

**340****REGULATION  
Of the National Security Authority****Of 10 May 2004,****Governing the details of Encryption Protection of Information**

The National Security Authority (hereinafter referred to as “Authority”) stipulates, pursuant to Article 69 of Act No. .../2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws (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 encryption protection of information (hereinafter referred to as “device”) into operation, their use, transfer, registration and the use of cipher materials;
- b) Keeping of records of employees in the section for encryption protection of information and verification of their professional qualification;
- c) Establishment of a departmental encryption body or other encryption body standing at the same level (hereinafter referred to as “departmental encryption body”).

**Article 2  
Certification of Devices**

(1) The 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 encryption protection of information and security standard for the protection against unfavourable electromagnetic radiation.

(2) The Authority shall certify devices, if asked for their certification by a departmental encryption body or legal entity that meets the industrial security conditions pursuant to special regulation<sup>1)</sup>.

(3) The departmental encryption body shall, within its competence, certify devices intended for the protection of classified information of the level of security classification “Confidential” and “Restricted”. It shall also certify devices intended for the protection of classified information of the level of classification “Confidential” or “Restricted”, if asked for by a legal entity that meets the industrial security conditions pursuant a special regulation<sup>1)</sup>, if expecting the possibility of their use.

---

<sup>1)</sup> Regulation of the National Security Authority No. 325/2004 (Coll.) on industrial security.

(4) Before a device is installed in conditions of a certification office, the applicant shall submit a protocol on the execution of operating 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.

(5) Documentation supplied with the relevant device shall be prepared in such a way as to allow the evaluation of its security and according to the level of security classification of protected classified information; it shall contain the following information:

a) For the level of security classification "Restricted":

1. Determination of the form of use of a device;
2. Type of the user's environment and systemic incorporation of a device;
3. Service instructions for the relevant device;
4. Instructions for the use of the relevant 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 intended 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 a part 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 licence policy;
15. Device installation procedure;
16. Device de-installation procedure,

b) For the level of security classification "Confidential", the information defined in letter a), as well as the following:

1. Method for the physical implementation of the relevant 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 damage of classified information by unfavourable electromagnetic radiation.
8. Description of the method used for the destruction of the relevant device.

c) For the level of security classification "Secret", the information defined in letters a) and b), as well as the following:

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 code 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 distribution of keys;
  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 level of security classification "Top Secret", the information defined in letter a) to c), as well as the following:
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 an occurrence of a fault in it;
  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 upon the serial production and service of the device;
  7. Method of liquidation of used or faulty carriers of cryptographic elements.

(6) The certification of a device 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 the certification of a device.

(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 for its completion. If the applicant does not complement 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 a device, verification of specified operating parameters of a device and appraisal of the service instructions and instructions for use of a device shall also form part of the device certification.

(11) The certification office shall draw up a certification protocol about the certification of the device, which shall especially contain the following:

- a) Name of the certification office;
- b) Name of the relevant 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 level of security classification;
- e) Level of security classification of protected information for which the device is certified;
- f) Results of its findings on the individual requirements of security standards;
- g) Category of the device according to the security standard for the protection against unfavourable electromagnetic radiation;
- h) Category of the area for the placement of the device according to the security standard for the protection against unfavourable electromagnetic radiation;
- 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 service 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 specific level of security classification.

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

(13) The managing person of the central state administration body (hereinafter referred to as “managing person”) 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 relevant device to protect classified information at the specific level of security classification.

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

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

(17) A device certificate shall contain the following information:

- a) Name of the central state administration body that issues 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) Level of security classification of protected information for which the relevant device is certified;
- f) Category of the device according to the security standard for the protection against unfavourable electromagnetic radiation;
- g) Category of the area for the location of the device according to the security standard for the protection against unfavourable electromagnetic radiation
- h) Qualification for the protection of classified information outside of protected areas or abroad;
- i) Identification data related to service instructions and instructions for the use of the device;
- j) Validity period of the relevant certificate;
- k) Date of issue of the certificate;
- l) Identification data and signature of the managing person approving the issue of the certificate.

(18) The Authority or managing person shall issue a device certificate, together with the service instructions and instructions for the use of the relevant device, pursuant to Annex No. 1.

