MILITARY UNIT 8116
TRENČÍN
N.:ZaSKIS-56/209

Trenčín, 31 march 2014
Only copy.
Number of sheets: 13

Approved by:_____
COL PaedDr. Marián PEŤOVSKÝ, PhD.
Director
SR MoD Security Office

CAMOSR
Time Stamp Policy

Area:	Administrative security PKI / ZEP
Elaborator:	Infromation security and safety Division/SkBTP
Version:	2.8
Retention date:	01. APR. 2014

Information Security Division
Olbrachtova 5, 911 01 TRENČÍN
Phone number: +421 960406300
Fax number: +421 960 406503
E-mail: pki@mil.sk
Web page: http://pki.mil.sk

Trademarks

Name of products mentioned in this document can be registered trademarks of relevant companies.

History of revisions

Version	Date	Revision Description
0.1.	10.10.2005	First draft version - comments
1.0.	26.10.2005	For approval
1.1.	14.11.2005	Approved
2.0.	26.7.2006	Revised
2.1.	17.10.2006	After language correction
2.2.	15.12.2008	Data
2.3.	30.11.2009	Revised; revision of the military unit
2.4.	1.3.2011	Formal revision, change OID
2.5.	19.8.2011	Revised
2.6.	6.7.2012	Change OID CP CAMOSR
2.7.	1.3.2013	Revised
2.8.	25.3.2014	Revised

Contents List

1. List of Figures and Tables 6
2. Introduction 7
3. Terms and abbreviations 8
   3.1. Terms 8
   3.2. Abbreviations 9
4. General Provisions 10
   4.1. Time Stamp Providing Service 10
   4.2. Time Stamp Authority 10
   4.3. Time Stamp User 11
5. Time Stamp Policy 12
   5.1. Review 12
   5.2. Identification 12
   5.3. Users and Validity of the Time Stamp Policy 13
   5.4. Compliance 13
6. Obligations and Responsibility at Providing and Using of Time Stamp Service 14
   6.1. Obligations of Provider of the Time Stamp Service 14
      6.1.1. Generally 14
      6.1.2. Obligations of Provider of the Time Stamp Service Towards Applicant 14
   6.2. Applicant's Obligations 14
   6.3. Obligations of Relying Parties 15
   6.4. Responsibility 15
7. Requirements For Execution of Time Stamp Service (TSA) 16
   7.1. Declaration on Service Execution and on Published Information 16
      7.1.1. Declaration on Service Execution 16
      7.1.2. Published Information 16
   7.2. Management of Keys Service Life 17
      7.2.1. Generating of Keys 17
      7.2.2. Protection of TSAMOSR Protective key 17
      7.2.3. Distribution of TSAMOSR Public Key 17
      7.2.4. Renewal of TSAMOSR Key 18
      7.2.5. Termination of Service Life of TSAMOSR Keys 18
      7.2.6. Management of Life Cycle of Cryptographic Module Being Used for Signing of Time Stamps 18

7.3. Time Stamp Creation 18
7.3.1. Time Stamp 18
7.3.2. Time Stamp Execution and Verification 19
7.3.3. Time Synchronization with UTC 19
7.3.4. Profile of Time Stamp Certificate 20
7.4. TSAMOSR Management and Operation 20
7.4.1. Security Management 20
7.4.2. Assets Classification and Management 21
7.4.3. Personal Security 21
7.4.4. Physical and Spatial Security 21
7.4.5. Operational Management 22
7.4.6. Management of Access to System 22
7.4.7. Installation and Maintenance of Credible Systems 23
7.4.8. Compromising of TSA MOSR Services 23
7.4.9. Termination of TSA MOSR Activities 23
7.4.10. Compliance with Legal Requirements 23
7.4.11. Recording of Data Concerning the Performance of Time Stamp Service 23
7.5. Organizational Aspects 24
8. References 26

1. List of Figures and Tables

Figures

This document doesn’t contain figures.

