Time-stamping Authority
KIBSTrust Momentum Policy

KIBSTrust Momentum

Version: 4.2

Date: 03.04.2020

11.45

OID 1.3.6.1.4.1.16305.1.1.3

KIBS AD Skopje

http://www.kibstrust.mk

Document Information

This document has been developed by KIBS AD Skopje (KIBS) and contains the conditions, according to which KIBS is acting as Trusted Services Provider (TSP) and Qualified Trusted Services Provider (QTSP).

The present document is based on and it is compatible with the standard ETSI EN 319 421 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps".

Intellectual Property Rights

Version History

Version	Date	Author	Changes
4.2	03.04.2020	Marin Piperkoski	In document on Macedonian language there was change in terminology according new legislation. TSA Termination and Termination Plan supplement. Liability related supplement.
4.1	16.10.2019	Marin Piperkoski	In document on Macedonian language there was change in terminology according new legislation. TSA Termination and Termination Plan supplement. Liability related supplement.
4.0	24.10.2018	Aleksandar Dzambaski, Suzana Tasevska	Policy adjusted according ETSI EN 319 421 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps.
3.0	17.10.2016	Aleksandar Dzambaski	Timestamping certificate issuer and profile changed. The new certificate is from DigiCert.
2.0	11.04.2016	Aleksandar Dzambaski	Policy adjusted according ETSI TS 102 023 V1.2.2 Policy requirements for time-stamping authorities. The persons defined for the preparation and approval of the document have been changed. The document is prepared in Macedonian and English version.
1.0	08.05.2012	Aleksandar Dzambaski, Suzana Tasevska	New document

Table of Contents

Introduction

Companies, authorities, and organizations of all kinds throughout the world are increasingly generating their processes electronically for purposes of optimization, cost reduction and speed. Thus, existing paper-based processes are being replaced by electronic processes and new processes made possible using digital information and communication.

These new, improved processes (using electronic information) are subject to the same statutory provisions, compliance and protection requirements, as traditional paper-based processes. To meet these requirements, both paper-based and electronic information must be protected, among other things, against manipulation and loss. To be able to assess the observation of compliance requirements in a professional environment, proof of integrity, completeness and confidentiality are often the main criteria.

Electronic time stamps can deliver this proof of integrity and completeness in a way that is simple, legally secure, permanent, inexpensive, and, on request, anonymous. A time stamp is an electronic certificate, which states when certain data existed. It thus documents the "when" and "what". An electronic signature, often referred to as personal signature, documents the "who" and "what". In contrast to an electronic signature, a time stamp is not bound to people and their actions. It can thus be integrated much more simply and fully-automatically into electronic processes. Time stamps are easier to use than electronic signatures as their application can be fully automatic and independent of specific individuals, or anonymous.

Timestamps are used to prove the existence of certain data before a certain point without the possibility that the owner can backdate the timestamps. Once a datum is signed, any change of data will cause the electronic signature to fail alerting the user. Unlike electronic signature, timestamps are not bound to persons and their actions.

Clearing House KIBS AD Skopje (KIBS) uses public key infrastructure and trusted time sources to provide qualified electronic timestamps under its brand name KIBSTrust Momentum.

1. Scope

This KIBSTrust Time-stamp Policy/Practice Statement (TSP/PS) defines the operational and management practices of the KIBS Time-Stamping Authority (KIBSTrust TSA) such that Subscribers and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

KIBSTrust TSA is compliant with the requirements of Regulation (EU) No 910/2014 (hereafter called the eIDAS Regulation) as well as under Law on Electronic Documents, Electronic Identification and Trusted Services (o.g. 101/19, 215/19) and bylaws, for issuing qualified electronic time stamps. Issued qualified timestamps can be used in support of electronic signatures or for any application requiring the proof that a datum existed before a specific time.

The structure and contents of this TSP/PS are laid out in accordance with ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps.

Web address of published documents: https://www.kibstrust.mk/repository.

In case of conflict between the original document in English and the Macedonian translation, document on Macedonian language shall prevail.

