

DECREE
132
of the National Security Authority

dated from 26 March 2009

on the conditions for providing accredited certification services and requirements for an audit, the extent of an audit and the qualification of the auditors

In accordance with Art. 13 Para. 2 and Art. 25 Para. 1 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:

- a) material, spatial, technical, organisational and legal conditions on the provision of accredited certification services,
- b) requirements for an audit, extent of an audit and qualification of the auditors and on the execution of an audit of the accredited certification authority.

Details on the conditions for the provision of accredited certification services

Art. 2

A certification authority wishing to provide accredited certification services shall:

- a) send an application for accreditation to the Authority; the certification authority shall submit requisites pursuant to Art. 13 Para. 3 of the Act with the application for accreditation,
- b) demonstrate to the Authority the fulfilment of conditions pursuant to Art. 3 to 5 on the provision of accredited certification services. .

Art. 3

(1) A certification authority applying for accreditation must own or have contractually rented spaces for the provision of accredited certification services which fulfil the security rules¹⁾ and conditions pursuant to Sections 2 to 5.

(2) In the case of accredited certification services provided in rented spaces, the building owner's capacity to enter the protected spaces on his own must be contractually limited exclusively to the essential and spontaneous resolution of accidents in the building.

¹⁾ 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 and the Certification Practice Statement .

(3) In addition to operational spaces, the accredited certification authority must provide further protected spaces for the secure storage of archive documents and data and monthly back-up copies of the accredited certification authority's system data; said spaces must be located in a building which is not physically connected to the building in which the provision of accredited certification services is conducted.

(4) Technical and organisational measures shall ensure the uninterrupted operation of the accredited certification authority even in event of the failure of the basic technical infrastructure, at least on the level of the accredited certification service provider's registration service provision requirements of

- a) administration of the qualified certificates pursuant to Art. 2 Letter 1) Item One of the Act, on the provision of a list of revoked qualified certificates,
- b) long-term storage of electronic documents signed by means of qualified electronic signature pursuant to Art. 2 Letter 1) Item Two of the Act, on the verification and display of the document,
- c) issuing time stamps pursuant to Art. 2 Letter 1) Item Three of the Act, on the registration of requirements for issuing the time stamp.

(5) The accredited certification authority providing the service of long-term storage of electronic documents signed by means of qualified electronic signature shall ensure the:

- a) display of the electronic document by means enabling its content to be determined,
- b) preservation of document integrity – confirmation that the content of the document has not been modified and is accessible in the form in which it was saved in the archive,
- c) preservation of document authenticity - confirmation that the electronic document was created and signed by the person who is entered as the signer of the electronic document,
- d) recording and storage of information important in light of the existence of the electronic document and data on the assumption, method of saving, access to the document, type of storage media, etc.,
- e) performance of such activities in the scope of electronic document manipulation which enable the saving of the non-repudiation of the existence and integrity of the data and ensure the required accessibility thereof.

(6) The standards specified in the international standardisation documents apply during the performance of activities pursuant to Section 5.²⁾

(7) The applications used in providing the service of long-term electronic document storage signed by means of qualified electronic signature shall ensure that it is possible to verify the qualified electronic signature even the validity period of the certificates used to verify the signature has expired. In ensuring the possibility of verifying the qualified electronic signature, the applications shall use the electronic signature formats for long-term verification specified in the European standardisation documents³⁾ and time stamps with the format specified in the international standardisation documents.⁴⁾

²⁾ ISO/TR 15801: 2004 Electronic imaging -- Information stored electronically – Recommendations for trustworthiness and reliability, ISO/TR 18492:2005 Long-term preservation of electronic document-based information.

³⁾ ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI). CMS Advanced Electronic Signatures (CAAdES). ETSI TS 101 903 XML Advanced Electronic Signatures (XAAdES). RFC 5126 Electronic Signature Formats for Long Term Electronic Signatures.

⁴⁾ RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

(8) The accredited certification authority providing the service of long-term storage of electronic documents signed by means of qualified electronic signature shall ensure that the documents are not made accessible to a third party without the owner's consent.

