

DECREE
133
of the National Security Authority

dated from 26 March 2009

**on the content and extent of operational documentation kept by the certification authority
and on the security rules for the execution of certification activities**

In accordance with Art. 14 Para. 1 Letter j) of Act No. 215/2002 Coll. on the electronic signature and on the amendment and supplementation of particular acts (hereinafter referred to as 'the Act'), the National Security Authority (hereinafter referred to as 'the Authority') establishes:

Art. 1

Subject of the regulation

This decree regulates:

- a) the content and extent of the certification authority's operational documentation,
- b) security rules and Certification Practice Statement of the accredited certification authority.

Art. 2

Definitions

For the purposes of this decree,

- a) paired data denotes a pair consisting of the public key and private key corresponding to the given public key,
- b) a security measure denotes a technical, personnel or administrative element of protection, the purpose of which is to maintain secure and reliable execution of certification activities,
- c) the type of certificate and time stamp denote a group of attributes characterising the issued certificate and time stamp with regard to price and recommended use; the certification authority may issue certificates and time stamps of various types.

Art. 3

Documentation of the certification authority

(1) The certification authority shall process, keep and update documentation on the execution of certification activities.

(2) The certification authority's documentation contains:

- a) operational documentation,
- b) security rules,
- c) Certification Practice Statement.

Art. 4

Operational documentation of the certification authority

The operational documentation of the certification authority contains:

- a) the certificate policy,
- b) template contracts on the issue and use of the certificate,
- c) the price list of certification services provided,
- d) operational records,
- e) other records which the certification authority deems expedient.

Art. 5

Certificate policy

(1) The certificate policy contains:

- a) information stating for whom and under which conditions the certification authority provides its services,
- b) restrictions in the provision of his services, if such restrictions exist,
- c) the types of certificates and time stamps which the certification authority issues,
- d) the signature policies and time stamp policies,¹⁾
- e) the rights and obligations of those using the certification authority's services,
- f) a template of the application for the provision of certification service,
- g) rules of use and certificate revocation.

(2) In addition to information specified in Section 1, the certificate policy may also contain further information, the publication of which the certification authority deems expedient.

(3) The certificate policy of the accredited certification authority describes the tasks of individual persons and the processes relating to certificate administration, as well as the:

- a) primary registration of the application for issuing the certificate,
- b) application for issuing the subsequent certificate,
- c) issuing of the certificate,
- d) application for certificate revocation,
- e) revocation of the certificate,
- f) issuing of the certificate revocation list.

(4) The accredited certification authority's certificate policy contains the classification of processed information, the method of its protection and rules for the provision of said information to other persons.

(5) For each certificate and time stamp type it issues, the accredited certification authority's certificate policy establishes the information necessary to issue the certificate and time stamp, the

¹⁾ National Security Authority Decree No. 135/2009 Coll. on the format and method of creating the qualified electronic signature, the method of publishing the Authority's public key, the conditions of validity for the qualified electronic signature, procedure during the verification and verification conditions of the qualified electronic signature, format of the time stamp and method of creating it, requirements on the source of time data and requirements for keeping time stamp documentation (on the creation and verification of the electronic signature and time stamp).

range of applicability of the certificates and time stamps and the accredited certification authority's guaranty for the certificate and time stamp of the given type.

(6) The accredited certification authority's certificate policy also establishes the extent and method of publishing information relating to the provision of certification services, comprising:

- a) the accredited certification authority's contract address,
- b) the supported standards and protocols for access to the published information,
- c) its own certificates with solution of the method of replacing them once their validity expires,
- d) issued certificates, their publication format and an updated index of issued certificates,
- e) certificate revocation lists, their publication format and updating; the accredited certification authority is recommended to ensure the publishing by means of at least two methods which are independent of one another.

(7) The accredited certification authority's certificate policy provides information on the execution of the audit and recording of the operational events.

(8) The accredited certification authority may have several certificate policies for the varying types of certificates issued.

(9) The structure of the accredited certification authority's certificate policy is specified in Appendix No. 1.

Art. 6

Template contract on the issue and use of the certificate

(1) The certificate is issued to the applicant for the certificate on the basis of a contract on the issue and use of the certificate.

