

**DECREE**  
**134**  
**of the National Security Authority**

dated from 26 March 2009

**stipulating the details on requirements for secure devices for the creation of time stamps  
and requirements on products for the electronic signature (on electronic signature  
products)**

In accordance with Art. 9 Para. 1 Letter d) and Art. 24 Para. 17 of Act No. 215/2002 Coll. on the electronic signature and on the amendment and supplementation of particular laws as amended by Act No. 214/2008 Coll. (hereinafter referred to as 'the Act'), the National Security Authority (hereinafter referred to as 'the Authority') establishes:

**Art. 1**  
**Subject of the decree**

This decree regulates

- a) details on the requirements for secure devices for the creation of the time stamp,
- b) requirements on products for the electronic signature.

**Art. 2**  
**Details on the requirements for the secure device for the creation of the time stamp**

The secure device for the creation of the time stamp pursuant to Art. 2 Letter x) of the Act is a device which meets the following requirements:

- a) the private key and public key of the time stamp issuer are created in a tested and controlled manner,
- b) the time stamp issuer's private key remains confidential and risks which may compromise its integrity are eliminated,
- c) the integrity and authenticity of the time stamp issuer's public key which serves to verify the signature, as well as each of the related parameters, is secured during the distribution provided by the recipient,
- d) the period of validity of the time stamp issuer's certificate may not be longer than the time interval during which the selected algorithm and length of the key serves its stated purpose,
- e) the time stamp issuer's private key may not be used after its validity has expired,
- f) the security of the cryptographic hardware serving to sign the time stamp is not compromised or breached during its lifetime,
- g) the installation, activation and creation of copies of the time stamp issuer's signature key in the cryptographic hardware are conducted in physically secure areas by dependable authorised persons,
- h) the installation, activation and creation of copies of the time stamp issuer's private key in the cryptographic hardware may be conducted by at least two persons authorised in their current activity,
- i) the cryptographic hardware serving to sign the time stamp functions in compliance with the technical-operational documentation and security policy and, in the event of malfunction, it shall be possible to identify the cause of the malfunction and the consequences caused by it,
- j) the time stamp issuer's private key saved on the time stamp issuer's cryptographic

- hardware must be erased upon the cryptographic hardware is put out of operation,
- k) the time stamp is issued in compliance with the security policy adopted and contains the correct time.

### Art. 3

#### **Requirements on products for the creation of the qualified electronic signature**

(1) Products for saving private keys and for the creation of the qualified electronic signature intended for the signer or verifier of the qualified electronic signature meet the requirements of the Act if

- a) they operate with approved signature schemes, algorithms and parameters of said algorithms,
- b) conformity is demonstrated with the following:
  1. the standard specified in the first item of Appendix No. 1,
  2. the cryptographic standards of the public key infrastructure specified in the second item of Appendix No. 1,
  3. the requirements specified in the special regulation,<sup>1)</sup>
- c) the Authority has issued a certificate for them pursuant to Art. 24 Para. 9 of the Act.

(2) Software products for the creation and verification of the qualified electronic signature meet the requirements of the Act if

- a) they operate with approved signature schemes, algorithms and parameters of said algorithms,
- b) conformity is demonstrated with the following:
  1. the approved qualified electronic signature format,
  2. the standard specified in the first item of Appendix No. 1,
  3. the cryptographic standards of the public key infrastructure specified in the second item of Appendix No. 1,
  4. the requirements specified in the special regulation,<sup>1)</sup>
- c) they form a certification path – a chain of certificates needed to verify the validity of the signer's certificate,
- d) they compile the certificate revocation list, or, as the case may be, process responses from the confirmations of existence and validity of the certificate,
- e) they add a time stamp, if the application offers the function of creating a qualified electronic signature with time stamp,
- f) they support chip cards or other media for saving the keys and certificates,
- g) the Authority has issued a certificate for them pursuant to Art. 24 Para. 9 of the Act.

(3) Certificate administration information systems intended particularly for providers of accredited certification services meet the requirements of the Act if

- a) they operate with approved signature schemes, algorithms and parameters of said algorithms,
- b) they fulfil the following characteristic functions
  1. they operate with a hardware module for protecting the certification authority's key, which must meet the required level of key protection,
  2. conformity with the approved formats of qualified certificates and certificates has been demonstrated,

---

<sup>1)</sup> Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products.

