

**DECREE  
of the National Security Authority**

of 9 September 2002

**on the manner and procedure of using an electronic signature  
in commercial and administrative intercourse**

The National Security Authority (hereinafter referred to as the “Authority”) pursuant to Article 27 of Act No 215/2002 Coll. on the electronic signature and on the amendment to certain acts (hereinafter referred to as “the Act”) lays down:

Article 1  
Scope

This Decree governs details on the manner and procedure of using an electronic signature in commercial and administrative intercourse.

Article 2  
Definitions

For the purposes of this Decree

- (a) commercial intercourse means the dispatch or receipt, or dispatch confirmation or receipt confirmation of an electronic document in relations which arise in electronic trade between the provider of an information company’s services and their recipient or consumer,
- (b) administrative intercourse means the dispatch or receipt, or dispatch confirmation or receipt confirmation of an electronic document signed by a valid qualified electronic signature between public authority bodies and the general government bodies, or between a public authority body and a natural person, or between a general government body and a natural person, or between a public authority body and a legal entity, or between a general government body and a legal entity,
- (c) format of an electronic document means its internal structure and manner of numerical coding of the document,<sup>1</sup>
- (d) electronic mail means a means enabling the dispatch or receipt of an electronic document,
- (e) data transmission network means the communication environment enabling the transmission of an electronic document from its sender to its recipient,
- (f) information kiosk means a publicly accessible technical device enabling the communication of a person with a public authority body or with its electronic registry, in particular with a view to submitting an electronic document, obtaining a confirmation on the submission of an electronic document, or obtaining information on handling a submitted electronic document.

Article 3  
Use of an electronic signature

---

<sup>1</sup> Article 2 (a) of Act No 215/2002 Coll. on electronic signature and on the amendment to certain acts.

(1) In administrative intercourse only a qualified electronic signature can be used for signing an electronic document.

(2) In commercial intercourse an electronic signature or a qualified electronic signature can be used for signing an electronic document.

#### Article 4

##### Electronic document in commercial intercourse

(1) An electronic document used in commercial intercourse, signed by a qualified electronic signature pursuant to a specific regulation<sup>2</sup> has the same legal force as a signature in the signer own hand, created in a written form.

(2) In signing an electronic document in commercial intercourse it is not essential whether the individual natural persons sign for themselves or on behalf of a legal entity.

(3) The procedure for generating an electronic document's qualified electronic signature in the commercial intercourse of a natural person, a legal entity on behalf of which a natural person signs, two or more natural persons, or two or more legal entities on behalf of which one or more natural persons sign is laid down in Annex 1.

#### Article 5

##### Electronic document in administrative intercourse

(1) An electronic document intended for administrative intercourse is generated and signed on technical devices in the property of a natural person, which are not generally accessible to the public, in the property of legal entities that are not public authority bodies and which are not generally accessible to the public, in the property of natural persons or legal entities that are not public authority bodies and which are public accessible, or on technical devices administered by public authority bodies or general government bodies.

(2) The specification of technical devices, required functional qualities and principles for using the time stamp are laid down in a specific regulation.<sup>3</sup>

(3) Persons disposing with technical devices under paragraph (1) ensure their operation pursuant to paragraph (2).

(4) A public authority body or general government body receives, dispatches, verifies, confirms and processes electronic documents by means of an electronic registry

#### Article 6

##### Electronic registry

(1) If a public authority body or general administration body uses a qualified electronic signature, it shall establish an electronic registry for the receipt, dispatch, verification,

---

<sup>2</sup> For example, the Civil Code.

<sup>3</sup> Decree of the National Security Authority No 539/2002 Coll. laying down details on requirements for secure devices for generating time stamps and requirements for electronic signature products (on electronic signature products).

confirmation and processing of electronic documents (hereinafter referred as the “handling of electronic documents”) in intercourse with natural persons or with legal entities, or with other public authority bodies or general government bodies.

