

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

of 9 September 2002

**on the content and scope of operating documentation administered by a certification authority and on the security rules and rules for performing certification activities**

The National Security Authority (hereinafter referred to as “the Authority”) pursuant to Article 14(1)(j) and (2) and Article 26(1)(b) of the first point 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 content and scope of a certification authority’s operating documentation,
- b) security rules and rules for performing the certification activities of an accredited certification authority,

Article 2

Definitions

For the purposes of this Decree

- a) data pair is a pair formed by a public key and private key pertaining to a given public key,
- b) security measure is a technical, personnel or administrative element of protection having the purpose of maintaining the secure and reliable performance of certification activities,
- c) type of a certificate and of a time stamp is a group of attributes characterising the issued certificate and time stamp from the aspect of price and recommended use; a certification authority can issue various types of certificates and time stamps.

Article 3

Documentation of the certification authority

- (1) A certification authority draws up, administers and updates documentation for performing certification activities.
- (2) A certification authority’s documentation contains
  - a) operating documentation,
  - b) security rules,

- c) rules for performing certification activities.

#### Article 4

##### Certification authority's operating documentation

A certification authority's operating documentation contains

- a) a certification code,
- b) model contracts on the issuance and use of a certificate,
- c) a price list of certification services provided,
- d) operating records,
- e) other records which the certification authority deems expedient.

#### Article 5

##### Certification code

(1) The certification code contains

- a) information on for whom and under what conditions the certification authority provides its services,
- b) limitations on the provision of its services, if any,
- c) types of certificates and time stamps issued by the certification authority,
- d) signature policies and time stamp policies<sup>1</sup>,
- e) rights and obligations of users of the certification authority's services,
- f) a model request for the provision of certification service,
- g) rules for the use and revocation of certificates.

(2) Besides the information stated in paragraph (1) above, the certification code can contain also further information the publication of which the certification authority deems expedient.

(3) The certification code of an accredited certification authority describes the tasks of individual subjects and the processes relating to the administration of certificates, this being

- a) the initial registration of a request for the issuance of a certificate,
- b) the request for the issuance of a subsequent certificate,
- c) the issuance of a certificate,
- d) the request for revocation of a certificate,
- e) the revocation of a certificate,
- f) the issuance of a certificate revocation list.

(4) An accredited certification authority's certification code contains a classification of processed information, the manner of its protection and the rules for making this information accessible to another subject.

(5) An accredited certification authority's certification code lays down for each type of certificate and time stamp issued by it the particulars necessary for the issuance of a certificate

---

<sup>1</sup> Decree of the National Security Authority No 537/2002 Coll. on the format and manner of generating a qualified electronic signature, the manner of publishing the Authority's public key, the verification procedure and verification conditions of a qualified electronic signature, time stamp format and the manner of its generation, requirements for the time source and requirements for holding documentation on time stamps (on the generation and verification of an electronic signature and time stamp).

and time stamp, the scope for which the certificates and time stamps can be used and the accredited certification authority's guarantee for a certificate and time stamp of a given type.

(6) An accredited certification authority's certification code provides also for the scope and manner of publishing information relating to the provision of certification services, this being on

- a) contact addresses of the accredited certification authority,
- b) standards and protocols supported for access to the published information,
- c) own certificates with the solution to the manner of their replacement following the expiry of their force,
- d) issued certificates, the format of their publication and updating of the list of issued certificates,
- e) lists of revoked certificates, the format of their publication and updating; it is recommended for a certification authority to ensure publication in at least two ways independent of one another.

(7) An accredited certification authority's certification code provides information on the performance of audit and on the recording of operating events.

(8) An accredited certification authority can have several certification codes for different types of certificates issued.

(9) The structure for an accredited certification authority's certification code is given in Annex 1.

## Article 6

### Model contract on the issuance and use of a certificate

(1) The issuance of a certificate to a certificate requester is done on the basis of a contract on the issuance and use of a certificate.

(2) The content of the contract on the issuance and use of a certificate is a definition of the relationship between the certificate requester and the certification authority in connection with the issuance of the certificate.

