Krajowa Izba Rozliczeniowa S.A.

CERTIFICATION POLICY OF KIR FOR A TIME-STAMPING SERVICE

Version 1.2

Document history

Numer wersji	Status	Data wydania
1.0	Document approved by the Management Board of KIR – previous version effective until 28 February 2010	22 June 2005
1.1	Document approved by the Management Board of KIR – previous version effective until 15 January 2015	1 March 2010
1.2	Document approved by the Management Board of KIR – version effective as from 16 January 2015	15 January 2015

LIST OF CONTENTS

1. INTRODUCTION

Pursuant to the Digital Signature Act, the "Certification Policy of KIR for Qualified Time-Stamping Service", hereinafter referred to as the Policy, shall specify detailed solutions, including technical and organisational, indicating the manner, the scope, and the terms and conditions for time stamps creation and application. An identifier of this Policy is the following: 1.2.616.1.113571.1.3

Krajowa Izba Rozliczeniowa S.A. NIP: 526-030-05-17, registered by the District Court under the registration number of RHB-30600, is a qualified entity to provide certification services within the meaning of the Digital Signature Act of 18 September 2001 (Journal of Laws No. 130, item 1450), entered in the register of qualified entities providing certification services under number 6, pursuant to Decision No. 20/014499/05 of the Minister of Economy, Labour, and Social Policy dated 5 September 2005.

Krajowa Izba Rozliczeniowa provides time-stamping services in accordance with the applicable Polish law and the rules governing qualified entities providing certification services specified in the Digital Signature Act and the secondary regulations that follow from that Act and in this Policy.

Krajowa Izba Rozliczeniowa provides time-stamping services pursuant to registration of Krajowa Izba Rozliczeniowa in the register of qualified entities providing certification services and a certification authority certificate issued by the minister competent for economy or an entity acting on behalf of such minister.

Any correspondence relating to the provision of certification services shall be sent to the office address of KIR:

Krajowa Izba Rozliczeniowa S.A.
ul. Pileckiego 65
02-801 Warszawa, Poland
with an annotation "time-stamping"

tel. +48 801 500 207
e-mail: bok@kir.pl

or to the address of field units of KIR, as well as electronically to the addresses provided at the website of KIR.

2. DEFINITIONS

Timestamping - a service consisting in attaching a time stamp to the electronic data at the moment when such service is performed and an electronic attestation of such created data.

Service recipient - a natural, legal person, or an organisational unit without corporate existence that has concluded an agreement with KIR for the provision of certification services consisting in time-stamping.

Subscriber - a natural, legal person, or an organisational unit without corporate existence that has a certificate, acting on its own behalf or another natural person, legal person, or an organisational unit without corporate existence, authorised to make requests for time stamps pursuant to the Agreement.

Electronic attestation - electronic data that together with other data to which they have been appended or with which are logically connected allow identification of an entity providing certification services and which comply with the following conditions:

a) have been prepared with the use of secure devices for affixing signatures that are subject to exclusive control of an entity that provides certification services and data used for submitting an electronic attestation;

b) any change of attested data shall be recognisable.

Certificate - an electronic certificate with the use of which data used for verification of digital signatures (public key) are assigned to the subscriber.

Qualified Certificate - a certificate that complies with the terms specified in the Digital Signature Act, issued by a qualified entity that provides certification services, complying with the requirements specified in the Digital Signature Act.

Private key - data used for affixing digital signatures or electronic attestations within the meaning of the Digital Signature Act.

Public key - data used for verification of digital signatures or electronic attestations within the meaning of the Digital Signature Act.

CRL - a certificate revocation list.

Digital Signature Act - the Digital Signature Act of 18 September 2001 (Journal of Laws, No. 130, item 1450), as amended.

Personal Data Protection Act - the Personal Data Protection Act of 29 August 1997 (Journal of Laws, No. 101, item 926), as amended.

Agreement - an agreement for the provision of certification services consisting in timestamping, concluded by and between KIR and a services recipient.

Digital signature - electronic data that together with other data to which they have been appended or with which are logically connected are used for identification of a subscriber.

