DIGITAL CERTIFICATION SERVICES

CP/CPS for Qualified Electronic Time Stamps

Version 1.0 - 15/06/2017

Approved for the following ATHEX "Certificate Policies":
(Approved for the following 'Certificate Policies':)

1. Certificate Policy for TimeStamping Certificates
   OID 1.3.6.1.4.1.29402.1.1.4.1.1.0

1. INTRODUCTION 3
1.1 Overview 3
1.2 Document Name and Identification 3
2. Scope 4
3. References 4
4. Definitions and Abbreviations 4
4.1 Definitions 4
4.2 Abbreviations 5
5. General Concepts 6
5.1 Time-stamping Services 6
5.2 Time-stamping Authority 6
5.3 Subscribers and Relying Parties 6
5.4 TSA Policy and Practices 7
6. Time-stamp Policy 7
6.1 Overview 7
6.2 Identification 7
6.3 User Community and Applicability 8
6.4 Conformance 8
7. Obligations and Liability 8
7.1 TSA Obligations 8
7.2 Subscriber Obligations 8
7.3 Relying Party Obligations 9
7.4 Liability 9
8. Practices 9
8.1 Practice and Disclosure Statements 10
8.2 Key Management Life Cycle 11
8.3 Time-stamping 12
8.4 TSA Management and Operation 12
8.5 Organisational 16
8.6 Compliance with Applicable Law 16
8.7 Miscellaneous Provisions 16
8.8 Other Provisions 16

1. INTRODUCTION

1.1 Overview

This HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. (or "ATHEX") Certificate Practice Statement (the "CPS") presents the principles and procedures HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. employs in the issuance and life cycle management of HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. Timestamping Certificates. This CPS and any and all amendments thereto are incorporated by reference into all of the above-listed HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. Certificates.

Regulation (EU) No 910/2014 ("eIDAS Regulation") includes requirements for Trust Service Providers (TSP) providing services to the public, including TSPs issuing time-stamps. Additionally, more specific requirements are identified in the Regulation for a specific class of TSP called a Qualified TSP. ATHEX is a Qualified TSP.
Electronic signatures are used to add security by creating a tamperproof cryptographic seal around electronic data. Once a datum is signed, any change to its content will cause the electronic signature to fail, alerting the user. Electronic signatures may be used in several ways:

• Individual electronic signatures support the integrity of electronic records by declaring WHO signed WHAT (in other words, who created particular content or changes).

• Time-stamps use electronic signatures, incorporating the time from an accurate source, to confirm WHAT happened WHEN.
Individual signatures may be used independently – or together with time-stamps – to increase the trustworthiness of electronic records and transactions.

1.2 Document Name and Identification

This document is the Hellenic Exchanges – Athens Stock Exchange S.A. Certification Practice Statement for TS Certificates. The object identifier (OID) values corresponding to the Hellenic Exchanges – Athens Stock Exchange S.A. Certificate Policy are as follows:

1.3.6.1.4.1.29402.1.4.1.0	Hellenic Exchanges – Athens Stock Exchange S.A. TimeStamping Certificate Policy / Practice Statement
1.3.6.1.4.1.29402	Object Identifier (OID) of Hellenic Exchanges – Athens Stock Exchange S.A. (ATHEX), registered in IANA
1	Independent department "Public Services Certification" of Hellenic Exchanges – Athens Stock Exchange S.A.
4	***Certification Policy for Timestamping***
1.0	***First and second digit of the version of the Certification Policy / Practice Statement***

2. Scope

The ATHEX Time-stamping Authority (ATHEX-TSA) uses public key infrastructure and trusted time sources to provide reliable, standards-based Electronic time-stamps. This ATHEX Time-stamp Policy/Practice Statement (ATHEX-TSP/PS) defines the operational and management practices of the ATHEX-TSA such that Subscribers and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

The ATHEX-TSA aims to deliver time-stamping services in accordance with the eIDAS regulation), as well as under other applicable national laws and regulations. However, ATHEX time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

The structure and contents of this ATHEX-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 Time-Stamps. The ATHEX-TSP/PS is administered and approved by the ATHEX Policy Management Authority, and should be read in conjunction with the current ATHEX Certificate Policy/Certification Practice Statement (CP/CPS).