Tables

Table No. 1: Used extensions (certificate extensions) of CAMOSR Time Stamp Certificate 20

2. Introduction

The Timestamping Service issues a time stamp assigning the date and time to a document in electronic form in strict cryptographic mode.

The time stamp can be used later for authentication of the fact that an electronic document (or electronic signature) existed prior to some concrete time moment mentioned in the time stamp. An electronic document together with a time stamp form a conclusive evidence in the case of any effort to question the existence of an intellectual property being mentioned in the document in given time.

The time stamp policy (hereinafter referred to as “policy”) of the Certification Authority of the Ministry of Defence of the Slovak Republic (hereinafter referred to as “CAMOSR”) is a set of rules stipulating the usability of the time stamp for a defined group of users and application classes with common safety requirements.

The policy strictly determines the participants of the time stamp issuing process, their responsibilities, rights and extent of time stamp use.

The described policy determines the principles of operation and control of the time stamp service for the applicant and relying party; this principles create their appropriate trust to activities of CAMOSR in this field.

The requirements of this policy are focused on time stamp service used for support of qualified electronic signatures or for optional application requiring evidence that an information existed prior to mentioned time; they are based on using of public keys cryptography, certificates and on reliable time source.

3. Terms and abbreviations

3.1. Terms

Time stamp – an information added or in another way logically connected to an electronic document and fulfilling the requirements of paragraph 9 of the Act No. 215/2002 Coll. on Electronic Signature, enabling to prove that an electronic document (or an electronic signature) existed prior to certain concrete time moment mentioned in the time stamp. The time stamp is a data object interconnecting the information representation with concrete time and so creating the evidence that this information (for example an electronic document, electronic signature) existed prior to mentioned concrete time.

Relying party – a recipient (user) of the time stamp relying upon its accuracy.

Reference time – a time providing some reference workplaces.

Time stamp authority – an (Certification) authority providing the time stamps issuing service and being referred to as TSA (Time Stamp Authority). Accordingly to the Act No. 215/2002 Coll. on Electronic Signature it can be made only by the accreditation certification authority using a private key intended for this purpose.

Hash (hash) function – a mathematic transformation assigning to digital documents of various length the numbers with non-zero fixed length specified in advance which enable to verify the integrity of digital document which they were derived from through transformation; they can't be used for re-derivation of a digital document (Edict of the National Security Authority No. 135/2009 Coll.).

Digital stamp (of documents or file) – a number (functional value) calculated from a document or file using hash function.

Applicant – a legal person or natural person applying for execution of time stamp by means of application form sent to time stamp publisher and agreeing with conditions of the provided service.

Application for time stamp execution (or application) – a date structure containing a digital stamp of a document, to which a time stamp should be executed and being created by the applicant by the means of approved hash function.

3.2. Abbreviations

CA – Certification Authority

MOSR – Ministry of Defence of the Slovak Republic

NBÚ – National Security Authority

TSA – Time Stamp Authority

UTC – Coordinated Universal Time

4. General Provisions

4.1. Time Stamp Providing Service

The time stamp providing service provided by the time stamp authority (hereinafter referred to as TSAMOSR) consists of the following two inseparable components:

- Time stamp providing – a component creating the time stamp itself,
- Control of time stamp execution – a component monitoring and controlling the course of time stamp execution in order to ensure that this service is provided accordingly to rules determined by TSAMOSR.

The second component of the service is at the same time responsible for installation and uninstallation of the time stamp providing service.

4.2. Time Stamp Authority

Accordingly to this policy the time stamp authority is:

Address:	**Military Unit 8116 Trenčín**
	Certification Authority MOSR (CAMOSR)
	Olbrachtova 5
	911 01 Trenčín
E-mail:	**pki@mil.sk**
www:	**http://pki.mil.sk**
Working time	
Phone number:	**+421 (0)960 406 400, 406 351-5**
Fax number:	**+421 (0)960 406 420**
Beyond working time	
Phone number:	**+421 (0)960 406 400, 40 22 00 (DRKIS)**
fax:	**+421 (0)960 406 420 (DRKIS)**

All the questions, complaints and claims concerning the providing of time stamp should be sent in written to mentioned address; the certification authority supports the electronic exchange of such information.

