ORDINANCE ON THE ELECTRONIC SIGNATURE CERTIFICATES IN THE ADMINISTRATIONS

Effective as of 13 June 2008

Adopted by Decree of the Council of Ministers No 97 of 16 May 2008

Promulgated SG, No. 48 of 23 May 2008

Chapter One

GENERAL PROVISIONS

Article 1. This Ordinance shall regulate the terms and conditions and the policies for the acquisition, use, renewal and termination of electronic signature certificates in the administrations.

Article 2. Pursuant to the terms and conditions of the Ordinance the following electronic signature certificates in the administrations shall be acquired, used, renewed and terminated:

1. Universal electronic signature certificates, which may be used by persons who are authorized to make electronic statements on behalf of the administration;

2. Universal electronic signature certificates which may be used by persons who are authorized to send electronic statements, made by the persons under point 1, on behalf of the administration and only for the purpose of sending such statements;

3. Electronic signature certificates for internal departmental needs within the internal Public Key Infrastructure of the administration or for all administrations, which may be used by all administration employees for the purpose of the assignment, the implementation of tasks and the tasks implementation control;

4. Electronic signature certificates for internal departmental needs, issued by an External Certificate Services Provider, which may be used by all administration employees for the purpose of the assignment, the implementation of tasks and the tasks implementation control;

5. Servers identification certificates, which may be used by the administrations to provide secure electronic communications for the purpose of sending electronic statements to the administrations and of the servers identification where their Internet sites and information systems are disposed;

6. Certificates for the provision of integrity and author’s rights on software code or on files containing other information or a realizable code, which may be used by the administrations as an exception.

Article 3. Universal electronic signature certificate shall be issued by a Certificate Services Provider, registered by the Communications Regulation Commission, and shall be granted for use to single public bodies, members of collective public bodies, employees or persons in the administrations, who have an employment relationship or a civil servant relationship, a civil contract, and to persons in professional military service.

Article 4. (1) Right to make electronic statements on behalf of the administrations shall be granted to persons who possess a valid universal electronic signature certificate and who have been authorized by virtue of a law or duly authorized.

(2) Right to send electronic statements under paragraph 1 on behalf of the administrations shall be granted to persons who possess a valid universal electronic signature certificate and who have been authorized by an order of the head of the administration.

(3) Right to make electronic statements within a relevant administration shall be granted to persons who possess a valid electronic signature certificate regardless of whether it has been issued for internal departmental needs within the internal Public Key Infrastructure (PKI) for the relevant administration or for all administrations, or has been issued by a Certificate Services Provider.

(4) In addition to the cases under paragraphs 1 and 2, right to make electronic statements on behalf of the administrations for the purpose of the provision of internal electronic administrative services shall be granted to persons who possess a valid electronic signature certificate issued within the internal PKI for all administrations, or issued by a Certificate Services Provider.

Article 5. (1) Universal electronic signature certificates may be issued pursuant to the terms and conditions of the Ordinance as an exception, where the holders are natural persons – employees in the administrations, upon a written order of the heads of the relevant administrations.

(2) The terms and conditions for using electronic signature certificates and other certificates using PKI technologies, in the exchange of documents through the Unified Environment for e-Documents Exchange shall be determined by the Ordinance under Article 41(2) of the Law on e-Governance.

Article 6. (1) The common organization, the administration and the control of the implementation of the Ordinance shall be effected by the Director of the Directorate or the Head of the Unit which is in charge of provision of information services and the information technologies in the relevant administration.

(2) The head of the administration shall authorize by an order the Director of the Directorate, respectively the Head of the Unit or another person, to represent him before the Certificate Services Provider in the issuance and management of the certificates.

Article 7. The universal electronic signature certificates and the electronic signature certificates shall be applied for issuance for a period of one year as of the date of issuance.

Chapter Two

ISSUANCE, USE, RENEWAL AND TERMINATION OF ELECTRONIC SIGNATURE CERTIFICATES

Section I

Issuance of Electronic Signature Certificates

Article 8. (1) The issuance of universal electronic signature certificates of the type under Article 2, points 1, 2 and 4 to the employees in the administrations shall be based on the lodging of a standard request in accordance with the Annex, addressed to the head of the relevant administration, which indicates the desired number and type of certificates. The request shall be signed by the Director of the Directorate where the employee is appointed, and respectively by the Head of the Unit, when the employee does not work in a directorate.