(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 concluded an agreement about the protection of classified information and agreed guarantees for the security level of devices. The operating documentation of a device according to a certificate issued by a foreign authority is not binding for the use of the device for the 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,<sup>2)</sup> on the basis of an international treaty by which the Slovak Republic is bound. This however does not refer to devices intended for the cooperation of the Slovak Information Service with intelligence services of other states carried out pursuant a special regulation.<sup>3)</sup>

(21) With reference to devices gained by the Slovak Information Service from intelligence services of other states within the cooperation carried out pursuant a special regulation<sup>3)</sup>, the relevant managing person may issue a device certificate on the bases of a certificate issued by foreign authority.

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

---

<sup>2)</sup> Article 60 paragraph 2 of Act No. 215/2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws.

<sup>3)</sup> Act of the National Council of the Slovak Republic No. 46/1993 (Coll.) on Slovak Information Service, as amended by later regulations.

(23) The departmental encryption body shall keep a register of device certificates issued in its competence and inform the Authority about all certificate issued within 15 days from the day of their issue. 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) If required by the departmental encryption body, the Authority shall inform about the certificates issued within 15 days from the day that the request is delivered.

### 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 managing person. The managing person is also authorized to approve devices into operation on the basis of certificates adopted from other central state administration bodies. The departmental encryption bodies shall inform the Authority about all adopted certificates.

(2) A device may be only approved into operation within protected area,<sup>4)</sup> if not further established otherwise, and within area complying with the security standard for the protection against unfavourable electromagnetic radiation.

(3) The managing person shall, in his competence, approve a device into operation on the basis of a written submission made by a departmental encryption body pursuant to Annex No. 2.

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

- a) Name of the relevant device;
- b) Proposed date of the approval of the device into operation;
- c) The highest level of security classification of protected information;
- d) Recommended period of operation of the device;
- e) Brief characteristics of the purpose of the use of the relevant device; in the case of the approval of a device into operation out of the protected area inland or abroad, also a special 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 any;
- g) Results from the operating tests of the device;
- h) If the service instructions or instructions for the use of the device, issued together with the device certificate, are not sufficient, complements to the service instructions and instructions for the use of a device issued by a departmental encryption body, shall form an integral part of the submission;

---

<sup>4)</sup> Regulation of the National Security Authority No. 336/2004 (Coll.) on physical and building security.

- 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 operation of the technical device;
- 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 unfavourable electromagnetic radiation;
- k) Determination of the category of the protected area of the device location and identification data of the processed documentation about the physical and building security of protected premises,<sup>4)</sup> in which the device is placed; in the case of approval of the operation of a device outside of the protected area in the territory of the Slovak Republic or abroad outside of a representative offices of the Slovak Republic, a complement to the instructions for the use of the device in specific conditions, stating the method of destruction of a device and other classified information, if endangered;
- l) Specification of the device users;
- m) Specification of the employees in the section for 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<sup>5)</sup>;
- o) Description of the provision of maintenance and repairs of the device;
- p) Identification data and signature of the managing person approving the relevant device into operation.

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

(6) Outside of protected areas in the territory of the Slovak Republic and abroad outside the 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) With reference to devices gained for the protection of foreign information on the basis of an international treaty that the Slovak Republic is bound by, the managing person shall approve the devices into operation on the basis of certificates issued by foreign authority, only with a written approval given by the central encryption body. This does not refer to devices intended for the cooperation of the Slovak Information Service with the intelligence services of other states carried out pursuant to a special regulation.<sup>3)</sup>

#### Article 4 Use and Transfer of Devices

(1) Only devices may be used. Devices may only be used if certified and approved into operation and in compliance with their service instructions and instructions for use.

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

---

<sup>5)</sup> Article 70 paragraph 1 letter c item 10 of Act No. 215/2004 (Coll.)

(3) A device used for the protection of information with various levels of security classification, must be certified to the highest level of security classification of the protected information.

(4) A transfer within the protected area is not considered to be the transfer of classified information by technical devices<sup>6)</sup>.

(5) The transfer of devices shall be carried out through persons, who are authorized for the transfer of classified information pursuant to a special regulation<sup>7)</sup>, appointed by the managing person.