CAMOSR takes over all the responsibility for providing of time stamp service in such manner as it is stipulated in section 4.1.

The time stamp is created using a TSAMOSR private key and the time stamp frame contains the identification of TSAMOSR as the time stamp authority.

At providing time stamp services TSAMOSR uses no other party.

TSAMOSR uses an equipment being certified accordingly to FIPS 140-2 standard – level 3 for providing the time stamp.

All the revisions concerning contact data will be published immediately on the web page of CAMOSR.

4.3. Time Stamp User

A time stamp user can be an individual natural person as the final user or a legal person representing several final users.

If the final time stamp user is individual natural person, such person is directly responsible for observance of all determined obligations.

If the user is legal persons representing several final users, such person is responsible for fulfilment of obligations of organization by final users; it is expected that such organization will inform them about this fact.

5. Time Stamp Policy

5.1. Review

The time stamp policy is a set of rules determining the usability of time stamp for defined group of users and/or application class with common safety requirements.

This document determines the policy of TSAMOSR and through this policy also the requirements for TSAMOSR, which issues the time stamps using qualified certificates published by CAMOSR.

5.2. Identification

The time stamp policy of CAMOSR is identified with the following identificator (OID):

Name:	**The time stamp policy of CAMOSR**
Name abbreviation:	**TSA CP CAMOSR**
Version:	**March 2013**
Object identificator being assigned to this document (OID):	**1.3.158.30845572.1.7.1.17**

5.3. Users and Validity of the Time Stamp Policy

The aim of this policy is to meet the requirements concerning the time stamp service for authentic electronic signature in accordance with requirements of the Act No. 215/2002 Coll. on Electronic Signature and their executive edicts (see section 3).

This policy can be used for time stamp service for closed group.

The time stamp service is provided by TSAMOSR for free, in the frame of CAMOSR.

5.4. Compliance

In executed time stamps TSAMOSR uses the time stamp policy identification accordingly to section 5.2; it is able to prove that it fulfils its obligations resulting from section 6.1 and established the inspections accordingly to section 7.

6. Obligations and Responsibility at Providing and Using of Time Stamp Service

6.1. Obligations of Provider of the Time Stamp Service

6.1.1. Generally

TSAMOSR, as provider of the time stamp service, undertakes to perform the following activities:

- to implement all the relevant requirements concerning the activities of the Time Stamp Authority, mentioned in section 7,
- to ensure the compliance of practise of the Time Stamp Authority with procedures determined by this policy and other related documents,
- to provide the time stamp services in accordance with operational guideline of the Time Stamp Authority and other related documents.

6.1.2. Obligations of Provider of the Time Stamp Service Towards Applicant

TSAMOSR fulfils its obligations in compliance with conditions concerning the providing of time stamp in such manner that this service is available for determined users and provided with maximum possible consistency.

6.2. Applicant's Obligations

This document contains no other documents concerning an applicant asking for the time stamp service, except the documents being determined in conditions for providing of this service.

After obtaining of a digital stamp the user is recommended to verify if this time stamp is correctly signed and that the private key used for signing of digital stamp of the document isn't compromised.

An applicant is obliged and entitled to ask for execution of a time stamp only through an interface or software application, which was agreed between him and CAMOSR or interface recommended by CAMOSR.

After receipt of a time stamp and applicant asked for such applicant automatically becomes a relaying party; therefore he underlies to obligations of relaying parties as well.

6.3. Obligations of Relying Parties

If the relying parties want to rely upon the time stamp, they must fulfil the following obligations:

a) to verify that the time stamp is correctly signed and that the private key used for signing the digital stamp of document was not compromised at the signing,
b) to take into account all the limitations concerning the using of time stamp mentioned in time stamp policy,
c) to take into account all the other determined safety precautions.

6.4. Responsibility

Legal responsibility of TSAMOSR is determined by valid legislation of the Slovak Republic.

