340

DECREE of the National Security Authority

of 10 May 2004

on Details of Encryption Protection of Information

The National Security Authority (hereinafter referred to as "Authority") stipulates, pursuant to Article 69 of Act No. 215/2004 (Coll.) on the Protection of Classified Information and on the Amendment and Supplementing of certain Acts (hereinafter referred to as "Act"), the following:

Article 1
Subject of Regulation

This regulation governs the details related to:

a) certification and approval of systems and devices for cryptographic information protection (hereinafter referred to as "device") into operation, their use, transfer, registration and the use of cipher materials;
b) keeping records of employees in the field of cryptographic information protection and verification of their professional qualification;
c) establishment of a departmental encryption body or other encryption body at the same level (hereinafter referred to as "departmental encryption body").

Article 2
Certification of Devices

(1) Certification of devices shall verify and certify the qualification of a device to protect classified information in compliance with the security standard for systems and devices for the cryptographic information protection and security standard for the protection against compromising electromagnetic emanation.

(2) The Authority shall certify devices, on request of a departmental encryption body or legal entity that meets the industrial security conditions pursuant to special regulation[11]).

(3) The departmental encryption body shall, within its competence, certify devices for protection of classified information of the security classification level "Confidential" and "Restricted". It shall also certify devices for protection of classified information of the security classification level "Confidential" or "Restricted", on request of a legal entity that meets the industrial security conditions pursuant to special regulation[1]), if their use is envisaged.

(4) Before a device is installed within a certification office, the applicant shall submit protocol on completed operation tests of the relevant device, certificates issued by other authorized persons, list of standards which the device complied with, as well as a necessary number of units of the device as required by the certification office or departmental encryption body.

[1]) Decree of the National Security Authority No. 325/2004 (Coll.) on Industrial Security.

(5) Documentation supplied with the relevant device shall be prepared so as to facilitate evaluation security of the device and according to the security classification level of protected classified information it shall contain the following information:

a) For the security classification level „Restricted”:
1. determination of the way of use of the device;
2. type of the user’s environment and systemic incorporation of the device;
3. operating instructions for the device;
4. instructions for the use of the device;
5. basic cryptographic parameters, type of cryptographic algorithm, mathematic model of all cryptographic methods used in the evaluated device;
6. verification data and programs for the verification of the mathematic algorithm model of a device;
7. verification data and programs for the verification and testing of device functions;
8. description of key management, scale and structure of device keys;
9. method of generation of device cipher keys;
10. flow diagram and description of parts of device, specifying the interactive relations of its individual parts;
11. device cryptographic analysis;
12. device security analysis;
13. documentation and results gained from security analyses carried out on the device;
14. examination of the possibility for changing the cryptographic algorithm with respect to the modification of the device and license policy;
15. device installation procedure;
16. device de-installation procedure.

b) For the security classification level “Confidential" besides the information defined in letter a), also the following information:
1. method of the physical implementation of the device;
2. technical documentation of the device and description of its functional and technical parameters;
3. method of administration of the key device management;
4. method of generation of initial device set-ups;
5. basic device diagnostics system;
6. description of the methods used for device authentication and identification;
7. means of device protection against compromise of classified information by compromising electromagnetic emanation;
8. description of the method for device destruction.

c) For the security classification level “Secret” besides the information defined in letters a) and b), also the following information:
1. method for physical algorithm implementation, all of its activity regimes used, including checking examples;
2. progress chart for basic functional statuses and partial blocks and description of the basic functional regimes of the device;
3. device circuit layout, including the technical description of the definitive content of programmable circuits, micro programmes, memories, etc.;
4. commented source codes of the entire software;
5. source code of the device software, allowing compilation into a configuration compatible with the certified device and its audit;
6. security attributes and technical attributes of the key carrier;
7. method of keys distribution;

