Timestamping authority KIBS Momentum Policy

Version 3.0

Date : 17.10.2016

11.45

OID 1.3.6.1.4.1.16305.1.2.3

KIBS AD Skopje

http://www.kibstrust.mk

Table of Contents:

Introduction

The Clearing House KIBS AD Skopje (KIBS) as a **Time Stamping Authority** (TSA), offers its clients time stamping services which are in compliance with the Law for electronic data and electronic signature[1].

This document represents **The policy of the Time Stamping Authority KIBS Momentum** (Policy). It describes the services for time stamps and specifies the obligations of KIBS as a TSA, in relation to those services. This Policy also describes the obligations and requirements of the subscribers and affected parties. Its structure and contents is compatible with the ETSI TS 102 023 V1.2.2 standard[2].

The time stamps issued in accordance with this Policy can be used for long term archiving of electronically signed documents (IETF RFC 3126)[3], transactions and other electronic records.

1. Scope

This document can be used by affected parties and subscribers of KIBS CA, as a basis for maintaining security and reliability of the services, which are outlined in this document. The Policy of TSA KIBS Momentum is based on X.509 certificates, reliable time source and cryptographic algorithms with a private and public key.

2. Publications and obligations in the documents

KIBS Momentum as a TSA issues the Policy. This document is available on the web address: http://www.kibstrust.mk/Repository/repositoryMK.aspx.

The TSA publicly issues the following information:

- The Policy
- The rules for qualified certificates, passed by KIBS CA
- The certificates for the devices for generating time stamps.

A new version of this Policy will be issued when:

- There are significant changes that affect the Policy
- There are changes in the legislation which affect this Policy

The certificates of the devices for generating time stamps are issued in a maximum of 24 hours, after they are generated and before their activation.

The documents which contain information for the TSA, the procedures, the legislations and directives are listed in this Policy, while the other literature is published in the Rulebook of KIBS for issuing qualified certificates.

All changes of the information are done by KIBS authorized personnel.

3. Definitions and abbreviations

3.1. Definitions

Subscriber: An entity seeking service from the TSA

Affected party: An entity which relies on the time stamp generated in accordance with the Policy of the TSA. An affected party is not necessarily a subscriber.

Auditor: A person who audits the TSA.

---

1 The Public Enterprise Official Gazette of the Republic of Macedonia 34/01 ... 98/08

2 ETSI TS 102 023 V1.2.2 Policy requirements for time-stamping authorities

3 IETF RFC 3126, Electronic Signature Formats for long term electronic signatures, September 2001

CRL: A certificate revocation list is a list which is digitally signed by the CA, which contains certificate identifiers revoked before their expiration date.

Hash value: Data with a fixed size (For example 256 bit) which is calculated with a oneway mathematical function – hash algorithm (For example SHA-256) from certain input data. If there are changes in the input data, the hash value changes.

Time stamp: A data object which connects the representation of data with a specific time, expressed in Coordinated Universal Time (UTC), which provides proof that the data has existed in the specified time.

Services by the TSA: A group of operations needed to manage and generate a time stamp.

Device for generating time stamps (DGTS): Hardware and software used for creating time stamps, characterized by an identifier of the device certified from a particular TSA, which has a unique key for signing time stamps.

System for issuing time stamps: A group of all devices for issuing time stamps, with certain administrative and supervised components which are used for securing the service of the TSA.

3.2. Abbreviations

CA:	Certification Authority	**ИС**	**Издавач на сертификати**
CRL:	Certificate Revocation List	**РПС**	**Регистар на поништени сертификати**
OID:	Object Identifier	**ИО**	**Идентификатор на објекти**
TSA:	Time-Stamping Authority	**Издавач**	**Издавач на временски печати**
TSP:	Time-Stamping Policy	**Политика**	**Политика на издавачот на временски печати**
TSS:	Time-Stamping Service	**Услуги на Издавачот**	**Услуги на издавачот на временски печати**
TST:	Time-Stamp Token	**/**	**Временски печат**
TSU:	Time-Stamping Unit	**УГВП**	**Уред за генерирање на временски печат**

4. General Terms

4.1. Services provided by the TSA

The ICT infrastructure of KIBS Momentum for issuing and managing time stamps is consisted of two components:

- Issuing time stamps – Service for generating time stamps
- Managing time stamps – Managing, monitoring and controlling of the process of issuing time stamps. With this service, among other things, a clock is provided which is precily synched with Universally Coordinated Time (UTC).