(2) The electronic registry ensures, via organisational measures and with the aid of technical devices, at minimum

- (a) the receipt, dispatch, verification, confirmation and processing of electronic documents by means of
  - 1. a data transmission network,
  - 2. electronic mail,
  - 3. standard data media,
- (b) the control of electronic documents received, in particular the ability of their problem-free reading by technical devices of the electronic registry, compliance with the set format and content, and absence of harmful codes and bit sequences (macros, viruses, Trojan horses, worms, etc.),
- (c) validation of a qualified certificate linked to the qualified electronic signature of the electronic document,
- (d) confirmation on the receipt or rejection of the electronic document by issuing an own electronic document, using a time stamp,
- (e) forwarding of the electronic document for its further handling within the public authority body or general government body,
- (f) receipt of the electronic document handled or created by the Authority for its dispatch outside the public authority body or general government body.

(3) In order to ensure the use of electronic registry services, the public authority body or general government body, following its establishment, issues in the written form and by means of the data transmission network in the electronic form

- (a) a list of full electronic addresses enabling intercourse with the public registry,
- (b) the address of the electronic registry and the address at which it is possible to communicate with the public authority body or with the general government body on questions of using and the activity of electronic registry,
- (c) a list of qualified certificates or full electronic address at which the list of qualified certificates of all employees of the public authority body or general government body, ensuring the operation of the electronic registry, can be found,
- (d) formats of electronic documents from the set of admissible formants according to Annex 3, which the electronic registry receives,
- (e) types and characteristics of data media on which the electronic registry receives electronic documents,
- (f) rules for sending electronic documents and confirming their receipt, including any time limitation for intercourse with the electronic registry,
- (g) list of types of electronic documents received and the manner of obtaining electronic models of submissions.

(4) In handling an electronic document, in particular in confirming its reception or forwarding for further handling the electronic registry use the services of a time stamp.<sup>4</sup>

(5) Security of an electronic registry operation corresponds to the security documents adopted by the public authority body and is based on its security policy.

---

<sup>4</sup> Article 9 of Act No 215/2002 Coll.

(6) A security project and security guidelines corresponding to at least degree “V” are processed and approved for the operation of an electronic registry and its technical devices.<sup>5</sup> The security measures adopted and realised must ensure the availability of information processed and stored in the electronic registry, their back-up and restoration following the occurrence of an extraordinary situation. The status and observance of security measures under security documents are subject to the control activity at least once every six months.

(7) Principles of the electronic registry activity are set out in Annex 2.

(8) For facilitating a person’s intercourse with a public authority body or its electronic registry, the public authority body or general government body can create information kiosks, where necessary.

#### Article 7

##### Submission of an electronic document

(1) An electronic document signed by a qualified electronic signature, submitted to the public authority body or general government body by means of an electronic registry are deemed equal to a written or printed document signed in the own hand of the person who, in the case that the electronic form of the document was used, is the signer of this document.

(2) Concurrently with the submitted electronic document, it is recommended that the public key qualified certificate of the electronic document’s signer be submitted to the electronic registry.

#### Article 8

##### Processing the electronic document

(1) A public authority body or general government body, following the receipt of an electronic document, handles it in a similar manner as a written document.

(2) A shredding code applies to the removal and liquidation of electronic documents.

(3) The provisions of paragraphs (1) and (2) apply, unless a specific law provides otherwise.<sup>6</sup>

#### Article 9

##### Electronic document formats

(1) In commercial intercourse an electronic document format is used the description of which is generally available and on which the parties have agreed.

(2) In administrative intercourse only those document formats given in Annex 3 are used.

(3) If the electronic document format admits the use of active elements, the electronic document containing these active elements may not be signed by an electronic signature and may not be used in commercial or administrative intercourse.

---

<sup>5</sup> Decree of the National Security Authority No 90/2002 Coll. on security of technical devices.

<sup>6</sup> Act No 241/2001 Coll. on the protection of classified materials and on the amendment to certain acts.

(4) If the technical device used for the creation of, or adjustment to electronic documents in administrative intercourse creates a document format other than those given in Annex 3, this document is signed electronically only in the case where it is saved in one of the electronic document formats given in Annex 3.