3. conformity with the standard specified in the first item of Appendix No. 1 has been demonstrated,
  4. they enable the creation of a hierarchical structure of certification authorities,
  5. they enable division into certification authority and registration authority,
  6. they enable cross-certification,
  7. they enable the implementation of the certificate revocation list, or, as the case may be, the implementation of confirmations of the existence and validity of the certificate,
  8. they ensure the operation of a fast and secure directory,
  9. they enable the implementation of the security policy,<sup>2)</sup>
  10. they enable work with administrative tools for the administration of the public key infrastructure,
  11. their conformity to the cryptographic standards of the public key infrastructure specified in the second item of Appendix No. 1 has been demonstrated,
  12. they enable the support of smart cards or other media for saving the keys and certificates,
  13. conformity with the requirements specified in the special regulation<sup>1)</sup> has been demonstrated,
- c) information systems of accredited certification service providers pursuant to Art. 2 Letter 1) Item Three of the Act also enable time stamp creation in addition to the characteristic functions specified in Letter b),
- d) the Authority has issued a certificate for them pursuant to Art. 24 Para. 9 of the Act.

(4) Cryptographic hardware modules for key protection intended particularly for providers of accredited certification services meet the requirements of the Act if

- a) protection is ensured from unauthorised disclosure of the cryptographic module's confidential content including the cryptographic key in a not ciphered form and further critical security parameters,
- b) protection is ensured from unauthorised and undetectable modification of the cryptographic module, including unauthorised modification, substitution, insertion and erasing of the cryptographic key and further critical security parameters,
- c) the operational status of the cryptographic module is indicated,
- d) the activity of the cryptographic module is ensured in compliance with the technical-operational documentation and security policy and, in the event of malfunction, it is possible to identify the cause of the malfunction and the consequences caused by it,
- e) operation errors in the cryptographic module are detected and damage to sensitive data and critical security parameters resulting from the errors detected is prevented,
- f) they meet the security requirements pursuant to FIPS-140-2 Security requirements for level 3 cryptographic modules for the protection of information which is not classified information pursuant to the special regulation<sup>3)</sup>,
- g) specifications for the cryptographic module and cryptographic interface exist,
- h) specifications for the model of the cryptographic module in the form of the machine module with a finite number of statuses exist,
- i) data inputs (ports) for critical security parameters are physically separated from the other data inputs,
- j) breach detection for the cryptographic module and reaction to breach of the protection and casing exists,

---

<sup>2)</sup> Art. 10 of National Security Authority Decree No. 133/2009 Coll. on the content and extent of operational documentation kept by the certification authority and on the security rules for the execution of certification activities.

<sup>3)</sup> Act. 215/2004 Coll. on the protection of classified information and on the amendment and supplementation of particular acts as amended by the most recent legislation.

- k) a dependable communication path exists,
- l) the key input and output are in ciphered form or, in the case of direct input and output with procedures, the key information is separated,
- m) they enable test functions to be executed and execution of automatic testing during start-up and have implemented tests of the operation conditions,
- n) operator identity verification is present, as is verification that the identified operator is authorised to execute the specific role and commensurate activity group,
- o) the Authority has issued a certificate for them pursuant to Art. 24 Para. 9 of the Act.

(5) Requirements pursuant to Section 1 may also be adequately applied to products for the creation of the electronic signature pursuant to Art. 3 of the Act.

#### Art. 4

#### **Annulling clause**

National Security Authority Decree No. 539/2002 Coll. stipulating the details on requirements for secure devices for the creation of time stamps and requirements on products for the electronic signature (on electronic signature products) is repealed.

#### Art. 5

#### **Final provision**

(1) The legal acts of the European Community and European Union specified in Appendix No. 2 are overtaken in this Decree.

(2) This Decree has been adopted in accordance with the applicable legal act of the European Community<sup>4)</sup> under notification number 2008/0530/SK.

#### Art. 6

#### **Legal effect**

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

---

<sup>4)</sup> European Parliament and Council Directive 98/34/EC on a procedure for the provision of information in the field of technical standards and regulations (OJ L 204, 21.7.1998, special edition of the OJ in chap. 3/vol. 20).

**Appendix No. 1**  
**to Decree No. 134/2009 Coll.**

**LIST OF STANDARDS RELATING TO PRODUCTS FOR THE CREATION OF THE  
QUALIFIED ELECTRONIC SIGNATURE**

1. Certificate of the public key infrastructure and profile of the certificate revocation list. The format is specified in the external standard.<sup>5)</sup>
2. Cryptographic standards of the public key infrastructure. Formats are specified in the external standard.<sup>6)</sup>

---

<sup>5)</sup> ITU-T RECOMMENDATION X.509 (08/2005) | ISO/IEC 9594-8 : Information technology – open systems interconnection - the directory: public key and attribute certificate frameworks, IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

<sup>6)</sup> EN 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic Services , EN 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices – Part 2: Additional Services, RSA Standard PKCS#7, PKCS#10, PKCS#11, PKCS#15.

**Appendix No. 2  
to Decree No. 134/2009 Coll.**

**LIST OF OVERTAKEN LEGAL ACTS OF THE EUROPEAN COMMUNITY  
AND EUROPEAN UNION**

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, special edition of the OJ EU, chap. 13/vol. 24).