(2) The content of the contract on the issue and use of the certificate defines the relationship between the applicant for the certificate and the certification authority in relation to the certificate issued.

(3) The accredited certification authority may have several template contracts on the issue and use of the certificate prepared for the varying types of certificates issued.

(4) The template contract on the issue and use of the certificate contains:

- a) the procedure for issuing and transferring the initial certificate to the applicant for the certificate,
- b) the procedure for issuing and transferring the subsequent certificate,
- c) the obligations of the certification authority,
- d) the obligations of the certificate holder,
- e) possible limitations of the certification authority's responsibility in the event that the applicant violates the rules for the presentation and work with the certificates,
- f) confirmation of certificate issuance and its transfer to the applicant for the certificate.

Art. 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 the specification of the current price of each service or information stating that the certification authority is providing the given service free of charge.

Art. 8

Operational records

(1) Operational records are records in written or electronic form which are created during the certification activity.

(2) The certification authority shall record all operational events during the:

- a) filing of the application for the certificate and issuing of the certificate,
- b) processing and storage of the applicant's personal data,
- c) issuing of the certificate,
- d) issuing of the cross-certificate,
- e) expiration of the certificate's validity,
- f) requirements for certificate revocation,
- g) revocation of the certificate,
- h) creation and publishing of the certificate revocation list,
- i) manipulation of the certification authority's private key,
- j) issuing of the time stamp.

(3) The records of events pursuant to Section 2 are created, stored and processed in such a manner as to preserve the demonstrability of the origin, accessibility, integrity, temporal authenticity and credibility of said records.

(4) The certification authority shall create written records on the:

- a) receipt of the application for the issue of a certificate,
- b) transfer of the certificate to the applicant for a certificate,
- c) receipt of the application and of the instigation of certificate revocation,
- d) familiarity of the persons intended to conduct the activities related to the provision of certification services with the documentation and guidelines of the certification authority,
- e) training of persons specified in Letter d) in such a manner that their qualification prerequisites correspond to the activities performed,
- f) introduction into operation and modification of the operation regime of tools for the creation of the certification authority's electronic signature, in which at least two natural persons suitable for the activity are required to conduct said operation and confirm it in written form,
- g) technical interventions related to the operation and regular control of the technical equipment and components of the operational information system.

(5) The certification authority may create records pursuant to Section 4 Letters a) through to c) in electronic form under the conditions defined in his certificate policy.

Art. 9

Security rules

(1) The accredited certification authority's security rules include the:

- a) security policy,
- b) security objective,
- c) security project,
- d) accident plan,
- e) security guidelines.

(2) The accredited certification authority shall implement security measures for the provision of accredited certification services. The security measures are drafted, documented and applied in accordance with the security rules.

(3) The security measures consist of mechanical and technical measures, of measures for the protection of the electronic signature product and of measures for the protection of the elements of the software and hardware infrastructure in which the electronic signature product operates.

(4) The mechanical measures are all types of safekeeping objects, lockable metal lockers, locking systems, doors, bars, safety foil, windows and glazing.

(5) The technical measures consist of:

- a) electromechanical locking equipment and access control systems to the building and protected areas and systems for the electronic verification of personnel authorisation and identity,
- b) alarm system equipment serving to detect and assess unauthorised entry to the building or protected area,
- c) a camera set within closed television circuit,
- d) electrical fire alarm equipment,
- e) equipment for the physical destruction of data carriers,
- f) equipment for the uninterrupted keeping of a log file on the activity of electronic signature means and systems for recording the certification services provided enabling the tracking and retroactive review of the record, as well as the determination of responsibility for activities performed,
- g) other technical means serving to secure the building, protected area, operation of the electronic signature product, systems for recording the certification services provided and media with backup and archived copies of the data of said systems.

(6) Measures to protect the electronic signature product are measures meeting the requirements of the special regulation.²⁾

(7) Security measures adopted by the accredited certification authority must meet at least the following conditions:

- a) in the case of accredited certification services provided in rented premises, the building

²⁾ National Security Authority Decree No. 134/2009 Coll. stipulating the details on requirements for secure devices for the creation of time stamps and requirements on products for the electronic signature (on electronic signature products).