Time stamp - a set of data referred to in Attachment 2 that have been electronically attested.

3. APPLICATION SCOPE OF THE CERTIFICATION POLICY

The Policy shall be applied to the provision of certification services by KIR consisting in timestamping as requested by subscribers indicated by a services recipient pursuant to an agreement.

4. PROVISION OF CERTIFICATION SERVICES

4.1. Certification Services Provision Agreement

Certification services consisting in time stamping are provided pursuant to an agreement.

The agreement may be concluded with a natural person, a legal person, or an organisational unit without corporate existence. After the agreement has been concluded a services recipient shall indicate subscribers to whose requests time stamps shall be issued. Indication of subscribers after agreement conclusion, as well as change of data concerning subscribers do not require an amendment to the agreement and shall be done by notifying such subscribers or data on a relevant form.

4.2. Application Scope of Time Stamps

The timestamping service provided by KIR in accordance with this Policy and the Digital Signature Act and the secondary regulations that follow from it, shall in particular have results of a certain date within the meaning of the Civil Code.

Pursuant to the Digital Signature Act, a digital signature that is time-stamped by a qualified entity that provides certification services has been affixed not later than at the time of provision of such service. Such presumption exists until the date when a certification authority certificate that is used for verification of such stamp has expired. Extension of the existence of such presumption shall require another timestamping of the stamped document.

4.3. Obligations of Krajowa Izba Rozliczeniowa

KIR undertakes to:

- provided certification services consisting in timestamping in accordance with the requirements of the Digital Signature Act and secondary regulations that follow from it;
- apply organisational and operational procedures preventing tampering with time used to provide the timestamping service;
- use for the provision of a timestamping service data that are used for affixing electronic attestations generated for this service only;
- protect its private keys used for issuing time stamps in accordance with this Policy;
- protect personal data of subscribers provided by a services recipient under the agreement, in accordance with the provisions of the Personal Data Protection Act;
- issue time stamps in response to properly verified requests for the issuance of time stamps;
- verify correctness of requests for the issuance of time stamps delivered to KIR

The subscriber and other third parties shall bear the entire risk relating to damage resulting from undertaken actions, despite that a time stamp has been negatively or incompletely verified or invalid, and also in case, when they abandon verification of the status or completeness of the time stamp.

Detailed obligations of KIR may be specified in the agreement.

4.4. Obligations of the Services Recipient

The services recipient undertakes to indicate to KIR subscribers entitled to use the timestamping service in the manner that does not default on interests of such persons.

Detailed obligations of the services recipient may be specified in the agreement.

After receiving the time stamp issued by KIR the services recipient or subscriber shall be obliged to check if:

- an electronic attestation submitted by KIR is correct;
- there are limitations in application of time stamps specified herein.

The services recipient shall be in particular required:

- not to modify the time stamp;
- to use the time stamp in accordance with the provisions of the Policy and for the purposes that are legal and fit;
- to perform obligations imposed under the agreement, this Policy, or other document it is bound by.

4.5. Liability of Krajowa Izba Rozliczeniowa

KIR shall be held liable towards certification services recipients within the meaning of the Digital Signature Act, including subscribers and services recipients, for any damage caused by failure to perform or default performance of its obligations with regard to the provided services, unless failure to perform or default performance of such obligations

has been caused by the circumstances for which KIR is not held liable and which it could not have prevented despite exercising best efforts.

KIR shall be held liable for storing and archiving data relating to the provision of a timestamping service.

KIR shall be held liable for security of infrastructure keys within the meaning of Art. 2.11 of the ordinance of the Council of Ministers on determining the technical and organisational conditions for qualified entities providing certification services, certification policies for qualified certificates issued by such entities and the technical conditions for secure devices used for affixing and verifying the digital signatures used in the process of provision of a timestamping service hereinafter referred to as "infrastructure keys" dated 7 August 2002.