4.2. Time stamping authority

The institution which is trusted by the users of the services for issuing time stamps (both subscribers and affected parties) is called a time stamping authority. The time stamping authority has an obligation for issuing time stamps through the service defined in Chapter 4.1. The time stamping authority also has an obligation to manage and use one or more Devices for generating time stamps, which are identified as in the description in Chapter 7.3.1.

4.3. Subscribers

A subscriber can be a legal entity or a person.

The obligations of the legal entity are transferred to the users of the services, which are employed by the legal entity. In any case, the legal entity will be held responsible if the obligations from those users are not met and correspondingly, it is expected that the legal entity will inform them regarding this matter.

When the subscriber is a person, he will be directly responsible if his obligations are not fully met.

4.4. General provisions and policies

This policy is part of the Rulebook of KIBS for qualified certificates, which regulate the operation of KIBS Momentum and its associated services.

The TSA issues time stamps to all interested parties without technical limitations. For issuing time stamps a fee is paid, which is defined in the tariff of KIBS AD Skopje, published on the web site http://www.kibstrust.mk.

4.4.1. Goal

This document is published publicly. The distribution of this document is limited in accordance to the Rules of KIBS for qualified certificates, Chapter 9.5 Intellectual property rights.

Personnel and physical security are also described in the Rules of KIBS for qualified certificates.

4.4.2. Level of specificity

This document describes the general rules for issuing and managing time stamps. A detailed description of the system is given in additional documents, which are not public. The documents which are not public, together with the reports, the results of the internal audits and all other documents regarding the equipment being used are only available to authorized personnel and the external auditors of the system of KIBS.

4.4.3. Aproach

This policy is a general document and does not contain technical details of the ICT system, organizational structure, the operating procedures or technical security. This policy also does not define the environment in which the system for issuing time stamps functions. The technical and operating details are part of the Rules of KIBS for qualified certificates and other documents.

5. Policy for issuing time stamps

5.1. Overview

The policy is “a set of rules which show the applicability of the time stamps in a certain environment and/or a class of applications with joint security requirements” (Chapter 3.1 and Chapter 4.4).

The time stamps are issud with an accuracy of 1 second or better.

To check the validity of the time stamps after the expiration date of the certificate of the Authority, the affected parties should take particular measures defined in the Annex of this policy.

The profile of the public key of the certificate, which is used by the Authority is in accordance with the IETF RFC 3161[4] recommendations. The certificates in the devices for generating time stamps of the Authority are issued by DigiCert, Inc., 2600 West Executive Parkway, Suite 500, Lehi, UT 84043, USA. Their specification is described in the documents in the repository of CA DigiCert (https://www.digicert.com/ssl-cps-repository.htm). The profile in the basic fields of the certificate for time stamps is given in the following table:

Field	Value
Version	3
Serial Number	0d 77 17 79 73 2f 19 c9 d2 ab 9e 94 7e 53 da c9
Signature	RSA/SHA-256
DN of the issuer	CN = DigiCert SHA2 Assured ID Timestamping CA OU = www.digicert.com O = DigiCert Inc C = US
Validity	Од 05.10.2016, до 05.11.2021
Subject DN	CN = KIBSTrust Momentum Timestamp Responder 2016 10 05 1 O = Clearing House Klirinski interbankarski sistemi AD SKOPJE C = MK
Public Key	RSA 2048 bits

The TSA KIBS Momentum issues time stamps in accordance to the ETSI TS 101 861[5] recommendations. Every time stamp contains the identifier of the policy, described in Chapter 5.2 of this document.