7. Requirements For Execution of Time Stamp Service (TSA)

The time stamp service provider - TSAMOSR has established system of rendering the services being in compliance with requirement of the Act No. 215/2002 Coll. and its implementing regulations.

7.1. Declaration on Service Execution and on Published Information

7.1.1. Declaration on Service Execution

TSAMOSR ensures necessary reliability at providing the time stamp service through the following measures:

- TSAMOSR has it own elaborated rules for execution of time stamp service and procedure or working procedures used for fulfilment of all requirements determined in this policy,
- TSAMOSR provides the sections of its rules being necessary for execution of time stamp service and other necessary documents to all applicants asking for time stamp service, as well as relying parties,

Note:	TSAMOSR needn't to access all the detailed information about its practise at execution of TSA.

- TSAMOSR publishes the conditions for using of time stamp services accordingly to section 7.1.2 for all the applicants and prospective relying parties,
- TSAMOSR approves all the documents describing the rules for execution of activities connected with the time stamp service by responsible managers of CAMOSR,
- TSAMOSR ensures proper establishment and using of all the procedures and practise of TSAMOSR through CAMOSR management,
- TSAMOSR defines the procedures concerning the examination of practise of TSAMOSR including responsibilities at maintaining the standard of provided services,
- TSAMOSR accesses all the changes concerning the rules for execution of activities related to providing of time stamp services to all touched parties immediately after their approval by responsible employees.

7.1.2. Published Information

TSAMOSR accesses the conditions concerning the providing of time stamp services to all the applicants and relying parties.

The published information contains the following items:

a) contact information,

b) used time stamp policy,
c) used hash function algorithm,
d) the service life of keys used for execution of time stamp,
e) time accuracy in executed time stamp taking into account UTC,
f) any limitations concerning the using of time stamp service,
g) applicant's obligations,
h) obligations of relying parties,
i) information concerning the method of time stamp verification in such manner that a relying party can consider it „adequately reliable" and any limitations of validity,
j) period of keeping the TSAMOSR records,
k) relevant legal regulations,
l) limitations of responsibility,
m) procedures concerning the filing of complaints and settling of disputes,
n) if TSAMOSR was judged in the view of its time stamp policy.

This information is continuously available by means of CAMOSR web page.

You can download them from CAMOSR web pages in electronic form.

This document is considered to be their basic source.

7.2. Management of Keys Service Life

7.2.1. Generating of Keys

TSAMOSR ensures that all the cryptographic keys used during the execution of time stamp service are generated under regulated circumstances in safe equipment and in physically safe environment (see section 7.4.4) by reliable and qualified persons (see section 7.4.3) in the presence and under control of determined number of persons.

7.2.2. Protection of TSAMOSR Protective key

TSAMOSR ensures that its private key will remain secret and its integrity will be kept.

A TSAMOSR private signature key is generated, kept and used in cryptographic module meeting the requirements stipulated in FIPS 140-2 standard - level 3 and is certified in NBÚ SR as a product for certification services providers.

7.2.3. Distribution of TSAMOSR Public Key

TSAMOSR will ensure that integrity and reliability of TSA MOSR public verification key will be kept during its distribution to relying parties; that means mainly the following matters:

- Public verification TSAMOSR key is available for relying parties through the public key certificate,
- CAMOSR issued the TSAMOSR certificate as a qualified certificate,
- a certificate is issued by the certification authority, whose certification policy provides the same or higher level of security than this time stamp policy.

7.2.4. Renewal of TSAMOSR Key

The service life of TSAMOSR certificate doesn't exceed the time interval during which the selected algorithm and key length are suitable for given purpose.

7.2.5. Termination of Service Life of TSAMOSR Keys

TSAMOSR guarantees that the private signature TSA key won't be used after the termination of its service life.

7.2.6. Management of Life Cycle of Cryptographic Module Being Used for Signing of Time Stamps

TSAMOSR ensures the security of cryptographic hardware (hardware module for time stamp signing) during its whole service life.