3. References

The following documents contain provisions which are relevant to the ATHEX-TSP/PS:

[1] ETSI EN 319.412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
[2] ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
[3] ETSI EN 319.422, Electronic Signatures and Infrastructures (ESI); Time-stamping Protocol and Time-stamp Token Profiles.
[4] ETSI EN 319.421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
[5] ETSI TS 102.176.1, Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms.
[
[6] RFC 3126, Electronic Signature Formats for Long Term Electronic Signatures.
[7] RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
[8] Regulation (EU) No 910/2014 of European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (eIDAS regulation)

4. Definitions and Abbreviations

4.1 Definitions

“Certificate Policy/Certification Practice Statement” or “CP/CPS” means is a publicly available document that details the ATHEX PKI and describes the practices employed in issuing Digital Certificates.

“Coordinated Universal Time” or “UTC” means the time scale, based on the second, as defined by the International Telecommunications Radio Committee (ITU-R) TF.460-5 and roughly corresponding to Greenwich Mean Time (GMT).

“Electronic time stamp” means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

"Qualified electronic time stamp" means an electronic time stamp which meets the following requirements:
(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
(b) it is based on an accurate time source linked to Coordinated Universal Time; and
(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

“Relying party” means an entity (an individual or organisation) which relies on a Time-Stamp Token provided by the ATHEX-TSA.
“ATHEX” means HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A.
“Subscriber” means an entity (an individual or organisation) which requires the services provided by a TSA and has entered into the ATHEX-TSA Subscriber Agreement.
“Time-Stamp Authority” or “TSA” means a trusted authority which issues time-stamp tokens.
“Time-Stamp Policy/Practice Statement” or “ATHEX-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.
“Time-Stamp Token” or “TST” means a data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.
“Time-Stamp Unit” or “TSU” means a set of hardware and software which is managed as a unit and has a single private signing key active at a time.
“Trust service” means an electronic service that enhances trust and confidence in electronic transactions.
“Trust Service Provider (TSP)” means an entity which provides one or more trust services.
“UTC(k)” means a time scale realized by a laboratory “k” as defined in Bureau International des Poids et Mesures (BIPM) Circular T and kept in close agreement with UTC.
Additional definitions are provided in the CP/CPS.

4.2 Abbreviations

5. General Concepts

5.1 Time-stamping Services

Time-stamping services 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 ATHEX-TSP/PS.

ATHEX adheres to the international standards in section 3 (References) of this document to increase the trustworthiness of the time-stamping services for both Subscribers and Relying Parties.

5.2 Time-stamping Authority

The TSA is trusted by the users (i.e. Subscribers as well as Relying Parties) to issue secure TSTs. The ATHEX-TSA takes overall responsibility for the provision of time-stamping services identified in section 5.1.

The ATHEX-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.

Below is a summary of the current ATHEX TSUs and their issuers:

ATHEX TSU Subject Distinguished Name	**TSU Issuer**
CN = Athex Qualified Timestamping Authority O = Athens Stock Exchange C = GR	ATHEX Root CA G2

ATHEX operates the ATHEX-TSA as part of its public key infrastructure (PKI). The ATHEX-TSA is identified in the Digital Certificates used in the time-stamping service.

5.3 Subscribers and Relying Parties

Subscribers are entities that hold a service contract with ATHEX and have agreed to the ATHEX Time-Stamping Authority Subscriber Agreement. A Relying Party is an individual or entity relies on a TST generated an ATHEX TSA. A Relying Party may or may not be a Subscriber. Organisations that are Subscribers are responsible for the activities of their associated users and Relying Parties and are expected to inform them about the correct use of time-stamps and the conditions of the ATHEX-TSP/PS. Subscribers must use a method or software toolkit approved by ATHEX to create time-stamps, unless otherwise specifically authorised in writing by ATHEX.

5.4 TSA Policy and Practices

5.4.1 Purpose

The ATHEX Time-Stamp Policy ("what is adhered to") and the ATHEX Time-Stamp Practice Statement ("how it is adhered to") have been merged into one document, the ATHEX-TSP/PS. This ATHEX-TSP/PS specifies a time-stamp policy and practice statement to meet general requirements for trusted time-stamping services.

For additional detail on the ATHEX-TSA, refer to section 8.1 (Practice and Disclosure Statements) of this document. All ATHEX policies and practices are under the control of the ATHEX Policy Management Authority.

5.4.2 Level of Specificity

This ATHEX-TSP/PS extends the CP/CPS which regulates the operation of the ATHEX-PKI and associated non-repudiation services. The ATHEX-TSP/PS and CP/CPS are public documents and may be downloaded at: http://www.athexgroup.gr/digital-certificates-pki-regulations.