(3) A certification authority can have several models prepared of contracts on the issuance and use of a certificate for the various types of certificates issued.

(4) The model contract on the issuance and use of a certificate contains

- a) the procedure for the issuance and take over of the first certificate for the certificate requester,
- b) the procedure for the issuance and take over of a subsequent certificate,
- c) undertakings of the certification authority,
- d) undertakings of the certificate holder,
- e) a possible limitation to the certification authority's liability in the case of a breach of the rules for issuance and work with certificates from the side of the requester,
- f) a confirmation on the issuance of a certificate and its handing over to the certificate requester.

## Article 7

### Price list of certification services provided

The price list of certification services provided contains a list of all certification services which the certification authority provides, together with a statement of the current price of

each service, or information that the certification authority provides a given service free of charge.

## Article 8

### Operating records

- (1) Operating records are records in a written or electronic form arising in certification activity.
- (2) A certification authority records all operating events in the case of
  - a) the submission of a certificate request and the issuance of a certificate,
  - b) the processing and storage of a requester's personal data,
  - c) the issuance of a certificate,
  - d) the issuance of a cross certificate,
  - e) the termination of certificate's validity,
  - f) a request for revocation of a certificate,
  - g) the revocation of a certificate,
  - h) the creation and publication of a certificate revocation list,
  - i) handling the certification authority's the private key,
  - j) time stamping.
- (3) Records on events pursuant to paragraph (2) is created, maintained and processed so that the provability of origin, the accessibility, integrity, time authenticity and confidentiality of these records is maintained.
- (4) A certification authority creates written records on
  - a) the acceptance of a request for the issuance of a certificate,
  - b) the handing over of a certificate to a certificate requester,
  - c) the receipt of a request and instigations for the revocation of a certificate,
  - d) an identification of the persons designated for performing activities relating to the provision of certification services with documentation and guidelines of the certification authority,
  - e) training of the persons stated in point (d) so that their qualification requirements correspond to the activities performed,
  - f) the putting into operation and change of an operating regime certification authority's electronic-signature-creation device, where it is required that this operation is performed and confirmed in writing by at least two natural persons designated for this activity,
  - g) technical interventions connected with the operation and regular control of technical equipment and components of the operated information system.
- (5) A certification authority may, under the conditions defined in its certification code, create records pursuant to paragraph 4(a) to (c) in electronic form.

## Article 9

### Security rules

- (1) The security rules of an accredited certification authority contains
  - a) a security policy,
  - b) a security objective,

- c) a security project,
- d) an emergency plan,
- e) security guidelines.

(2) For the provision of accredited certification services an accredited certification authority realises security measures. The security measures are drafted, documented and used according to the security rules.

(3) Security measures comprise mechanical and technical measures, electronic signature product protection measures and measures for protecting software and hardware elements of the infrastructure in which the electronic signature product is operated.

(4) Mechanical measures are all types of secure storage objects, lockable metal cabinets, locking systems, doors, grilles, security foils, windows and glassing.

(5) Technical measures are

- a) electromechanical locking equipment and systems for entry control into buildings and protected premises and systems serving for the electronic proof of person's authorisation and identification,
- b) alarm system equipment serving for the detection and evaluation of an unauthorised entry into a building or protected premises,
- c) a camera system in the framework of closed circuit television,
- d) electrical fire signalling equipment,
- e) equipment for the physical destruction of information media,
- f) equipment for the constant maintenance of a control record on the activity of the electronic signature device and registration systems of the provided certification services with the possibility of tracking and retrospective review of a record, as well as determining responsibility for activities performed,
- g) other technical means serving to secure an object, protected premises, electronic signature product operations, registration systems of certification services provided and media with back-up and archive copies of these systems' data.

(6) Measures for protecting an electronic signature product are measures fulfilling requirements pursuant to a specific regulation<sup>2</sup>.

