

Regulation N. 525 of 14 December 2005

on Conducting Certification in Providing the Cryptographic Protection of Classified Information

Legal Disclaimer

The following text is a translation of the original promulgated in the Czech language in the Collection of Laws. This translated version has been effected by the National Security Authority of the Czech Republic and cannot be relied upon as an authentic wording, nor causes any legal effect. Any liability of the author is hereby excluded.

The National Security Authority lays down the following according to S. 53(a), (b), (c), (d), (g), (h) and (i) of the Act N. 412/2005 Coll., on the Protection of Classified Information (hereinafter “the Act”):

Section 1

Elements of the request for cryptographic device certification

(amending S. 49 par. 1 of the Act)

(1)The request for cryptographic device certification shall contain the following

- a) the identification of the requesting subject
 1. by the name of the company or by the name, location and registration number should the applicant be a legal person;
 2. by the name of the company or by the name and surname or any differentiating affix, permanent residence address and the place of business activity if these are different from the permanent residence, by date of birth and identification number should the applicant be a natural person pursuing business; or
 3. by the name, location, registration number and the name and surname of the responsible person in the case of the State body;
- b) the name and surname of a contact officer of the applicant and his/her contact address;
- c) the number of the valid facility security clearance and security classification of classified information to which the facility is authorised to

- d) have access on the basis of this clearance, should the applicant be the facility;
- d) the trade name and the full type designation of the cryptographic device;
- e) the determination of the cryptographic device (purpose of its use and classification level for which the cryptographic device is to be used);
- f) the name of the company, location or the place of business activity of the cryptographic device producer;
- g) the method of securing the production and distribution of the cryptographic key;

(2)For the purposes of certification of the cryptographic device of the European Union or any of its member state or for the purposes of certification of the cryptographic device of the North Atlantic Treaty Organization, which is designed to protect classified information, the subject that requested the certification shall submit the request according to paragraph 1 and the copy of the certificate or of any similar document issued by the certification authority of the European Union or by the corresponding national certification authority of its member state or by the North Atlantic Treaty Organization.

Section 2

Elements of the request for cryptographic site certification

(amending S. 50 par. 1 of the Act)

The request for cryptographic site certification shall contain the following

- a) the identification of the requesting subject according to S. 1 par. 1(a);

- b) the name and surname of a contact officer of the requesting subject and his/her contact address
- c) the number of the valid facility security clearance and security classification of classified information to which the facility is authorised to have access on the basis of this clearance, should the applicant be the facility;
- d) the identification of the cryptographic site (the name, address and location);
- e) the determination of the cryptographic site (purpose of use);
- f) the list of enclosed documents necessary to conduct the certification of the cryptographic site.

Section 3

Elements of repeated requests for cryptographic device certification

(amending S. 49 of the Act)

The repeated request for cryptographic device certification shall contain the following

- a) the identification of the requesting subject according to S. 1 par 1(a);
- b) the full identification of the certificate issued (the holder of the certificate, registration number, date of issuance, period of validity);
- c) the identification of the certified cryptographic device (trade name, type designation, variant performance, determination, the name and location of the cryptographic device producer);
- d) the name and surname of a contact officer of the applicant and his/her contact address;
- e) the statement of the reasons of the repeated request.

Section 4

Elements of the repeated request for the cryptographic site certification

(amending S. 50 of the Act)

The repeated request for cryptographic site certification shall contain the following

- a) the identification of the requesting subject according to S. 1 par. 1(a);
- b) the full identification of the certificate issued (the holder of the certificate, registration number, the name of the cryptographic site date of issuance, period of validity)
- c) the identification of the cryptographic site (detailed specification of the determination and location of the site);

- d) the statement of the reasons of the repeated request.

Section 5

Documents necessary to conduct the cryptographic device certification

(amending S. 49 of the Act)

(1)The cryptographic device, documentation and other supporting documents necessary to conduct the certification shall be submitted for the purpose of the cryptographic device certification.