7.3. Time Stamp Creation

7.3.1. Time Stamp

TSAMOSR ensures that the time stamp is issued safely and contains correct time.

It ensures first of all the following activities:

a) the time stamp contains an identificator of time stamp policy,
b) the time stamp has a unique identification number,
c) time value being given to executed time stamp is derived from the value of real time provided through UTC (as a reliable time source),
d) the time being given to executed time stamp is synchronized with UTC value in the frame of accuracy defined in this policy,
e) if some deviation of TSA hours is detected, exceeding this accuracy declared by this policy, TSAMOSR won't issue a time stamp,
f) the time stamp contains a has function value provided by an applicant, applied for data to which the time stamp should be executed,
g) the time stamp is signed with TSAMOSR key being used only for this purpose,
h) certificate of time stamp contains:
    - identification of Slovensk republik,
    - identification of TSA CAMOSR.

7.3.2. Time Stamp Execution and Verification

An applicant will send (through an agreed interface) an application for time stamp execution to TSAMOSR as time stamp publisher. Such application contains a digital stamp of document to which the time stamp should be executed, created by means of approved hash function.

If an application is in approved format and there are no obstacles prohibiting TSAMOSR to execute a time stamp, TSAMOSR will execute a time stamp on submitted digital stamp of document by means of safety equipment for time stamp execution and time source and send it to the applicant in on-line mode.

If an application for time stamp execution haven't approved format or some obstacles prohibiting TSAMOSR to execute a time stamp arose in TSAMOSR (for example some time deviation beyond the declared accuracy was determined), TSAMOSR won't execute the time stamp to submitted digital stamp of the document.

The verification of time stamp validity is performed by relying party based on given time stamp and document, to which such time stamp was executed and time stamp policy concerning such time stamp.

A time stamp is valid under the following circumstances:

- if a guaranteed electronic signature of time stamp is valid,
- a time stamp is in compliance with used time stamp policy.

7.3.3. Time Synchronization with UTC

TSAMOSR ensures that the time it used is synchronized with UTC with declared accuracy 500 milliseconds; it uses first of all the following measures:

a) the calibration of TSAMOSR clock is performed in such manner that an expected time deviation doesn't exceed the declared accuracy,
b) the clock of TSAMOSR equipment is protected from threats that could cause some undetectable interventions to the clock, which could result their deviation from calibration,
c) TSAMOSR ensures that if a time recorded in time stamp doesn't correspond with synchronization with UTC, such fact will be determined and a time stamp won't be issued,
d) TSAMOSR ensures the performance of clock synchronization if the authorized body sent it a notification about the occurrence of correction second.

7.3.4. Profile of Time Stamp Certificate

Table No. 1: Used extensions (certificate extensions) of CAMOSR time stamp certificate

Extension name	Extension value	Criticality
AuthorityInfoAccess	URL=http://pki.mil.sk/camosr2.cer	Not critical
AuthorityKeyIdentifier	KeyID = určí sa výpočtom Certificate Issuer= Directory Address of Certificate Authority CA Certificate SerialNumber= SerialNumber of Certificate Authority CA	Not critical
CertificatePolicies	Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 Policy Identifier= 1.3.158.30845572.1.7.1.17 CPS= http://pki.mil.sk/TSA_CP.pdf Policy Identifier= 1.3.158.30845572.1.7.1.19 CPS= http://pki.mil.sk/ACA2/CP2.pdf	Not critical
crlDistributionPoints	URI: http://pki.mil.sk/ACA2/camosr2.crl URI: http://crl.mil.sk/ACA2/camosr2.crl	Not critical
KeyUsage	Non-Repudiation	Not critical
subjectKeyIdentifier	Will be calculated	Not critical
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	critical
ExtendedKeyUsage	Time Stamping (1.3.6.1.5.5.7.3.8)	critical

7.4. TSAMOSR Management and Operation

7.4.1. Security Management

TSAMOSR ensures applying of management and administrative procedures being suitable and in compliance with the best professional practise in the following manner:

a) TSAMOSR takes the whole responsibility for all the aspects concerning the providing of services related the time stamp and described in this policy,
b) TSAMOSR provides the guidelines on information security through its management being responsible for defining of information security,
c) all the touched employees are acquainted with this policy,
d) an information security infrastructure being necessary for ensuring the security in the frame of TSAMOSR is kept during all the activities of TSAMOSR,
e) any changes that could affect the security level are approved by CAMOSR management,

f) TSAMOSR safety measures and working procedures, system and information assets providing the time stamp services are documented, established and maintained.