8. method for the protection of keys and the cryptographic algorithm against any compromise;
9. method for the removal of cryptographic traces after de-installation;
10. description of methods, attributes and security levels of audit functions used;
11. rules for the design of the topological network of devices;
12. resistance of the device against the modification of cryptographic parts;
13. resistance and method of protection of program parts of the device against attacks by a virus or other harmful programs or against their partial modification;
14. diagnostics, course and methods of testing and initialisation of cryptographic parts upon device certification;
15. diagnostics, course and methods of testing and initialisation of cryptographic parts upon serial production of the relevant device;
16. security measures upon serial production of the device;;
17. method of executing the service of the device at the user's premises
18. detection of cryptographic errors;
19. description of the device self-destruction method.

d) For the security classification level "Top Secret" besides the information defined in letter a) to c), also the following information:

1. reaction of the device to external interference signals;
2. reactions of the device to incidental or intentional changes of work environment;
3. reactions of the device to occurrences of own defect;
4. resistance of the device against an error caused by operating staff;
5. security measures in the production of cipher keys;
6. method of liquidation of faulty parts and components in the serial production and service of the device;
7. method of liquidation of used or faulty carriers of cryptographic elements.

(6) Device certification may begin after the verification of the completeness of the documentation necessary for device certification, pursuant to paragraph 5.

(7) The certification office shall draw up a written record about the verification of completeness of the documentation for device certification.

(8) If the documentation submitted is incomplete, the certification office shall inform the applicant about this fact in writing, at the same time calling upon him to complete it. If the applicant does not complete the documentation within the specified period, the certification office shall inform him that the device certification will not be carried out.

(9) If the documentation is complete, the certification office shall inform the applicant, in writing, about the acceptance of the application, as well as the date upon which the completion of the certification is expected.

(10) The laboratory performance tests of the device, device test operation for verification of specified operating parameters of the device and evaluation of the operating instructions and instructions for use of the device shall also form part of the device certification.

(11) The certification office shall draw up a certification protocol about the device certification entailing:

a) name of the certification office;
b) name of the respective device (identification of type, version), designation of the device

producer and his identification data;
c) name of the applicant for certification and his identification data;
d) brief characteristics of the device and description of the clear identification of the device and its individual components, including their security classification level;
e) security classification level of protected information for which the device is certified;
f) results of its findings on the respective requirements of security standards;
g) category of the device according to the security standard for the protection against compromising electromagnetic emanation;
h) category of the area for placement of the device according to the security standard for the protection against compromising electromagnetic emanation;
i) results of the laboratory performance tests of the device, description and results of the device test operation;
j) operating parameters of the device found;
k) standpoint on the operating instructions and instructions for use of the device, with suggestions for their potential modification;
l) conclusion stating the compliance or non-compliance with all of the security standards requirements and the qualification or non-qualification of the device to protect classified information at the particular security classification level.

(12) With respect to devices intended for operation outside of protected areas either nationally or abroad, a device certification protocol shall contain a separate part, stating compliance with the security standard requirements for systems and devices and the qualification of the particular device to protect classified information in the proposed conditions.

(13) The head of the central state administration body (hereinafter referred to as “head”) is the person authorized to approve a device certification protocol.

(14) A device certificate may only be issued, if the findings of a device certification protocol state compliance with all of the security standards requirements, as well as the qualification of the particular device to protect classified information at the relevant security classification level.

(15) If a device certification protocol gives a negative finding stating non-compliance with the security standards requirements and the non-qualification of the particular device to protect classified information at the relevant security classification level, the certification office shall inform the applicant thereof in writing.

(16) In the case of devices that are also intended for operation outside of protected areas or abroad, these facts shall be stated in the certificate.

(17) A device certificate shall contain the following information:
a) name of the central state administration body issuing the certificate;
b) certificate registration number;
c) name of the device (type identification, version), designation of the producer of the device and his identification data;
d) name of the applicant for the certification and his identification data;
e) security classification level of protected information for which the particular device is certified;
f) category of the device according to the security standard for the protection against compromising electromagnetic emanation;
g) category of the area for the location of the device according to the security standard for the protection against compromising electromagnetic emanation;
h) qualification for the protection of classified information outside of protected areas or abroad;

i) identification data related to operating instructions and instructions for the use of the device;
j) validity period of the particular certificate;
k) date of issuance of the certificate;
l) identification data and signature of the head approving the issuance of the certificate.