KIR shall not be held liable for damage caused due to:

- reasons not attributable to KIR and, in particular, caused by damages in the telecommunications infrastructure made by persons for whom KIR is not responsible;
- defective teleinformation equipment that is not under control of KIR;
- acceptance of invalid or negatively or incompletely verified time stamps by the subscriber or third persons;
- force majeure;
- improper use or installation of applications or cryptographic equipment used by the subscriber or a third person to support time stamps;
- refusal to executed a service in the event of invalidity or suspension of the subscriber's certificate, defects in the request for the issuance of a timestamp, arrears in payments or other justified cases, including events indicated in the agreement or this Policy;
- discontinuance of the provision of a timestamping service;
- temporary suspension of the timestamping service or its unavailability, e.g. due to a failure or modification of the system used for service provision or the software or hardware that operates with it, or breakdown of Internet connections;
- expiry of the validity of the certificate attestation that is used to verify the time stamp;
- cancellation of the certificate attestation that is used to verify the time stamp.

If a complaint about the time stamp is not lodged within 24 hours, KIR shall not be held liable for damage relating to the occurrence of complaint circumstances that are referred to in Section 4.12.

A more detailed liability of KIR may be specified in the agreement.

4.6. Liability of the Services Recipient

The services recipient shall be held liable for proper compliance with the obligations imposed on it under the agreement, law, this Policy, or other document it is bound by.

4.7. Financial Liability

The total liability under certification services provided by KIR that consist in timestamping may not exceed EUR 1,000,000. The amount of non-recurring compensation due under improper use of the certificate issued by KIR may not exceed EUR 250,000. The said financial liability shall apply to periods of 1 calendar year starting as from the date when KIR is entered into the register of qualified entities providing certification services.

4.8. Fees

Fees for the provision of certification services have been specified in the agreement.

4.9. Audit

Within the scope specified in the Digital Signature Act, KIR shall be subject to audit by the minister competent for economy.

4.10. Compromise of the Private Key of KIR

In the event the private key of KIR that is used for issuing time stamps is compromised, the request for cancelling a certificate attestation shall be forwarded to the minister competent for economy. After the minister has cancelled the certificate attestation, information about it shall be published in the CRL generated by the minister competent for economy or an entity authorised by it.

4.11. Discontinuance of Certification Services Provision with Regard to Timestamping by KIR

Pursuant to the Digital Signature Act, KIR shall have the right to discontinue provision of certification services consisting in timestamping. In such event all subscribers and certification services recipients shall be informed about it with a 90-day notice. Pursuant to the requirements of the Digital Signature Act, all time stamps that have been issued by KIR and related documents shall be delivered to the minister competent for economy or an entity indicated by the minister.

4.12. Complaint Procedure

The subscriber or services recipient shall have the right to make a complaint about a timestamping service, in particular, when:

- the time stamp contains formal errors;
- the time stamp does not contain all data;
- data timestamped are differed from those submitted for stamping in the timestamping request;
- while creating the time stamp a set of data submitted for stamping has not been electronically attested by KIR.

The complaint shall include its justification, in particular, it shall indicate one of the above complaint-related circumstances.
In the event there are justified grounds for making the complaint KIR shall restore the right of using the timestamping service to the services recipient or the subscriber.
The subscriber or the services recipient may lodge a complaint within 12 months as from dispatch of the time stamp to the subscriber or the services recipient.
If the complaint, however, has not been lodged within 24 hours as from the dispatch of the time stamp to the subscriber, KIR shall not be held liable for damage relating to the use of the time stamp, despite occurrence of one of the complaint circumstances.
Any actions undertaken in reliance on the defective time stamp shall be recognised as its acceptance.

5. DESCRIPTION OF THE MANNER OF CREATING AND TRANSMITTING DATA THAT SHALL BE APPENDED WITH ELECTRONIC ATTESTATIONS

5.1. Secure Devices for Affixing Signatures

Secure devices for affixing digital signatures are used to generate time stamps. These devices are used only to provide certification services hereunder. Secure devices for affixing signatures used by KIR have FIPS 140 certificate level 3. Secure devices for affixing signatures that are used by KIR are protected against unauthorised access. Access to devices is provided to authorised persons only. Each attempt at accessing a specific device, irrespective of its outcome, and in particular, actions related to generation of data used for electronic attestation of time stamps or their use are monitored and recorded in the IT system used for the provision of certification services.