5.2. Identification of the Time stamping authority

This Policy is identified withing the KIBS documentation with its OID 1.3.6.1.4.1.16305.1.2.3

This OID is derived from the following:

1.3.6.1.4.1.16305	The number of KIBS registered in IANA
1.3.6.1.4.1.16305.1	Branch for objects connected with PKI-X.509
1.3.6.1.4.1.16305.1.2	Branch for rules and policies
1.3.6.1.4.1.16305.1.2.3	Policy of the time stamping authority

The OID refers to the time stamp, which is in accordance with this Policy. That value is included in the "Policy" field of the time stamp. Other important elements also exist (name, version, date of change) which can identify the Policy.

5.3. Area of applicability

This policy is focused on satisfying the needs for issuing time stamps for Long term validity of documents signed with qualified digital certificates, as defined in ETSI 101 733, however it is generally applicable for whatever other need with equivalent requirements.

This policy can be used for closed corporate systems or public services for issuing time stamps, like electronic transactions, archived data or forms.

[4] IETF RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001
[5] ETSI TS 101 861 Time stamping profile V1.4.1, July 2011

5.4. Compliance

The issued time stamps contain an identifier described in Chapter 5.2 of this document. The Authority supports only the requests that have a time stamp from this policy.

The Authority guaranties the fulfillment of the obligations defined in Chapter 6.1 and the implemented controls described in Chapter 7 of this document.

6. Obligations and responsibilities

6.1. Obligations of the Authority

6.1.1. General

The Authority fulfills the requirements and procedures defined in Chapter 7 of this document.

The Authority fulfills all obligations in accordance with his defined conditions for using the services.

The Authority provides technical conditions for issuing time stamps.

The Authority guarantees that the Rules of KIBS for qualified certificates are applied and that the specific requirements in the current Policy are met.

6.1.2. Responsibilities of the Authority towards the subscribers

KIBS guarantees permanent access to the KIBS Momentum service everyday 24/7, except in cases of planned technical interuptions, defined in other documents for maintaining the equipment and infrastructure. The time that is inserted in the time stamps is with an accuracy better of one second in relation to UTC. KIBS guarantees that:

- Its activities and services are legal and do not breach intellectual rights, licensing and other rights
- The issued time stamps do not contain incorrect data or errors
- Издадените времески печати не содржат неточни податоци или грешки

The rest of the information which define KIBS Momentum are described in the Rules of KIBS for qualified certificates.

6.2. Responsibilties of the subscribers

Upon requesting an issuance of a time stamp, the subscriber needs to check the validity of the certificate of the device which is used to get a time stamp, with checking the CRL list of DigiCert (http://crl3.digicert.com/sha2-assured-ts.cr и http://crl4.digicert.com/sha2-assured-ts.crl) and whether the private key of the certificate for issuing time stamps is compromised.

This policy does not require a connection between the hash data, on which a time stamp should be put and the original electronic data from which the hash is derived. The subscriber is responsible for that connection.

6.3. Responsibilities of the affected party

The affected party must check whether:

- The time stamp is correctly signed with a certificate from the device for time stams. For that purpose, the affected party must check whether the time stamps include a reference towards a KIBS device

- During verification, the certificate is not revoked. For that purpose, the affected party must check the public CRL lists published from DigiCert (http://crl3.digicert.com/sha2-assured-ts.cr и http://crl4.digicert.com/sha2-assured-ts.crl)
- The cryptographic hash function which is used in the process of requesting a time stamp is still sufficiently secure
- The size of the key of the certificate of the Authority and the rest of the cryptographic algorithms are still secure

If the verification of the time stamps is done after the expiry of the corresponding certificate of the Authority, the affected parties should follow the recommendations defined in the Annex of this document.

The affected parties should take in consideration the limitations described in the Policy.

