

DE C R E E
of the National Security Authority

of 9 September 2002

laying down details on the requirements for secure-time-stamping devices and the requirements for electronic signature products (on electronic signature products)

The National Security Authority (hereinafter referred to as “the Authority”) pursuant to Articles 9 (1) (d) and 24 (8) 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

- a) the requirements for secure-time-stamping devices,
- b) the requirements for electronic signature products.

Article 2

Details on requirements for secure-time-stamping devices

A secure-time-stamping device¹ is equipment fulfilling the following requirements

- a) the private key and public key of a time stamp issuer are generated in a controlled and managed manner,
- b) the time stamp issuer’s private key remains secret and risks which may cause the violation of its integrity are removed,
- c) the integrity and authenticity of the time stamp issuer’s public key, serving for signature verification, as well as that of each of the related parameters is secured during distribution to recipients,
- d) the life of a time stamp issuer’s certificate may not be longer than the time interval during which the selected algorithm and length of the key satisfy the specified purpose,
- e) the time stamp issuer’s private key may not be usable following the elapsing of its validity,
- f) the security of the cryptographic hardware serving for signing the time stamp is not diminished nor violated at any time during its life,

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

- g) the installation, activation and creation of copies of the time stamp issuer's signature keys in cryptographic hardware takes place at premises physically secured by trustworthy authorised persons,
- h) the installation, activation and creation of copies of the time stamp issuer's private key in the cryptographic hardware can be performed by at least two authorised persons through their concurrent activity,
- i) cryptographic hardware serving to sign a time stamp works in accordance with technical-operating documentation and security policy, and in the case of faults it is possible to identify their cause and consequences caused,
- j) the time stamp issuer's public key, stored on the time stamp issuer's cryptographic hardware, must, following retirement of the cryptographic hardware from operation, be deleted,
- k) the time stamp is issued in accordance with the adopted security policy and contains the correct time.

Article 3

Requirements for qualified electronic signature creation products

- (1) Products intended for storing private keys and for creating a qualified electronic signature satisfy requirements, if
- a) they work with approved signature schemes, algorithms and parameters of these algorithms,
 - b) they enable the use of the following functions and properties
 1. key renewal,
 2. key updating,
 3. key back-up,
 4. key division,
 5. hardware protection of a certification authority's key, which must fulfil the protection level of the key set out in Annex 1,
 6. use of additional modules and encryption software instruments,
 7. compatibility with the standard set out in point 1 of Annex 2,
 8. compatibility with public key infrastructure management standards,
 9. creation of a hierarchical structure of certification authorities,
 10. division into a certification authority and registration authority,
 11. cross certification,
 12. rendering of the certificate revocation list,
 13. time stamp creation,
 14. attribute certification,
 15. secure certification for the certification authority and registration authority,
 16. bulk certification,
 17. rendering of the certificate revocation list,
 18. directory structure,
 19. a protocol for access to the directory,
 20. enforcement of the security policy,
 21. work with the protocol for a secure electronic commerce operation,
 22. work in a virtual private network environment,
 23. work with administrator instruments for public key infrastructure administration,
 24. compatibility with cryptographic standards of the public key infrastructure set out in point 2 of Annex 2,

25. support for chip cards or other media for storing keys and certificates,

c) the Authority has issued a certificate for them by law.

(2) The requirements according to paragraph (1) may be applied *mutatis mutandis* also to the products for electronic signature generation².

Article 4

Entry into force

This Decree shall enter into force on 1 October 2002.

Ján Mojžiš in his own hand

² Article 3 of Act No 215/2002 Coll.

**FUNCTIONALITY REQUIREMENTS FOR CRYPTOGRAPIC MODULE OF THE
HARDWARE PROTECTION OF THE KEY**

- The cryptographic module of the hardware protection of the key satisfies the requirements if
- (a) protection against unauthorised disclosure of the non-public content of the cryptographic module, including the cryptographic key, in non-encrypted form and of other critical security parameters is ensured,
 - (b) protection against unauthorised and non-detectible modification of the cryptographic module, including the unauthorised modification, substitution, entry or deletion of cryptographic key and other critical security parameters is ensured,
 - (c) the operating status of the cryptographic module is indicated,
 - (d) the activity of the cryptographic module is ensured in accordance with technical-operating documentation, security policy and in the case of faults it is possible to identify the cause and consequences caused,
 - (e) errors in operations of the cryptographic module are detected and any damage to sensitive data and critical security parameters as a result of detected errors is prevented,
 - (f) it satisfies the approved security methods for the protection of unclassified information under FIPS-140-2 Security Requirements for Cryptographic Modules,
 - (g) there is a specification of cryptographic module and specifications of cryptographic interface,
 - (h) there is a specification of the cryptographic module's model in the form of an automatic machine with the final number of statuses,
 - (i) data ports for critical security parameters are physically separated from other data ports,
 - (j) there is verification of the operator's identity,
 - (k) there is detection of violation to the cryptographic module and a reaction to the violation of protection and covers,
 - (l) a high-level language is used for implementation of cryptographic module,
 - (m) the operating system contains protection by means of instructions and a trustworthy communication channel,
 - (n) entry and exit of the key is in encrypted form or if there is direct entry and exit with procedures for dividing the key's knowledge,
 - (o) there is the ability to provide the performance of statistical tests of a request's randomness,
 - (p) there is use of algorithms for the protection of unclassified information according to FIPS-140-2 Security Requirements for Cryptographic Modules,
 - (q) requirements for electromagnetic interferences and electromagnetic compatibility are fulfilled at least within the scope the level 3 of FIPS-140-2 Security Requirements for Cryptographic Modules,
 - (r) in switching on, automatic testing starts running,
 - (s) tests for operation conditions are implemented and functioning,
 - (t) there is verification of the operator's identity and verification that the identified operator is authorised to perform the specific role and respective groups of activities.

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

1. Public key infrastructure certificate and the profile of the certificate revocation list. The format is given in the foreign standard.¹
2. Cryptographic standards of the public key infrastructure. Formats are given in the foreign standard.²

¹ RFC 2459: Internet X.509.

² RSA Standard PKCS#7, PKCS#10, PKCS#11, PKCS#12.