#### Article 10

##### Devices for handling an electronic document

Devices enabling the creation, alteration, printing and display of an electronic document to the signer or verifier under the condition of secure verification of the signed or verified content of the electronic document are technical devices enabling the handling of an electronic document in the formats given in Annex 3 in interoperation with a security device for generating electronic signatures under Article 2 of the Act.

#### Article 11

##### Electronic document transmission between the sender and the recipient

The transmission of an electronic document between the sender and the recipient is done pursuant to the transmission protocols and data formats of qualified and definite electronic document transmission set out in Annex 4.

#### Article 12

##### Entry into force

This Decree enters into force on 1 October 2002.

**Ján Mojžiš**, in his own hand

**USE OF A QUALIFIED ELECTRONIC SIGNATURE  
IN COMMERCIAL INTERCOURSE**

**I. The signer is an individual natural person at the place of the generation of an electronic document**

In this case the signer creates a qualified electronic signature of the electronic document pursuant to Article 4 (1) and (3) of the Act. The signed document must be furnished with a time stamp.<sup>7</sup>

**II. The signers are multiple natural persons at the place of generation of an electronic document**

For signing an electronic document in commercial intercourse it is possible to use only a secure-electronic-signature-creation device for generating an electronic signature and secure-time-stamping device. The following procedure is laid down for the signing itself:

- (a) the electronic document's hash is created pursuant to the adopted signature scheme,
- (b) each of natural persons create from the electronic document's hash under point (a) a qualified electronic signature on the basis of its private key for which it holds a valid qualified certificate,
- (c) each qualified electronic signature generated under point (b) is furnished with a time stamp,
- (d) all qualified electronic signatures under point (c), deemed as a sequence of signs, are chained into a summary sequence from which a hash is created again pursuant to the adopted signature scheme,
- (e) natural persons representing the electronic document's signer parties are identified,
- (f) if there are more than two signer parties, each of them are designated by an identifier, e.g. A, B, C,
- (g) each of the natural persons representing the signer party creates, on the basis of its private key for which holds a valid qualified certificate, a qualified electronic signature from the summary sequence hash under point (d) and attaches it to or logically connects it with the signed electronic document,
- (h) an electronic document signed under point (g) is sent by each of the natural persons representing the signer party to each of the natural persons representing the other signer parties.

**III. The signers are multiple natural persons**

In the case where for signing an electronic document in commercial intercourse two secure devices or more are used for the generation and verification an electronic signature and secure-time-stamping devices, the procedure is as follows:

- (a) each of the signing natural persons is designated by an indicator, e.g. A, B, C, where the natural person with the identifier A is the signer holding the unsigned electronic document (hereinafter the "primary signer"),
- (b) the primary signer creates, on the basis of the own private key for which it holds a valid qualified certificate, a qualified electronic signature of an electronic document, furnished with a time stamp,

---

<sup>7</sup> Article 9 of Act No 215/2002 Coll.

- (c) the qualified electronic signature created is attached to or logically connected with the signed electronic document and sent to the natural person with the identifier B,
- (d) the natural person with the identifier B verifies the integrity of the received electronic document and the validity of the primary signer's signature and as a proof of consent signs the electronic document with its own qualified electronic signature, furnishes it with a time stamp and attaches it to or logically connects it with the received electronic document signed by the primary signer,
- (e) an electronic document signed under point (d) is sent to a natural person with the following identifier, who performs on its own behalf operations analogous to those described in point (d),
- (f) the last of the signing natural persons sends the signed electronic document, supplemented with the signatures of the individual preceding signer natural persons, to the primary signer,
- (g) the primary signer chains all the qualified electronic signatures attached to the signed electronic document and deemed as a sequence of signs into a summary sequence from which it again creates a hash under the adopted signature scheme, signs it with its qualified electronic signature, furnishes it with a time stamp and attaches it to or logically connect it with the signed electronic document,
- (h) the electronic document with signatures under point (g) is sent by the primary signer to all other signer natural persons.