(18) The Authority or head shall issue a device certificate, together with the service instructions and instructions for the use of the device. A model certificate shall be published by the Authority on its website.

(19) The central encryption body may, in justified cases, issue a device certificate on the basis of a certificate issued by a foreign authority, with which the Slovak Republic had concluded agreement about protection of classified information and on the basis of agreed upon guarantees for the security level of devices. The operating documentation of a device according to the certificate issued by a foreign authority is not binding for the use of the device for protection of classified information of the Slovak Republic.

(20) The certified devices may only be provided to a foreign authority, in compliance with the law,[2]) on the basis of an international agreement binding for the Slovak Republic. This does not apply to devices intended for cooperation of the Slovak Information Service with intelligence services of other countries carried out in accordance with special regulation.[3])

(21) Regarding the devices gained by the Slovak Information Service from intelligence services of other countries within the cooperation carried out in accordance with special regulation[3]), the relevant head may issue a device certificate on the basis of a certificate issued by foreign authority.

(22) The departmental encryption body may request the central encryption body for recognition of a certificate issued by the NATO or EU member state on the basis of bilateral agreement about mutual protection of classified information.

(23) The departmental encryption body shall keep a register of device certificates issued in its competence and inform the Authority about all certificates issued within 15 days. This information shall include the photocopies of the certificates issued.

(24) The Authority shall keep a register of device certificates issued in its own competence, as well as in the competence of departmental encryption bodies.

(25) On request of the departmental encryption body, the Authority shall inform about the certificates issued within 15 days from delivery of the request.

Article 3
Approval of Devices into Operation

(1) Devices may only be approved into operation on the basis of their certificates issued by the Authority or the head. The head is also authorized to approve devices into operation on the basis of certificates adopted from other central bodies of state administration. The departmental encryption bodies shall inform the Authority about all adopted certificates.

(2) A device may be only be approved into operation within protected area,[4]) unless stated

[2]) Article 60 paragraph 2 of Act No. 215/2004 (Coll.) on Protection of Classified Information and on the Amendment and Supplementing of certain Laws.
[3]) Act of the National Council of the Slovak Republic No. 46/1993 (Coll.) on Slovak Information Service, as amended.
[4]) Decree of the National Security Authority No. 336/2004 (Coll.) on Physical and Building Security.

otherwise, and within area complying with the security standard for the protection against compromising electromagnetic emanation.

(3) The head shall approve a device into operation on the basis of a written application made by a departmental encryption body. Model decision on approval of an encryption protection device into operation shall be published by the Authority on its website.

(4) An application for the approval of a device into operation pursuant to paragraph 3 shall contain the following information:

a) name of the device;
b) proposed date of the approval of the device into operation;
c) the highest security classification level of protected information;
d) recommended period of operation of the device;
e) brief characteristics of the purpose of the use of the device; in case of the approval of device into operation out of the protected area either nationally or abroad, also a separate reasoning for the purpose of its use, supported by relevant documents justifying the increased risk of endangerment to classified information and the need for the use of devices for this purpose;
f) identification data of the device certificate, as well as certificates of its components, if available;
g) results from the operation tests of the device;
h) if the operating instructions or instructions for the use of the device, issued together with the device certificate are not sufficient supplements to the operating instructions and instructions for the use of the device issued by a departmental encryption body, shall form an integral part of the application;
i) if the device being approved is not separate, but forms an integral part of a technical device, the identification data of the certificate of the technical device and document approving the technical device into operation;
j) specification of the location of the device, stating the category of the device and category of the area according to the security standard for the protection against compromising electromagnetic emanation;
k) category determination of the protected area of the device location and identification data of the processed documentation about the physical and building security of protected premises,[4]) where the device is located; in case of approval of device into operation outside of the protected area in the territory of the Slovak Republic or abroad outside of a representative offices of the Slovak Republic, a supplement to the instructions for the use of the device in the specific conditions, stating the method of destruction of the device and other classified information, should a threat arise;
l) specification of the device users;
m) specification of the employees in the field of cryptographic information protection, necessary for the provision of the operation, maintenance and repairs of the device;
n) specification of the method, scope and conditions of the device administration and production of encrypted materials for the device in compliance with the law[5]);
o) description of the provision of maintenance and repairs of the device;
p) identification data and signature of the head approving the relevant device into operation.

