

DECREE
131
of the National Security Authority

dated from 26 March 2009

**on the format, content and administration of certificates and qualified certificates and
the format, periodicity and method of issuing a list of revoked qualified certificates (on
certificates and qualified certificates)**

In accordance with Art. 6 Para. 10, Art. 7 Para. 8 and Art. 8 Para. 6 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 regulation

This decree regulates

- a) the format and content of the certificate for administration and the qualified certificate,
- b) details on the administration of certificates,
- c) the format of certificate revocation list ,
- d) the periodicity of issuing the certificate revocation list ,
- e) the method of issuing the certificate revocation list ,
- f) the format and content of the confirmation of the existence and validity of certificates.

Art. 2

Common definitions

For the purposes of this decree,

- a) a certificate for administration denotes the certificate being used for the verification of the validity of the qualified certificate – a certificate of the Authority , certificate of the accredited certification authority, time stamp certificate, certificate for the verification of the confirmation of the existence and validity of certificates¹⁾ and a certificate for the verification of the certificate revocation list ,²⁾
- b) a digital data imprint denotes the number calculated from the data by means of the hash function.³⁾

Art. 3

Format and content of the certificate for administration and the qualified certificate

(1) The format and content of the certificate for administration and the qualified certificate determine the ordering and method of the data record in the certificate for administration and

¹⁾ IETF RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol.

²⁾ 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.

³⁾ ETSI TS 102 176-1: Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

the qualified certificate. The Authority publishes approved formats of these certificates on its internet site.

(2) The content of the certificate for administration and the qualified certificate consists of data entered in the body of the certificate in accordance with Art. 6 and 7 of the Act.

(3) The identification data specified in the qualified certificate must contain

- a) the identification data of the issuer of the certificate consistent with the identification data of the certificate holder specified in the certificate issued to the competent accredited certification authority for the applicable public key,
- b) the business name and head office of the accredited certification authority.

(4) The identification data of the qualified certificate holder must consist of

- a) the name and surname or pseudonym, and
- b) supplementary identifier ensuring the uniqueness of the certificate holder's identification data.

(5) The certificate for administration and the qualified certificate contain the identifier of the certificate policy of the accredited certification services, the value of which is published by the Authority in the approved certificate formats. The identifier of the certificate policy of the accredited certification services may only be used in the certificate for administration and the qualified certificates of a natural person.

(6) The qualified certificate contains a mandate in the wording specified in the power of attorney.

Art. 4

Details on the administration of qualified certificates

(1) Before issuing a qualified certificate, the accredited certification authority or registration authority acting on certification authority's behalf shall conduct a control of whether

- a) personal data of the applicant specified in the application for the issue of a qualified certificate conform with data in the identity document submitted,
- b) the identification data which are to be entered as the certificate holder's identification data conform with the data specified in the application for the issue of a qualified certificate,
- c) the applicant applying for the issuing of a qualified certificate has a private key corresponding to the public key which is to be entered in the qualified certificate as the certificate holder's public key,
- d) the public key which is to be entered in the qualified certificate as the certificate holder's public key is not identical to the certificate holder's public key entered in a different certificate or qualified certificate issued by the same accredited certification authority,
- e) the public key which is to be entered in the qualified certificate as the certificate holder's public key and the private key corresponding to said public key are generated using a secure signature creation device.

(2) The accredited certification authority shall send the Authority an index of the qualified certificates and certificates for administration it has issued on a monthly basis. The index of said certificates shall contain the serial number of the certificate, the name of the issuer, the certificate holder's data, the date of the certificate validity, etc. The Authority publishes the

technical details on the method of delivery, format and content of the index of issued certificates on its internet site.

Art. 5

Format of the certificate revocation list

(1) The format of the certificate revocation list is determined by the ordering and method of the record of data in the list. The list contains the list issuer's data, the date and time the list is issued, the serial number of the revoked certificate, the date and time of the certificate revocation, etc.

(2) The identification data of the certificate issuer specified in the certificate revocation list must be consistent with the identification data of the issuer specified in the certificates, the identification numbers of which are found in said certificate revocation list.