(2) The request shall be submitted along with the documents for the issuance of an electronic signature certificate, required by the Certificate Services Provider.

(3) Where the Certificate Services Providers require that registration forms be submitted along with the request under paragraph 1, they shall be filled in by the persons for whom certificates of the types under Article 2, points 1, 2 and 4 will be issued.

(4) Summarized references, containing information from the registration forms, shall be prepared by authorized persons within the meaning of Article 6(2).

(5) The request under paragraph 1 and the Annexes thereto, shall be send with a certificate to the Director of the Directorate or the Head of the Unit under Article 6 in the relevant administration for harmonization that may require additional information from the person to whom a certificate should be issued.

(6) Following an approval by the head of the administration, the person under Article 6(2) shall send the approved requests along with the Annexes thereto to be implemented to the Certificate Services Provider and shall informed the head of the applying unit about the unapproved ones.

Article 9. (1) Universal electronic signature certificates under Article 2, points 1 and 2 shall be issued by the Certificate Services Provider at the request of the administrations of the natural persons who have a civil contract and who have been authorized to make electronic statements and to represent the administration, and of the persons authorized to send electronic statements on behalf of the administration.

(2) The issuance of universal electronic signature certificates under Article 2, points 1 and 2 shall be made at request of the authorized person before the head of the administration. Besides the necessary documents required by the Certificate Services Provider, it is also obligatory to attach to the request a certified copy of the order of the head of the administration which authorizes the requesting person to make electronic statements and to represent the administration to the request. When the order is issued electronically, a hard copy shall be attached thereto.

(3) The submission of the issued universal electronic signature certificates and their acceptance by the natural persons to whom they have been issued personally shall be effected at the Certificate Services Provider.

Article 10. (1) The issuance of universal electronic signature certificates under Article 2, point 3 to the employees in the administrations for internal departmental needs shall be based on the lodging of a standard request in accordance with the Annex to the head of the relevant administration, which indicates the desired number of certificates. A list of all employees in the administration to whom a certificate should be issued shall be attached to the request.

(2) The request under paragraph 1 shall be agreed in advance with the persons under Article 6(1).

Article 11. (1) Certificates of the type under Article 2, points 5 and 6 shall be issued by the Certificate Services Provider based on a request approved by the head of the administration, made by the Director of the Directorate or the Head of the Unit under Article 6, in a form stipulated in the Annex. The person under Article 6(2) shall submit to the provider the documents required by the latter, along with the request.

(2) The submission of the issued certificates of the type under Article 2, points 5 and 6 and their acceptance by the persons under Article 6(2) shall be effected at the Certificate Services Provider.

Article 12. (1) The persons authorized under Article 6(2) shall submit all documents necessary for the issuance of electronic signature certificates personally to the Certificate Services Provider and shall obtain personally from him a reference with extracts from the Public Register of the Provider containing the certificates issued by him.

(2) The persons authorized under Article 6(2) have the obligation to keep in secret the information about the personal data of the natural persons, which became known to them in relation to the issuance and the management of the electronic signature certificates.

Article 13. (1) A list of all types of issued electronic signature certificates shall be held and maintained by the Directorate or the Unit under Article 6, containing the following information:

1. Data identifying the Certificate Services Provider if certificates under Article 2, points 1, 2 and 4 have been issued; if certificates under Article 2, point 3 have been issued, it shall be also indicated whether PKI is internal or for all administrations;

2. Type and number of the electronic signature certificates;

3. The names and the position of the employees, respectively the names of the persons who have a civil contract, who are authorized to make, respectively to send statements on behalf of the administrations;

4. The extent of the representative power regarding the right to make or send electronic statements on behalf of the administrations;

5. The name of the Directorate respectively of the Unit in which the employee works;

6. Date of issuance and period of validity of the certificates;

7. Status of the issued certificates;

8. The name and the position of the authorized person within the meaning of Article 6(2);

9. The number and the date of the authorization order within the meaning of Article 6(2);

10. The number and the date of the authorization order within the meaning of Article 9.

(2) The Director of the Directorate or the Head of the Unit under Article 6, or a person authorized by him, shall cover any change in the data kept in the list on the basis of information obtained from the Certificate Services Provider or by the organization or the unit which maintains the internal Public Key Infrastructure for issued, extended or terminated certificates.

