

**DECREE**  
**of the National Security Authority**

of 9 September 2002

**on the format and manner of creating a qualified electronic signature, the manner of issuing the Authority's public key, the verification procedure and verification conditions of a qualified electronic signature, time stamp format and the manner of time stamping, requirements for the source of time data and requirements for holding documentation on time stamps (on the creation and verification of an electronic signature and time stamp)**

The National Security Authority (hereinafter referred to as the "Authority") pursuant to Articles 4 (4) and (5), 5 (5), 9 (2) of Act No 215/2002 Coll. on the electronic signature and on the amendment to certain acts (hereinafter referred to as "the Act") lays down:

Article 1  
Scope

This Decree governs:

- (a) the format and manner of creating a qualified electronic signature,
- (b) details on the conditions for the validity of a qualified electronic signature, the verification procedure for a qualified electronic signature and the conditions for validating a qualified electronic signature,
- (c) the manner of issuing the Authority's public key,
- (d) signature schemes, algorithms and parameters of these algorithms for creating a qualified electronic signature,
- (e) the format of a time stamp and the manner of time stamping,
- (f) requirements for holding documentation on time stamps.

Article 2  
Definitions

For the purposes of this Decree

- (a) signature scheme means the unique definition of algorithms for the creation and verification of a qualified electronic signature and their parameters,
- (b) approved signature scheme means a signature scheme from the list of signature schemes approved and issued by the Authority,
- (c) hash function means a mathematical transformation assigning to digital document of various length such values of a pre-set non-zero fixed length that enable integrity verification of the digital document from which the value were derived via the transformation, and where it is not possible to invert the digital document from them,
- (d) approved hash function means a hash function stated in the list of approved signature schemes listed in the annex,
- (e) digital fingerprint of a document means a value calculated from the document with the aid of the hash function,

- (f) digital signature of an electronic document means the result of a transformation of a digital fingerprint of a given electronic document with the aid of an algorithm for creating an electronic signature and a private key of the signer,
- (g) signature policy identifier means data uniquely identifying the given signature policy,
- (h) reference time means the time which one of the reference workplaces provide,
- (i) time stamp issuer (hereinafter referred to as the “Issuer”) means an accredited certification authority providing a time stamp service,
- (j) relying party means the recipient of a time stamp relying on its precision.

### Article 3

#### Formats of a qualified electronic signature

- (1) A qualified electronic signature has a format
  - (a) without time stamp,
  - (b) with time stamp,
  - (c) with complete information for validation,
  - (d) archive, or
  - (e) a combination of formats according to points (a) to (d).
- (2) A qualified electronic signature without time stamp contains
  - (a) the signature policy identifier used in creating and verifying the given qualified electronic signature,
  - (b) signature data, which the signer included in the qualified electronic signature (e.g. place and time of creating the given electronic signature, name of natural person signing on behalf of a legal person, etc.),
  - (c) digital signature, which was created on the basis of
    - 1. a digital fingerprint of the document signed,
    - 2. signature policy identifier,
    - 3. data included by the signer in the electronic signature.
- (3) A qualified electronic signature with time stamp has the form of a qualified electronic signature to which is attached or is otherwise logically connected a time stamp created on the basis of the given qualified electronic signature procedure provided for in Article 7.
- (4) A qualified electronic signature with full information for validation has the form of a qualified electronic signature with time stamp, to which is attached full information on all qualified certificates of public keys necessary for validating the given qualified electronic signature, as well as full information on certificate revocation lists or information on the status of qualified certificates that are decisive in validating the given qualified electronic signature.
- (5) An archive qualified electronic signature has the form of a qualified electronic signature with time stamp to which are attached all data necessary for verification of the given archive qualified electronic signature under Article 11(1). A time stamp is created for data necessary for the verification of the given archive qualified electronic signature, and which is attached to these data.
- (6) The Authority issues the valid formats of qualified electronic signatures and their formal specifications on its website.

## Article 4 Signature policy

- (1) A signature policy is a set of rules governing the creation and verification of qualified electronic signatures. A qualified electronic signature is created by the signer in accordance with the set signature policy. The validity of a qualified electronic signature is validated by the verifier with regard to the signature policy used in creating this electronic signature.
- (2) The party receiving the documents signed by a qualified electronic signature determines the signature policy it accepts.
- (3) The signer and verifier of a qualified electronic signature use the same signature policy.
- (4) The content and structure of the signature policy is issued on the Authority's website.