- owner's capacity to enter the protected areas on his own must be contractually limited exclusively to the essential and spontaneous resolution of accidents in the building,
- b) in addition to operational premises, the accredited certification authority must provide further protected areas for the secure storage of archive documents and data and monthly backup copies of the accredited certification authority's system data; said areas must be located in a building which is not physically connected to the building in which the provision of certification services is conducted,
 - c) the provision of certification services must be supported by technical and programme means reserved exclusively for this purpose and must accordingly be separated from other systems for the certification authority's ordinary administrative work,
 - d) the technical and organisational measures must ensure the uninterrupted operation of the accredited certification authority even in event of the failure of the basic technical infrastructure, at least on the level of the registration service provision requirements for the time stamp function,
 - e) it is necessary to elaborate and operate an own system for the continuous control of the functioning and security of the security means and measures used,
 - f) it is necessary to elaborate and operate a system for the continuous documentation of all of the key activities in the system used as well as of the regular and random assessment of records created in this manner,
 - g) records on the continuous documentation of the key activities of the system used must be securely stored on media and in a form which can be used for control for a period of not less than three years.

(8) The accredited certification authority shall elaborate the security rules itself or with the aid of external natural persons or legal entities. Regardless of the method of elaboration, the accredited certification authority shall ensure qualified external opposition proceedings of the security rules. For this purpose, the following shall be submitted to the Authority:

- a) data on the responsible designer of the security project and his qualifications in the field of information security,
- b) an opposition assessment of the security project submitted from an independent external specialist in information security who is professionally authorised to conduct audits pursuant to the special regulation,³⁾
- c) in the event of objections from the external opponent specified in the opposition assessment, the certification authority shall also submit its own statement on the opposition assessment.

(9) In the event of changes to the applicable security rules, the accredited certification authority shall provide qualified assessment of the effect of said changes on the security of the accreditation services provided and inform the Authority without delay of the proposed changes and the evaluation of their effect on security.

Art. 10 Security policy

³⁾ National Security Authority Decree No. 132 2009/ Coll. on the conditions for the provision of accredited certification services and requirements for an audit, the extent of an audit and the qualification of the auditors is repealed.

(1) The security policy determines the basic requirements for the protection of sensitive information and the obligations of individual persons regarding security.

(2) The goal of the security policy is to determine objects and describe the method of ensuring the certification authority's overall security.

Art.11 **Security objective**

(1) The security objective determines the requirements for the protection of information gathered, created, processed, transmitted or stored in relation to the provision of certification services.

(2) The security objective contains:

- a) the determination of information which is necessary to protect,
- b) the characteristics and description of the use of technical and programme means by means of which the future accredited certification authority will conduct its activity,
- c) the future accredited certification authority's anticipated organisational structure with specification of authorisation for each job title,
- d) a description of the space in which the implements specified in Letter b) are located,
- e) requirements for the accredited certification authority's overall security, which is composed of personnel security, building security, administrative security and security of the technical and system implements.

Art. 12 **Security project**

(1) The security project is a regulation of the accredited certification authority which determines the method of protecting the performance of certification activities and the protection of the electronic signature product by means of security measures.

(2) The security project is comprised of:

- a) a risk analysis of the infrastructure by means of which the accredited certification authority performs certification activities, with emphasis on procedures related to the performance and recording of certification activities and the electronic signature product,
- b) a description of security risks related to the performance of certification activities and operation of the electronic signature product,
- c) a description of security measures for reducing identified security risks,
- d) a description of the implementation, application and control of the security measures.

(3) The determination of the method of protecting personal data for certification services pursuant to the special act⁴⁾ is part of the security project.

Art. 13

⁴⁾ Art. No. 428/2002 Coll. on the protection of personal data as amended by the most recent legislation.

Accident plan

(1) The content of the accident plan is the establishment of procedures which will apply in the event of an extraordinary event. For the purposes of this decree, an extraordinary event is deemed to be an event which jeopardises the provision of certification services and is caused by a failure of the information system for certification services.