## PRINCIPLES OF AN ELECTRONIC REGISTRY'S ACTIVITY

### I. Receipt and confirmation of electronic documents at the electronic registry

#### A. Receipt of an electronic document (submission)

- (a) the electronic registry receives electronic documents by means of the data transmission network or electronic mail
  1. in a permanent online connection regime,
  2. in a time limited connection regime when the online connection is provided at least during the set working hours of the public authority body or general government body,
- (b) an electronic registry receives electronic documents on a data medium during the set working hours of the public authority body or general government body, at least however during half of this time,
- (c) electronic registry, following the receipt of the electronic document
  1. under point (a) automatically places the document received into the queue of the received document or under point (b) transfers the electronic document from the data medium to the queue of the received documents,
  2. immediately following the receipt, attaches to the electronic document time data corresponding to the objective time of the document's receipt; technical and system devices of the electronic registry ensure the definite and unalterable assignment of time data of the received electronic document and its protection against modification or destruction,
  3. the electronic registry records on an automatic or manual basis the received document into the list of received documents,
  4. it examines the electronic document pursuant part B and decide on its further processing or its rejection,
  5. where the electronic document is not rejected under point 4., the electronic registry verifies the validity of the qualified certificate, qualified electronic signature and inviolability of the received document's integrity,
  6. if the verification under point 5. confirms the validity of the facts verified, the electronic registry creates an electronic confirmation message and include the electronic document in the queue of the verified received documents; otherwise it excludes the electronic document from the queue of the received documents, make a record in the list of the received documents and reject the receipt of the document,
- (d) in accordance with the internal regulations of the public authority body or general government body the received electronic documents are gradually collected, manually or automatically, form a queue of verified received documents and according to need are printed out to the paper form or are forwarded for further handling in electronic form by means of the public authority body's internal data transmission network,
- (e) the electronic registry archives the lists of received, verified received and rejected electronic documents and the file of electronic confirmations on the receipt of documents for handling according to a specific act<sup>8</sup> in paper or electronic form.

---

<sup>8</sup> Act No 395/2002 Coll. on archives and registries and on the amendment to certain acts.

## B. Confirmation of a electronic document received

The verification and subsequent receipt of the electronic document are confirmed by the electronic registry by

1. creating an electronic confirmation message in the case of its receipt under part A, point (a), at latest within 60 minutes from the electronic document's inclusion in the queue of verified received documents, to the address of the sender of the received electronic document; if it is not possible to deliver the electronic confirmation message, the electronic registry makes also further attempts at delivery, at least twice, or according to the internal regulations of the public authority body or the general government body; if also the repeated attempts at delivery are not successful, the electronic registry makes a record on the list of received documents and attaches the undelivered electronic confirmation message to the file so that it is logically bound to the record on receipt of the respective electronic document,
2. the creation of a written confirmation to the deliverer of the data medium with the received electronic document, and to whom it at the same time returns this data medium.

## **II. Devices for verifying the qualified electronic signature of the electronic document and creating an electronic confirmation message and their administration**

- (a) Devices for verifying the qualified electronic signature of a received electronic document, for creating the qualified signature of an employee in charge of an electronic registry and of the time stamp on the electronic confirmation message confirming the receipt of the electronic document at the electronic registry are devices pursuant to Article 2 (h), (i) and (x) of the Act,
- (b) only a natural person professionally trained for such an activity and charged by a public authority body or general government body may handle devices under point (a) above,
- (c) devices under point (a) above can be located only at premises secured pursuant to the principles of physical and object security by the technical security and mechanical prevention means of at minimum degree "V" pursuant to a specific regulation.<sup>9</sup>

---

<sup>9</sup> Decree of the National Security Authority No 88/2002 Coll. on physical security and object security.