6.4. Responsibility

The responsibility of each entity connected with the service for issuing time stamps is specified in a mutual contract. All other responsibilities are described in the Rules of KIBS for qualified certificates.

7. Authority requirements

The Authority implements controls which enable issuing or nonrepudiation of the services defined in the regulation of this policy. Logs are kept for monitoring of the operation of the service for issuing time stamps, as well as monitoring of the activities of the personnel and users in the information system.

It is necessary for every party which is in some way connected with the procedures for time stamps to log their activities. The records for this information should be part of a corresponding log and should be kept in way so that every affected party in the process should have adequate access to it. By doing so, informing of the affected parties will be done in a correct and accurate manner, for resolution of potential disputes or flaws in the security of the ICT systems. Those records should be regularly included in the process of backing up. The procedure for making backing up is an internal procedure of KIBS.

7.1. Rules for work and non-disclosure of information

7.1.1. Rules for work

The Authority guarantees that they have the capacity for providing services for issuing time stamps, as described in the policy.

The Authority concludes risk analysis for assessing the threats to the assets, to determine the appropriate controls and operating procedures.

The Authority establishes procedures for implementing rules for work identified in this Policy.

The Authority publicly publishes the corresponding documents so the users and affected parties can asses the compliance of their activities with the Policy.

The Authority establishes a corresponding organization structure for approval and verification of the Policy.

The people in charge at the Authority are concerned with the correct implementation of the rules for work.

The Authority defines procedures for periodic control, to check the application and compliance of the rules for work with the Policy.

The Authority is managed by the management of the Authority. The management of the Authority adopts the Policy and the documents associated with the services of the Authority, which are provided by the Authority. The management of the Authority is responsible for:

- Specifying and approving the infrastructure and the functioning of the service from the Authority;
- Approving of Policy;
- The promptness of the Policy from a functional, organizational and technical aspect;
- The compliance during implementation of the devices for generating time stamps with the Policy of the Authority;
- Publishing the Policy of the Authority, as well as the corresponding revision of the documents towards the users and affected parties.

7.1.2. Publicly published information defined in the Policy

The Policy of the Authority and the Rules of KIBS for qualified certificates are publicly published documents.

The information for the contact connected to the contents of this document are listed in the Rules of KIBS for qualified certificates, Chapter 1.5.

Every time stamp issued by KIBS Momentum contains a policy identificator, defined in Chapter 5.2 of this document.

The cryptographic Hash functions, used in the process of issuing time stamps are in compliance with the normative references of NIST[6].

The validity of the time stamp is 6 years from the moment of expiration of the corresponding certificate, if the terms described in Chapter 6.3 are met.

The accuracy of the clock in the time stamps is synchronized with UTC, with an accuracy to one second.

The limitations connected with the system of the Authority are defined in Chapter 5.3 of this policy.

The obligations of the subscribers are described in Chapter 6.2, while the obligations of the affected parties are described in Chapter 6.3 of this policy.

The verification of the time stamps should be done according to the instructions for using software connected with the operation of issuing time stamps and the Annex of the policy.

The logs are kept for period defined in the Rules of KIBS for qualified certificates.

This document is regulated in accordance with Macedonian laws and EU regulation. In case of a dispute between the parties, that has risen from interpretating, requesting and/or requesting a mutual agreement, and in the absence of agreement between the parties, the only competent court is the court in Skopje.

The limitations of liability are described in Chapter 6.4.

All suggestions, complaints and objections regarding the functioning of KIBS Momentum should be addressed to the contacts described in Chapter 1.5 of the Rules of KIBS for qualified certificates.

KIBS makes backups of the data and critical functions outside of its primary location, in order to fulfill the obligations for maintaining continuity in case of an incident.

KIBS takes care about exporting the backups outside of its primary location and their protection in terms of confidentiality and integrity.

---

6 National Institute of Standards and Technology, http://www.nist.gov/

7.2. Managing key lifecycle

7.2.1. Key generation

KIBS guarantees that all cryptographic keys are generated in a controlled environment.