7.4.2. Assets Classification and Management

TSAMOSR ensures that its information and other assets are protected on required level; that means first of all the following activity:

a) TSAMOSR has a list of all the assets and their classification in view of requirements for protection being not in compliance with executed risk analysis.

7.4.3. Personal Security

TSAMOSR ensures that the personal work procedures support its credibility.

That means first of all the following facts:

a) TSAMOSR is operated by authorized employees having corresponding knowledge, experiences and necessary qualification for provided services and being suitable for a working position in question,
b) In view of organizational structure TSAMOSR consists of several levels (roles); the term role (level) means a group of persons executing the same activities or activities being related in some aspect. At some especially important activities it is required that many persons performing the role in question are present at their execution (the so-called “k” of “n” principle),
c) Credible levels (roles) and their responsibilities are described in operational guidelines and eventually in other documents and the levels (roles) being necessary for TSAMOSR security are clearly defined,
d) Individual credible roles in the frame of TSAMOSR have their work descriptions defined taking into account the division of obligations and minimum privileges, determination of position sensitiveness in the view of responsibility and access rights level, their previous practise, training level and knowledge level,
e) The employees apply the administrative and management processes and procedures being in compliance with procedures of information security management (see section 7.4.3).

7.4.4. Physical and Spatial Security

TSAMOSR ensures that the physical access to its crucial assets is controlled and possible risk of physical access is minimized.

This includes first of all the following activities:

a) For providing as well as management of time stamp:
   - only authorized persons can physically access the premises connected with time stamp services,
   - Establishment of control preventing possible assets losses, damage or compromising of assets and interruption of trade activities,
   - Establishment of control avoiding the disclosure or abstraction of information or equipment processing or containing information,
b) Implementation of control of access to cryptographic module in order to guarantee the requirements concerning the security of cryptographic module accordingly to sections 7.2.1 and 7.2.2.,
c) All the equipment being used for rendering the time stamp service is operated in an environment, physically protecting this equipment from compromising by means of unauthorized access to systems or data,
d) implementation of regulation of physical and spatial security in order to protect the equipment, system sources by themselves and supporting equipment .

7.4.5. Operational Management

TSAMOSR ensures the security and right work of system components with minimum risk of fault.

This includes first of all the following activities:

a) integrity of TSAMOSR system components is protected from viruses, harmful and unauthorized software,
b) recording of incidents and reactions on incidents are established in such manner that the losses caused with security incidents and failure are minimized,
c) the media used in the frame of credible TSAMOSR system are handled in such manner to avoid their damage, abstraction, unauthorized access and their obsolence.

7.4.6. Management of Access to System

TSAMOSR ensures that the access to system is reserved only for authorized persons.

This includes first of all the following activities:

a) Implementation of security avoiding an unauthorized access through the network,
b) effective administration of users´ access (including the users in credible roles) in order to keep the security of the system,
c) continuous using of monitoring and alarm equipment to enable the detection and registration of unauthorized effort to access TSA systems and react on them in appropriate manner.

7.4.7. Installation and Maintenance of Credible Systems

TSAMOSR uses credible systems and products being protected from modification.

Established procedures or processes recommended by software manufacturer a (for example updating, patche, fixes, etc.) are used to modify used software.

7.4.8. Compromising of TSA MOSR Services

TSAMOSR ensures that in case of event affecting its services, including the compromising of TSA private key or detection of calibration deviation the information in question are available to all the applicants and relying parties.