(2) A recovery plan is part of the accident plan. The recovery plan establishes procedures intended to restore the proper functioning of the information system for certification services after an extraordinary event has occurred.

Art. 14

Security guidelines

(1) Security guidelines are regulations of the accredited certification authority which elaborate the establishment of the security objective into procedures and work processes which are binding for all employees of the certification authority.

(2) Security guidelines regulate at least the following security measures:

- a) the placement and use of the certification authority's cryptographic equipment,
- b) access control to the certification authority's cryptographic equipment,
- c) the process of data backup and the storage of media with backup data copies,
- d) procedures during accidents and malfunctions of the electronic signature product, accidents and malfunctions of the infrastructure jeopardising the activity of the electronic signature product and its security as well as the security of backup data copies, as well as during accidents and malfunctions jeopardising the authenticity and integrity of the certification services provided,
- e) safeguarding of the operation of the certification authority's cryptographic equipment in emergency or accident situations,
- f) principles of work with the media,
- g) the creation and evaluation of operational records in written or electronic form,
- h) administration of security means,
- i) principles of the secure conduct of users and administrators of the electronic signature document,
- j) detection of security incidents and the rectification thereof,
- k) monitoring and detection of unauthorised activities in the electronic signature product,
- l) security procedures related to the performance of certification activities.

Art. 15

Certification Practice Statement

(1) The Certification Practice Statement determines the procedure which the accredited certification authority applies in providing the certification services.

(2) The Certification Practice Statement of the accredited certification authority contains procedures and processes related to the:

- a) generation of the certification authority's paired data, to the method of protecting the

certification authority's private key and to the method of obtaining the certification authority's certificate,

- b) generation of the paired data of the applicant for the certificate,
- c) archiving of the certificates,
- d) security of the computer equipment,
- e) control of the procedural security, physical security, computer network security, information system security and the security of the cryptographic module.

(3) The Certification Practice Statement of the accredited certification authority also includes technical specifications of:

- a) the data formats relating to the provision of certification activities,
- b) references to the applicable regulations,
- c) the standards used in the execution of certification activities.

(4) The structure of the Certification practice Statement is specified in Appendix No. 2.

Art. 16

Annulling clause

National Security Authority Decree No. 541/2002 Coll. on the content and extent of operational documentation kept by the certification authority and on the security rules for the execution of certification activities is repealed.

Art. 17

Final provision

(1) The legal acts of the European Community and European Union specified in the Appendix No. 3 are overtaken in this Decree.

(2) This Decree has been adopted in accordance with the applicable legal act of the European Community⁵⁾ under notification number 2008/0532/SK.

Art. 18

Legal effect

This Decree shall enter into force on the day of its declaration.

⁵⁾ European Parliament and Council Directive 98/34/EC on a procedure for the provision of information in the field of technical standards and regulations as amended (OJ L 204, 21.7.1998, special edition of the OJ in chap. 3/vol. 20).

**STRUCTURE OF THE CERTIFICATE POLICY OF THE ACCREDITED
CERTIFICATION AUTHORITY**

1. INTRODUCTION

Basic information on the purpose of the document. A determination of the extent of the usability of the certificates and time stamps may be part of the certification authority's certificate policy. The introductory provisions also contain contact information on the certification authority, consisting of at least its e-mail address and telephone and fax number.

2. GENERAL PROVISIONS

The basic points of departure for legislative relations and procedures of the provision of accredited certification services.

2.1. The obligations of all subjects entering into processes related to the provision of accredited certification services include obligations of the:

- a) certification authority,
- b) registration authority,
- c) certificate applicant or holder,
- d) subject operating on the basis of trust in the given certificate and/or on the basis of the electronic signature verified 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 damages covered,
- c) limitation of potential losses,
- d) other limitations of responsibility.

2.3. Financial responsibility

The definition of the certification authority's financial responsibility and the precise definition of its limitations.

2.4. Arbitration procedure and resolution of disputes

Determination of the method of interpreting the certificate policy, such as the arbitration procedure, method of resolution of disputes and similar.

2.5. Fees

The specification of fees which the certification authority or registration authority charges for services related to issuing and administrating the certificates.