2. References

2.1. Normative references

[1] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
[2] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
[3] ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".
[4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
[5] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
[6] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

2.2. Informative references

[i.1] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".
[i.2] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
[i.3] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".
[i.4] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[i.5] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[i.6] BIPM Circular T.
NOTE: Available from the BIPM website http://www.bipm.org/.
[i.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
[i.8] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for timestamping authorities".
[i.9] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service

Providers".
[i.10] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
[i.11] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
[i.12] CEN EN 419 231: "Protection profile for trustworthy systems supporting time stamping".
[i.13] CEN EN 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup".
[i.14] CEN EN 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services".
[i.15] CEN EN 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup".
[i.16] CEN EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services".

3. Definitions and abbreviations

3.1. Definitions

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [1].
Relying party: recipient of a timestamp who relies on that timestamp.
Subscriber: legal or natural person to whom a timestamp is issued and who is bound to any subscriber obligations.
Timestamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.
Time-Stamp policy/Practice Statement" or **TSP/PS** (this document) means a set of rules that indicate the applicability of a time-stamp token to a particular community or class of application with common security requirements.
Trust Service Provider (TSP): entity which provides one or more trust services.
Time-Stamping Authority (TSA): TSP providing time-stamping services using one or more time-stamping units.
Time-stamping service: trust service for issuing timestamps.
Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single timestamp signing key active at a time.
Trust service: electronic service that enhances trust and confidence in electronic transactions.
TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements.
TSA practice statement: statement of the practices that a TSA employs in issuing timestamp.
TSA system: composition of IT products and components organized to support the provision of time-stamping services.
UTC(k): time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ± 100 ns.
MK-eIDAS: Law on Electronic Documents, Electronic Identification and Trusted Services. The law transposed EU Regulation 910/2014 known as the eIDAS.
National supervisory body: according to the MK-eIDAS law it is the Ministry of Information Society and Administration.

3.2. Abbreviations

BTSP Best practices Time-Stamp Policy
CA Certification Authority
GMT Greenwich Mean Time
IERS International Earth Rotation and Reference System Service
IT Information Technology
TAI Temps Atomique International (International Atomic Time)
TSA Time-Stamping Authority
TSP Trust Service Provider
TSU Time-Stamping Unit
UTC Coordinated Universal Time

4. General Concepts

4.1. General policy requirements concepts

The present document references ETSI EN 319 401 [4] for generic policy requirements common to all classes of trust service providers service.

These policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources.

4.2. Time-stamping Services

Time-stamping service include the following components:

- **Time-stamping provision**: the technical component that issues the Time-Stamp Tokens (TSTs).
- **Time-stamping management:** the service component that monitors and controls the time-stamping operation, including synchronization with the reference UTC time source, according to the TSP/PS**.**

4.3. Time-stamping Authority

KIBSTrust TSA is trust service provider as described in ETSI EN 319 401 [4] providing time-stamping services to the public.

The KIBSTrust TSA takes overall responsibility for the provision of time-stamping services identified in Section 4.2.

KIBSTrust TSA has responsibility for the operation of one or more Time-Stamping Units (TSU) which create and sign TSTs on behalf of the TSA. Each TSU has a different key.

KIBS operates KIBSTrust TSA as part of PKI. KIBSTrust TSA is identified in the digital certificates used in TSU.

KIBSTrust TSA is a qualified trust service provider as described in eIDAS which issues timestamps.

Below is a summary of the current TSU certificates and their issuers:

Field	Value
Version	3
Serial Number	072ac472580d94c601e7c6fa85e7d10a
Signature	sha256RSA

DN of the issuer	CN = DigiCert SHA2 Assured ID Timestamping CA OU = www.digicert.com O = DigiCert Inc C = US
Validity	10.05.2019 - 05.10.2022
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

KIBS hereby confirms that the KIBSTrust TSA is audited at least every 12 months by a conformity assessment body, delivering the assessment report as soon as possible once it is received. When the supervisory body requires the TSA to remedy any breach of the requirements, the TSA shall act accordingly and in due course. The control body will be informed of any changes to the TSA provision.

4.4. Subscriber and Relying Party

When the subscriber is an organization, it comprises several end-users or an individual end user and some of the obligations that apply to that organization must apply as well to the end- users. In any case, the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

Relying party is an individual or entity that acts in reliance of a TST generated under KIBS TSP/PS. A Relying Party may or may not also be a subscriber.