Article 14. The Director of the Directorate or the Head of the Unit under Article 6 shall inform the Directorate in charge of human resources management in the administration and the Heads under Article 8(1) of the issued electronic signature certificates under Article 2, points 1 to 4 immediately after their issuance.

Section II

Use and renewal of electronic signature certificates

Article 15. The use of electronic signature certificates under Article 2, points 1 to 4 shall be in accordance with the Law on Electronic Document and Electronic Signature (LEDES), the regulations on its application, the rules and the procedures of the Certificate Services Provider (customer manual of the provider), the Ordinance and the other rules established for work with electronic documents in the administrations.

Article 16. (1) The electronic signature certificates under Article 2, points 1 to 4, shall be personal. Authorized person has the right to make electronic statements on behalf of the administration only within the scope of his competences arising from the position respectively from the representative power delegated to him.

(2) A person who has the right to sign by using an electronic signature under Article 2, points 3 and 4, may not confer the rights of access to the means of creating an electronic signature where such rights are preserved in the work station of the person, and that station is used by other persons.

(3) A person who has the right to sign by using an electronic signature under Article 2, points 3 and 4, may not confer to other persons the holding of the device conferred to him for a secure

creation of the signature, on which the Private Key for signatures creation is recorded (a Smart Card, an USB token, etc.). The device shall be used by inserting it into a card reading device (card reader) or in another device by means of a relevant interface, and the access to the Private Key shall be provided through PIN or biometric identifier.

(4) A person who has the right to sign by using an electronic signature may not, under any circumstances, make available to other persons his or her personal identification number (PIN) for access to the Private Key for signing except for the cases under Article 18(3) and Article 22(2) and (3).

Article 17. (1) Information systems, which enable automatic signing of electronic documents in the cases of handling requests for internal electronic administrative services and in the cases of automatic generation of statements by the administrations for the purpose of providing electronic administrative services to the citizens and the organizations, may be used in the administrations.

(2) Automatic signing shall be made by using a mechanism for secure signature creation with minimal security requirements EAL 4 under the Common Criteria for Information Technology Security Evaluation - CC 2.1 adopted by the International Standardization Organization (ISO) in the international standard ISO/IEC 15408:1999.

(3) Automatic signing shall be made respectively:

1. on behalf of person under Article 4(1) – for the statements made on behalf of the administration;

2. on behalf of person under Article 4(2) – for the purpose of sending electronic statements signed by persons under point 1.

(4) Where the maintenance of the program-technical devices under paragraphs 1 and 2 is assigned to an external organization, the contract shall precisely specify the person on behalf of whom signing will be made.

(5) The heads of the administrations shall assign an employee possessing the required qualification the task of being responsible for the maintenance of the program-technical devices providing the automatic signing. The setting, the installation of Private Keys and certificates, commissioning into exploration and decommissioning of the program-technical devices for automatic signing shall be duly documented and shall be implemented under the control of the Director of the Directorate respectively of the Head of the Unit under Article 6.

Article 18. (1) The renewal of the electronic signature certificates issued under Article 2, points 1, 2 and 4, shall be implemented in accordance with the provider’s procedure and under the terms and conditions of Article 8, respectively of Article 9.

(2) The renewal of issued certificates shall be implemented through the policy of renewal.