(2)The list of the documentation and of other supporting documents, their form and content shall be determined by the security standard, which the National Security Authority (hereinafter “the Authority”) will provide to the applicant. The Authority will provide the schedule of providing documentation and other supporting documents necessary to conduct the certification to the applicant.

(3)In particular the following documentation shall be required to conduct the cryptographic device certification, which shall contain

- a) the determination and limitation of the method of the cryptographic device use;
- b) the type of the user environment and the system incorporation of the cryptographic device;
- c) the technical description and service instructions of the cryptographic device;
- d) the installation and testing requirements for the cryptographic device;
- e) the valid cryptographic device certificates or certificates already issued;
- f) the description of the solution and structure of cryptographic keys used;
- g) the block diagram and the description of the cryptographic device with an indication of interoperability links of its individual parts.

(4)The provided cryptographic device, technical means, materials and original technical documentation of the cryptographic device shall be returned to the Authority after the termination of the certification. Other documents submitted in connection with the certification will not be returned to the applicant.

Section 6

Documentation necessary to conduct the cryptographic site certification (amending S. 50 of the Act)

(1)The following shall be enclosed to the request for the cryptographic site certification

- a) the documentation concerning the ensuring the physical security of the cryptographic site as described in the special legal regulation¹.
- b) the documents covering operational-security safeguarding of the cryptographic site;
- c) the statement of the responsible person or of the person authorised by him/her of fulfilment requirements for the physical and personnel security of the cryptographic site;

(2)The documents enclosed to the request for the certification and other supplementary documents, if any, which are necessary to conduct the certification, will not be returned to the applicant.

Section 7

The format of the cryptographic device certificate and the content of the certification report (amending s. 46 par. 7 and 13 of the Act)

(1)The format of the cryptographic device certificate is shown in Annex 1 to this Regulation.

(2)The certification report shall be enclosed to the cryptographic device certificate, which shall contain the following

- a) the production, transport and maintenance requirements for the cryptographic device;
- b) the cryptographic device specification;
- c) the results of the certification procedure;
- d) the equivalent value of the S1 parameter according to the special legal regulation¹;
- e) the operating conditions of the cryptographic device;
- f) limitations, if any, conditioning the validity of the cryptographic device certificate.

Section 8

The format of the cryptographic site certificate and the content of the certification report (amending s. 46 par. 8 and 13 of the Act)

(1)The format of the cryptographic site certificate is shown in Annex 2 to this Regulation.

(2)The certification report shall be enclosed to the cryptographic site certificate, which shall contain the following

- a) the explicit determination of the cryptographic site;
- b) the operating conditions of the cryptographic site;
- c) the scope of changes, if any, conditioning the validity of the cryptographic site certificate.

Section 9

The method and conditions of conducting cryptographic device certification (amending S. 49 of the Act)

(1)The Authority shall determine the priority of conducting the cryptographic device certification, its scope and the method.

(2)The process of the cryptographic device certification is subdivided into several separately closed stages, which shall be performed by specialized sites of the Authority, by the specialized site of the State body, legal person or the natural person pursuing business. The Authority shall issue a decision based on results of evaluation of individual stages. The following shall be evaluated separately

- a) the submitted request for the cryptographic device certification and the submitted documentation;
- b) the cryptographic parameters of the cryptographic device;
- c) the technical parameters of the cryptographic device;
- d) the production of the key material and its distribution;
- e) the requirements for the production, operating and protection of the cryptographic device;
- f) the requirements for integration of the cryptographic device to the communication or information system;
- g) the applicability for the protection of classified information of the Czech Republic, European Union or the North Atlantic Treaty Organization.

(3)The Authority shall keep records of certified cryptographic devices. The certification file shall be kept on the certified cryptographic device, on which

¹ The Regulation N. 528/2005 Coll., on the Physical Security and Certification of Technical Means.

the request for the certification, documentation and other documentary material provided by the applicant will be placed, as well as other requested supplementary documents necessary to conduct certification, the certification report and the copy of the certificate issued.

(4)The destruction period of the certification file begins to run upon expiration of the period of validity of the certificate.