4.5. TSA Policy and Practice Statement

KIBS Time-Stamp Policy and KIBS Time-Stamp Practice Statement are merged into one document – KIBS Time-stamp Policy/Practice Statement – TSP/PS.

Present KIBS TSP/PS specifies a time-stamp policy and practice statement to meet general requirements for trusted time-stamping services as defined by the standards in Chapter 2 (References) of this document.

For additional detail on the KIBSTrust TSA, refer to Chapter 5 of this document.

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

https://www.kibstrust.mk,

or according contract.

This TSP/PS and all related public documents may be downloaded from:

https://www.kibstrust.mk/repository.

5. Time-Stamp Policy

5.1. General

Present Time-stamp policy defines a set of processes for the trustworthy creation of time-stamp tokens in accordance with ETSI EN 319 421. The private keys and the TSU meet the technical specifications of ETSI EN 319 422 and RFC 3161.

The KIBSTrust TSA signs timestamps using private keys that are reserved specifically for that purpose. Each TST contains an identifier to the applicable policy, and timestamps are issued with time **accurate to ±1 second of UTC**.

Timestamps are requested by means or Hypertext Transfer Protocol (HTTP), as described by RFC 3161.

TSU certificates used for generating timestamps are issued by DigiCert, Inc., 2801 North Thanksgiving Way, Suite 500, Lehi, Utah 84043. Their specification is described in the documents in the repository of DigiCert's policies are located at https://www.digicert.com/legal-repository/.

5.2. Identification

The identifier of the time-stamp policy specified in the present document is:

OID: 1.3.6.1.4.1.16305.1.1.3

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) KIBS AD Skopje (16305) Objects Related to PKI-X.509 (1) Certification Policies and CPSs (1) KIBS Momentum TSA Policy (3)}

This OID is referenced by every issued timestamp, In the KIBS TSP/PS and in the TSA Disclosure statement that is available to both Subscribers and Relying Parties.

The ETSI time-stamping identifier **0.4.0.2023.1.1** (BSTP) is supported.

5.3. User Community and Applicability

This policy is aimed at meeting the requirements of timestamp for long term validity (as defined in ETSI EN 319 122 [i.1]) but is generally applicable to any use which has a requirement for equivalent quality.

This policy may be used for public time-stamping services or time-stamping services used within a closed community.

6. Policies and practices

6.1. Risk assessment

KIBS carries out a risk assessment to identify, analyze and evaluate trust service risks considering business and technical issues. The risk treatment measures ensure that the level of security is commensurate to the degree of risk. Appropriate risk treatment measures are selected, taking account of the risk assessment results.

The risk assessment is regularly reviewed and revised to ensure the quality and reliability of the time-stamping services.

Security Controls that are defined in a security concept of the time-stamping services are controlled regularly to ensure the efficiency of the controls.

KIBS management approves the risk assessment and accepts the residual risk identified.

6.2. Trust Service Practice Statement

The KIBS TSP/PS establishes the general rules concerning the operation of the KIBSTrust TSA. Additional internal documents define how KIBS meets the technical, organizational, and procedural requirements identified in the TSP/PS.

TSP/PS, TSA Disclosure Statement and other public documents may be found at https://www.kibstrust.mk/repository.

Internal documents may be provided only under strictly controlled conditions.

The KIBS TSP/PS identifies the obligations of external organizations supporting the TSA services including the applicable policies and practices.

The KIBS TSP/PS is approved by KIBS Policy Management Group. KIBS Policy Management Group has responsibility to ensure that the practices are properly implemented. Any new version is immediately published, replacing the previous version.

6.2.1. Hash algorithms

- Acceptable Time-stamp request hashes: SHA-256, SHA-384, SHA-512
- Signature: sha256WithRSAEncryption (2048 bit key)

6.2.2. Time accuracy

Time-stamp tokens are issued with time accurate to ±1 second of UTC. If a trusted UTC time source cannot be acquired - the timestamp will not be issued.

6.2.3. Service limitations

Not applicable.

6.2.4. Subscriber obligations.

Subscriber obligations are described in Section 6.5.2 of this document.

