

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

of 9 September 2002

**on the conditions for providing accredited certification services and on the requirements  
for audit, the scope of audit and qualification of auditors**

The National Security Authority (hereinafter referred to as “the Authority”) pursuant to Articles 13 (2) and 25 (1) 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

- a) the material, premises, technical, organisational, and legal conditions for providing accredited certification services,
- b) requirements for audit, the scope of audit and qualification of auditors and on the performance of the audit of an accredited certification authority.

**Details on the conditions for providing  
accredited certification services**

Article 2

A certification authority wanting to provide accredited certification services

- a) delivers to the Authority a request for accreditation; together with the request for accreditation the certification authority submits the particulars pursuant to Article 13 (3) of the Act,
- b) prove to the Authority fulfilment of conditions pursuant to Articles 3 to 5 for providing accredited certification services.

Article 3

(1) A certification authority requesting accreditation must own, or have contractually ensured, rental of premises for the provision of accredited certification services, where these premises shall satisfy security rules<sup>1</sup> and conditions pursuant to paragraphs (2) to (5).

(2) In the case of providing accredited certification services in rented premises the independent entry of the building's owner into the protected premises must be contractually

---

<sup>1</sup> Decree of the National Security Authority No 541/2002 Coll. on the content and scope of operating documentation administered by a certification authority and on the security rules and rules for performing certification activities.

restricted only to the essential and immediate solution of emergency situations in the building.

(3) Besides operating premises, an accredited certification authority must ensure other protected premises for the secure storage of archived documents and data and monthly back-up copies of the accredited certification authority's system data; these premises must be located in a building not physically connected with that in which the provision of the accredited certification services is performed.

(4) Technical and organisational measures must ensure the constant operation of the accredited certification authority even in the case of a failure in basic technical infrastructure, at minimum at the level of providing a service registering requests for the time stamp function.

(5) The certification authority must have its own system for ongoing control over the functionality and security of the security means and measures used.

#### Article 4

A certification authority requesting accreditation submits, besides basic technical parameters and documentation of devices pursuant to a specific regulation<sup>2</sup>, also documentation of devices which it plans to use for supporting the provision of certification services for

- a) administering and securing document archives pursuant to Article 18 of the Act,
- b) operating and securing its website.

#### Article 5

An accredited certification authority must have organisational conditions created in the following scope:

- a) security rules of the certification authority for a secure regime of providing certification services and for performing certification activities,
- b) measures defining conditions for the access of persons into protected premises, conditions for work with electronic signature products and measures determining activities for the occurrence of a situation endangering the provision of certification services,
- c) organisational separation of activities connected with the provision of certification services between various persons and sections so as to enable mutual as well as independent control of the performed activities,
- d) administration of the certification authority's operating documentation pursuant to a specific regulation<sup>1</sup>,
- e) principles for the performance of personnel work in the framework of the certification authority,
- f) principles for the performance of internal control in the framework of the certification authority,
- g) principles for ensuring security in concluding contractual relations with legal entities or with natural persons on the provision of services supporting the provision of services by the certification authority.

#### Article 6

Details on the requirements for audit,  
scope of audit and qualification of auditors

---

<sup>2</sup> Decree of the National Security Authority No 539/2002 Coll. laying down details on requirements for secure-time-stamping devices and requirements for electronic signature products (on electronic signature products).

- (1) A security audit of the provision of certification activities can be performed only by an authorised natural person or legal entity.
- (2) A natural person or legal entity may be authorised to perform a security audit of certification activities, if
  - a) it is the holder of a valid international or Slovak information systems audit certificate,
  - b) has provable professional practice in the field of information systems audit not shorter than five years.
- (3) An audit comprises verification of
  - a) the security properties of an electronic signature product and of the security properties of the environment in which the electronic signature product is operated,
  - b) the security of encryption devices and the regime of work with them,
  - c) protection of an electronic signature product against unauthorised manipulation, misuse and failure,
  - d) the security of processes for performing certification activities,
  - e) protection of the communication infrastructure against attacks and failures,
  - f) the accordance of items in paper and electronic records in performing certification activities,
  - g) the suitability and sufficiency of the security objective, project and security guidelines,
  - h) the suitability and sufficiency of security measures and means specified in security guidelines,
  - i) security measures connected with the provision of activities by other legal entities or natural persons,
  - j) other security measures and means which the certification authority has adopted with the aim of ensuring reliability and security in providing certification services,
  - k) the preparedness of the certification authority for potential events endangering its operations - plans for emergencies and plans for restoring the certification authority's activity,
  - l) other required security requirements for performing certification activities under the Act.
- (4) The performance of an audit is completed with a concluding report comprising
  - a) the auditor's statement and assessment of the overall state of the certification authority's security at the time of performing the security audit,
  - b) a description of findings on shortcomings of a security nature,
  - c) recommendations for removing shortcomings found.

#### Article 7

#### Entry into force

This Decree enters into force on 1 October 2002.

**Ján Mojžiš** in his own hand