Data used for electronic attestation of time stamps are secured with keys. These keys are divided into parts according to a threshold pattern (m, n), where "m" is 2, while "n" is 5. Each of the parts is stored in separate key module held by persons authorised by KIR or in safes. Data for submitting electronic attestations are disclosed in full in a technical component only.

5.2. Infrastructure Keys

Infrastructure keys are used for:

- ensuring integrity of the transmission of data relating to the provision of services (requests for time stamp issuance, information on errors resulting from the process of time stamp issuance);
- ensuring integrity of event logs kept at KIR;
- ensuring integrity of data relating to the provision of archiving services at KIR;
- securing access to the software and devices for affixing signatures used for the provision of certification services consisting in timestamping.

5.3. Timestamping Service

The process of issuing time stamps shall be carried as follows:

- the services recipient and subscribers it has indicated shall be registered in the system;
- the subscriber sends to KIR a request for the time stamp issuance;
- the request is verified on the basis of data submitted in the registration process;
- a time stamp is generated or information about an error in case of negative verification of the request by KIR;
- the prepared time stamp or message about the terror is sent to the subscriber using the same manner that the request for the time stamp issuance has been delivered by the subscriber;
- the subscriber or the services recipient checks the correctness of the time stamp it has received.

5.4. Request for the Time Stamp Issuance

A time stamp shall be issued by KIR in response to a proper request for the issuance of a time stamp. A description of the format of the request to issue a time stamp acceptable by KIR has been specified in Attachment 2 hereto. The request for the time stamp issuance shall contain an abbreviation of the document to which a time stamp is to be issued, and affixed with a digital signature verified with the use of a certificate issued by KIR or a secure digital signature verified with the use of a valid qualified certificate.

A secure digital signature that is affixed on the request for the issuance of a time stamp and data used for submission and verification of a secure digital signature shall be created by the subscriber in accordance with the requirements of the Digital Signature Act and secondary regulations that follow from that Act.

6. VALIDITY PERIOD OF TIME STAMPS

The maximum validity period of a certification authority certificate used for verification of electronic attestations of time stamps issued by the minister competent for economy or an entity indicated by it shall be 5 years starting from the date of certificate issuance.

A time stamp issued by KIR shall be valid until the end of the validity period of a certification authority certificate issued for KIR that is used for verification of a specific electronic attestation of a time stamp. If the period of validity or storing the document for which a time stamp has been issued is longer, the subscriber shall make a request for issuance of another time stamp before the end of the validity period for the certification authority certificate that is referred to above.

7. PRINCIPLES OF IDENTIFICATION AND AUTHENTICATON

This section governs the identification procedures of subscribers who request the issuance of time stamps.

7.1. First Registration

Commencement of provision of certification services by KIR that consist in timestamping shall require conclusion of an agreement with KIR.

Following conclusion of the agreement the services recipient shall deliver to KIR:

- a list of subscribers authorised to obtain time stamps;
- a list of certificates that the subscribers who request issuance of time stamps shall use.

7.2. Subscriber’s Identification

Data received from the services recipient in the registration process shall be used to verify subscribers making requests for the issuance of time stamps.

After receiving the request, its correctness is verified in terms of its compliance with the format of the request to issue a time stamp as specified in Attachment 2 hereto. In the event of discrepancy, the request for time stamp issuance shall be rejected.

After the correctness of the request format has been verified, KIR shall check whether the subscriber requesting the time stamp is authorised to receive the service and whether the digital signature that is affixed on the request for time stamp issuance is valid. Certificates that the services recipient has indicated to KIR in the registration process shall be used to verify the signature. Each of the certificates shall be additionally checked whether it has not been put on a CRL that is relevant for a specific certificate.

The request for time stamp issuance shall also be rejected in case when the limit of time stamps agreed with the services recipient has been exceeded.