6.2.5. Relying Party obligations

Relying Party obligations are described in Section 6.6 of this document.

6.2.6. Time-stamp verification

Time-stamp verification includes the following tasks:

1. **Verification of the time-stamp issuer**

Issuer is a time-stamping authority that uses appropriate electronic certificates for issuing the time-stamp. Public keys of the used certificates included in the TSU and CA certificates are published to enable the verification that the timestamp has been signed correctly by the TSA.

The certificates may be found in the following links:

http://cacerts.digicert.com/DigiCertSHA2AssuredIDTimestampingCA.crt and
http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt.

2. **Verification of the time-stamp revocation status**

An OCSP service and CRL list is available to verify the revocation status of the certificates used in the timestamp. The address for accessing the OCSP responder service is http://ocsp.digicert.com. CRL Distribution lists are published at http://crl3.digicert.com/sha2-assured-ts.crl and http://crl4.digicert.com/sha2-assured-ts.crl.

3. **Verification of the integrity of the timestamp**

The cryptographic integrity of the timestamp, for example the ASN.1 structure is correct, and the datum (the data that has been time-stamped) belong to the application. It can be verified through the KIBSTrust TSA's web service form, that is offered free of charge in the following address: https://www.kibstrust.mk.

6.2.7. Applicable law

This document is regulated in accordance with Macedonian laws and EU regulation and standards. In case of a dispute between the parties, that has risen from interpretation, 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.

6.2.8. Service availability

KIBSTrust TSA has implemented the following measures to ensure availability of the service:

- Redundant IT systems to avoid single point of failures.
- Redundant high-speed internet connections to avoid loss of service
- Use of uninterruptable power supplies.

Although these measures ensure service availability, KIBS TSA aims to provide an availability of the service of 99% per year.

6.3. Terms and conditions

Terms and conditions are described in the document “Terms and conditions for using timestamping service Momentum” located at address https://www.kibstrust.mk/repository.

6.4. Information security policy

KIBS has implemented an Information Security Policy throughout the company. All employees must adhere to the regulations stated in this policy and the derived security concepts. The information security policy is reviewed on a regular basis and especially when significant changes occur. The Management of KIBS approves the changes in the Information security policies.

6.5. TSA Obligations

6.5.1. General

KIBS TSA fulfills the requirements and procedures defined in Chapter 6 of this document as well as the provisions of eIDAS, which are implemented as applicable to the selected trusted time-stamp policy.

KIBS is a party to the mutual agreements and obligations between the TSA, Subscribers, and Relying Parties. The TSP/PS is integral component of these agreements.

6.5.2. TSA Obligations towards Subscribers

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the document “Terms and conditions for using timestamping service Momentum”.

6.6. Information for relying parties

Relying parties must verify that the timestamp has been correctly signed and that the private key used to sign the timestamp has not been revoked. The Relying Party should consider any limitations on usage of the timestamp indicated by this KIBS TSP/PS. During the TSU Certificate validity period, status of the private key can be verified using the relevant CRLs, KIBS CA Certificates, TSU Certificates and related. CRLs are published at http://crl3.digicert.com/sha2-assured-ts.crl and http://crl4.digicert.com/sha2-assured-ts.crl.

7. TSA management and operation

7.1. Introduction

KIBS has implemented an information security management system to maintain the security of the service.

The provision of a timestamp in response to a request is at the discretion of KIBS TSA depending on any service level agreements with the subscriber.

7.2. Internal organization

a) KIBS is legal entity according to the Macedonian law.
KIBS AD Skopje
+389 2 5513 401, +389 2 3297 401
helpdesk@kibstrust.mk
https://www.kibstrust.mk
1, bul. "Kuzman Josifovski Pitu",
1000 Skopje, Republic of North Macedonia

b) KIBS has a system for quality and information security management appropriate for the provided time-stamping services.

c) KIBS personnel have necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

7.3. Personnel security

KIBS ensures that employees and contractors support the trustworthiness of the TSA's operations.

KIBS staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.

KIBS's personnel can fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two. This should include regular (at least every 12 months) updates on new threats and current security practices.

