

**DECREE**  
**136**  
**of the National Security Authority**

dated from 26 March 2009

**on the method and procedure of using the electronic signature in business and administrative relations**

Pursuant to Art. 27 of Act No. 215/2002 Coll. on the electronic signature and on the amendment and supplementation of particular acts (hereinafter referred to as 'the Act'), the National Security Authority (hereinafter referred to as 'the Authority') establishes:

Art. 1

**Subject of the regulation**

This decree regulates details on the method and procedure of using the electronic signature in business relations and administrative relations.

Art. 2

**Definition of terms**

For the purposes of this decree,

- a) business relations denote the delivery, receipt or conformation of delivery or confirmation of receipt of a document in electronic form (hereinafter referred to as 'an electronic document') in relations which arise in and during electronic transaction between a provider of information society services <sup>1)</sup> and the receiver or consumer of said services,
- b) administrative relations denote the delivery, receipt or conformation of delivery or confirmation of receipt of an electronic document signed with a valid electronic signature or qualified electronic signature between public authorities or between a public authority and a natural person or between a public authority and a legal entity,
- c) the format of an electronic document denotes its internal structure and the method of numerical coding of the document pursuant to Art. 2 Letter a) of the Act.

Art. 3

**Electronic document formats**

(1) If the format of an electronic document permits the use of active elements, the electronic document containing said active elements may not be signed with an electronic signature neither with a qualified electronic signature.

(2) The kind of electronic document format which the subjects have agreed upon is used in business relations.

(2) In administrative relations, only those document formats specified in Appendix No. 2 are used for signing with a qualified electronic signature.

(4) If the technical means used for the creation, or, as the case may be, modification of electronic documents in administrative relations creates a document format other than those specified in Appendix No. 2, said document shall only be signed with a qualified electronic signature if it is saved in several of the electronic document formats specified in Appendix No. 2.

(5) Improvements of the precision of the content of electronic document formats in administrative relations and their formal specifications are published by the Authority on its internet site.

Art. 4

**Means for the manipulation of the electronic document**

Means enabling the signer or verifier to create, change, print and display an electronic document under the conceptions of secure verification of the signed or verified content of an electronic document are technical instruments enabling the manipulation of an electronic document in the formats specified in Appendix No. 2 in conjunction with the secure signature creation device pursuant to Art. 2 Letter h) of the Act.

Art. 5

**Transfer of an electronic document between sender and recipient**

The transfer of an electronic document between sender and recipient is conducted in accordance with transfer protocols and data formats which ensure the unique and secure transfer of electronic documents.

Art. 6

**Electronic registry**

(1) An electronic registry, the electronic address of which has been announced to the Authority by a public authority pursuant to Art. 29 Para. 1 of the Act, shall ensure administrative relations.

(2) By means of organisational measures and with the aid of technical instruments, the electronic registry ensures the:

a) receipt, delivery, verification, confirmation and processing of electronic documents by means of:

1. data transfer networks,
2. electronic mail,
3. standard data carriers,

b) control of electronic documents received, primarily regarding their ability to be read by the electronic registry's technical instruments without problems, conformity to the stipulated format and content and absence of harmful codes and bit sequences (such as macros, viruses, Trojan horses, worms),

c) verification of the validity of qualified certificates attached to the qualified electronic signature of the electronic document,

d) confirmation of receipt or rejection of an electronic document by issuing its own electronic document using a time stamp,

e) sending of an electronic document for further processing at a public authority,

f) receipt of an electronic document processed or created by the Authority in order to send it outside of the public authority,

g) and further activities related to the operation of the electronic registry.

(3) In order to provide for the use of the electronic registry's services, the public authority publishes the following, both in written form and in electronic form by means of a data transfer network:

a) a list of the complete electronic addresses enabling relations with the electronic registry,

b) the address of the electronic registry locations and an address enabling communication with the public authority on questions on the use and activity of the electronic registry,

- c) a list of qualified certificates or the complete electronic address at which a list of qualified certificates of all employees of the public authority who ensure the operation of the electronic registry can be found,
- d) electronic document formats from a number of permissible formats pursuant to Appendix No. 2 which the electronic registry accepts,
- e) the types and characteristics of data carriers on which the electronic registry accepts electronic documents,
- f) rules on sending electronic documents and confirmation of their receipt including potential time restrictions on relations with the electronic registry,
- g) a list of the types of electronic documents received and the method of obtaining electronic submission forms.