2.6. Publication of information

The certification authority's obligations related to information publication, comprising:

- a) publication of information on the certification authority's own processes and procedures, certificates and the status of said certificates,
- b) the periodicity of the publication of information,
- c) requirements on the use of published information administered by a third party of the certification authority.

2.7. Compliance audit

The certification authority's declaration in the field of audit performance.

2.8. Confidentiality

The certification authority's obligations related to information protection

- a) types of information which the certification authority must protect,
- b) types of information which are not classified as confidential,
- c) who will be notified of the revocation of a certificate,
- d) policy of providing information required pursuant to the Act,
- e) cases in which confidential information may be disclosed.

2.9. Protection of intellectual rights

A description of owner rights to the certificates, procedures and keys.

3. IDENTIFICATION AND AUTHENTICATION

A description of the procedures related to the authentication of applicants for a certificate before the certificate is actually issued. These procedures are also partially used for applications for certificate revocation and for issuing the subsequent certificate.

3.1. Initial registration

The basic characteristics of the processes of identification and authentication when registering a subject and issuing a certificate. The basic questions addressed in this section include:

- a) types of names, rules on interpreting names, requirements on the uniqueness and advisability of names,
- b) method of resolving disputes regarding names,
- c) whether and by which means the applicant for a certificate must demonstrate ownership of the private key to the public key in the application for a certificate,
- d) authentication requirements for organisations and representatives thereof.

3.2. Issuing the subsequent certificate

Processes related to issuing the subsequent certificates upon expiration or before the expiration of the existing certificate, if said certificate has not been revoked.

3.3. Issuing the subsequent certificate after certificate revocation

Processes related to issuing the subsequent certificate in the event that the existing certificate has been revoked.

3.4. Application for certificate revocation

Processes related to the processing of requirements for the identification of the subject during application for certificate revocation.

4. OPERATIONAL REQUIREMENTS

Description of procedures related to the issuance of certificates.

4.1. Application for the issuing of a certificate

Processes related to the registration of the applicant and the compilation of the application for the issuing of the certificate.

4.2. Issuing of the certificate

Processes related to the issuing of the certificate and notification of the applicant of the issuing of the certificate.

4.3. Transfer of the certificate

Processes related to the transfer of the certificate and the subsequent publication of the certificates.

4.4. Certificate revocation

Processes related to certificate revocation, comprising:

- a) determination of the circumstances under which a certificate may be revoked,
- b) determination of who may request certificate revocation,
- c) procedure for the compilation and processing of the certificate revocation application,
- d) interval for certificate revocation on the basis of requirement,
- e) establishment of the periodicity of publication of the certificate revocation list ,
- f) requirements on certificate users for monitoring the certificate revocation list ,
- g) description of the possibilities of online detection of certificate status and requirements on certificate users for the use of on-line mechanisms of certificate status detection,
- h) other possibilities of notifying of certificate revocation and requirements on certificate users for the use of other mechanisms for the publication of certificate revocation,
- i) any combination of the preceding mechanisms in the event that the private key is compromised which is the reason for the certificate revocation.

4.5. Security audit

The certification authority's declaration on the recording of operational events.

4.6. Archiving of the records

The certification authority's declaration on archiving records.

4.7. Change of keys

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

4.8. Accident plan for extraordinary events

The certification authority's declaration on the resolution of accidents.

4.9. Termination of the certification authority's activity

Information on the method of terminating the certification authority's activity and the publication of notifications on the termination of activity including document archiving.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY MEASURES

The certification authority's declaration on measures for ensuring secure operation.

6. TECHNICAL SECURITY MEASURES

The certification authority's declaration on measures for ensuring secure operation as well as specification of the cryptographic means of generating the certification authority's keys.

7. PROFILE OF THE CERTIFICATES AND CERTIFICATE REVOCATION LISTS

Description of the profiles of the certificates and certificate revocation lists.

7.1. Profile of the certificate

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

7.2. Profile of the certificate revocation list

Format and content of the certificate revocation list.

8. SPECIFICATION ADMINISTRATION

Description of the method of processing, updating and publishing the certificate policy, as well as information on the validity of the certificate policy.