Appropriate disciplinary sanctions shall be applied to personnel violating KIBS's policies or procedures.

Security roles and responsibilities, as specified in the KIBS's information security policy, are documented in job descriptions and are available to all concerned personnel.

Trusted roles, on which the security of the KIBS TSA's operation is dependent, are clearly identified, named by the management, and accepted by the management and the person to fulfil the role.

All KIBS's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the KIBS TSA's operations.

7.4. Asset management

All IT systems used within the service are clearly identified, categorized and filed in an asset management database.

All media is handled securely.

Data from disposed media is securely deleted, either by an electronic erase of the data or by physically destroying the disposed media.

7.5. Access control

Different security layers in relation to physical and logical access ensure a secure operation of the time-stamping service. For instance:

- Secured physical environment
- Segregation of network segments
- Segregation of duties
- Firewalls, IPS/IDS
- Network and Service Monitoring
- Strengthening of IT Systems
- In case a person, which carries out operations for the time-stamping services, changes the role or leaves the organization, all the security tokens from that person are withdrawn.

7.6. Cryptographic controls

7.6.1. General

The TSA uses private keys to fulfill its service. One private key pair is used to be issued the public-key time-stamp certificate that is used within the TSUs. One private key pair is used within the TSU to issue the timestamps.

All private keys are stored in a FIPS 140-2 Level 3 Hardware Security Modules.

7.6.2. TSU's key generation

The TSU uses RSA key pair with a length of 2048-bit. This key pair is used only for signing TSTs.

All cryptographic modules are associated with the same public key certificate.

a) The generation of the TSU's signing key(s) is undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3), under at least control of two trusted personnel. The personnel authorized to carry out this function is limited to those required to do so under the TSA's practices.

b) The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS PUB 140-2 [I.9], level 3, or ISO 15408 Common Criteria EAL 4+.

c) The TSU key generation algorithm, the signature algorithm, the length of the key used to sign the timestamps, is recognized by the national supervisory entity and by the current technical state of art as being fit for the signing of timestamps issued by the TSA.

7.6.3. TSU private key protection

The practices of TSU key protection, storage, backup, and recovery, described in section 6.2 and 6.3 of KIBS TSA/PS are applicable.

The TSU's private key shall be backed up and stored safely for the unlikely event of key loss due to unexpected power interruption or hardware failure.

A key backup shall be obtained in the Keys Generation Ceremony. The backup of the private key is kept in secret and its integrity and authenticity is preserved in a safe box.

7.6.4. TSU Public key certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

a) TSU signature verification (public keys) are available to relying parties that trust in a public key certificate. The certificates are published in the following link: https://www.kibstrust.mk/en-GB/Home/Support/.
b) The TSU does not issue a timestamp before its signature verification (public key). When the certificate is loaded in the TSU, the TSA verifies that the certificate was duly signed (including verification of the certificate chain of a trusted certification authority).
c) Only one TSU certificate with its private key is issued.
d) TSU certificates are not renewed.
e) Validity information regarding the TSU certificates is updated periodically and the CRLs or OCSP services are available with the references located in the certificates.

7.6.5. TSU's key renewal

The life-time of the TSU certificate corresponds to the period of the chosen algorithm and the key length (see clause 7.6.2c).

A certificate can be issued for all expected lifetime. The duration of the TSU class is limited by:

- The period of validity of the root issuer entity certificate.
- Once a year or when significant changes occur, the person holding the function "Security Officer" verifies all cryptographic algorithms used in the TSA checking that each algorithm is recognized as suitable, as indicated in clause 7.6.2c).
- If an algorithm enters a situation of risk, it shall no longer be considered as adequate; the Security Manager shall instruct the TSA the cease of usage of the affected keys and load new keys.

7.6.6. Life cycle management of cryptographic hardware

The used cryptographic hardware is inspected by trustworthy personnel (in the presence of two persons) during shipment and storing. Specifically, the hardware is verified for

a) Any damages of security seals
b) Any damages of the case of the hardware (e.g. scratches, bumps...)
c) Any damages of the packing of the hardware

The inspection is recorded.