(3) The identification data of the certificate issuer specified in the certificate revocation list must be consistent with the identification data of the certificate holder specified in the certificate for the public key corresponding to the private key used in creating the electronic signature of the certificate revocation list.

Art. 6

Periodicity of issue of the certificate revocation list

Certificate revocation lists are issued with a period not exceeding 24 hours and at the same time no more than 24 hours will elapse between the time the application for the certificate revocation is received and the time the initial certificate revocation list containing its number is published.

Art. 7

Method of issuing the certificate revocation list

(1) The accredited certification authority issues a new certificate revocation list in such a manner that it specifies all certificate identification numbers of the certificates which were entered in the previous certificate revocation list together with the dates and times of their revocation in the list of identification numbers of the certificates which were revoked and adds the identification numbers of all certificates for which the circumstances arose pursuant to Art. 15 of the Act; the date and time of their revocation are in the interval between the time the previous certificate revocation list was issued and the time of issue of the certificate revocation list. The identification number of the revoked certificate is cited in the certificate revocation list for at least until the expiration of the original validity period of the certificate. The revoked certificate must be specified at least once in the certificate revocation list before the expiration of the original validity period.

(2) The accredited certification authority shall publish the current certificate revocation list and all prior certificate revocation lists on its internet site.

(3) The accredited certification authority shall send to the Authority each new certificate revocation list it has issued during the specified timeframe on a monthly basis. The Authority

publishes the technical details on the format and content of the issued certificate revocation list and the method of its delivery on its internet site.

Art. 8

Format and content of the confirmation of the existence and validity of certificates

(1) The accredited certification authority receives applications on the confirmation of the existence and validity of certificates in the form of an unsigned index of certificate identifiers. The certificate identifier is composed of the following items:

- a) the identifier of the hash function used,
- b) the digital imprint of the name of the certificate issuer,
- c) the digital imprint of the public key of the certificate issuer,
- d) the serial number of the certificate.

(2) The accredited certification authority confirms the existence and validity of the certificates by means of confirmation in the form of an electronic document.

(3) The confirmation is composed of the body of the confirmation, the electronic signature of the body of the confirmation and the index of certificates for verifying the signature of the body of the confirmation.

(4) The body of the confirmation is an electronic document containing:

- a) identification data of the confirmation issuer who administers the information on the certificates,
- b) the date and time the confirmation is issued,
- c) an index of individual confirmations for a single certificate, containing
 1. certificate identifier defined in Section 1,
 2. status of the certificate, which is valid, revoked or unknown,
 3. the date and time at which the status of the certificate was known and correct,
 4. an extension of the individual confirmation and positive statement containing the identifier of the hash function and the digital imprint from the certificate, the status of which is found in the response, etc.

(5) The electronic signature of the confirmation body is created by the issuer of the confirmation who administers the information for those certificates by means of the private key intended for it.

(6) The confirmation of existence and validity of the certificates is the index of certificate identifiers, by means of which the issuer of the confirmation who administers the information on those certificates announces the existence or premature termination of their validity. The confirmation shall meet the requirements pursuant to Sections 1 to 5 and

- a) is issued by an accredited certification authority or the Authority,
- b) the electronic signature of the body of the confirmation was created by means of the private key intended for this purpose,
- c) the accredited certification authority or the Authority has issued a certificate for the public key corresponding to the private key pursuant to Letter b).

(7) The Authority publishes the technical details on the format and method of issuing the confirmation of existence and validity of certificates on its internet site.

Art. 9
Annuling clause

National Security Authority Decree No. 538/2002 Coll. on the format and content of the qualified certificates, on the administration of qualified certificates and on the format, periodicity and method of issuing a list of revoked qualified certificates (on qualified certificates) is repealed.

Art. 10
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 Community⁴⁾ under notification number 2008/0529/SK.

Art. 11
Legal effect

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

⁴⁾ 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 EU chap. 3/vol. 20).

**Appendix
to Decree No. 131/2009 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 in OJ EU, chap. 13/volume. 24).