The generation of cryptographic keys on the device for generating time stamps is executed by authorized personnel on Hardware Security Modules (HSM), FIPS 140-1 Level 3 certified.

The devices for generating time stamps use RSA private keys with a length of 2048 bits.

7.2.2. Protection of the private key

KIBS guarantees that the private keys of the devices for generating time stamps are kept secret and guarantees their integrity.

The keys are kept in HSM FIPS 140-1 Level 3 certified.

The private keys on the devices for generating time stamps cannot be exported outside of these modules.

KIBS prohibits archiving and backing up the private keys of the devices for generating time stamps.

7.2.3. Public key distribution

The certificates for the time stamps, together with the corresponding public keys are published on the web site http://www.kibstrust.mk.

The request for a certificate from the devices for generating time stamps is sent to the Certificate Authority DigiCert, in accordance with the rules defined in the corresponding Policy of the Certificate Authority.

The certificates obtained from the Certificate Authority are in accordance with the profile defined in the policy for certificates.

The Authority is keeping his obligations defined in the Policy of the Certificate Authority.

During the import of the certificate on the device for generating time stamps, the Authority checks whether it is issued by DigiCert.

7.2.4. New keys for the Authority

KIBS guarantees that the lifecycle of the certificates in the devices for generating time stamps will not be greater than the period in which the cryptographic algorhithms and key length is permitted for corresponding use.

The Authority generates new keys after the expiration of the certificate of the Authority. The keys of the certificates which are expired are kept for a period of 5 years. After this period, they are destroyed. The public keys of the Authority are kept further 20 years, so a verification of the time stamps issued in the past can be made.

7.2.5. Destroying of the private keys

The Authority guarantees that the private keys used for signing the devices for generating time stamps will not be used after their expiration.

KIBS guarantees that the private keys of the device for issuing time stamps are destroyed after the period of their archiving has expired.

The system for issuing time stamps KIBS Momentum will reject any request with keys which are expired.

7.2.6. Managing the Hardware Security Modules (HSM)

The Authority guarantees the security of the cryptographic hardware during its lifecycle.

The HSM devices, intended for the keys for time stamps, are shipped and stored in KIBS, in a strictly controlled environment. KIBS guarantees that the devices are not opended during transport, nor are manipulated while being stored in their premises.

The installation and initialization of these devices is being done by authorized personnel, with a witness in place, in a physically secured environment (Chapter 7.4.4).

In case of device replacement or device transfer because of servicing, the keys are erased and destroyed in accordance to the recommendations of the manufacturer.

KIBS guarantees that the number of active devices, in any time, is sufficient for maintaining reliable service.

7.3. Time stamps

7.3.1. Time stamp specifications

The Authority guarantees that the time stamps are generated securely and contain the exact time.

Every time stamp issued by KIBS Momentum has its own unique identifier and contains the policy identifier.

The time stamps have a date and time record connected to the UTC referent time, while the time that KIBS Momentum uses is provided by the time servers ntp.kibs.mk and time.kibs.mk (satellite time and atomic clock). Time is synchronized with Coordinated Universal Time (UTC) with an accuracy that is defined in this document.

In case of compromise, real or assumed, or miscalibration of the device for generating time stamps, which could affect the generated time stamp, KIBS will take all necessary action so that the devices would not generate new time stamps until business continues as normal.

KIBS issues time stamps in accordane to the document RFC 3161. The time stamp is an electronically signed confirmation from the Authority, for certain data in an exact time and date. With the time stamp it is confirmed that particular data exists in a particular time. For that purpose, the time stamp univocally binds the data (i.e. his hash value together with the identifier of the hash algorithm) with a particular time. The content of the time stamps is signed with a certificate based on a 2048 bit RSA private key, which has its own profile and extensions defined in Chapter 5.1 of this document.