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

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

#### Article 5 Registration of Devices

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

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

(3) A departmental encryption body shall, on a yearly basis, carry out a physical inventory control of devices, whilst notifying the Authority of its result. This obligation does not refer to devices intended for the collaborative interconnection of the Slovak Information Service with intelligence services of other states, carried out pursuant to a special regulation.<sup>3)</sup>

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

#### Article 6 Use of cipher materials

(1) Cipher materials, as a part of a device<sup>8)</sup>, shall mean the passwords, keys, variable parameters of cryptographic algorithms identified according to the type of device and level of protection of classified information. The cipher materials may only be used in compliance with the instructions for the use of a device.

---

<sup>6)</sup> Article 6 paragraph 3 of Act No. 215/2004 (Coll.)

<sup>7)</sup> Regulation of the National Security Authority No.338/2004 (Coll.) on administrative security

<sup>8)</sup> Article 2 letter p) of Act No. 215/2004 (Coll.)

(2) The Authority or departmental encryption body, in its operation, carries out the administration of devices and production of cipher materials

(3) Cipher materials already used that are damaged, where there is suspicion of any unauthorized manipulation, cannot be further used for the encryption protection of information. The cipher materials the validity of which expired also cannot be further used for cryptographic information protection.

#### Article 7

#### Verification of the Professional Qualifications of an Employee in the Section for Cryptographic Information Protection

(1) An employee in the section for cryptographic information protection shall show his professional qualifications by the knowledge of generally binding legal regulations and internal rules about the protection of classified information and, if working with a device, also the knowledge of its service instructions, instructions for its use and its practical operation.

(2) The Authority and a departmental encryption body, in its operation, shall carry out the professional preparation for the acquiring of professional qualification in the section for cryptographic information protection, whilst specifying the scope and method used for the verification of professional qualification of an employee in the section for cryptographic information protection.

(3) A departmental encryption body, in its operation shall verify and acknowledge the professional qualifications of an employee in the section for cryptographic information protection for the levels of security classification “Restricted”, “Confidential” and “Secret”.

(4) The Authority, or a departmental encryption body authorized by the Authority, shall verify the professional qualifications of employees in the section for cryptographic information protection for the level of security classification “Top Secret”.

(5) A protocol shall be drawn up about the professional qualifications of employees in the section for cryptographic information protection.

(6) The Authority or a departmental encryption body, in its operation, shall acknowledge the professional qualification of an employee in the section for cryptographic information protection by issuing a licence on the professional qualification in the section for cryptographic information protection pursuant to Annex No. 3.

(7) A managing person shall issue a licence for work in specified section for cryptographic information protection pursuant to Annex No. 4 to an employee who meets the necessary conditions.

(8) A departmental encryption body shall keep a register of the certificates issued.

## Article 8

## Keeping a Register of Employees in the Section for Cryptographic Information Protection

(1) A departmental encryption body shall keep a register of employees in the section for cryptographic information protection in its operation. The Authority shall keep a register of employees in the section for cryptographic information protection of departmental encryption bodies.

(2) On the basis of a written proposal given by a departmental encryption body, the managing person shall approve the entry of an employee into the register in the section for cryptographic information protection.

(3) A register of employees in the section for cryptographic information protection<sup>9)</sup> shall contain the following:

- a) Name and surname (surname at birth);
- b) Surname at birth;
- c) Date and place of birth;
- d) Birth number; it is not necessary to state in the register of employees in the section for cryptographic information protection kept with the departmental encryption body of the Slovak Information Service;
- e) Personal registration number;
- f) Name and address of the employer;
- g) Position held;
- h) Level of security clearance;
- i) Date of issue and number of certificate for acquaintance with classified information;
- j) Date of the execution of a record stating the assignment of the proposed person to acquaint with classified information;
- k) Date of execution of a confidentiality declaration;
- l) Date of the registration;
- m) Registration number and date of issue of a licence on professional qualification of an employee in the section for cryptographic information protection, scope of professional qualification;
- n) Date of the withdrawal of a licence for work in a specified section for cryptographic information protection.