(5) The decision about the approval of a device into operation shall be kept together with the application of a departmental encryption body with the departmental encryption body for a minimum of the approved operation time of the device.

(6) Outside of protected areas in the territory of the Slovak Republic and abroad outside of the

[5]) Article 70 paragraph 1 letter c) item 10 of Act No. 215/2004 (Coll.).

representative offices of the Slovak Republic only special types of devices determined for this purpose may be approved into operation in compliance with the security standard for the systems and devices of cryptographic information protection.

(7) The devices gained for the protection of foreign information on the basis of an international agreement binding for the Slovak Republic shall be approved into operation by the head on the basis of certificates issued by foreign authority, only with a written approval given by the central encryption body. This does not apply for devices intended for cooperation of the Slovak Information Service with the intelligence services of other countries carried out according to special regulation.[3])

Article 4
Use and Transfer of Devices

(1) Operated may be only devices that have been certified and approved into operation and in compliance with their operation instructions and instructions for use.

(2) The method of destruction of devices intended for cryptographic information protection shall be specified in their instructions for use.

(3) Device used for protection of information with various security classification levels shall be certified to the highest security classification level of the protected information.

(4) A transfer of classified information within the protected area is not considered to be the transfer of classified information by technical devices[6]).

(5) Transport of devices shall be carried out only through persons authorized to transport classified information in accordance with special regulation[7]), appointed by the head.

(6) Only the addressee within the encryption body or employee in the field of cryptographic information protection appointed by him may open the transported shipments with devices.

(7) The devices intended for cryptographic information protection and cryptographic materials intended for these devices shall be transported and stored separately, if allowed by their technical design.

Article 5
Registration of Devices

(1) A departmental encryption body shall keep a central registry of all devices in its operation.

(2) The registry of devices shall be kept as an independent material class and separately from other material registries.

(3) A departmental encryption body shall on a yearly basis carry out physical inventory of devices. The Authority shall be notified of its results. This obligation does not apply to devices intended for the collaborative interconnection of the Slovak Information Service with intelligence services of other countries according to special regulation[3]).

(4) Only the employees in the field of cryptographic information protection are authorized to carry out the physical inventory of devices.

---

[6]) Article 6 paragraph 3 of Act No. 215/2004 (Coll.)

[7]) Decree of the National Security Authority No.338/2004 (Coll.) on Administrative Security.

Article 6
Use of Cryptographic Materials

(1) Cryptographic materials as part of a device[8]) shall mean passwords, keys, variable parameters of cryptographic algorithms identified according to the type of device and security classification level of protection of classified information. The cryptographic materials may only be used in compliance with the instructions for the use of the device.

(2) The Authority or departmental encryption body, in their competence, carry out the administration of devices and production of cryptographic materials.

(3) Cryptographic materials already used that are damaged or suspected to have been manipulated without authorization must not be further used for the encryption protection of information. The cryptographic materials whose validity expired must not be further used for cryptographic information protection.

Article 7
Verification of Professional Qualification

(1) Professional qualification in accordance with Article 68 paragraph 1 of the Act is proven by a confirmation of passing the security employee examination in the field of cryptographic information protection according to special legislation[8a]).

(2) Certificate for working at the specified field of cryptographic information protection in accordance with Article 68 paragraph 2 of the Act shall be issued after fulfilling the requirements set by the head. Model certificate for working at the specified field of cryptographic information protection shall be published by the Authority on its website.

Article 8
Keeping a Registry of Employees in the Field for Cryptographic Information Protection

(1) The departmental encryption body shall keep a registry of employees in the field of cryptographic information protection in its competence. The Authority shall keep a register of employees in the field of cryptographic information protection of departmental encryption bodies.