(5)Paragraphs 1 to 4 shall apply similarly for the cryptographic device certification conducted on the basis or the repeated request according to S. 3.

Section 10
Method and conditions of conducting the cryptographic site certification
(amending S. 50 of the Act)

(1)The Authority shall determine the priority of conducting the cryptographic sites certification, its scope and the method.

(2)The process of the cryptographic site certification is subdivided into several separately closed stages, which shall be performed by specialized sites of the Authority, by the specialized site of the State body, legal person or the natural person pursuing business. The Authority shall issue a decision based on results of evaluation of individual stages. The following shall be evaluated separately

- a) the submitted request for the cryptographic site certification and the submitted documentation;
- b) the purpose of the cryptographic site and its technical equipment;
- c) the operational security safeguarding of the cryptographic site;
- d) compliance with requirements for the physical and personal security of the cryptographic site;
- h) the result of the inspection of the cryptographic site by the Authority.

(3)The Authority shall keep records of certified cryptographic sites. The certification file shall be kept on the certified cryptographic site, on which the request for the certification, documentation and other documentary material provided by the applicant will be placed, as well as other requested supplementary documents necessary to conduct certification, the certification report and the copy of the certificate issued.

(4)The destruction period of the certification file begins to run upon expiration of the period of validity of the cryptographic site certificate.

(5)Paragraphs 1 to 4 shall apply similarly for the cryptographic site certification conducted on the basis or the repeated request according to S. 4.

Section 11
Elements of the request of the State body or facility to conclude a contract for providing services
(amending S. 52 of the Act)

(1)The request for conclusion of a contract for providing services² shall contain the following

- a) the identification of the requesting subject according to S. 1 par. 1(a);
- b) the number of the facility security clearance and security classification of classified information, to which the facility is authorised to have access on the basis of this clearance, should the applicant be a facility;
- c) the name and surname of a contact officer of the applicant and his/her contact address;
- d) the volume of the documentation being enclosed.

(2)The documentation shall be enclosed to the request according to paragraph 1, which shall contain the following

- a) the address of the location of the site undertaking required activities;
- b) the statement of the responsible person or by a person authorised by him/her of compliance with requirements for the physical and personal security of the site;
- c) the volume of required activities;
- d) personnel ensuring of required activities;
- e) technical and organization ensuring of required activities.

² S. 46 par. 15 and S. 52 of the Act N. 412/2005 Coll., on the Protection of Classified Information.

Section 12
Coming into force

This Regulation shall come into force on 1 January 2006.

Director

Signed
Mgr. Mareš

NATIONAL SECURITY AUTHORITY

P.O. Box 49
150 06 Praha 56

The National Security Authority issues according to S. 46 of the Act N. 412/2005 Coll., on the protection of Classified Information

CERTIFICATE

of the cryptographic device

Registration number:

.....
(name, type designation of the cryptographic device)

Identification of the certificate holder:

Company/name and surname/name of the State body:
Registration (identification) number:
Location/permanent residence/place of business:

Identification of the cryptographic device producer:

Company/name of the State body:
Registration (identification) number:
Location/permanent residence/place of business:

This is to certify the capability of the cryptographic device to protect classified information up to and including the level

.....

Valid from the date:
Date of expiry:
Date of issuance:

Stamp

Enclosures: (e.g. the certification report)

Signature of the authorised representative

NATIONAL SECURITY AUTHORITY

P.O. Box 49
150 06 Praha 56

The National Security Authority issues according to S. 46 of the Act N. 412/2005 Coll., on the protection of Classified Information

CERTIFICATE

of the cryptographic site

Registration number:

.....
(designation of the cryptographic site)

Identification of the certificate holder:

Company/name and surname/name of the State body:

Registration (identification) number:

Location/permanent residence/place of business:

Identification of the cryptographic site:

Specification (location, category):

This is to certify the capability of the cryptographic site to undertake activities connected with the cryptographic protection to the following extent

.....
(specification of activities to be undertaken)

Valid from the date:

Date of expiry:

Date of issuance:

Stamp

Enclosures: (e.g. the certification report)

Signature of the authorised representative