(7) The security measures adopted by the accredited certification authority must fulfil the following conditions:

- a) in the case of certification services provided in rented premises, the independent entry of the building's owner to the protected premises must be contractually restricted only to the essential and immediate solution of emergency situations in the building,
- b) besides operating premises, the accredited certification authority must ensure further protected premises for the secure storage of archived documents and data and monthly back-up copies of system data of the certification authority; these premises must be located in a building not physically connected with that in which the certification services are provided,
- c) the provision of certification services must be supported by technical and program means reserved exclusively for this purpose and thoroughly separated from other systems for the ordinary administration activities of the certification authority,
- d) technical and organisational measures must ensure constant operation of the accredited certification authority, even in the case of a failure of the basic technical infrastructure,

---

<sup>2</sup> Decree of the National Security Authority No 539/2002 Coll. laying down details on the requirements for secure-time-stamping device and the requirements for electronic signature products (on electronic signature products).

at least at the level of providing the service of registering requests for the time stamp function,

- e) an own system of ongoing control of the functionality and security of secure devices and measures used must be drawn up and operated,
- f) a system of ongoing documentation of all key activities in the system used and of regular and random evaluation of records thus created must be drawn up and operated,
- g) records of the ongoing documentation of key activities of the system used must be securely stored on media and in a form usable for control over the course of at minimum three years.

(8) Security rules are drawn up by the accredited certification authority itself or with the help of external natural persons or juristic persons. Regardless of the manner of their drawing up, the accredited certification authority also ensures a qualified external critical assessment of the security rules. For this purpose it submits to the Authority

- a) data on the responsible author of the security project and his/her qualification for the field of information security,
- b) the critical assessment of the submitted security project from an independent external specialist for information security professionally authorised to perform an audit pursuant to a specific regulation<sup>3</sup>,
- c) in the case of reservations from the side of the external critical assessor being stated in the critical assessment, the certification authority also submits its own opinion on the critical assessment.

(9) The accredited certification authority in the case of changes to its applicable security rules assesses in a qualified manner their impact on the security of accreditation services provided and immediately informs the Authority of proposed changes and of the assessment of their impact on security.

## Article 10

### Security policy

- (1) A security policy specifies the basic requirements for the protection of sensitive information and the obligations of individual subjects in relation to security.
- (2) The aim of the security policy is to specify aims and to describe the manner of ensuring the certification authority's overall security.

## Article 11

### Security objective

- (1) A security objective determines the requirements for the protection of information gathered, created, processed, transmitted or stored in connection with the provision of certification services.
- (2) The security objective contains
  - a) a definition of the information which it is necessary to protect,
  - b) characteristics and a description of the use of the technical and program means by which the future accredited certification authority is to perform its activity,

---

<sup>3</sup> Decree of the National Security Authority No 540/2002 Coll. on the conditions for providing accredited certification services and on the requirements for audit, the scope of audit and qualification of auditors.

- c) the expected organisational structure of the future accredited certification authority with a statement of the authorisations for each job position,
- d) a description of the premises in which the means stated in point (b) are to be located,
- e) requirements for the overall security of the accredited certification authority, where this comprises personnel security, building security, administrative security and security of the technical and system means.

## Article 12

### Security project

- (1) A security project is a regulation of the accredited certification authority specifying the manner of protecting the performance of certification activities and the protection of the electronic signature product by means of security measures.
- (2) A security project comprises
  - a) a risk analysis of the infrastructure with the aid of which the accredited certification authority performs certification activities, with emphasis on procedures relating to the performance and registration of certification activities and to the electronic signature product,
  - b) a description of security risks relating to the performance of certification activities and the operation of the electronic signature product,
  - c) a description of security measures for limiting the security risks identified,
  - d) a description of the implementation, use and control of security measures.
- (3) A component of the security project is a definition of the manner of personal data protection for certification services pursuant to a specific act<sup>4</sup>.

## Article 13

### Emergency plan

- (1) The content of the emergency plan is a specification of the procedures to be applied in the case of an extraordinary event. An extraordinary event, for the purposes of this Decree, means an event endangering the provision of certification services and which happens in consequence of a failure of the information system for certification services.
- (2) A restoration plan forms a part of the emergency plan. The restoration plan lays down procedures aimed at restoring the proper functionality of the information system for certification services following the occurrence of an extraordinary event.