(2) The head shall approve the registration of an employee into the registry in the field of cryptographic information protection based on a written proposal given by a departmental encryption body.

(3) The registry of employees in the field of cryptographic information protection[9]) shall contain the following information:

a) name and surname;
b) surname at birth;
c) date and place of birth;
d) birth number; this does not apply to the registry of employees in the field of cryptographic information protection kept with the departmental encryption body of the Slovak Information Service;
e) personnel registration number;

---

[8]) Article 2 letter p) of Act No. 215/2004 (Coll.)

[8a]) Article 1 paragraph 2 letter e) of the Decree of the National Security Authroity No. 135/2016 Coll. on Security Employee Examination.

[9]) Article 2 paragraph 2 letter c) of Act No. 428/2002 (Coll.) on Personal Data Protection.

f) name and address of the employer;
g) position held;
h) security classification level of the clearance;
i) date of issuance and number of certificate for acquaintance with classified information;
j) date of signing the record stating the assignment of the individual proposed for acquaintance with classified information;
k) date of signing the confidentiality declaration;
l) date of the registration;
m) registration number and date of issuance of the certificate on professional qualification of the employee in the field of cryptographic information protection, scope of professional qualification;
n) date of the withdrawal of the certificate for working in a specified field of cryptographic information protection.

(4) Departmental encryption bodies shall inform the Authority about all changes in data kept in the registry of employees in the field of cryptographic information protection of the departmental encryption bodies.

Article 9
Establishment of a Departmental Encryption Body

(1) The application for the approval of the central encryption body for the establishment of a departmental encryption body, made by the head, shall contain the following information:

a) name of the central body of state administration;
b) reasons for establishment;
c) proposed date of establishment;
d) integration of a departmental encryption body into the organisational structure of the central state administration body.

(2) After approval given by the central encryption body the head shall issue a decision about the establishment of a departmental encryption body as a special place of work[10]) in accordance with Article 9 paragraph 1 and Article 66 paragraph 1 of the Act. Model decision about the establishment of the departmental encryption body shall be published by the Authority on its website.

(3) An employee in the field of cryptographic information protection of a departmental encryption body may only be an individual authorized for acquaintance with classified information. If the departmental encryption body fulfils the duties according to Article 6 paragraph 2, at least one employee in the field of cryptographic information protection of a departmental encryption body shall be an individual authorized for acquaintance with classified information of the security classification level “Top Secret”.

(4) The central encryption body shall verify and certify the professional qualification of an employee assigned for the management of the activity of a departmental encryption body in the field of cryptographic information protection.

(5) Classified papers and documentation in the field of cryptographic information protection shall be registered in separate protocols of classified papers and registration instruments. An

[10]) Article 66 paragraph 1 and Article 9 paragraph 1 of Act No. 215/2004 (Coll.).

appointed person registered as employee in the field of cryptographic information protection shall keep the protocols of classified papers and registry of documentation in the field of cryptographic information protection. Registration and manipulation of classified papers in the field of cryptographic information protection shall follow a special regulation.[7])

Article 10
Cancellation of a Departmental Encryption Body

(1) The head shall cancel a departmental encryption body in case of

a) no further need for the cryptographic information protection in a central body of state administration;
b) dissolution or cancellation of a central body of state administration;
c) integration of a central body of state administration within another central body of state administration, which has got an already established departmental encryption body.

(2) The head shall in advance notify the Authority of the cancellation of a departmental encryption body, stating the reasons and date of cancellation.

(3) The head shall assign a committee for the cancellation of a departmental encryption body, consisting of individuals authorized for acquaintance with classified information of the relevant security classification level, to verify the entirety of devices and classified information of the relevant departmental encryption body and to suggest the form of material settlement of devices and transfer of classified information pursuant to a special regulation[7)], to the head.

Article 11
Entry into Force

This decree shall enter into force on 1 June 2004.

Aurel Ugor, by hand