Additionally, the following applies:

a) The Installation, and activation of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles using, at least, dual control in a physically secured environment.
b) The TSU private signing keys stored in a TSU cryptographic module are erased upon retiring the device in a manner that is practically impossible to recover them.

7.6.7. End of TSU's key life cycle

After expiration of the private keys, the private keys within the cryptographic module are destroyed in a way the private keys cannot be retrieved.

The "Security Officer" defines the key validity in accordance to clause 7.6.2c.

7.6.8. Root certification authority

KIBS TSA is signed by DigiCert. DigiCert's policies are located https://www.digicert.com/legal-repository/.

7.7. Timestamping

7.7.1. Time-stamp issuer

KIBS TSA offers time-stamping services using RFC 3161 “Time Stamp Protocol (TSP)”. The service URL is specified in the subscriber's agreement. Each TST contains the Time-Stamping Policy identifier, a unique serial number and a certificate containing the identification information of the KIBS TSA's TSU.

The TSU in the time-stamp requests accepts SHA256, SHA384, SHA512 hash algorithms and uses the SHA-256 cryptographic hash function to sign TST.

The TSU keys are 2048-bit RSA keys. The key is used only for signing TSTs.

TSA logs all issued TSTs. The TSTs are logged for an indefinite period. KIBS TSA can prove the existence of a TST at the request of a relying party. KIBS TSA can request the relying party to cover the costs of such service.

The TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

7.7.2. Clock synchronization with UTC

KIBS ensures that its clock is synchronized with UTC within an accuracy of 1 (one) second or better, using the NTP protocol.

KIBS monitors its clock synchronization and ensures that, if the time indicated in a TST drifts or jumps out of synchronization with the UTC, this is detected. In case the TSA clock drifts out of accuracy, no timestamp shall be issued until the clock is synchronized.

Specifically, the following topics are covered:

- Continuous calibration of the TSU clock
- Monitoring of the accuracy of the TSU clock
- Thread analysis against attacks on time-signals
- Behavior while skipping/adding leap seconds
- Behavior while drifting larger that 1s from the UTC

7.7.3. Time-stamp Token (TST) Profiles

Field	Meaning/Value
Version	1
Hash Algorithm	SHA-256, SHA-384, SHA-512
Message Data	Hash value of data
Policy OID	OID=1.3.6.1.4.1.16305.1.1.3 (enhances OID=0.4.0.2023.1.1)
Serial Number	TST serial number
Generated Time	TST generation time
Accuracy	±1 second of UTC
Ordering	FALSE
Nonce	supported
TSA	CN = KIBSTrust Momentum Timestamp Responder 2016 10 05 1 O = Clearing House Klirinski interbankarski sistemi AD SKOPJE C = MK
	CN = DigiCert SHA2 Assured ID Timestamping CA OU = www.digicert.com O = DigiCert Inc C = US

7.8. Physical and environmental security

A highly secured physical environment is available. This physically secured environment houses the TSA.

The time-stamping management facilities are operated in an environment that protects physically and logically the transaction services with controls of unauthorized access to systems or data. Each entry in the physically secure area is subjected to independent monitoring of the TSA. In the security area, the person who accesses the facilities is accompanied, registering the identity, entry and exit time. The measures taken with regard to the physical protection are part of the Information Security system developed and implemented in KIBS, corresponding to the requirements of ISO/IEC 27001:2013, ETSI EN 411 401 and ETSI EN 411 421 standards.

KIBS has implemented security controls to avoid:

- loss, damage or compromise of assets and interruption to business activities.
- loss, damage, or compromise of resources;
- compromise or theft of information and information processing facilities.

Physical protection is achieved through the creation of clearly defined security perimeters (e.g. physical barriers) around the time-stamping management and physical access to critical components of the TSA system is limited to authorized individuals.

TSA's critical components are in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

Access controls are applied to the HSM to meet the requirements of security of cryptographic modules as identified in clause 7.6.

Controls are applied to protect against equipment, information, media, and software relating to the time-stamping services being taken off-site without authorization.