The time stamp is a signed structure which includes:

- A hash value of the data on which time is stamped
- Date and Coordinated Universal Time (UTC)
- The identifier of the Authority KIBS Momentum and a certificate identifier

7.3.2. Clock synchronization with UTC

The system for time synchrozation of the services for time stamps of KIBS Momentum guarantees the subscriber a delivery of a time stamps with an accuracy of less that 1 second in terms of Coordinated Universal Time (UTC) and:

- Time calibration of the devices for generating time stamps is done in a way that time does not differ more than the declared accuracy;
- The time in the devices is protected against threats connected to the environment which can lead to desynchronization in terms of UTC, outside of the declared accuracy;
- KIBS guarantees that the deviations of the internal time of the devices outside of the declared frame will be noted immidetelly. KIBS will make sure the information about the deviations will be available on the web site http://www.kibstrust.mk.
- If on some of the devices for generating time stamps the time is out of the allowed limits, then time stamps will not be generated.

The clocks of the devices for generating time stamps are locally monitored from referent servers for correct time in KIBS. These servers are autonomous and synchronized with UTC time. The mechanisms which are enforced enable the system security from attach whose target is to desynchronize the time source, even from attacks from radio or satellite signals.

KIBS guarantees that synchronization will be done when a leap second appears, noted by a relevant authority. The change for the leap second will be done in the last minute of the day that will happen. The record for that event (withing the declared accuracy) will be done after the change.

7.4. Control and management of the Authority's system

7.4.1. Security controls

The Authority has implemented administrative and operating procedures which reflect the best practices in the corresponding field. All subjects connected to the security controls are described in Chapter 5.2 from the Rules of KIBS for qualified certificates.

7.4.2. Managing and classifying the assets

The Authority has implemented procedures for corresponding information security and working assets.

The Authority keeps an inventory of all assets and has implemented procedures for asset classification in accordance with the internal procedures of KIBS AD Skopje for risk analysis.

7.4.3. Control of personnel

The characteristics of personnel, as well as the confidentiality of the roles they execute are described in Chapter 5.3 of the Rules of KIBS for qualified certificates.

7.4.4. Spatial control and controls of the working conditions

The description of the controls of physical space and working conditions are described in Chapter 5 of the Rules of KIBS for qualified certificates. These security controls correspond with the regulatory requirements of the ISO 27001 standard.

7.4.5. Control of operations

The Authority guarantees that the components of the system for issuing time stamps are secure and that they are managed correctly, with a minimal risk from an outage. KIBS AD Skopje has security procedures which are part of the internal documentation of the company. That documentation is periodically controlled by internal and external auditors.

7.4.6. Access management

The controls for identification and authentication are defined in accordance with the policy for access control and working responsibility.

The services of the Authority are setup on a system protected by firewalls. These devices are configured to accept only the necessary connections.

KIBS always keeps the security procedures to be divided from the standard procedure for operation and they always execute under an employee assigned with a confidential role.

The profiles and access rights to the equipment of the Authority are assigned and documented together with the procedures for sign-in/sign-out of the operators.

Security controls for protection against unauthorized access are adopted to the local components of the information system.

The systems, applications and databases univocally identify and authenticate the operators and administrators. The interaction between the system and the operator is only possible after a successful identification and authentication. For each interaction, the system checks the identity of the operator.

The information about authentication are kept in such a way that only authorized users have access to them.

The person which is not an authorized user cannot give or revoke access rights to subjects. Only authorized users can create new users and disable or exclude current users.

The Authority keeps a log of records which contains records connected to the following events:

- Generating time stamps;
- Administering the system for issuing time stamps;
- Synchronizing and keeping the exact time;

Each record in the log contains a date and time of the event.

The reliability of the records log is secured through corresponding physical measures, as well as through system defined and network access controls.

The physical access to the components of the information system is defined in Chapter 5.1.2 from the Rules of KIBS for qualified certificates.

7.4.7. Managing and maintaining of the reliable systems

The services of the Authority are setup on reliable components which are protected from external modifications. More precisely, the devices for generating time stamps comply with the regulatory requirements.