STRUCTURE OF CERTIFICATE PRACTICE STATEMENT

1. INTRODUCTION

Basic information on the purpose of the document. The introductory provisions also contain contact information on the certification authority, consisting of at least its e-mail address and telephone and fax number.

2. GENERAL PROVISIONS

The basic points of departure for legislative relations and procedures of the provision of accredited certification services.

2.1. Duties

Definition of the obligations of all subjects entering into processes related to certificates and time stamps

- a) certification authority,
- b) registration authority,
- c) certificate applicant or holder,
- d) certificate user,
- e) directory administrators.

2.2. Legal guarantees

Description of each subject's responsibility

- a) guarantees and the limitations of guarantees provided,
- b) types of damages covered,
- c) limitation of potential losses,
- d) other limitations of responsibility.

2.3. Financial responsibility

The definition of the certification authority's financial responsibility and the precise definition of its limitations.

2.4. Arbitration procedure and resolution of disputes

Determination of the method of interpreting the certificate policy, such as the arbitration procedure, method of resolution of disputes and similar.

2.5. Fees

The specification of fees which the certification authority or registration authority charges for services related to issuing and administrating the certificates.

2.6. Publication of information

The certification authority's obligations to publish information

- a) publication of information on the certification authority's own processes and procedures, certificates and the status of said certificates,

- b) the periodicity of the publication of information,
- c) requirements on the use of directories administered by the certification authority by a third party.

2.7. Compliance audit

Information related to regular compliance audits with the declared obligations

- a) frequency and periodicity of the audit,
- b) the auditor's identity and qualifications as well as his relationship with the subject being audited,
- c) a list of the areas covered in the compliance audit,
- d) a list of measures taken on the basis of the audit's findings.

2.8. Confidentiality

The certification authority's obligations related to information protection

- a) types of information which the certification authority must protect,
- b) types of information which are not classified as confidential,
- c) who will be notified of the revocation of a certificate,
- d) policy of providing information required pursuant to the Act,
- e) cases in which confidential information may be disclosed.

2.9. Protection of intellectual rights

A description of owner rights to the certificates, procedures and keys.

3. IDENTIFICATION AND AUTHENTICATION

A description of the procedures related to the authentication of applicants for a certificate before the certificate is actually issued. These procedures are also used for applications for certificate revocation and for issuing the subsequent certificate.

3.1. Initial registration

The basic characteristics of the processes of identification and authentication when registering a subject and issuing a certificate. The basic questions addressed in this section include:

- a) types of names, rules on interpreting names, requirements on the uniqueness and advisability of names,
- b) method of resolving disputes regarding names,
- c) whether and by which means the applicant for a certificate must demonstrate ownership of the private key to the public key in the application for a certificate,
- d) authentication requirements for organisations and representatives thereof.

3.2. Issuance of the subsequent certificate

Processes related to issuing the subsequent certificates upon expiration or before the expiration of the existing certificate, if said certificate has not been revoked.

3.3. Issuance of the subsequent certificate after certificate revocation.

Processes related to issuing the subsequent certificate in the event that the existing certificate has been revoked.

3.4. Application for certificate revocation.

Processes related to the processing of requirements for the identification of the subject during application for certificate revocation.

4. OPERATIONAL REQUIREMENTS

Description of procedures related to the issuance of certificates.

4.1. Application for the issuing of a certificate

Processes related to the registration of the applicant and the compilation of the application for the issuing of the certificate.

4.2. Issuing of the certificate

Processes related to the issuing of the certificate and notification of the applicant of the issuing of the certificate.

4.3. Transfer of the certificate

Processes related to the transfer of the certificate and the subsequent publication of the certificates.

4.4. Certificate revocation

Processes related to certificate revocation, comprising:

- a) determination of the circumstances under which a certificate may be revoked,
- b) determination of who may request certificate revocation,
- c) procedure for the compilation and processing of the certificate revocation application,
- d) interval for certificate revocation on the basis of requirement,
- e) establishment of the periodicity of publication of the certificate revocation list,
- f) requirements on certificate users for monitoring the certificate revocation list,
- g) description of the possibilities of online detection of certificate status and requirements on certificate users for the use of on-line mechanisms of certificate status detection,
- h) other possibilities of notifying of certificate revocation and requirements on certificate users for the use of other mechanisms for the publication of certificate revocation,
- i) any combination of the preceding mechanisms in the event that the private key is compromised which is the reason for the certificate revocation.