5.4.3 Approach

The ATHEX-TSP/PS establishes the general rules concerning the operation of the ATHEX-TSA. Additional internal documents define how ATHEX meets the technical, organizational, and procedural requirements identified in the ATHEX-TSP/PS. These documents may be provided only under strictly controlled conditions.

6. Time-stamp Policy

6.1 Overview

This TSP 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 ATHEX-TSA signs time-stamps using private keys that are reserved specifically for that purpose. Each TST contains an identifier to the applicable policy, and TSTs are issued with time accurate to ±1 second of UTC.

Time-stamps are requested by means of either the Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP), as described by RFC 3161.

The URL for the ATHEX-TSP/PS is: http://www.athexgroup.gr/digital-certificates-pki-regulations

6.2 Identification

The object-identifier (OID) of the ATHEX Time-Stamping Policy is:
1.3.6.1.4.1.29402.1.4.1.0.

This OID is referenced in every ATHEX-issued time-stamp, and the ATHEX-TSP/PS is available to both Subscribers and Relying Parties.

This ATHEX Time-Stamping Policy is based on the ETSI BTSP best practices policy for time-stamps (OID 0.4.0.2023.1.1).

6.3 User Community and Applicability

The user community for ATHEX time-stamps includes only Subscribers and their Relying Parties. All Subscribers are automatically deemed to be Relying Parties.
ATHEX does not provide public time-stamp services.
ATHEX time-stamps may be applied to any application requiring proof that a datum existed before a particular time.

6.4 Conformance

ATHEX references the policy identifier in section 6.2 (Identification) of this document in all time-stamps to indicate conformance with this policy. ATHEX is subject to periodic independent internal and external reviews to demonstrate that the ATHEX-TSA meets its obligations defined in section 7.1 (TSA Obligations) and has implemented appropriate controls in line with section 8 (TSA Practices). Refer to http://www.athexgroup.gr/digital-certificates-pki-regulations for a list of ATHEX′ audits and accreditations.

7. Obligations and Liability

7.1 TSA Obligations

7.1.1 General Obligations

ATHEX Limited operates the ATHEX-TSA and assumes responsibility that the requirements of section 8 (TSA Practices) of this document - as well as the provisions of eIDAS, are implemented as applicable to the selected trusted time-stamp policy.
ATHEX is a party to the mutual agreements and obligations between the TSA, Subscribers, and Relying Parties. The ATHEX-TSP/PS and CP/CPS are integral components of these agreements.

7.1.2 TSA Obligations Towards Subscribers

ATHEX undertakes the following obligations to TSA Subscribers:

• To operate in accordance with this ATHEX-TSP/PS, the CP/CPS, and other relevant operational policies and procedures.
• To ensure that TSUs maintain a minimum UTC time accuracy of ± 1 second.
• Undergo internal and external reviews to assure compliance with relevant legislation and internal ATHEX policies and procedures.
• To provide high availability access to ATHEX-TSA systems except in the case of planned technical interruptions and loss of time synchronization.

7.2 Subscriber Obligations

Subscribers must verify that the time-stamp token has been correctly signed and check that the private key used to sign the time-stamp token has not been compromised. Subscribers must use secure cryptographic functions for time-stamping requests.

Subscribers must inform its end users (including any relevant Relying Parties) about the ATHEX-TSP/PS, the CP/CPS. Subscriber obligations are also defined in the Time-Stamping Authority Subscriber Agreement.

7.3 Relying Party Obligations

Before placing any reliance on a time-stamp, subject to section 8.1.2 (TSA Disclosure Statement) of this document, relying parties must verify that the TST has been correctly signed and that the private key used to sign the TST has not been revoked. The Relying Party should take into account any limitations on usage of the time-stamp indicated by this ATHEX-TSP/PS and any other precautions prescribed in this agreement or the ATHEX Subscriber Agreement. During the TSU Certificate validity period, the status of the private key can be checked using the relevant ATHEX CRL. ATHEX CA Certificates, TSU Certificates and the related CRLS are published at www.athexgroup.gr/digital-certificates-repository If this verification takes place after the end of the validity period of the Certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421.

ETSI EN 319 421 contains some additional requirements for Qualified electronic time-stamps as per the eIDAS Regulation. ETSI EN 319 421 states:

"The relying party is expected to use a Trusted List to establish whether the time-stamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified."
ATHEX are currently operating under the transitional measures (Article 51) of the eIDAS Regulation. The public keys of the ATHEX TSUs are not currently listed on any Trusted List. The issuers of ATHEX TSUs are listed on Trusted Lists.