**ELECTRONIC DOCUMENT FORMATS IN ADMINISTRATIVE INTERCOURSE**

Formats of electronic documents in administrative intercourse:

1. ASCII in one of the encryption of signs under ISO.
2. Microsoft/Apple Rich Text Format (RTF) Version 1.5. Format is defined in the foreign standard.<sup>10</sup>
3. Adobe Portable Document Format (PDF) Version 1.3. Format is defined in the foreign standard.<sup>11</sup>
4. Adobe Portable Document Format (PDF) Version 1.4. Format is defined in the foreign standard.<sup>12</sup>
5. HTML 4.01. Format is defined in the foreign standard.<sup>13</sup>
6. XML 1.0. Format is defined in the foreign standard.<sup>14</sup>
7. XHTML 1.0. Format is defined in the foreign standard.<sup>15</sup>
8. XHTML 1.1. Format is defined in the foreign standard.<sup>16</sup>
9. Open Office, org XML File Format. Format is defined in the foreign standard.<sup>17</sup>
10. Secure Hyper Text Transfer Protocol. Format is defined in the foreign standard.<sup>18</sup>
11. S/MIME Version 3. Format is defined in the foreign standard.<sup>19</sup>
12. Security Services for S/MIME. Format is defined in the foreign standard.<sup>20</sup>

---

<sup>10</sup> Rich Text Format (RTF) Specification and Sample RTF Program, RTF Version 1.5, Microsoft Technical Support Application Note 4/97-GC0165.

<sup>11</sup> Portable Document Format Reference Manual Version 1.3, Adobe Systems Incorporated, ISBN 0-201-62628-4.

<sup>12</sup> PDF Reference third edition, Adobe Portable Document Format Version 1.4, Adobe Incorporated / Addison-Wesley, ISBN 0-201-75839-3.

<sup>13</sup> W3C HTML 4.01 Specification, <http://www.w3c.org/TR/html401>.

<sup>14</sup> Extensible Markup Language (XML) 1.0 (Second Edition), <http://www.w3c.org/TR/REC-xml>.

<sup>15</sup> XHTML 1.0: The Extensible Hyper Text Markup Language, <http://www.w3c.org/TR/xhtml1>.

<sup>16</sup> XHTML 1.1 – Module-based XHTML, <http://www.w3c.org/TR/xhtml11>.

<sup>17</sup> Open Office, org XML File Format 1.0, Technical Reference Manual Version 1.0, July 2002, Sun Microsystems, [http://xml.openoffice.org/xml\\_specification.pdf](http://xml.openoffice.org/xml_specification.pdf).

<sup>18</sup> RFC 2660 S-HTTP.

<sup>19</sup> RFC 2633 S/MIME V3.

<sup>20</sup> RFC 2634 ESS S/MIME.

**TRANSMISSION PROTOCOLS AND DATA FORMATS OF SECURE AND UNAMBIGUOUS TRANSMISSION OF ELECTRONIC DOCUMENTS**

1. Mutual interconnection of information systems is realised in the manner which is defined in the STD 3 (Requirements for Internet Hosts) and STD 4 (Requirements for Internet Gateways) standards. In the text below this manner of connection is referred to as IP connectivity.
2. All specific technical questions relating to the creation and maintenance of IP connectivity not explicitly governed by this Annex to the Decree are solved in accordance with the applicable Internet standards (STD and RFC).
3. Signs of national alphabets are not used in the names of domains and nodes and in electronic mail addresses which are published for other entities and which are used by other entities.
4. Transmission of electronic mail between individual entities is solved on the basis of SMTP (STD 10) protocols and the standard (STD 11). The format is defined in the foreign standard.<sup>21</sup>
5. If the transmission of non-text attachments between individual entities is ensured via electronic mail, this transmission is solved on the basis of the MIME standard. The format is defined in the foreign standard.<sup>22</sup>
6. If the transmission of non-text attachments under point 5 of this Annex is ensured in the text itself of messages transmitted via electronic mail, signs of national alphabets can be used; these are solved on the basis of the MIME standard using the sign file ČSN ISO/IEC 8859-2.
7. Uuencode technology is also used for the transmission of non-text attachments and texts in national alphabets via electronic mail between individual entities.
8. Where the information between entities are mutually made available by means of the www service (World Wide Web), they are made available by means of the http protocol, HTML language and URL indicators. The indicators are defined in the foreign standard.<sup>23</sup>

---

<sup>21</sup> RFC 822.

<sup>22</sup> RFC 1521, RFC 1522, RFC 1523, RFC 1590.

<sup>23</sup> RFC 1738.