the confidentiality of generation processes for such data,
8. sufficient financial resources for operations in compliance with the requirements set for the operation of financial institutions, particularly with reference to liability risks (suitable liability insurance),
9. a system to store all relevant information pertaining to limited-time key certificates, particularly for providing records of certificates for *legal proceedings,
10. *assurances that such authority neither stores nor copies electronic signature development data for persons on whose behalf encryption key management services are provided,
11. *assurances that before entering into contractual transactions with a person who seeks certification services, such person shall be informed by means of permanent forms of communication on the precise conditions for the utilisation of services, including any limitations, the existence of applied accreditation schemes and procedures to resolve claims and appeals. Such information, which may be submitted electronically, shall be written and prepared in intelligible form in the Croatian language. The relevant components of this information must also be available at the request of third parties who use the certificate,
12. *utilisation of reliable systems to store certificates in a form conducive to authentication such that:
 - a. entry and alterations are only done by authorised persons,
 - b. information can be verified for authentication,
 - c. the certificate is publicly available for searches only in those cases wherein the registered signatory is given authorisation,
 - d. the certification authority is aware of any technical changes which could damage security requirements.

Article 18

The certification authorities which issue key certificates shall render such services pursuant to a licence issued by the Ministry at the request of the certification authority.

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

The licence to issue key certificates (hereinafter: licence) shall have the legal significance of a ruling issued in administrative proceedings.

The licence shall be issued within a period of 15 days after the date on which a complete and accurate request is submitted.

During administrative proceedings held to issue a licence, the provisions of the *General Administrative Proceedings Act shall be applied in matters not regulated by this Act.

Article 19

*Qualified certification authorities issuing key certificates which have been granted a licence shall be entered into the *Register of Qualified Certification Authorities in the Republic of Croatia (hereinafter: the Register), which shall be maintained by the Ministry.

The licence may contain the registration number whereunder the certification authority is entered into the Register and the date of entry into the Register.

The *qualified certification authority may commence rendering services upon entry into the Register. The content and procedures for maintaining the Register and content of the applications for licences, as well as the designation of the necessary attachments to such applications, shall be stipulated in regulations issued by the Minister of Economy.

Article 20

Certification services may additionally be provided by government bodies if they comply with all conditions stipulated by this Act and the regulations enacted pursuant to this Act.

The scope of operations, content and providers of certification services in and for government bodies shall be established by a *directive of the Government of the Republic of Croatia.

Article 21

Certification services in the Republic of Croatia may be rendered only by registered certification authorities.

Certification authorities entered in the *Register of Qualified Certification Authorities may indicate this fact in issued key certificates.

Article 22

The *Register of Qualified Certification Authorities and the Directory of Certification Authorities shall be public and maintained in electronic form.

The *Register of Qualified Certification Authorities and the Directory of Certification Authorities and all amendments thereto shall be published in *Narodne novine* (the Official Gazette of the Republic of Croatia).

IV. RIGHTS, OBLIGATIONS AND RESPONSIBILITIES OF SIGNATORIES AND CERTIFICATION AUTHORITIES

Article 23

Signatories shall select certification authorities at their own discretion.

The signatory may use the certification services of one or more certification authorities.

Signatories who so desire may engage the certification services of a certification authority based abroad.

Signatories shall engage certification services pursuant to contracts concluded with the selected certification authorities.

Signatories employed in government bodies or by legal persons vested with public authority may be excluded from the application of the provisions contained in Paragraphs (1) to (3) hereof when such

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

body or legal person has its own developed certification system and conducts certification operations for its employees.

Article 24

A key certificate may be issued to any and all persons at their request and on the basis of unmistakably established identity and other data which more expansively speak of the person for whom the key certificate is issued.

The certification authority shall issue certificates for each individual signatory pursuant to contracts concluded with such signatories.

Article 25

Each signatory shall be obliged to undertake all necessary organisational and technical measures to protect against loss and damages which may be incurred by other signatories, certification authorities and third parties.

Article 26

The signatory shall be obliged to mindfully utilise and safeguard electronic signature development tools and data, utilise electronic signature development tools and data in accordance with the provisions of this Act, and protect and safeguard electronic signature development tools and data from unauthorised access and use.

Article 27

The signatory shall be obliged to submit to the certification authority all necessary information on changes which influence or may influence the accuracy of electronic signatures within a period of two days after the emergence of such changes.

The signatory shall be obliged to immediately seek the revocation of its confirmation in all cases of loss or damages to the tools or data to generate its electronic signature.

Article 28

Signatories shall be accountable for irregularities which emerge as the result of failure to fulfil the obligations stipulated by the provisions of Articles 25, 26 and 27 of this Act.