In case verification of the time stamp has ended in failure, a message with an error shall be sent to the subscriber.

8. THE MANNER OF CREATING AND MAKING TIME STAMPS AVAILABLE

8.1. Encryption Algorithms

KIR shall issue time stamps to subscribers for requests to issue time stamps generated with the help of an SHA-1 hash function.

8.2. Time Sources

To provide the service of timestamping of electronic documents, KIR uses its own clocks NTS-3000 by Elproma. KIR has two NTS-3000 clocks, with one located in each centre. The clocks used to issue time stamps are synchronised with the Universal Coordinated Time based on a GPS signal that reaches the devices from satellites orbiting the earth. Accuracy of GPS synchronisation stands at +/-500 nanosecond. Each of the clocks has a time input through three independent network interfaces using the network time protocol (NTP) and the simple network time protocol (SNTP). The time accuracy at NTP stands at +/- 10 millisecond. All computer used to provide the time stamping service are automatically synchronised with Elproma NTS-3000 time pattern.

8.3. Time Stamp Issuance

When issuing a time stamp KIR shall append the data included in the time stamp issuance request, the service execution time. Data prepared in such way shall be appended with an electronic attestation, using for that purpose a secure device for affixing digital signatures. The electronic attestation attached by KIR below the time stamp shall be generated with the use of an RSA algorithm and an SHA-1 hash function, whose identifiers and characteristics are specified in Attachment 6 hereto. Data used by KIR for making an electronic attestation have the length of 2048 bits.

8.4. Publication of Information Relating to the Timestamping Service

Information on certification services consisting in timestamping that are provided by KIR, included herein, shall be made available to all interested parties at the web site of KIR at *www.kir.pl* or in the offices of Krajowa Izba Rozliczeniowa.

Certification authority certificates issued for KIR by the minister competent for economy necessary to verify time stamps are made available free of charge to all interested parties at the web site of KIR, at *www.kir.pl*.

9. DESCRIPTION OF THE TIME STAMP STRUCTURE

In response to a proper request for time stamp issuance, KIR shall generate a time stamp using the time source that is referred to in Section 8.2 and information included in the request. The time stamp contains an abbreviated document included in the request and the current time from the moment when such time stamp is generated. In the event of an incorrect request or other obstacles making submission or issuance of a correct time stamp impossible, the subscriber shall receive information about an error.

The syntax of the response and the time stamp complies with a Time Stamp Protocol (TSP) defined in [RFC 3161] and [ETSI TS 101 861] and has the following profile:

```
TimeStampResp  ::= SEQUENCE    {
status                    PKIStatusInfo,
timeStampToken            TimeStampToken       OPTIONAL    }
```

If the status field indicates an error preventing generation of the time stamp, timeStampToken is not present.

```
PKIStatusInfo ::= SEQUENCE {
status              PKIStatus,
statusString        PKIFreeText         OPTIONAL,
failInfo            PKIFailureInfo      OPTIONAL   }

PKIStatus ::= INTEGER {
granted                        (0),
-- when the PKIStatus contains the value zero a TimeStampToken, as
requested, is present.
grantedWithMods                (1),
-- when the PKIStatus contains the value one a TimeStampToken, with
modifications, is present.
rejection                      (2),
waiting                        (3),
revocationWarning              (4),
-- this message contains a warning that a revocation is
-- imminent revocationNotification   (5)
-- notification that a revocation has occurred      }

-- When the TimeStampToken is not present
-- failInfo indicates the reason why the
-- time-stamp request was rejected and
-- may be one of the following values.

PKIFailureInfo ::= BIT STRING {
badAlg                       (0),
-- unrecognized or unsupported Algorithm Identifier
badRequest                   (2),
-- transaction not permitted or supported
badDataFormat                (5),
-- the data submitted has the wrong format
timeNotAvailable       (14),
-- the TSA's time source is not available
unacceptedPolicy       (15),
-- the requested TSA policy is not supported by the TSA.
unacceptedExtension    (16),
-- the requested extension is not supported by the TSA.
addInfoNotAvailable    (17)
-- the additional information requested could not be understood
-- or is not available
systemFailure          (25)
-- the request cannot be handled due to system failure    }

TimeStampToken  ::= ContentInfo
-- contentType is id-signedData   ([CMS])
-- content is SignedData ([CMS])
```

```
SignedData ::= SEQUENCE {
       version CMSVersion,
       digestAlgorithms DigestAlgorithmIdentifiers,
       encapContentInfo EncapsulatedContentInfo,
       certificates [0] IMPLICIT CertificateSet OPTIONAL,
       crls [1] IMPLICIT   CertificateRevocationLists OPTIONAL,
       signerInfos SignerInfos   }
```