Physical and environmental security controls protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. KIBS physical and environmental security policy for systems concerned with time-stamping management address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

7.9. Security of operations

KIBS TSA has implemented a mature system of system and security controls to ensure service quality and availability. These controls are:

a) An analysis of security requirements is carried out on the design specifications and the requirements for any stage of the systems development project undertaken by the organization or on behalf of the TSP to ensure that security is built into the information technology's systems.

b) As a change control procedure, version control is applied for modifications and corrections of the software.

c) The integrity of TSP's systems and information is protected against viruses, malicious and unauthorized software.

d) The means used within the TSP systems are secure and protect against damage, theft, unauthorized access and obsolescence.

e) Within the period in which records need to be retained, the media management procedures protect against obsolescence and deterioration of the means of telecommunication.

f) Application of appropriate procedures for all administrative functions of trust and that have an impact on service delivery.

g) The TSP has specified and applied procedures for ensuring that security patches are applied within a reasonable time after they have become available. A security patch does not need to be applied if it introduces additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. The reason for not applying any security patches shall be documented.

7.10. Network security

The TSP protects its network and systems from attacks:

a) The TSP network is segmented into networks or zones based on risk assessment considering the functional, logical, and physical (including location) relationship between trustworthy systems and services.

b) The TSP restricts access and communications between zones to those necessary for the operation of the TSP. Not needed connections and services are explicitly forbidden or deactivated. The established rule set is reviewed on a regular basis.

c) All the elements of the TSPs critical systems (e.g. Root CA systems, TSU) are kept in a secured zone.

d) A dedicated network for administrating the IT systems, which is separated from the operational network, is established. Systems used for administration shall not be used for no administrative purposes.

e) The test platform and the production platform are separated. The test platform is found in an environment not concerned with live operations (e.g. development).

f) Communication between the different trustworthy systems can only be established through trusted channels that are logically distinct from other communication channels and provide an assured identification of its end points and protection of the data from modification or disclosure.

g) The external network connection to the internet is redundant to ensure availability of the services in case of a single failure.

h) The TSP performs a regular vulnerability scan on public and private IP addresses identified by the TSP, the vulnerability of each analysis is performed by a person or entity with the skills, tools, proficiency, code of ethics and independence necessary to provide a reliable report.

i) The TSP, after configuring the infrastructure with updates or modifications that the TSP considers relevant, it performs a penetration test in the systems.

j) The TSP obtains evidence records that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

7.11. Incident management

Further information can be obtained in the document "Control of inconsistencies, incidents and problems". An incident management process was implemented to react quickly to incidents.

System activities concerning access to IT systems, its user systems, and service requests are monitored. Especially:

a) Monitoring activities take account the sensitivity of any information collected or analyzed.

b) Abnormal system activities that indicate a potential security violation, including intrusion into the TSP network, are detected and reported as alarms.

c) The TSP IT systems monitor the following events: Start-up and shutdown of the logging functions; availability and utilization of the needed services with the TSP network.

d) The TSP acts in a timely and coordinated manner to respond quickly to incidents and to limit the impact of security breaches. The TSP appoints trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

e) The TSP notifies the corresponding parties, in line with the applicable regulatory rules of any security breach or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

f) The national supervisory body is informed within 24h after the discovery of a critical security breach.

g) Audit logs are monitored or reviewed regularly to identify evidence of malicious activity.

h) The TSP shall resolve critical vulnerabilities within a reasonable period after their discovery. If this is not possible the TSP will create and implement a plan to mitigate the critical vulnerability or the TSP will document the factual basis for the TSP's determination that the vulnerability does not require remediation.

i) Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

7.12. Collection of evidence

At the time a security incident becomes detected, it might be not obvious, if that security incident is subject of further investigations. Therefore, it is important, that any proof, the status of IT system or information is securely saved before they become unusable or destroyed.

The TSP records are kept accessible for an appropriate period, including after the activities of the TSP have ceased. All the relevant information concerning data issued and received by the TSP are guarded to provide evidence in legal proceedings and to ensure continuity of the service. Especially:

a) The confidentiality and integrity of current and archived records concerning operation of services is maintained.

b) Records concerning the management of services are confidential and filed in accordance with described business practices.

c) Records concerning the management of services, if necessary, are made available for the purposes of providing evidence of the correct operation of the services for legal proceedings.

d) The TSP registers in the precise moment, the significant environmental events, key management and clock synchronization. The time used to record events, as required in the audit log, is synchronized with the UTC continuously.

e) Records concerning services are held for a period after the expiration of the validity of the signing keys or of any service token to provide trust for the necessary legal evidence in accordance to the present document.

f) The events are logged in a way that they cannot be deleted or destroyed (except if they can be reliably transferred to long-term media).