(3) Where the key or the security in its using has been discredited, or the terms of validity of the keys have expired, the certificate shall be terminated under the terms and conditions of Article 22 and subsequent, and where encrypted documents have been accepted by the employee, they together with the PIN for access to the Private Key, shall be submitted by a protocol to the Director of the Directorate or the Head of the Unit under Article 6 (2). The employee shall mark off in the list under Article 13 and submit the device for secure creation of the signature, if he is the holder, and the PIN, in a sealed envelope, to the Director of the Directorate, which is in charge of human resources management, who shall attach it to the employee’s personal file. In this case a new electronic signature certificate shall be issued to the employee, with a new couple of keys of a new device.

(4) The renewal of certificates under Article 2, point 3 shall be performed under the terms and conditions of Article 10.

Article 19. (1) The renewal of certificates under Article 2, points 1, 2 and 4 shall be performed under the terms and conditions of Article 9, in accordance with the terms and procedures of the Certificate Services Providers.

(2) The documents to be submitted to the Certificate Services Providers regarding a renewal of an electronic signature certificate shall be described in the official sites of the Certificate Services Providers.

Article 20. (1) The renewal of certificates shall be made only for the same electronic signature certificate prior to the expiry of its term of validity and provided that no data has been changed to the moment of issuance of the initial certificate.

(2) Where the data is changed or the term of validity of the old certificate is expired, it is necessary to make a request for issuance of a new certificate in accordance with Articles 8 and 9.

Article 21. The renewal of certificates under Article 2, points 5 and 6 shall be performed under the terms and conditions of Article 11.

Section III.

Termination

Article 22. (1) The validity of an electronic signature certificate shall be terminated:

1. In case of expiration of the term of validity of the certificate unless it is renewed under Article 18 and subsequent;

2. In case of termination of the employment relationship or the civil servant relationship of the person as well as upon withdrawal of the representative power of the authorized person.

3. In case of termination of the contract between the administration and the Certificate Services Provider for the certificates under Article 2, points 1, 2, 4 to 6;

4. In case of loss, theft, damage or destruction of the Private Key and/or the carrier on which it is recorded; in that case the person is obligated to inform immediately the Director of the Directorate or the Head of the Unit under Article 6 and the Certificate Services Provider of its termination;

5. In case of death or placing under disability of the natural person – an employee or an authorized person;

6. In case of changing of personal or official data of the person, related to that person's identification, authorization or official position;

7. In case of a request made in writing by the administration to the Certificate Services Provider;

8. In case of doubt for a discredit of the Private Key, the employee shall inform this immediately to the Director of the Directorate or the Head of the Unit under Article 6, and to the Certificate Services Provider, of the termination of the certificate;

9. In case of establishing that the certificate has been issued on the grounds of false data.

(2) The persons, for whom the ground for using an electronic signature certificate has become invalid, are obligated to submit immediately the carrier, on which the Private Key is recorded, to the Director of the Directorate or the Head of the Unit under Article 6, together with the PIN for

access, where with the certified public key were send encrypted messages to the person for whom the ground for using the electronic signature certificate has become invalid. The latter shall mark off in the list under Article 13 and shall submit the carrier and the PIN for access in a sealed envelope to the Director of the Directorate, which is in charge of the human resources management, to be attached to the employee's personal file.

(3) In case of termination of the employment relationship or the civil servant relationship, the submission of the Private Key carrier (the card or other) shall be attested by certification (signature) on the return list, by the Director of the Directorate or the Head of the Unit under Article 6.

Article 23. (1) The Director of the Directorate, which is in charge of human resources management, shall inform immediately the Director of the Directorate or the Head of the Unit under Article 6 by providing him or her with data about the person and the date of his or her discharge, or data about the change in his or her statute (position, rank, change in the type of the relationship etc), so that notifications can be made to the Certificate Services Provider concerning the status of the certificate under Article 2, points 1, 2 and 4, or respectively a change in the status of the certificate under Article 2, point 4, as well as a marking in the list under Article 13 can be made.

(2) The person under Article 6(2) shall send immediately a notification to the Certificate Services Provider of the existing a ground for termination of the certificate under Article 2, points 1, 2 and 4. The communication can be made by fax, e-mail or in accordance with the procedures established by the provider.

Article 24. (1) The termination of electronic signature certificates of the type under Article 2, points 1, 2 and 4 of the employees in administrations and of the persons who have a civil contract shall be performed by the person under Article 6(2) by meeting the requirements of the Law on Electronic Document and Electronic Signature and of the rules of the Certificate Services Provider.