4.5. Procedures for the security audit

Processes related to the recording of operational events and system of auditing, comprising

- a) types of recorded events,
- b) frequency of processing and audit of operational records,
- c) period of saving the operational records,
- d) protection of operational records for the purposes of access rights, protection from modification and deletion,
- e) backup of operational records,
- f) method of informing subjects of recording activities.

4.6. Archiving of the records

Processes related to archiving the records, comprising

- a) types of recorded events,
- b) period of saving the archives,

- c) access rights and protection of the archived records from modification and deletion,
- d) backup of the archives,
- e) requirements for time data in the records,
- f) procedures for verifying archived information.

4.7. Change of keys

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

4.8. Accident plan

Processes related to accident management. Each of these areas shall be elaborated separately:

- a) procedures for the recovery of activities in the event that the certification authority's computational sources, programme equipment or data are damaged or suspected of being damaged. Procedures are describing the method of recovering the secure environment, determination of which certificates are revoked, whether the certification authority's private key can still be used if a new public key is published.
- b) recovery procedures for the event that the certification authority's certificate is revoked. Procedures are describing the method of recovering the secure environment and method of publishing a new public key.
- c) recovery procedures for the event that the certification authority's private key is compromised. Procedures are describing the method of recovering the secure environment and method of publishing a new public key.
- d) the certification authority's procedures for the operation and recovery of operation in the event of natural disaster and before restoration of the secure operational environment in the original or backup operational premises.

4.9. Termination of the certification authority's activity

Processes related to the termination of the certification authority's activity and the publication of notifications on the termination of activity including document archiving.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY MEASURES

A description of the certification authority's security measures to ensure secure operation and activity. In the scope of the measures described, separate attention is paid to the certification authority, directory services, registration authority as well as users.

5.1. Physical security measures

A description of the physical security measures related to the certification authority's operational premises. The areas described include:

- a) localisation and construction of the operational premises,
- b) physical access,
- c) electrical supply and ventilation,
- d) water distribution and sewage lines,
- e) fire prevention measures,
- f) media storage,
- g) waste management,
- h) backup operational premises.

5.2. Procedural measures

Description of roles which are critical to security and their responsibilities in ensuring operation. Number of persons required to fulfil each task. Requirements on the identification and authentication of the defined roles may also be formulated in this section.

5.3. Personnel security measures

Definition of requirements for:

- a) procedures for the examination of persons who play roles which are critical to security as well as of other personnel of the certification authority,
- b) requirements for the training and procedures for the performance of employee training,
- c) requirements for employee training intervals,
- d) requirement for the frequency and rotation of employees in the scope of operational roles,
- e) penalties for unauthorised activity, unauthorised use of rights granted and access to the systems,
- f) security requirements for activities performed on a contractual basis,
- g) documentation provided to individual employees.

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, PIN numbers, keys, etc. This section may also define requirements on directory services and further subjects such as registration authorities related to the protection of cryptographic keys and critical security parameters. Description of the technical security measures used for the secure generation of key pairs, user authentication, issuing of certificates, certificate revocation, audits and archiving.

6.1. Generation and installation of keys

The generation and installation of key pairs is necessary to describe for the certificate issuer, registration authorities, directory services, and certificate holders and users. These areas elaborate:

- a) who generates the pair of private and public keys for the given subject,
- b) which method shall be used to securely provide the private key to the given subject,
- c) which method shall be used to securely provide the subject's public key to the certificate issuer,
- d) which method shall be used to securely provide the public key to the user, if the subject is the certificate authority,
- e) what length the keys shall have,
- f) who generates the public key parameters,
- g) how the quality of parameters is controlled in the key generation process,
- h) whether the keys are generated by software or hardware means,
- i) for which use the key is generated and/or to what purposes is the use of the key restricted.