(4) Departmental encryption bodies shall inform the Authority about all changes in data kept in the register of employees in the section for 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 managing person, shall contain the following:

---

<sup>9)</sup> Article 2 paragraph 2 letter c) of Act No. 428/2002 (Coll.) on the protection of personal data.

- a) Name of the central state administration body;
- 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 managing person shall issue a decision about the establishment of a departmental encryption body as a special place of work<sup>10)</sup> pursuant to Annex No. 5.

(3) An employee in the section for cryptographic information protection of a departmental encryption body may only be a person authorized for acquaintance with classified information. If the departmental encryption body fulfils the duties pursuant to Article 6 paragraph 2, a minimum of one employee in the section for cryptographic information protection of a departmental encryption body must be a person authorized for acquaintance with classified information of the level of security classification "Top Secret".

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

(5) Classified papers and documentation in the section for cryptographic information protection shall be registered in separated protocols of classified papers and registration instruments. An appointed person registered as an employee in the section for cryptographic information protection shall keep the protocols of classified papers and register of documentation in the section for cryptographic information protection. Registration and manipulation of classified papers in the section for cryptographic information protection shall follow a special regulation.<sup>7)</sup>

## Article 10

### Cancellation of a Departmental Encryption Body

- (1) The managing person shall cancel a departmental encryption body, upon
- a) No further need for the encryption protection of information in a central state administration body;
  - b) Dissolution or cancellation of a central state administration body;
  - c) Integration of a central state administration body with another central state administration body, which disposes of an already established departmental encryption body.

(2) The managing person shall, beforehand, notify the Authority of the cancellation of a departmental encryption body, stating the reason and date of cancellation.

(3) The managing person shall assign a committee for the cancellation of a departmental encryption body, consisting of persons authorized to acquaint with classified information of the relevant level of security classification, which verifies the entirety of devices and classified information of the relevant departmental encryption body and suggests the form

---

<sup>10)</sup> Article 66 paragraph 1 and Article 9 paragraph 1 of Act No. 215/2004 (Coll.)

of material settlement of devices and submission of classified information pursuant to a special regulation<sup>7)</sup>, to the managing person.

Article 11  
Operation

This regulation shall enter into force on 1 June 2004.

**Aurel Ugor**, by hand

## Annex No. 1 to Regulation No. 340/2004(Coll.)

---

(Name of the central state administration body that issues the certificate)

Pursuant to Article 66 paragraph 3, letter d) of Act No. 215/2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws,

I s s u e s  t h i s

## C E R T I F I C A T E

**Reg. No.: .C..... level of security classification/encryption protection of information**

For the cryptographic information protection device

---

(Name, type identification, version, designation of the device producer and his identification data)

Applicant:

Registered seat:

Company Reg. No.:

On the basis of the findings of the certification protocol, document No. ...., stating the compliance with requirements in accordance with the security standards issued by the National Security Authority, the qualification of the device is hereby certified, for the protection of classified information with the following level of security classification:

---

(State the specific level of security classification)

According to the security standard for the protection against unfavourable electromagnetic radiation, the following category of the device ..... and area category ..... is specified.

The device may only be used for work with classified information of the level of security classification: ..... (inclusive) **in protected areas in the territory** of the Slovak Republic<sup>1)</sup>, in compliance with the conditions specified in the service instructions, document No.: ..... and the instructions for use, document No.: ....., which are issued together with the certificate.

Validity period of the device certificate until:

Date of issue:

Managing person of a central state ministration body  
(Signature and imprint of the stamp)

---

<sup>1)</sup> If it also concerns devices intended for the operation outside of protected areas or abroad outside of the representative offices of the Slovak Republic, these facts must be specified in the certificate.

Annex No. 2 to Regulation No. 340/2004 (Coll.)

(Name of the central state administration body)

Document No.: .....

**D E C I S I O N****About the approval of a cryptographic information protection device into operation**

Pursuant to Article 66 paragraph 3 letter c) of Act No. 215/2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws,

**I hereby approve**

The cryptographic information protection device into operation,  
in the conditions of .....  
(State the name of the central state administration body)

Device name:	
Date of approval into operation:	
Highest level of security classification of protected information:	
Operation approved until:	
Category of the area according to the security standard for the protection against electromagnetic radiation:	
Category of the device according to the security standard for the protection against electromagnetic radiation:	
Category of the protected area of the device placement:	
Identification data of the service instructions and instructions for use of the device and their appendices:	

Reasoning: On the basis of the submission of the departmental encryption body, document No.: .....  
The device is certified for the level of security classification .....,  
certificate with reg. No.: ....., issued by:  
..... on ....., valid until:  
.....