7.13. Business continuity management

Backups of the databases of all issued TSTs by KIBS TSA are kept in an off-site storage.

If the TSU private key is compromised or suspected to be compromised, KIBS TSA shall inform Subscribers and Relying Parties and shall stop using the compromised key.

7.14. TSA termination and termination plans

The practices identified in document “Plan for termination of activity of a Trusted Services Provider” are applicable. Furthermore, KIBS as QTSP had undertaken necessary measures that ensure retention of all the relevant archived records prior to termination of the service.

7.15. Compliance

KIBS TSA ensures compliance with applicable law and standards.

a) MK-eIDAS
b) Regulation (EU) N°910/2014
c) ETSI TS 319 421, ETSI EN 319 401, ETSI TS 319 421
d) IETF (RFC 3161)

Validation of the compliance with these regulations is performed during the conformity assessment.

Whenever possible, the TSP makes its services available to persons with disabilities.

Annex A: Potential liability in the provision of time-stamping services

The liability of KIBS acting as QTSSP and of Subscribers and Relying Parties connected with the services is specified in the document “Terms and Conditions” or is as foreseen in the applicable legislation.

KIBS may not be held liable for any damage arising from any incorrect usage of timestamping service Momentum other than that permitted by this KIBSTrust Time-stamp Policy/Practice Statement and Terms and Conditions for using timestamping service Momentum.

KIBS is responsible for possible damages directly determined, intentionally or by negligence, to any natural or legal person, because of failure to comply with the obligations set out in KIBSTrust Time-stamp Policy/Practice Statement.

KIBS as Qualified Timestamping Service Provider limit its liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. This also includes a liability cap regarding the combined aggregate liability of KIBS to any and all persons concerning Time Stamp Services, which is limited to an amount not exceeding respective amount stated in Terms and Conditions or prepaid purchase of the time stamping service, which will be calculated on a pro rata basis, regardless of the nature of the liability and the type, amount or extent of any damages suffered.

The liability limitations shall be the same irrespective to the number of time stamps or claims related to such Time Stamp.

KIBS TSA declines any responsibility regarding the usage of TST’s it delivers and signs.

Annex B: TSA disclosure statement

The KIBS TSA disclosure statement is identified in “Disclosure Statement for using timestamping service Momentum” located at address https://www.kibstrust.mk/repository.

Annex C: Coordinated Universal Time (UTC)

Coordinated Universal Time UTC is is the international time standard that became effective on January 1, 1972. UTC has superseded Greenwich Mean Time (GMT). Universal time is based on a 24 hour clock.

Coordinated Universal Time (UTC): Time scale, based on the second, as defined and recommended by the International Telecommunications Radio Committee (ITU-R), maintained by the International Atomic Time (TAI) and calculated by the Bureau International des Poids et Mesures (BIPM) from the readings of more than 200 atomic clocks located in metrology institutes and observatories in more than 30 countries around the world. Information on TAI is made available every month in the BIPM Circular T (ftp://62.161.69.5/pub/tai/publication). This calculation is helped by International Earth Rotation Service (IERS) (http://hpiers.obspm.fr/) to ensure that irregularities, are taken into account.

The full definition of UTC is contained in Recommendation ITU-R TF.460-6 [1].

Annex D: Long term verification of timestamps

If at the time of verification:

- the TSU private key has not been compromised at any time up to the time that a relying part verifies a timestamp;
- the hash algorithms used in the timestamp exhibits no collisions at the time of verification;
- the signature algorithm and signature key size under which the timestamp has been signed is still beyond the reach of cryptographic attacks at the time of verification;

then verification of a timestamp can still be performed beyond the end of the validity period of the certificate from the TSU.

The validity may be maintained by applying an additional timestamp to protect the integrity of the previous one. Alternatively, the time-stamped data may be placed in secure storage.

End of Document