6.2. Protection of the private key

All subjects must analyse the requirements for the protection of the private key

- a) which standards are required for the key generation module, such as FIPS 140-2,
- b) if the private key is under the control of N persons of a total number of M persons, it is necessary to establish parameters; the instance of dual control is a special case of this principle, in which $N = 2$, $M = 2$,
- c) if the private key reconstruction is possible, to determine who shall conduct the

reconstruction, in which form the applicable key is reconstructed and what the security measures are in such a system; the reconstruction of the private key is understood to be the so-called 'key escrow' method.

d) if the private key is backed up, to determine who conducts the backup process, what method is used to conduct the backup process and how the backup key is protected,

e) if the private key is archived, to determine who conducts the archive process, what method is used to conduct the archive process and how the archived key is protected,

f) who feeds the private key into the cryptographic module, what method is used to feed the key and what method is used to save the private key to the cryptographic module,

g) who may activate and use the private key, what method is used to activate it, such as user registration, PIN number, token, automatically, etc. In the event the key is activated, how long the key will remain activated – one time, for a specific period of time, for an unlimited period of time,

h) who may deactivate the private key and by what method,

i) who may destroy the private key and by what method.

6.3. Paired data management

Description of further aspects of paired data management for all subjects

a) whether the public key is archived and if it is, who conducts the archiving and what the security measures shall be,

b) what time intervals are used for the private and public keys.

6.4. Activation data

Description of security measures for the protection of activation data for the entire life cycle of the activation data, from their generation to their use, archiving and destruction. As with key protection, it is necessary to resolve analogous problems for activation data.

6.5. Computer security measures

Description of computer security measures, such as the use of secure systems, access control, auditing, security testing and penetration testing. The method of product acquisition and computer system security evaluation may also be described, for example based on the ISO IEC 15408 international standard, requirements for product evaluation and testing and product certification and accreditation.

6.6. Security measures for security development and administration

Description of security measures for development, such as the security of the development environment, security of the development team, security system for administration of proper configuration and maintenance, developmental procedures, modularity, use of designs ensuring resistance to failures and errors. Measures for security administration may describe performance tests concentrating on ensuring the compliance of systems and networks with the defined standards. Said means may be intended for the control of the integrity of the security software, firmware and hardware in order to ensure their current and controlled operation.

6.7. Network security measures

Measures for the protection of network infrastructures including the use of firewalls.

6.8. Measures for cryptographic modules

Measures for the protection, design and use of cryptographic modules, determination of the boundaries and surroundings of the module, inputs/outputs, roles and services, status diagram, physical and software security, conformity with approved algorithms, electromagnetic compatibility and internal tests. Requirements may also be defined by referring to the standard used, such as FIPS 140-2,

7. PROFILE OF THE CERTIFICATES AND CERTIFICATE REVOCATION LISTS

Description of the profiles of the certificates and certificate revocation list.

7.1. Certificate profile

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

7.2. Certificate revocation list profile

Format and content of the certificate revocation list.

8. SPECIFICATION ADMINISTRATION

Method of administrating and updating the certificate policy and Certificate Practice Statement.

8.1. Change procedures

Procedures for conducting changes if updates or changes to the certificate policy are needed.

Contains:

- a) a list of specification components which may be changed without notification and without changing the identifier of the certificate policy,
- b) a list of specification components which may be changed after the notification interval has elapsed without changing the identifier of the certificate policy. Procedures for the notification of changes are also described including deadlines for comments and processing of the comments, mechanisms for the final processing of the changes before implementing the changes.
- c) a list of specification components the change of which requires changing the identifier of the certificate policy.

8.2. Publication and announcement procedures

- a) a list of documents, information and procedures which exist, but are not published,
- b) mechanisms for the distribution of the certificate policy including the access controls in said distribution.

8.3. Approval procedures

Method of determining the conformity of the relevant specific certificate policy with the general certificate policy.

**LIST OF INCORPORATED LEGISLATION OF THE EUROPEAN COMMUNITY
AND EUROPEAN UNION**

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (special issue of the OJ EU, chap. 13/vol. 24).