(2) The documents required by the Certificate Services Provider shall be attached to the request.

(3) Where the Certificate Services Providers require that registration forms be submitted along with the request under paragraph 1, they shall be filled in accordance with the requirements of Article 13.

Article 25. The termination of electronic signature certificates of the type under Article 2, point 3 to the employees in the administrations and to the persons, who have a civil contract, shall be performed immediately by the persons under Article 6(1) in case that the ground for termination occurs.

Section IV

Safe-keeping of the Private Keys and notification

Article 26. (1) The persons to whom electronic signature certificates have been issued in accordance with the Ordinance are obligated to keep and not to disclose the data providing access to the Private Key (PIN), to protect from damage or destruction the carrier (a Smart Card or other carrier) on which the Private Key is recorded and not to allow other persons to make statements from their profile using signatures under Article 2(3).

(2) A person who uses an electronic signature shall not have the right to set up a computer system, from which he or she signs electronic statements, to save the personal identification number for access to the Private Key.

(3) Any person who has doubts that his or her or another employee's Private Key is discredited, is obligated to undertake immediately actions under Article 22(1) point 8.

Chapter Three

ELECTRONIC SIGNATURES VERIFICATION

Article 27. (1) The persons who verify electronic signatures under Article 2, points 1 and 2 shall have to use a secure mechanism for verification of signatures and the supporting certificates.

(2) The persons who carry out the verification of a universal electronic signature must apply a combination of software and hardware, which guarantees that:

1. The data regarding the verification of the use of the electronic signature correspond to the data visualized before the person who carries out the verification;

2. The signature is duly verified and the verification results are visualized before the person who carries out the verification;

3. The content of the signed statement can be duly identified;

4. The authorship and the validity of the electronic signature certificate have been duly verified at the time of verification;

5. The verification results and the author's identity have been reproduced correctly;

6. All changes relating to security can be established.

Supplementary provisions

§ 1. Within the meaning of the Ordinance:

1. "Smart Card" means the tangible electronic carrier comprising a plastic body and a chip on which the Private Key for the creation of an electronic signature is safely stored.

2. "Discredit of the Private Key" is an event when the Private Key is made known to third persons regardless of the circumstances under which it has happened.

3. "Registration body" is a unit commissioned by the Certificate Services Provider to carry out its activities in relation to the acceptance, verification, approval or rejection of requests for the issuance of electronic signature certificates, the registration of requests, submitted to the provider, for issuance and introduction of changes in the certificates status, caring out of relevant verifications to establish the identity, respectively the identity of the holder and the author as well as specific data for them by admissible means and in accordance with the policies and practices for the provision of the relevant certificate services, submission of the respective carriers on which the certificates and the Private Keys for the creation of electronic signatures are recorded, if the couple of keys is generated at the provider, and concludes contracts for the provision of certificate and other cryptographic, information and consulting services with the holders on behalf of the provider. The Registration body shall be a separate unit within the Certificate Services Provider or

a unit within a legal entity, different from the provider, to which rights to carry out the activities on behalf of the provider have been delegated.

Final provisions

§ 2. The Ordinance shall be adopted on the grounds of Article 37 of the Law on e-Governance.

§ 3. The Ordinance shall be effective from the date of entry into force of the Law on e-Governance.

Annex to Article 8(1), Article 10(1) and Article 11(1)

TO

THE HEAD

OF

Dear/Mr./Mrs.……

In relation to ……

.....

.....

(description of the arising need of using ESC)

I kindly request you to assign the issuance/renewal of .....
(number) electronic signature certificates of the type ..... .

It is necessary to provide us with …… (number) card-readers.

Annexes:

1. Order of ..... No …… of ..... (original).

(name of the Head of Unit)

2. Filled in registration forms (original) - ..... (number).

3. Summarized reference containing information from registration forms on a hard copy and an electronic carrier.

4. Others .....

DIRECTOR OF DIRECTORATE:

HEAD OF UNIT:

(...../signature)

(name)