## Article 14

### Security guidelines

- (1) Security guidelines are regulations of an accredited certification authority which elaborate the provisions of the security objective into procedures and operating procedures binding for all employees of the certification authority.
- (2) The security guidelines governs at least the following security measures:
  - a) the location and use of the certification authority's cryptographic equipment,

---

<sup>4</sup> Act No 428/2002 Coll. on personal data protection.

- b) management of access to the certification authority's cryptographic equipment,
- c) the procedure of backing up data and storing media with back-up copies of data,
- d) procedures in the case of emergencies and faults in the electronic signature product, emergencies and faults in the infrastructure threatening the activity of the electronic signature product, its security, as well as the security of data back-up copies, as well as in the case of emergencies and faults endangering the authenticity and integrity of the certification services provided,
- e) securing the operation of the certification authority's cryptographic equipment in exigent or emergency situations,
- f) principles of work with media,
- g) the creation and assessment of operating records in written or electronic form,
- h) the administration of security means,
- i) the principles of the secure behaviour of users and administrators of the electronic signature product,
- j) detection of security incidents and their solution,
- k) the monitoring and revealing of unauthorised activities in the electronic signature product,
- l) security procedures connected with performing certification activities.

## Article 15

### Rules for the performance of certification activities

- (1) Rules for the performance of certification activities determine the procedure that the accredited certification authority applies in securing the certification services provided.
- (2) Rules for the performance of certification activities of the accredited certification authority contain procedures relating to
  - a) the generation of the certification authority's pair data, and to the way of protecting the certification authority's private key, and to the manner of obtaining the certification authority's certificate,
  - b) the generation of a certificate requester's pair data,
  - c) archiving of certificates,
  - d) security of computer equipment,
  - e) supervision of procedural security, physical security, computer network security, information system security and security of the cryptographic module.
- (3) The rules for the performance of certification activities of the accredited certification authority contain also technical specifications of
  - a) data formats connected with the provision of certification services,
  - b) references to respective regulations,
  - c) standards used in performing certification services.
- (4) The structure of the rules for the performance of certification activities is given in Annex 2.

## Article 16

### Entry into force

This Decree enters into force on 1 October 2002

**Ján Mojžiš** in his own hand

**STRUCTURE OF THE CERTIFICATION CODE  
OF AN ACCREDITED CERTIFICATION AUTHORITY**

**1. INTRODUCTION**

Basic information on the purpose of the document. A component of the certification authority's certification code can be a definition of the scope of the usability of certificates and time stamps.

Introductory provisions contain also contact information on the certification authority, at minimum however the e-mail address, telephone and fax contact.

**2. GENERAL PROVISIONS**

Basic starting points for legislative relations and procedures for the provision of accredited certification services.

2.1 Obligations of all subjects featuring in processes relating to the provision of accredited certification services

- a) the certification authority,
- b) the registration authority,
- c) a certificate's requester or holder,
- d) a party acting on the basis of confidence in the given certificate and/or on the basis of an electronic signature validated by the given certificate (hereinafter referred to as the "certificate user"),
- e) directory administrators.

2.2 Legal guarantees

Description of each subject's responsibility

- a) guarantees and limitations of guarantees provided,
- b) types of losses covered,
- c) limitation of possible losses,
- d) other liability limitations.

2.3 Financial liability

Definition of the certification authority's financial liability and a precise definition of its limitations.

2.4 Arbitration proceedings and dispute settlement

Definition of the manner of interpreting the certification code, for example arbitration proceedings, the manner of dispute settlement, etc.

2.5 Fees

Specification of fees which the certification authority or registration authority charges for services connected with the issuing and administration of certificates.

2.6 Publication of information

Obligations of the certification authority relating to the publication of information, these being

- a) the publication of information on own procedures, own certificates and on the status of these certificates,
- b) the periodicity of information publication,
- c) the requirements for the use by a third party of published information processed by the certification authority.

## 2.7 Conformity audit

Certification authority's declaration in the field of audit performance.

## 2.8 Confidentiality

Obligations of the certification authority relating to the protection of information, these being

- a) types of information which the certification authority protects,
- b) types of information that are not classified as confidential,
- c) who is to be informed of a certificate's revocation,
- d) the policy of providing information required by law,
- e) cases in which confidential information may be published.