In the event whereby the certReq field in the request has the value TRUE, the 'certificates' field shall contain a certificate of the entity providing the service and the certificate of a 'Time Attribute Certificate') attribute.

```
id-ct-TSTInfo   OBJECT IDENTIFIER ::= { iso(1) member-body(2)
   us(840)  rsadsi(113549)  pkcs(1)  pkcs-9(9)  smime(16)  ct(1)  4}

TSTInfo ::= SEQUENCE   {
    version                      INTEGER   { v1(1) },
    policy                       TSAPolicyId,
    messageImprint               MessageImprint,
      -- MUST have the same value as the similar field in
      -- TimeStampReq
    serialNumber                 INTEGER,
      -- Time-Stamping users MUST be ready to accommodate integers
      -- up to 160 bits.
    genTime                      GeneralizedTime,
    accuracy                     Accuracy                 OPTIONAL,
    ordering                     BOOLEAN              DEFAULT FALSE,
    nonce                        INTEGER                  OPTIONAL,
      -- MUST be present if the similar field was present
      -- in TimeStampReq.   In that case it MUST have the same value.
    tsa                          [0] GeneralName          OPTIONAL,
    extensions                   [1] IMPLICIT Extensions  OPTIONAL
```

10. THE MANNER OF MANAGING DOCUMENTS RELATING TO THE PROVISION OF CERTIFICATION SERVICES

The Policy is made available to all interested parties in an electronic form at the web site of KIR at www.kir.pl.

KIR shall store and archive documents and electronic data, directly relating to the provision of certification services consisting in timestamping, in the manner that ensures safety of the stored documents and data. Access to documents and data relating to the provision of a timestamping service shall be provided only to persons authorised by KIR, who have been trained in personal data protection and admitted to their processing.

Documents and electronic data shall be kept in the personal data database of SZAFIR system that has been registered in the register maintained by the Inspector General for Personal Data Protection. Storage shall be carried in accordance with the use of technologies that ensure data integrity in accordance with the requirements provided for under the Personal Data Protection Act.

The following shall be stored and archived for a period of 20 years as from the moment of creation of a specific document and data**:**

- time stamps issued by KIR;
- certification authority certificates issued for KIR that are necessary for verification of correctness of time stamps issued by KIR;
- agreements.

Logs of events relating to the provision of a timestamping service shall be stored and archived for a period of 3 years, as from the moment of data creation.

In the event whereby the provision of the service of timestamping of electronic documents by KIR has been discontinued, all the above-mentioned documents and data shall be delivered to the minister competent for economy or an entity indicated by it. Subscribers and services recipients shall not incur any costs related to the delivery of data that are referred to above.

11. CONFIDENTIALITY OF INFORMATION AND PROTECTION OF PERSONAL DATA

KIR shall guarantee that all information relating to the provision of certification services that concern timestamping of electronic documents, in particular including personal data of services recipients and subscribers that has not been explicitly recognised as not classified shall be subject to protection against its disclosure pursuant to the provisions established in the applicable regulations of law.

The following information held by KIR shall be subject to protection:

- internal procedures relating to the provision of certification services;
- private keys of the infrastructure of KIR used for the provision of certification services;
- archives, entries of the logs on functioning of the teleinformation system used for the provision of certification services;
- data on subscribers relating to the provision of a timestamping service.