(4) The electronic registry uses a time stamp service pursuant to Art. 9 of the Act in the manipulation of the electronic document, particularly when confirming its receipt or progressing to a further manipulation.

(5) The electronic registry is operated in accordance with the approved security project and security guideline; a technical standard <sup>2)</sup> applies to the content and structure of said security project and security guideline.

(6) The principles of the electronic registry's activity are specified in Appendix No. 1.

#### Art. 7

#### **Annulling clause**

National Security Authority Decree No. 542/2002 Coll. on the method and procedure of using the electronic signature in business and administrative relations, as amended by National Security Authority Decree No. 233/2007 Coll., is repealed.

#### Art. 11

#### **Final provision**

This Decree has been adopted in accordance with the applicable legal act of the European Community <sup>3)</sup> under notification number 2008/0533/SK.

#### Art. 12

#### **Legal effect**

This Decree shall enter into force on the day of its declaration.

## **PRINCIPLES OF THE ELECTRONIC REGISTRY'S ACTIVITY**

### **I. Receipt and confirmation of electronic documents in the electronic registry**

#### **A. Receipt of the electronic document (submission)**

a) the electronic registry receives electronic documents by means of a data transfer network or electronic mail

1. in the permanent online connection regime,

2. in the time-bound connection regime, in which the online connection is provided at least during the public authority's defined business hours,

b) the electronic registry receives electronic documents on data carriers during the public authority's defined business hours, but at least during half of that time,

c) upon receiving the electronic document, the electronic registry

1., automatically files the received document in the queue of documents received, pursuant to Letter a), or, , transfers the electronic document from the data carrier to the queue of documents received, pursuant to Letter b),

2. allocates the time data corresponding to the objective time of the document's receipt to the electronic document immediately upon receipt; the electronic registry's technical and system instruments ensure the unique and unalterable allocation of the time data to the electronic document received and ensure its protection from modification or destruction,

3. records the received document in the list of received documents, either automatically or manually,

4. reviews the electronic document pursuant to section B and decides on its subsequent processing or rejection,

5. verifies the validity of the received document's qualified certificate, qualified electronic signature and undisturbed integrity if it does not reject the electronic document pursuant to Item 4,

6. issues an electronic confirmation notice and the electronic document is filed in the queue of verified documents received if the verification pursuant to Item 5 confirms the validity of the information verified,; otherwise the electronic document is discarded from the queue of documents received, a record is made in the list of documents received and the receipt of the document is rejected,

d) in accordance with the internal regulations of the public authority, electronic documents received are gradually selected from the queue of verified documents received (either manually or automatically), and are printed in paper form or transferred for further processing in electronic form by means of the public authority's internal data transfer network,

e) the electronic registry archives lists of the records of received, verified received and rejected electronic documents and the file of electronic confirmations of document receipt for processing pursuant to a special regulation <sup>4)</sup> in paper or electronic form.

#### **B. Receipt of the electronic document**

The electronic registry confirms verification and subsequent acceptance of the electronic document by

1. issuing an electronic confirmation notice in the event of acceptance pursuant to Section A Letter a) within not more than 60 minutes of filing the electronic document 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 notice, the electronic

registry makes additional attempts at delivery at least twice, or according to the public authority's internal regulations; if the repeated attempts at delivery are unsuccessful, the electronic registry makes a record in the list of received documents and the undelivered electronic confirmation notice is attached to the file in such a manner as to connect it logically to the record on the receipt of the corresponding electronic document,

2. issuing a written confirmation to the sender of the data carrier with the electronic document received, at the same time returning the data carrier.