## Article 5 Creation of a qualified electronic signature

- (1) A qualified electronic signature of an electronic document is created by the signer with the aid of a secure-signature-creation device<sup>1</sup> on the basis of an electronic document and private key of the signer, according to one of the approved signature schemes under Article 6.
- (2) A qualified electronic signature with time stamp is created by the signer on the basis of a qualified electronic signature by means of the time stamp issuer so that the time stamp issued by the accredited certification authority for the given qualified electronic signature is attached to the qualified electronic signature or is logically connected with the qualified electronic signature for which the given time stamp was issued.
- (3) A qualified electronic signature with full information for validation is created by the signer following the creation of the qualified electronic signature with time stamp or verifier of the qualified electronic signature with time stamp so that to the qualified electronic signature with time stamp it attaches references to all data necessary for the verification of the given qualified electronic signature with time stamp under Article 11.
- (4) An archive electronic signature is created by the signer following the creation of a qualified electronic signature with time stamp whereby it attaches to the qualified electronic signature with time stamp all data necessary for the verification of the given qualified electronic signature with time stamp pursuant to Article 7 and the time stamp issued for these data.

## Article 6 Signature schemes for creating a qualified electronic signature with time stamp

The list of approved signature schemes, approved algorithms and parameters of approved algorithms for creating qualified electronic signatures is given in the Annex.

---

<sup>1</sup> Decree of the National Security Authority No 539/2002 Coll. laying down details on requirements for secure-time-stamp-creation devices and requirements for electronic signature products (on electronic signature products).

Article 7  
Creation and verification of the time stamp

(1) A time stamp policy is a set of rules laying down the usability of a time stamp of a given sphere of users of time stamps and of a class of applications with common security requirements.<sup>1</sup> The time stamp policy is created by time stamp users and time stamp issuers.

(2) A legal or natural person requesting time stamping (hereinafter referred to as the “requester”) sends to the time stamp issuer a time-stamping request. The request contains a digital fingerprint of the document for which the time stamp is to be created, created by means of an approved hash function.

(3) If the request is in accordance with requirements laid down in paragraph 2 and there are no obstacles to the creation of the time stamp from the side of the issuer under Article 9(4), the issuer issues by means of the secure-time-stamp creation device and a time source a time stamp for the submitted digital fingerprint of the document and sends it within the time set by the time stamp policy to the requester.

(4) If the time-stamping request does not satisfy the requirements laid down in paragraph 2 above, or any obstacles arise at the issuer preventing the issuance of a time stamp under Article 9 (4), the issuer does not issue the time stamp for the submitted digital fingerprint of document, and advises the requester of this fact and its cause within the time set by the time stamp policy.

(5) Authentication of the time stamp is carried out by the relying party on the basis of the time stamp and document for which the given time stamp was issued, and the time stamp policy applying for the given time stamp. The time stamp is valid if

- (a) it is in accordance with the time stamp policy used,
- (b) the time stamp’s qualified electronic signature of the issuer is valid according to Article 11 (1) and (2).

(6) The format of the time-stamping request the format of the time stamp and format of the reply to the time-stamping request is issued on the Authority’s website.

Article 8  
Requirements for the time source for a time stamp

The time source used by the issuer for issuing a time stamp fulfils the following requirements:

- (a) the time source is synchronised with the reference time source with the declared precision,
- (b) calibration of the time source is maintained so as to ensure that no deviation beyond the framework of the declared precision occurs,
- (c) the time source is protected against any danger that could result in undetectable changes in the time source, leading to a deviation outside the calibration framework,
- (d) there is ensured the detection of cases where the time data that is to be stated in the time stamp deviates from the synchronisation with the reference time source; the issuer must notify relying parties of this,

---

<sup>1</sup> Decree of the National Security Authority No 539/2002 Coll. laying down details on requirements for secure-time-stamp-creation devices and requirements for electronic signature products (on electronic signature products)

- (e) the issuer performs synchronisation of the time source in the case of issuing a corrective second on the basis of a notice from the reference time administrator,
- (f) the issuer performs a change in which it sets the corrective second in the last minute of the day for which the change is planned; the issuer makes a record on the precise time, with the declared precision of making this change.