Processing of personal data at KIR shall be performed in accordance with the principles specified in the Personal Data Protection Act and its secondary regulations. Each person whose personal data are processed by KIR further to provision of a timestamping service shall be entitled to the rights provided for under such Act, taking into account the provisions of the Digital Signature Act.

12. TECHNICAL AND ORGANISATIONAL PROTECTION

12.1. Physical Protection

Premises where data are processed that are related to the generation of time stamps shall be subject to physical protection pursuant to the requirements of the Digital Signature Act and the Personal Data Protection Act. Applied protective measures shall protect against:

- premises being accessed by unauthorised persons**;**
- consequences of natural disasters and fortuitous events;
- fire;
- infrastructure failure;
- flooding**,** theft**,** burglary, and assault.

Applied measures of physical protection shall, among others, include:

- premises access control system**;**
- fire-protection system;
- class SA3 alarm system.

12.2. Technical Protection

Access to the teleinformation system that is used for the provision of certification services, shall be secured in accordance with the requirements specified in the Digital Signature Act and the secondary regulations that follow from that Act.

12.3. Back-up Centre

In the event of a failure of the primary centre making operations of KIR impossible, operations of the system shall be taken over by a back-up system located in the back-up location. In the event of a breakdown, the backup system shall take over operations relating to the provision of a timestamping service on an ongoing basis.

12.4. Security Relating to Staff

The staff who are involved in the provision of certification services have qualifications required under the Digital Signature Act, and in particular knowledge of the public key infrastructure and personal data processing.

Attachment 1. Identifiers and Requirements for Encryption Algorithms and Hash Functions

No.	Algorithm	Algorithm identifier	Requirements
1.	RSA	{join-iso-ccitt(2) ds.(5) module (1) algorithm(8) encryptionAlgorithm(1) 1}	- minimum length of the key understood as module *p* p*q is 1020 bits; - length of prime numbers p and q, making up the module may not differ by more than 30 bits.
2.	SHA-1	{iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWAlgorithm(2) 26}	

Attachment 2. Format of the Time Stamp Issuance Request

The subscriber who makes a request for time Stamp issuance shall prepare a signed request in accordance with the syntax of a TSP protocol according to [RFC 3161] and [ETSI TS 101 861] while using the following request profile:

Apart from a time stamp request format defined in RFC 3161 a mechanism of signing requests in accordance with CMS (PKCS#7) TimeStampReq shall be applied. Only signed requests shall be accepted (CMS SignedData). The request must contain a single digital signature. The request must contain a subscriber's certificate that submits the request for time stamp generation. The request may not contain other certificates. The request may not contain CRLs. The request size may not exceed the established maximum at 32000B.

```
TimeStampReqToken  ::= ContentInfo
     -- contentType is id-signedData   ([CMS])
     -- content is SignedData ([CMS])
```

SignedData shall contain a digital signature pursuant to CMS (PKCS#7) TimeStampReq.

```
SignedData ::= SEQUENCE {
     version CMSVersion,
     digestAlgorithms DigestAlgorithmIdentifiers,
     encapContentInfo EncapsulatedContentInfo,
     certificates [0] IMPLICIT CertificateSet OPTIONAL,
     crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
     signerInfos SignerInfos   }

TimeStampReq ::= SEQUENCE   {
   version                  INTEGER   { v1(1) },
   messageImprint           MessageImprint,
      -- a hash algorithm OID = SHA-1 hash
   reqPolicy                TSAPolicyId                    OPTIONAL,
   nonce                    INTEGER                        OPTIONAL,
   certReq                  BOOLEAN                        DEFAULT FALSE,
   extensions               [0] IMPLICIT Extensions        OPTIONAL   }

MessageImprint ::= SEQUENCE   {
   hashAlgorithm                  AlgorithmIdentifier,
   hashedMessage                  OCTET STRING   }

– a hash from the file must be created with the use of SHA1 algorithm (hashAlgorithm)

TSAPolicyId ::= OBJECT IDENTIFIER
```

The request may not contain a policy identifier, however, in case it does, it has to be an identifier of the policy of KIR. Requests containing other policy identifier shall be rejected.