By way of derogation, signatories may be exempted from accountability in cases when they may prove that the damaged party did not undertake or incorrectly undertook the operations associated with the authentication of electronic signatures.

Article 29

Certification authorities shall be obliged to:

1. ensure that each confirmation contains all necessary data pursuant to Article 11 hereof,
2. conduct a comprehensive authentication of the identity of the signatories for whom the certification service is being provided,
3. ensure the accuracy and integrity of the data incorporated into the records of issued certificates,
4. incorporate *specific data on themselves into each confirmation,
5. make available to all interested parties the identification data on the certification authority and the licence for issuing key certificates,
6. maintain accurate records on certificates protected by secure measures which must be publicly accessible,
7. maintain accurate records on invalid certificates protected by secure measures,
8. ensure that the date and time (hour and minute) of the issuing or revocation of certificates is visible and ascertainable in the records of issued certificates,

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

9. safeguard all data and documentation on issued certificates for a period of not less than ten years, in which time such information and accompanying documentation may be in electronic form,
10. apply the provisions of laws and other *subordinate legislation which regulate the protection of personal data.

Article 30

Certification authorities shall be obliged to discontinue the service of providing certificates, or execute the revocation of certificates to those signatories:

1. who explicitly seek this,
2. for whom inaccuracies or incomplete data in certificate records has been determined,
3. for whom an official death notice has been issued,
4. for whom an official notice of occupational disability has been issued.

Certification authorities shall be obliged to maintain updated records of all revoked certificates.

Certification authorities shall be obliged to inform signatories of the revocation of certificates within a period of 24 hours after receiving notification of the justification for revoking such certificate.

Certification authorities shall be obliged to inform the Ministry of each revocation of a certificate within a period of 24 hours after receiving the notification from Paragraph (3) hereof.

Article 31

Certification authorities that issue key certificates must safeguard all documentation on issued and revoked certificates as means of providing evidence and verification in judicial, administrative and other proceedings within a period of not less than ten years of their issuing.

Article 32

Certification authorities shall be obliged:

1. to apply the *appropriate organisational and technical measures to safeguard certificates and data associated with signatories,
2. to apply security systems for access to records on certificates and revoked certificates that secure access exclusively to authorised persons that will be able to ensure the authentication of the accuracy of data transmission and that will be able to secure the timely review of any possible shortcomings in technical means and equipment,
3. to inform signatories of all technical requirements and organisational procedures necessary for certification services.

The measures and procedures from Paragraph (1) hereof shall be established in regulations issued by the Minister of Economy.

Article 33

Certification authorities shall be obliged to inform each signatory and the Ministry of the termination of a contract due to possible bankruptcy or overriding necessity or the intent to cease operations within a period of not less than three months prior to the expiry of the certification services entrusted thereto by the said contract.

The certification authority shall be obliged to secure the continuation of certification services with another certification authority for the signatories to whom certificates were issued. Inasmuch as this proves impossible, the certification authority shall be obliged to revoke all issued certificates and immediately inform the Ministry thereof.

Certification authorities in the process of ceasing to provide certification services shall be obliged to submit all documentation pertaining to certification services to another certification authority to whom certification services are being transferred, or to the Ministry if there is no other certification authority.

The Ministry shall forthwith secure the revocation of all certificates issued by the certification authority which for any reason whatsoever ceased to provide certification services, failed to secure the

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

continuation of such services with another certification authority and did not revoke all issued certificates.

Article 34

A certification authority shall facilitate links between its own records of issued and revoked certificates with that of other certification authorities with the application of available information technology and the use of technical and software tools the performance of which complies with ***international application standards**.

The technical rules to secure links between the records of issued and revoked certificates of certification authorities in the Republic of Croatia shall be established in regulations issued by the Minister of Science and Technology after obtaining the prior opinion of the State Bureau of Standards and Metrology.

The technical rules from Paragraph (2) hereof shall incorporate the currently available scientific and technological achievements and internationally accepted standards and may be valid for a period not to exceed two years.

Certification Authorities Based Abroad

Article 35

Certification services may be rendered by certification authorities based abroad which are registered for such services in one of the member states of the European Union.

Certification services may additionally be rendered by certification authorities based abroad when they fulfil the conditions stipulated by this Act and when they are entered in the ***Register of Qualified Certification Authorities**.

Key certificates issued by foreign certification authorities based abroad in a member state of the European Union shall be deemed ***identical** to key certificates issued in the Republic of Croatia.