## **II. Means of verifying the qualified electronic signature of the electronic document and creating an electronic confirmation notice and the administration thereof**

a) means of verifying the qualified electronic signature of the received electronic document, creating the qualified electronic signature of the electronic registry employee performing the service and the time stamp for the electronic confirmation notice confirming acceptance of the document in the electronic registry are means pursuant to Art. 2 Letters h), i) and x) of the Act,

b) pursuant to Letter a), only a natural person who has been trained in this specialised activity and commissioned by a public authority may manipulate the means of verification;

c) the means of verification pursuant to Letter a) may only be located in premises secured in accordance with the principles of physical security and facility security by means of technical security devices and mechanical barrier devices of a security classification level of at least 'Restricted' pursuant to the special regulation.<sup>5)</sup>

## **ELECTRONIC DOCUMENT FORMATS**

Electronic document formats in administrative relations:

1. ASCII in any of the sign codings according to the ISO.
2. Microsoft/Apple Rich Text Format (RTF) Version 1.5.<sup>6)</sup>
3. Adobe Portable Document Format (PDF) Version 1.3.<sup>7)</sup>
4. Adobe Portable Document Format (PDF) Version 1.4.<sup>8)</sup>
5. HTML 4.01.<sup>9)</sup>
6. XML 1.0.<sup>10)</sup>
7. XHTML 1.0.<sup>11)</sup>
8. XHTML 1.1.<sup>12)</sup>
9. OpenOffice.org XML File Format.<sup>13)</sup>
10. Secure Hyper Text Transfer Protocol.<sup>14)</sup>
11. S/MIME Version 3.<sup>15)</sup>
12. Security Services for S/MIME.<sup>16)</sup>
13. Tag Image File Format for image technology (TIFF). The format is defined in the international standard.<sup>17)</sup>
14. Portable Network Graphics (PNG). The format is defined in the international standard.<sup>18)</sup>
15. PDF/A-1. The format is defined in the international standard.<sup>19)</sup>
16. Open Document Format for Office Applications (OpenDocument) v1.0 (ODF). The format is defined in the international standard.<sup>20)</sup>

1) Art. 2 Letter b) of Act No. 22/2004 Coll. on electronic commerce and on the amendment and supplementation of Art No. 128 /2002 Coll. on state control of the internal market in matters of consumer protection and on the amendment and supplementation of particular laws as amended by the most recent legislation.

2) STN ISO/IEC 27002. Information technologies. Security technology. Rules of good practice in the management of information security.

3) European Parliament and Council Directive 98/34/EC on a procedure for the provision of information in the field of technical standards and regulations as amended (OJ L 204, 21.7.1998, special edition of the OJ in chap. 3/vol. 20).

4) Act No. 395 /2002 Coll. on archives and registries and on the supplementation of particular laws as amended by the most recent legislation.

5) National Security Authority Decree No. 336/2004 Coll. on physical security and facility security as amended by National Security Authority Decree No. 315/2006 Coll.

6) Rich Text Format (RTF) Specification and Sample RTF program, RTF Version 1.5, Microsoft Technical Support Application Note 4/97-GC0165.

7) Portable Document Format Reference Manual Version 1.3, Adobe Systems Incorporated, ISBN 0-201-62628-4.

8) PDF Reference third edition, Adobe Portable Document Format Version 1.4, Adobe Incorporated/Addison-Wesley, ISBN 0-201-75839-3.

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

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

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

12) XHTML 1.1 - Module-based XHTML, <http://www.w3c.org/TR/xhtml11>.

13) OpenOffice.org XML File Format 1.0, Technical Reference Manual Version 2, December 2002, Sun Microsystems, [http://xml.openoffice.org/xml\\_specification.pdf](http://xml.openoffice.org/xml_specification.pdf).

14) RFC 2660 S-HTTP.

15) RFC 2633 S/MIME V3.

16) RFC 2634 ESS S/MIME.

17) ISO 12639: 2004 Graphic technology -- Prepress digital data exchange -- Tag image file format for image technology (TIFF/IT).

- 18) ISO/IEC 15948:2004 Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification.
- 19) ISO 19005-1:2005 Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1).
- 20) ISO/IEC 26300:2006 Information technology -- Open Document Format for Office Applications (OpenDocument) v 1.0.