7.4 Liability

ATHEX undertakes to operate the ATHEX-TSA in accordance with the ATHEX-TSP/PS, the CP/CPS, and the terms of agreements with the Subscriber. ATHEX makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service. ATHEX shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of the ATHEX-TSP/PS or CP/CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss. ATHEX bears specific liability for damage to Subscribers and Relying Parties in relationship to valid qualified Digital Certificates relied upon in accordance with specific national laws and regulations.

8. Practices

The provision of a time-stamp token in response to a request is at the discretion of ATHEX depending on agreements with the Subscriber.

8.1 Practice and Disclosure Statements

8.1.1 TSA Practice Statement

This ATHEX-TSP/PS establishes the general rules concerning the operation of the ATHEX-TSA. The CP/CPS and additional internal documents define how ATHEX meets the technical, organizational, and procedural requirements identified in the ATHEX-TSP/PS.

The ATHEX-TSP/PS, TSA Disclosure Statement, and other public documents may be found at http://www.athexgroup.gr/digital-certificates-pki-regulations. Internal documents may be provided only under strictly controlled conditions.

ATHEX conducts risk assessments to evaluate threats and to determine the necessary security controls and operational procedures.
The ATHEX-TSP/PS identify the obligations of external organizations supporting the TSA services including the applicable policies and practices.
The ATHEX Policy Management Authority has responsibility for maintaining and approving all ATHEX-PKI policies and practices according to the terms of section 1.5 (Policy Administration) of the CP/CPS. ATHEX management has responsibility to ensure that the practices are properly implemented.

8.1.2 TSA Disclosure Statement

This document discloses to all Subscribers and potential Relying Parties the terms and conditions regarding use of ATHEX time-stamping services. Elements of the ATHEX-TSA Disclosure Statement are below:

• Each time-stamp token issued by the ATHEX-TSA contains the policy object-identifier contained in section 6.2 (Identification) of this document.
• The cryptographic algorithms and key lengths used by the ATHEX-TSA comply with ETSI EN 319 422 and are currently:
- Acceptable Time Stamp request Hashes: SHA-256, SHA-384, SHA-512
- Signature: sha256WithRSAEncryption (2048 bit key)

• The ATHEX TSUs have a validity period of up to ten years.
•. ATHEX will post public notice on its website if it determines that cryptographic algorithms and key lengths used in the ATHEX-PKI are no longer considered secure.
• The ATHEX-TSA assures time with ±1 second of a trusted UTC time source. If a trusted UTC time source can not be acquired the time stamp will not be issued.

• Use of the ATHEX TSA may be limited to Certificate Holders of a valid ATHEX Digital Certificate.
• Subscriber obligations are described in section 7.2 (Subscriber Obligations) of this document.
• Relying Party obligations are described in section 7.3 (Relying Party Obligations) of this document.
• ATHEX maintains secure records concerning the operation of the ATHEX-TSA.
• ATHEX makes no express or implied representations or warranties relating to the availability or accuracy of the ATHEX-TSA. ATHEX bears specific liability for damage to Subscribers and Relying Parties in relationship to valid Digital Certificates relied upon in accordance with specific national laws and regulations.

• ATHEX may charge fees for the services provided by the ATHEX TSA.
• The applicable legal system and dispute resolution procedures relating to the ATHEX-TSA are dealt with in the underlying Subscriber Agreement.
• TSA event logs are retained for 11 years in accordance with the retention period for audit logs in the CP/CPS.

8.2 Key Management Life Cycle

8.2.1 TSA Key Generation

ATHEX generates the cryptographic keys used in its TSA services under M of N control by authorised personnel in a secure physical environment. The personnel authorized to carry out this function shall be limited to those requiring to do so under ATHEX practices. The keys are generated within TSU hardware security modules that are certified to FIPS 140-2 Level 3. Algorithms and key size are described in section 8.1.2 (TSA Disclosure) of this document.

8.2.2 TSU Private Key Protection

ATHEX takes specific steps to ensure that TSU private keys remain confidential and maintain their integrity. These include use of HSMs certified to FIPS 140-2 Level 3 or higher to hold and sign with the keys. When TSU private keys are backed up, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The personnel authorized to carry out this function shall be limited to those requiring to do so under ATHEX practices. .