## 2.9 Protection of intellectual property rights

Description of property rights to certificates, procedures and keys.

# 3. IDENTIFICATION AND AUTHENTICATION

A description of procedures relating to the authentication of certificate requesters before the actual issuance of the certificate. These procedures can partially be used also in the case of a request for certificate revocation and for issuance of a subsequent certificate.

## 3.1 Initial registration

The basic attributes of identification and authentication processes in registering a subject and issuing a certificate. The basic issues solved in this part include

- a) types of names, rules for interpreting names, requirements for uniqueness and meaningfulness of names,
- b) the manner of settling disputes concerning names,
- c) whether and in what manner a certificate requester must prove ownership of a private key pertaining to a public key in its request for a certificate,
- d) authentication requirements for organisations and their representatives.

## 3.2 Issuance of a subsequent certificate

Processes relating to the issuing of a subsequent certificate following or prior to the expiry of the validity of an existing certificate, providing this certificate was not revoked.

## 3.3 Issuance of a subsequent certificate following revocation of a certificate

Processes relating to the issuance of a subsequent certificate in the case that the existing certificate was revoked.

## 3.4 Request for revocation of a certificate

Processes relating to the processing of requests for identifying a subject in a request for revocation of a certificate.

# 4. OPERATING REQUIREMENTS

A description of processes relating to the issuing of certificates

## 4.1 Request for certificate issuance

Processes relating to the registering of a requester and to the making of a request for certificate issuance.

## 4.2 Certificate issuance

Processes relating to the issuance of a certificate and the informing the requester of its issuance.

## 4.3 Takeover of the certificate

Processes relating to the taking over of a certificate and the subsequent publication of certificates.

## 4.4 Revocation of a certificate

Processes relating to revocation of a certificate, these being

- a) definition of the circumstances under which a certificate can be revoked,
- b) definition of who can request revocation of a certificate,
- c) procedure for making and processing a request for the revocation of a certificate,
- d) time interval for the revocation of a certificate on the basis of a request,
- e) definition of the periodicity of publishing a certificate revocation list,
- f) requirements for certificate users for monitoring the certificate revocation list,
- g) description of the option for ascertaining online the status of a certificate and the requirements on certificate users for using online mechanisms for ascertaining a certificate's status,
- h) other possibilities for gaining information on the revocation of a certificate and requirements for a certificate uses for using other mechanisms for the publication of a certificate's revocation,
- i) any combination of the preceding mechanisms for the case that the reason for a certificate's revocation is the private key having been compromised.

#### 4.5 Security audit

Certification authority's declarations on the recording of operating events.

#### 4.6 Archiving of records

Certification authority's declarations on the archiving of records.

#### 4.7 Change of keys

Processes relating to the publication of a new public key of the certification authority.

#### 4.8 Emergency plan for extraordinary events

Certification authority's declarations on the solution of emergency situations.

#### 4.9 Termination of the certification authority's activity

Information on the manner of terminating the certification authority's activity and publication of a notice on the termination of activity, including archiving of source documentation.

### 5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY MEASURES

Certification authority's declarations on measures for ensuring secure operation.

### 6. TECHNICAL SECURITY MEASURES

Certification authority's declarations on measures for ensuring the secure operation and also a specification of cryptographic means for the generation of the certification authority's keys.

### 7. PROFILES OF CERTIFICATES AND LISTS OF REVOKED CERTIFICATES

Description of the profiles of certificates and profiles of lists of revoked certificates.

#### 7.1 Certificate profile

The format, content and setting of typical values of individual items of certificates issued.

#### 7.2 Profile of the certificate revocation list

The format and content of the certificate revocation list.

### 8. ADMINISTRATION OF SPECIFICATIONS

A description of the manner of processing, updating and publishing the certification code, as well as information on the certification code's validity.

**STRUCTURE OF RULES FOR THE PERFORMANCE  
OF CERTIFICATION ACTIVITIES**

1. INTRODUCTION

Basic information on the purpose of the document. Introductory provisions contain also contact information on the certification authority, at minimum however the e-mail address, telephone and fax contact.