Risk analysis is done on the services of the Authority to identify the possible threats for the devices for generating time stamps. The set controls are in accordance with the strategy of KIBS for risk management of information systems.

The infrastructure for development and testing is separated from the production infrastructure of the services of the Authority.

The criteria for accepting and checking new systems, updates and new versions are documented and before acceptance and putting in production, tests are being executed.

7.4.8. Compromising the Authority's services

In case of events which influence the security of the services of the Authority and which could influence the generated time stamps, KIBS guarantees that a corresponding information will be available to the subscribers and affected parties.

The compromise of the Authority can be from:

- Compromising the private keys of the devices for generating time stamps
- Compromising the private key of the Certificate Authority which is used for generating the certificates for the devices for generating time stamps
- Operational problem

The potential compromise of the services of the Authority is taken into consideration in the Plan for disaster recovery of KIBS.

The plan for disaster recovery describes the real od assumed compromises of the private key for signing on the device for generating the time stamps, or losing the time calibration on the device for generating time stamps, which can affect the issued time stamps.

KIBS guarantees that all necessary measures are taken to evade operational incidents.

KIBS continuously updates the Plan for disaster recovery in order to secure the best possible protection from the following threats:

- Compromising of the private key;
- Network outage;
- Unavailabe qualified personnel;
- Problems with time calibration;
- Hardware component outages;

Generally, the incidents involving the services of the authority will be concluded according to the procedure for reporting and handling with security incidents which is in power in KIBS.

In case of a compromise, real or assumed, or losing the calibration of the device for generating time stamps, which can influence the generated time stamp, KIBS will secure a corresponding information available to the subscribers and affected parties.

In case of an operational compromise of KIBS or losing calibration, which could affect the issued time stamps, KIBS will secure information for its subscribers and affected parties which can be used to identify possibly affected time stamps, except in situations where this compromises the security of the services of the Time Stamping Authrority.

7.4.9. End of operation of the Authority

The procedures for managing the end of operations are defined by KIBS. Through these procedures, KIBS ensures that in case of service termination of the Authority, the potential distortions for the subscribers and affected parties will be minimal. More precisely, KIBS guarantees that they will secure every information to verify the accuracy of the time stamps, even after the termination of services by the Authority.

Before service termination of the Authority, the following activities will be concluded:

- KIBS will notify all of its subscribers and affected parties for the expected termination, by publishing this information on its web page
- KIBS will revoke all authorizations of its partners which can act on their behalf for any function connected to the issuing of the time stamps

- KIBS will transfer its tasks to a corresponding authority, with a goal to keep the logs of events and audit archives which are needed to confirm the valid operation of the Authority, in a reasonable time frame.
- KIBS will maintain the obligation to enable access to the public keys and certificates towards the affected parties for a reasonable time frame
- The private keys of the device for generating time stamps will be irretrievably destroyed, in accordance to the procedure described in Chapter 7.2.5

KIBS will take over all necessary measures to cover the expenses for fullfiling the minimum for the demands in case of bankruptcy or because of other reasons, they are not in a condition to independently cover the expenses.

The provisions for terminating the services include:

- Notifying the subscribers and other affected parties
- Transfer of the obligations of KIBS to other authorities

The Authorite will revoke all certificates on the devices for generating time stamps.

7.4.10. Legal compliance

The Authority operates in accordance to the regulation of the positive legal legislation in the Republic of Macedonia.

The subscribers are informed that the personal data they give to KIBS, can be transferred and processed from KIBS and its partners which are included in the process.

KIBS takes all necessary measures to keep the personal data safely and securely, in accordance to the Law for personal data protection. KIBS demands from its employees to adhere to the legal acts of the Law for personal data protection.

The employees do not have a right to collect or use the personal data to which they have access in an inappropriate manner and generally, to act in way in which will most likely be damaging to the private life or personal reputation of the owner of the data.

KIBS is obliged to keep the information obtained from the subscribers securely, unless their display is approved from the subscriber or allowed by law.