7.4.9. Termination of TSA MOSR Activities

TSAMOSR ensures the minimization of eventual violation of services provided to applicants and relying parties caused with termination of time stamp service and mainly necessary subsequent support in the form of information required for verification of time stamp validity.

7.4.10. Compliance with Legal Requirements

TSAMOSR ensures the compliance of its activities with legal requirements. The performance of time stamp service follows valid legislation of the Slovak Republic taking into account the Act No. 215/2002 Coll. on Electronic Signature and related edicts (edicts of NBÚ No. 131/2009 Coll., 132/2009 Coll., 133/2009 Coll., 134/2009 Coll., 135/2009 Coll., 136/2009 Coll., 32/2010 Coll.)

At the same time it ensures the following matters:

a) the legal requirements of the legislative of the European Union are met in such way as they are projected into Slovak legislation,
b) TSAMOSR uses relevant technical and organizational measures against unauthorized and illegal processing of personal data and against accidental loss, damage or destruction of personal data applied by CAMOSR,
c) Information provided by applicants asking for TSAMOSR services are protected against publication until such publication is approved by applicant or ordered by court or other competent state body.

7.4.11. Recording of Data Concerning the Performance of Time Stamp Service

TSAMOSR ensures the recording of all the important information concerning the performance of time stamp service and its keeping during determined period mainly in order to provide the evidences for eventual legal proceedings.

This includes first of all the following activities:

a) TSAMOSR documents which concrete cases and data should be recorded,
b) maintenance of confidentiality and integrity of current and archived records concerning the activities of time stamp service,
c) safe and complete archiving of records concerning the activities of time stamp service in compliance with published practise,
d) the records concerning the activities of time stamp service are available if there is some requirement concerning the providing of evidences of correct performance of time stamp service in case of legal acts,
e) recording of exact time of important events concerning the TSAMOSR environment, key management and time synchronization,
f) storage of records concerning the activities of time stamp service during an adequate period after expiration of TSAMOSR key validity in order to provide a legal evidence and as mentioned in declaration concerning the publishing of information (see section 7.1),
g) recording of events in such manner that these records must not be easy cancelled destroyed and their keeping during a required period,
h) any information about an applicant are kept as confidential excepting the cases where the applicant agrees with their publication or excepting the cases listed in section 7.4.10,
i) recording of all the records concerning all the events related to the life cycle of TSAMOSR keys,
j) recording of all the records concerning all the events related to the life cycle of TSAMOSR certificates,
k) recording of all the records concerning all the events related to synchronization of TSAMOSR timer,
l) recording of all the records concerning all the events related to detection of timer synchronization loss.

7.5. Organizational Aspects

TSAMOSR ensures the reliability of its organization; it accentuates the assurance of the following matters:

a) The policy and procedures used by TSAMOSR are not discriminatory,
b) TSAMOSR enables the access to its activities to the applicants performing the activities in the field of its competence and agreeing with observance of their obligations as they are specified in this document,
c) TSAMOSR has a system ensuring the quality management and information security management being suitable also for rendering the services concerning the time stamp,
d) TSAMOSR has adequate means for covering its responsibility resulting from performance of its activities,
e) TSAMOSR is financially stable and has its own sources required for performance of its activities in compliance with this policy,

f) TSAMOSR employs sufficient number of employees having necessary education, training, technical knowledge and experiences concerning the rendering of service connected with time stamp,

g) TSAMOSR has the procedure for solving the complaints and suggestions of applicants or other parties; such solving concerns the rendering of time stamp service or other related services.

8. References

This policy is based on the following documents:

- ETSI TS 102 023 V1.2.2 (2008-10) „Policy requirements for time-stamping authorities“
- RFC 3628, November 2003 „Policy requirements for time-stamping authorities (TSAs)“
- RFC 3161, August 2001 „Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)“
- Act No. 215/2002 Coll. on Electronic Signature and related edicts (edicts of the National Security Authority No. 131/2009 Coll., 132/2009 Coll., 133/2009 Coll., 134/2009 Coll., 135/2009 Coll. and 136/2009 Coll.)