2. GENERAL PROVISIONS

Basic starting points for legislative relations and procedures for the provision of accredited certification services.

2.1 Obligations

Definition of the obligation of all entities featuring in the process relating to certificates and time stamps

- a) the certification authority,
- b) the registration authority,
- c) a certificate's requester or holder,
- d) a certificate user,
- e) directory administrators.

2.2 Legal guarantees

Description of each subject's responsibility

- a) guarantees and limitations of guarantees provided,
- b) types of losses covered,
- c) limitation of possible losses,
- d) other liability limitations.

2.3 Financial liability

Definition of the certification authority's financial liability and a precise definition of its limitations.

2.4 Arbitration proceedings and dispute settlement

Definition of the manner of interpreting the certification code, for example arbitration proceedings, the manner of dispute settlement, etc.

2.5. Fees

Specification of fees which the certification authority or registration authority charges for services connected with the issuing and administration of certificates.

2.6 Publication of information

Obligations of the certification authority relating to the publication of information

- a) the publication of information on own procedures, own certificates and on the status of these certificates,
- b) the periodicity of information publication,
- c) the requirements for the use by a third party of directories administered by the certification authority.

2.7 Conformity audit

Information relating to regular conformity audits, with declared obligations

- a) frequency and periodicity of audit,

- b) identity and qualification of the auditor, as well as its relation to the audited subject,
- c) lists of fields covered in the conformity audit,
- d) list of measures undertaken on the basis of audit results.

#### 2.8 Confidentiality

Obligations of the certification authority relating to the protection of information

- a) types of information which the certification authority protects,
- b) types of information that are not classified as confidential,
- c) who is to be informed of a certificate's revocation,
- d) the policy of providing information required by law,
- e) cases in which confidential information can be published.

#### 2.9 Protection of intellectual property rights

Description of property rights to certificates, procedures and keys.

### 3. IDENTIFICATION AND AUTHENTICATION

A description of procedures relating to the authentication of certificate requesters before the actual issuance of the certificate. These procedures are partially used also in the case of a request for certificate revocation and for issuance of a subsequent certificate.

#### 3.1 Initial registration

The basic attributes of identification and authentication processes in registering a subject and issuing a certificate. The basic issues solved in this part include

- a) types of names, rules for interpreting names, requirements for uniqueness and meaningfulness of names,
- b) the manner of settling disputes concerning names,
- c) whether and in what manner a certificate requester must prove ownership of a private key pertaining to a public key in its request for a certificate,
- d) authentication requirements for organisations and their representatives.

#### 3.2 Issuance of a subsequent certificate

Processes relating to the issuance of a subsequent certificate following or prior to the expiry of the validity of an existing certificate, providing this certificate was not revoked.

#### 3.3 Issuance of a subsequent certificate following revocation of a certificate

Processes relating to the issuance of a subsequent certificate in the case that the existing certificate was revoked.

#### 3.4 Request for revocation of a certificate

Processes relating to the processing of requests for identifying a subject in a request for revocation of a certificate.

### 4. OPERATING REQUIREMENTS

A description of procedures relating to the issuing of certificates

#### 4.1 Request for certificate issuance

Processes relating to the registering of a requester and to the making of a request for certificate issuance.

#### 4.2 Certificate issuance

Processes relating to the issuance of a certificate and informing the requester of its issuance.

#### 4.3 Takeover of a certificate

Processes relating to the taking over of a certificate and the subsequent publication of certificates.

#### 4.4 Revocation of a certificate

Processes relating to revocation of a certificate, these being

- a) definition of the circumstances under which a certificate can be revoked,
- b) definition of who can request the revocation of a certificate,
- c) procedure for making and processing a request for the revocation of a certificate,
- d) time interval for the revocation of a certificate on the basis of a request,
- e) definition of the periodicity of publishing a certificate revocation list,
- f) requirements for certificate users for monitoring the certificate revocation list,
- g) description of options for ascertaining online a certificate's status and the requirements on certificate users for using online mechanisms for ascertaining a certificate's status,
- h) other options for gaining information on the revocation of a certificate and requirements on certificate users for using other mechanisms for the publication of a certificate's revocation,
- i) any combination of the preceding mechanisms for the case that the reason for a certificate's revocation is the private key having been compromised.