Date of issue:

Managing person of the central state  
administration body  
(Signature and imprint of the stamp)

Annex No. 3 to Regulation No. .340/2004 (Coll.)

(Name of the departmental encryption body)

Reg. No.:

# L I C E N C E

## OF THE PROFESSIONAL QUALIFICATION IN THE SECTION FOR CRYPTOGRAPHIC INFORMATION PROTECTION

On the basis of the verification of professional qualification carried out on: .....

Protocol No.:.....

### I hereby issue

Pursuant to Article 7 paragraph 3 to 6 of the Regulation of the National Security Authority No. 340/2004 (Coll.) laying down details about the encryption protection of information

.....  
(Name, surname, place of birth, birth No.)

### l i c e n c e

.....  
(Specify the actual scope of professional qualification, e.g., work with a device, certification of devices, etc. and the highest level of security classification of information with which the employee is authorized to acquaint within the scope of his professional qualification).

Date of issue:

Identification data of the employee in the section for cryptographic information protection appointed for the management of the departmental encryption body

(Signature and imprint of the stamp)  
Annex No. 4 to Regulation No. 340/2004 (Coll.)

(Name of the central state administration body)

Reg. No.:

# L I C E N C E

## FOR WORK IN THE SPECIFIED SECTION FOR CRYPTOGRAPHIC INFORMATION PROTECTION

On the basis of the licence for the acquaintance with classified information No. ....  
issued on ..... and licence on the professional qualification in the section for  
cryptographic information protection, reg. No. .... issued by the departmental  
encryption body on .....

### I hereby issue

Pursuant to Article 68 paragraph 2 of Act No. 215/2004 (Coll.) on the protection of  
classified information and on the amending and supplementing of certain laws and Article 7  
paragraph 7 of Regulation of the National Security Authority No. 340/2004 (Coll.) laying  
down the details about the encryption protection of information.

.....  
(Name, surname, place of birth, birth No.)

### l i c e n c e

.....  
(State the specified section for cryptographic information protection, e.g., for the performance of duties of an  
executive encryption body, execution of device certification, device administration, device operation, etc., and  
highest level of security classification on which the employee is authorized to acquaint with classified  
information in the specified section)

Date of issue:

Head of the central state administration body  
(Signature and imprint of the stamp)

Annex No. 5 to Regulation No. 340/2004 (Coll.)

(Name of the central state administration body)

Document No.: .....

**DECISION**

**About the establishment of a departmental encryption body**

For the provision of cryptographic information protection, in operation of

.....  
(State the name of the central state administration body)

Pursuant to Article 66 paragraph 1 of Act No. 215/2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws and Article 9 paragraph 2 of Regulation of the National Security Authority No. 340/2004 (Coll.) laying down the details about cryptographic information protection, on the basis of the approval of the central encryption body

Document No.: ..... of.....

**I hereby establish**

The departmental encryption body

Date of establishment: .....

I integrate the execution of the function of the departmental encryption body into

.....  
(State the organisational unit, e.g., into the Security Authority)

which is directly subject to the managing person of the central state administration body in compliance with Article 66 paragraph 2 of Act No. .215/2004 (Coll.).

For the management of activity of the departmental encryption body, I assign:

.....  
(Name, surname, position of the employee in the section for cryptographic information protection)

Pursuant to Article 66 paragraph 3 letter b) of Act No. 215/2004 (Coll.), I specify the scope of duties of the departmental encryption body

.....  
(State the document, which specifies the scope of duties, e.g., in the system of organisation)

This decision is made in two copies, whilst one copy is intended for the central encryption body of the Slovak Republic, the functions of which are carried out by the National Security Authority and the second copy is kept with the departmental encryption body.

Date of issue:

Head of the central state administration body

(Signature and imprint of the stamp)