7.4.11. Log of records of the Authority

Monitoring of the operations of the Authority is enabled through a review of the logged events, for purposes of retrieving evidence for legal action. Every event is recorded in a database from which all of the events for the service can be tracked, including the incidents. If an incident occur, KIBS will act in a corresponding manner with a goal to quickly intervene, to limit the influence of the incident on security and to renew the service in the fastest possible time.

The specific records of the system of the Authority are separately documented.

The Authority guarantees the integrity and reliability of the current and archived records of the service operation.

The records referring to the Authority’s operations will be fully and securely archived, in accordance to the internal procedures of KIBS AD Skopje. All media with confidential information of the services of the Authority are included in the procedures for maintainance, with a goal to secure accessability to the functions and information. The scrapping of the equipment is documented to secure non-disclosure of the confidential information that may be contained in it.

The records of the operation of the Authority will be published if there is a need for obtaining proof intended for legal entities, regarding a certain activity with the service of the Authority.

The exact time of important events connected to key management or clock synchronization will be recorded.

The records for the service of issuing time stamps will be kept long enough after the expiry of the keys, suitably for legal evidence and described in the Publicly published information defined in the Policy, Chapter 7.1.2.

The form of keeping the records does not enable simple erasement or destruction.

All information regarding the subscribers will be kept securely, except in case where it is mutually agreed that those data can be used by a wider audience.

All records regarding key lifecycle and the certificates are separately documented.

All records regarding the synchronization or recalibration of clocks, as well as loss of synchronization are separately documented.

7.5. Organizational chart

KIBS Momentum is a part of KIBS AD Skopje.

The organization is based in the Republic of Macedonia.

KIBS has documented the security of the information for human resources. The employees in KIBS, who have a confidential role are carefully chosen and are clearly informed for the operations and rules they must adhere to.

The person who have a confidential role, have commited themselves to protect the confidentiality of their work. KIBS guarantees that the professional skills of the employees with a confidential role is in accordance with the necessary qualifications of their functions. The management of KIBS posseses appropriate competence and proficiency in the security procedures. Every person with a confidential role is informed about his responsibilities through his job description and/or the procedures connected to system security and employee control.

The employees who work with the services of the Authority have appropriate proficiency in:

- The technology of time stamping
- The technology of digital signatures
- The mechanisms for setting or synchronizing the clocks of the device for generating time stamps with Coordinated Universal Time
- The procedures for security, for the employees responsible for security
- Information security and risk assesment

The requirements regarding sub-contractors are regulated with agreements.

The obligations include SLA agreements and information confidentiality.

The employees are informed about the security rules connected with their roles right after they are in force. The persons who work on the services of the Authority and have an operational role have the procedures connected to their work delivered.

Annex: Longterm verification of time stamps

Usually, the time stamps cannot be verified after the expiration of the certificate from the devices for generating time stamps. However, the verification of the time stamp can be done is spite of these limitations of the certificates on the devices for generating time stamps, if during the verification the following conditions are met:

- The private key in the device is not compromised in any time until the moment when the affected side requests a verification of the time stamp
- The hash algorithms which are used for generating the time stamp are still allowed in the time of verification
- The algorithms for signing and key size of the certificates when the time stamp was signed are still known to be resisting cryptographic attacks in the time of verification

If these conditions are not met, then the validity can be extended with adding an additional time stamp to protect the integrity of the previous one. Alternatively, the data which are time stamped can be stored on a secure place.

As addition to this process are the records which KIBS Momentum keeps for the hash values which are time stamped and with this, securing evidence that the data existed before the exact specified time. This technique is called “Time marking” and is an important alternative for longterm verification of the digital signatures.

***

Преодни одредби

Овој Политика е во сила од 17.10.2016 година и се применува од денот на нејзиното објавување на веб страницата на издавачот на сертификати КИБС: http://www.kibstrust.mk/.

Генерален директор

Горан Анастасовски