#### 4.5 Procedures for security audit

Processes relating to the recording of operating events and the audit system, these being

- a) types of recorded events,
- b) the frequency of processing and frequency of the audit of operating records,
- c) the periodicity for archiving operating records,
- d) protection of operating records, focusing on access rights, protection against modification and deletion,
- e) backing up of operating records,
- f) manner of informing subjects on the recording of activity.

#### 4.6 Archiving of records

Processes relating to archiving, focusing on

- a) types of recorded events,
- b) period of maintaining archives,
- c) access rights and protection of archive records against modification and deletion,
- d) backing up of archives,
- e) requirements for time data in records,
- f) procedures for verifying archive information.

#### 4.7 Change of keys

Processes relating to the publication of a new public key of the certification authority

#### 4.8 Emergency plan

Processes relating to managing emergency situations. Each of the following fields are elaborated separately:

- a) procedures for restoring activities in the case that computer resources, software or data of the certification authority are damaged, or there is a suspicion that they are damaged. The procedures describe the manner of restoring a secure environment, determining which certificates are revoked, whether to continue to use the certification authority's private key, how the new public key is issued.
- b) restoration procedures for the case that the certification authority's certificate is revoked. Procedures describe the manner of restoring a secure environment and the manner of issuing the new public key.
- c) restoration procedures for the case that the certification authority's public key is compromised. Procedures describe the manner of restoring a secure environment and the manner of issuing the new public key.

- d) the certification authority's procedures for the operation and restoring operations in the case of a natural disaster and prior to restoring a security environment in the original or replacement operating premises.

#### 4.9 Termination of the certification authority's activity

Processes relating to the termination of the certification authority's activity and publication of an announcement on the termination of activity, including archiving of source documentation.

### 5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY MEASURES

Description of the certification authority's security measures for ensuring secure operation and activity. In the framework of the measures described, attention is focused separately on the certification authority, directory services, the registration authority, as well as users.

#### 5.1 Measures for physical security

A description of physical security measures relating to the certification authority's operating premises. The fields described include

- a) the location and construction of the operating premises,
- b) physical access,
- c) power supply and air conditioning,
- d) water distribution and sewerage facilities,
- e) fire prevention measures,
- f) maintenance of media,
- g) waste management,
- h) back-up operating premises.

#### 5.2 Procedural measures

Description of roles critical for security and their responsibilities relating to securing the operation. The number of persons required for fulfilling each task. Requirements for identification and authentication of defined roles can also be formulated in this part.

#### 5.3 Personnel security measures

Definition of the requirements for

- a) procedures for screening persons connected with fulfilling roles critical to security, as well as other staff of the certification authority,
- b) training requirements and procedures for performing staff training,
- c) requirements for the interval of staff retraining,
- d) requirements for the frequency and rotation of staff in the framework of roles in the operation,
- e) sanctions for unauthorised activity, unauthorised use of assigned rights and access to systems,
- f) security requirements for contractually ensured activities,
- g) documentation provided by individual staff members.

### 6. TECHNICAL SECURITY MEASURES

Description of the certification authority's technical security measures for the protection of cryptographic keys and activation data such as passwords, PINs, keys, etc. This part can also define requirements for directory services and other subjects, such as registration authorities connected with the protection of cryptographic keys and critical security parameters. The description of technical security measures used for the secure generation of key pairs, user authentication, certificate issuance, certificate revocation, audit and archiving.

## 6.1 Generation and installation of keys

The generation and installation of the key pair must be described for the certificate issuer, registration authorities, directory services, certificate holders and users. The following fields are elaborated:

- a) who generates the key pair of the private and public key for a given subject,
- b) in what way is the private key securely provided to a given subject,
- c) in what way is the subject's public key securely provided to the certificate issuer,
- d) if the subject is a certification authority, in what way is its public key securely provided to users,
- e) what is the length of the key,
- f) who generates the public key's parameters,
- g) how is the quality of the parameters controlled in the process of generating keys,
- h) how are the keys generated by the software or hardware,
- i) for what use is the key generated, or respectively to what purposes is its use restricted.