#### Article 9

##### Requirements for time data for a time stamp

- (1) The issuer performs time stamping in a reliable manner. Time stamps contain the correct time data.
- (2) For time stamping the issuer uses at least one time source providing reliable time data, satisfying the requirements pursuant to Article 8.
- (3) Time data contained in the time stamp is provably derived from at least one value of the reference time.
- (4) If the time data source does not achieve the requested precision, i.e. deviates from the reference time source by more than specified in the time stamp issuer's operating code, the issuer does not issue the time stamp.

#### Article 10

##### Time stamp documentation

- (1) All information on the provision of a time stamp creation service is recorded and archived in accordance with the time stamp policy.
- (2) In time stamping the issuer maintains
  - (a) a list of time stamps issued by the issuer, where the time stamp is, from its issuance, maintained for a period set by the time stamp policy used by the issuer,
  - (b) records on extraordinary events in the system used in the time stamp management,
  - (c) records on important events in the environment of the time stamp issuer, in the management of cryptographic keys and in the synchronisation of time sources, including the precise time data.

#### Article 11

##### Validation of a qualified electronic signature

- (1) In order to verify the validity of a qualified electronic signature the verifier uses
  - (a) the electronic document for which the qualified electronic signature was issued,
  - (b) the qualified electronic signature of the electronic document,
  - (c) the valid public key pertaining to the private key, by means of which the qualified electronic signature was created,
  - (d) the signature policy, the identifier of which is stated in the qualified electronic signature.
- (2) In order to validate an electronic document's qualified electronic signature on the basis of data mentioned in paragraph (1) above and algorithms given in the signature scheme used for creating the qualified electronic signature, it is necessary to ascertain whether

- (a) the digital signature contained in the qualified electronic signature is valid,
- (b) the qualified electronic signature of the electronic document was issued according to the set signature policy.

(3) The validity of a qualified electronic signature cannot be verified if the verifier does not have available the data set out in paragraph (1) above.

(4) Validation of a qualified electronic signature with time stamp consists of the verification of

- (a) the validity of the qualified electronic signature under paragraphs (1) and (2),
- (b) the validity of the time stamp of the qualified electronic signature under Article 7 (5).

(5) Validation of a qualified electronic signature with full information, as regards validation, comprises the verification of

- (a) the availability and completeness of information for validation of the qualified electronic signature,
- (b) validity of the qualified electronic signature with time stamp pursuant to paragraph (4).

(6) Validation of an archive qualified electronic signature comprises the verification of

- (a) the validity of the time stamp under Article 7 (5), which was issued on the basis of data under paragraph (1),
- (b) completeness of information for verification of the qualified electronic signature,
- (c) the validity of time-stamped qualified electronic signature under paragraph (4).

#### Article 12

##### The Authority's public key

(1) The Authority's public key is a public key pertaining to the Authority's private key. With the aid of the Authority's private key the Authority

- (a) creates a qualified electronic signature of public key qualified certificates of accredited certification authorities,
- (b) creates a qualified electronic signature for the qualified certificate of the own public key,
- (c) issues a qualified electronic signature for the certificate revocation list issued by the Authority.

(2) The Authority issues its public key by issuing the Authority's public key qualified certificate in the press and on the Authority's Internet website. The Authority can issue its public key also in another manner.

(3) The Authority issues a new public key of the Authority 30 days prior to the expiry of the validity of the Authority's current public key and issues it in the manner set out in paragraph (2) above.

#### Article 13

##### Entry into force

This Decree enters into force on 1 October 2002.

**Ján Mojžiš**, in his own hand

**SIGNATURE SCHEMES, ENCRYPTION ALGORITHMS AND THEIR  
PARAMETERS**

**Signature schemes**

Signature scheme  
Asymmetric algorithm  
Minimum parameters of the asymmetric algorithm  
Algorithm for key creation  
Padding  
Hash function

**Algorithms for key creation**

Key creator designation  
Designation used  
Asymmetric algorithm  
Random figure creation method  
Random creator parameters

alebo = or

**Random figure creation method**

Random creator designation  
Name used  
Random creator parameters

**Hash functions**

Hash function designation  
Name used