Key certificates issued by foreign certification authorities based abroad but outside of the European Union **and which are registered in the Republic of Croatia** shall be deemed identical to key certificates issued in the Republic of Croatia:

- if the certification authority fulfils the conditions stipulated herein to issue key certificates and if such certification authority is registered in the Republic of Croatia,
- if a domestic certification authority recorded in the Register of Qualified Certification Authorities attests to the quality of such a key certificate,
- if so determined by a bilateral or multilateral agreement between the Republic of Croatia and other countries or international organisations,
- if the key certificate or qualified certification authority is recognised on the basis of a bilateral or multilateral agreement between the European Union and third countries or international organisations.

V. OVERSIGHT

Article 36

***Oversight** of the activities of certification authorities shall be conducted by the Ministry.

***Oversight** of the activities of certification authorities in the collection, use and safeguarding of personal data of signatories may additionally be conducted by government and other bodies determined by law and other legal instruments which regulate the protection of personal data.

Article 37

Within the framework of its ***oversight** authority, the Ministry shall conduct inspections of the operations of registered and recorded certification services, and:

- ensure that the conditions stipulated by this Act and the ***subordinate legislation** adopted hereunder are fulfilled,

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

– oversee the legality of the application of stipulated procedures and organisational and technical measures, as well as the internal rules pertaining to the conditions stipulated by this Act and the *subordinate legislation adopted hereunder.

If the registered or recorded certification authority does not fulfil the conditions stipulated by this Act and *subordinate legislation adopted hereunder, a public official of the Ministry authorised to conduct *inspections shall issue a ruling in an administrative proceeding whereby the certification authority is temporarily prohibited from rendering certification services.

Article 38

In the interest of facilitating *oversight, the certification authority shall be obliged to provide unrestricted access to data on operations, operating documentation, the register of signatories and the associated computer equipment and devices to authorised *inspectoral officials of the Ministry.

VI. PENALTIES

Article 39

A *monetary fine of HRK 2,000.00 to 10,000.00 shall be charged to a natural person who:
– gains unauthorised access to and uses electronic signature and advanced electronic signature development data and tools.

Article 40

A signatory, meaning a natural person or accountable person of the legal person representing such signatory, shall be charged with a *fine of HRK 2,000 to 10,000 if:

1. the electronic signature development tools and data are used imprudently and irresponsibly (Article 26),
2. a notification on changes in data which influence or may influence the *validity of an electronic signature is not submitted to the certification authority (Article 27(1)),
3. a request for revocation of the certificate is not submitted to the certification authority in due time (Article 27(2)).

Article 41

The certification authority shall be charged with a fine of HRK 5,000 to 100,000 in cases when such certification authority:

1. issues a key certificate which does not contain all necessary data or contains data which had not been foreseen (Article 11(2)),
2. does not conduct the appropriate protective measures whereby the unauthorised collection or copying of data to generate electronic signatures is prevented (Article 17(1)10),
3. fails to inform the signatory to whom the certificate is issued of all important conditions for the use of the issued certificate (Article 17(1)11),
4. fails to establish the *legally-valid identity of the natural or legal person for whom the key certificate is to be issued (Article 29(1)2),
5. does not maintain *updated records of issued certificates and fails to facilitate their *public review and access (Article 29(1)6),
6. does not maintain updated records of all revoked certificates (Article 30(2)),
7. fails to inform the signatory of the completed revocation of the certificate in due time (Article 30(3)),
8. fails to inform the Ministry of the completed revocation of a certificate (Article 30(4)),
9. fails to duly inform the signatories to whom certificates were issued and the Ministry of the possible commencement of bankruptcy proceedings or other circumstances which may lead to the cessation of performing certification services (Article 33(1)).

MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION

VII. TRANSITIONAL AND FINAL PROVISIONS

Article 42

The Government of the Republic of Croatia shall enact the directive from Article 20(2) hereof within a period not to exceed three months after the date of entry into force of this Act.

Article 43

The Minister of Economy shall issue the regulations from Article 7(2), Article 11(4), Article 12(2), Article 16(3), Article 19(4) and Article 32(2) hereof within a period not to exceed three months after the date of entry into force of this Act.

Article 44

The Minister of Science and Technology shall issue the regulations from Article 34(2) hereof within a period not to exceed six months after the date of entry into force of this Act.

Article 45

This Act shall enter into force on the eighth day of its publication in *Narodne novine* (the Official Gazette of the Republic of Croatia), and its application shall commence as of 1 April 2002.

Class.: 650-05/01-01/01
Zagreb, 17 January 2002

CROATIAN PARLIAMENT
Zlatko Tomčić (*signed*)
Speaker of the Croatian Parliament