(9) The certification authority must have elaborated its own system for the continuous control of the function and security of the security means and measures used.

(10) The provider shall apply the standards specified in the European standardisation documents⁵⁾ during the provision of accredited certification services pursuant to Art. 2. Letter l) Item One of the Act.

Art. 4

In addition to the description and documentation of the basic technical parameters and documentation of means pursuant to the special regulation⁶⁾, a certification authority applying for accreditation shall also submit documentation of means which it plans to use to support the provision of certification services for:

- a) keeping and securing a document archive pursuant to Art. 18 of the Act,
- b) operating and securing its internet site.

Art. 5

An accredited certification authority will have to have created organisation conditions comprising the following:

- a) the certification authority's security rules for the secure accredited certification service provision regime and for the Certification Practice Statement ,
- b) measures determining the conditions of personal entry to the protected space, conditions for work with the product for the electronic signature and measures determining activities in the event a situation arises which jeopardises the provision of accredited certification services,
- c) an organisational division of activities related to the provision of accredited certification services among various persons and agencies in such a manner as to enable mutual control, as well as an independent control of the activities conducted,
- d) keeping the certification authority's operational documentation pursuant to the special regulation¹⁾ in a manner suitable according to the type of accredited certification service provided,
- e) policies on the performance of human resource management work in the scope of the certification authority,
- f) policies on the performance of internal control in the scope of the certification authority,
- g) policies on security assurance in the conclusion of contractual relationships with legal entities or with natural persons on the provision of services supporting the services provided by the certification authority.

Art. 6

⁵⁾ ETSI TS 101 456 Electronic signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing qualified certificates, CWA 14172-2 EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes.

⁶⁾ National Security Authority Decree No. 134/2009 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).

Details on audit requirements, extent of the audit and qualification of the auditors

(1) Only an authorised natural person or legal entity may conduct an audit of the security of the provision of certification activities.

(2) The natural person or legal entity may be authorised to conduct an audit of the security of certification activities if

- a) he holds a valid international or Slovak certification for the performance of an audit of information systems,
- b) has demonstrable professional experience in the field of auditing information systems amounting to not less than five years.

(3) The performance of the audit consists of verification of the

- a) security characteristics of the product for the electronic signature and security characteristics of the environment in which the product for the electronic signature operates,
- b) security of ciphered means and the regime of work with them,
- c) protection of the product for the electronic signature from unauthorised manipulation, misuse and failure,
- d) security of the processes of performing certification activities,
- e) protection of the communication infrastructure from attacks and failures,
- f) conformity of the items in paper and electronic indices of the execution of certification activities,
- g) suitability and sufficiency of the security purpose, project and security guidelines,
- h) suitability and sufficiency of the security measures and means which are specified in the security guidelines,
- i) security measures related to 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 goal of ensuring the reliability and security of the provision of certification services,
- k) certification authority's preparedness in the occurrence of events jeopardising its operation – plans for the event of an accident and plans for the recovery of the certification authority's activity,
- l) other required security requirements on the execution of certification activities pursuant to the Act.

(4) The performance of the audit shall conclude with a final report consisting of:

- a) the auditor's judgement and assessment of the certification authority's overall security status at the time the security audit was performed,
- b) a description of findings on security-related shortcomings,
- c) recommendation on the elimination of shortcomings found.

Art. 7

Annuling clause

National Security Authority Decree No. 540/2002 Coll. on the conditions for the provision of accredited certification services and requirements for an audit, the extent of an audit and the qualification of the auditors is repealed.

Art. 8

Final provision

(1) The legal acts of the European Community and European Union specified in the Appendix are overtaken in this Decree.

(2) This Decree has been adopted in accordance with the applicable legal act of the European Community⁷⁾ under notification number 2008/0531/SK.

Art. 9

Legal effect

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

⁷⁾ 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).

**Appendix
to Decree No. 132/2009 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).