## 6.2 Protection of the private key

All subjects must analyse requirements for protecting the private key

- a) what standards are required for the key generation module, e.g. FIPS 140-2,
- b) if the key is under the control of N persons out of a total number of M persons, it is necessary to set parameters; the case of dual control is a special case of this principle, where  $N = 2$ ,  $M = 2$ ,
- c) if there is a possibility of reconstructing the public key, to determine who is the reconstructor, in what form the respective key is reconstructed and what are the security measures in such a system; reconstruction of a public key should be understood as the key escrow method,
- d) if the private key is backed up, to determine who performs the backing up, in what manner the backing up is done and how the back-up is protected,
- e) if the private key is archived, to determine who performs the archiving, in what manner the archiving is done and how the archived key is protected
- f) who deposits the private key in the cryptographic module, in what way is the key deposited, and in what way the private key is kept in the cryptographic module,
- g) who can activate and use the private key, in what way is the activation performed, e.g. user log-in, PIN number, token, automatically. In the case of a key's activation, how long is the key activated – once, for a certain time, unlimited,
- h) who and in what way can deactivate a private key,
- i) who and in what way can destroy a private key

## 6.3 Pair data management

Description of further aspects of pair data management for all subjects

- a) whether the public key is archived, if yes, who performs the archiving and what are the security measures,
- b) what are the time intervals of use for private and public keys.

## 6.4 Activation data

Description of security measures for the protection of activation data for the whole life-cycle of the activation data from their generation through their use, archiving and destruction. For activation data it is necessary to solve analogous problems as in the case of key protection.

## 6.5 Computer security measures

Description of computer security measures, e.g. use of secure systems, access management, audit, testing security and penetration testing. There can also be

described the manner of obtaining products, an assessment of the computer system's security, e.g. on the basis of the international standard ISO IEC 15408, requirements for assessing and testing products, their certification and accreditation.

#### 6.6 Security measures for development and management of security

Description of security measures for development, e.g. security of the development environment, security of the development team, security of the system of managing configurations and maintenance, development procedures, modularity, utilisation of a proposal ensuring resistance against failures and errors.

Security management measures can describe tests performed, aimed at ascertaining the accordance of systems and networks with defined standards. These resources can be aimed at controlling the integrity of security software, firmware and hardware in order to ensure their correct and controlled operation.

#### 6.7 Network security measures

Measures for protecting the network infrastructure, including the use of firewalls.

#### 6.8 Measures for cryptographic modules

Measures for protecting the design and use of cryptographic modules, definition of the interface and the module's environment, inputs/outputs, roles and services, status diagram, physical and software security, accordance with the approved algorithms, electromagnetic compatibility and internal tests. Requirements can be defined by a reference to the standard used, e.g. FIPS 140-2.

### 7. PROFILES OF CERTIFICATES AND LISTS OF REVOKED CERTIFICATES

Description of the profiles of certificates and lists of revoked certificates.

#### 7.1 Certificate profile

The format, content and setting of typical values of individual items of certificates issued.

#### 7.2 Profile of the certificate revocation list

The format and content of the certificate revocation list.

### 8. ADMINISTRATION OF SPECIFICATIONS

The manner of administering and updating the certification code and rules for performing administration activities.

#### 8.1 Change procedures

Procedures for the realisation of changes in the case of the need to update or change the certification code. It contains

- a) a list of the specifications' components that can be changed without notification and without changes to the identifier of the certification code,
- b) a list of the specification's components that can be changed following the elapsing of a notification period specification without changes to the identifier of the certification code. Procedures for notifying changes are described also with the inclusion of dates for the commenting on and incorporation of comments, mechanisms for the final incorporation of changes prior to their implementation.
- c) a list of the specification's components the changing of which requires a change to the certification code's identifier.

#### 8.2. Procedures for publication and notification

- a) a list of documents, information and procedures that exist, but are not published,
- b) mechanisms for distributing the certification code, including the management of access in this distribution.

#### 8.3 Procedures for approval

The manner of determining the conformity of any specific certification code with the general certification code.