8.2.3 TSU Public Key Distribution

ATHEX TSU Public Keys are made available in a Digital Certificate. Refer to the "ATHEX Timestamping Authority" section of the following ATHEX web page for a list of ATHEX TSUs http://www.athexgroup.gr/digital-certificates-repository

8.2.4 Rekeying TSU's Key

TSU private signing keys are replaced before the end of their validity period, (i.e., when the algorithm or key size is determined to be vulnerable).

8.2.5 End of TSU Key Life Cycle

TSU private signing keys are replaced upon their expiration. The TSU rejects any attempt to issue time-stamps once a private key has expired.

8.2.6 Life Cycle Management of the Cryptographic Module used to Sign Time-stamps

ATHEX has in place procedures to ensure that hardware security modules intended for non-repudiation services are not tampered with in shipment or storage. Acceptance testing is performed to verify that cryptographic hardware is performing correctly. Installation and activation is performed only by M of N authorised personnel in trusted roles, and the devices operate in a physically secured environment. Private keys are erased from modules when they are removed from service in according with the manufacturer's instructions.

8.3 Time-stamping

8.3.1 Time-stamp Token

ATHEX has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. In line with the protocols referenced in section 3 of this document, each TST includes:

• a representation (e.g., hash value) of the datum being time-stamped as provided by the requestor;
• a unique serial number that can be used to both order TSTs and to identify specific TSTs;
• an identifier for the time-stamp policy;

• the time calibrated to within 1 second of UTC, traceable to a UTC(k) source;
• an electronic signature generated using a key used exclusively for time-stamping; and
• an identifier for the TSA and the TSU.

The ATHEX TSUs maintain audit logs for all calibrations against the UTC(k) references.

8.3.2 Clock Synchronization with UTC

The ATHEX TSA provides time with ±1 second of UTC by calibration with multiple independent time sources including GPS and National Measurement Institutes providing UTC(k) time.
The ATHEX TSUs have technical measures in place to ensure that their time is synchronized with UTC within the declared accuracy. Audit and calibration records are maintained by ATHEX. The ATHEX TSA ensures that clock synchronisation is maintained when a leap second occurs as notified by the appropriate body.
TSU clocks are protected and are recalibrated at least twice daily against the reference UTC time source. TSU clocks are also able to monitor time drift outside preset boundaries and request additional recalibrations as needed. If the TSU clock drifts outside the declared accuracy, and recalibration fails, the TSA will not issue time-stamps until correct time is restored. Manual administration of the TSU clock requires M of N authorized personnel.

8.4 TSA Management and Operation

8.4.1 Security Management

ATHEX has an active security management program designed to document, implement, and maintain adequate security provisions for the ATHEX-PKI according to best practice and the requirements of relevant standards. The ATHEX Policy Management Authority is the body responsible for setting policies and practices for the overall PKI and is therefore responsible for defining the ATHEX Information Security Policy.

8.4.2 Asset Classification and Management

In order to ensure that information and other assets receive appropriate security treatment, ATHEX maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

8.4.3 Personnel Security

To enhance the trustworthiness of its PKI operations, ATHEX maintains appropriate personnel practices fulfilling security best practice and the requirements of relevant standards.

In particular:

a) ATHEX employs personnel whom possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.
b) Security roles and responsibilities are summarized in job descriptions. Trusted roles, on which the security of the ATHEX operation is dependent, are clearly identified in the CP/CPS.
c) ATHEX personnel shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.
d) Personnel shall exercise administrative and management procedures and processes that are in line with the ATHEX Information Security Policy

The following additional controls shall be applied to time-stamping management:

e) Managerial personnel shall be employed who possess:

• knowledge of time-stamping technology;
• knowledge of digital signature technology;
• knowledge of mechanisms for calibration or synchronization the TSU clocks with UTC;
• familiarity with security procedures for personnel with security responsibilities; and
• experience with information security and risk assessment.

f) All ATHEX personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSA operations.
g) Trusted roles include roles that involve the following responsibilities:
• Security Officers: Overall responsibility for administering the implementation of the security practices.
• System Administrators: Authorized to install, configure and maintain the TSA trustworthy systems for time-stamping management.

• System Operators: Responsible for operating the TSA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.
• System Auditors: Authorized to view archives and audit logs of the TSA trustworthy systems.

h) TSA personnel shall be formally appointed to trusted roles by senior management responsible for security.

i) The TSA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

8.4.4 Physical and Environmental Security

The ATHEX-TSA operates from a resilient and secure hosting facility in accordance with the relevant provisions of ETSI EN 319 421.

In particular:

a) For both the time-stamping provision and the time-stamping management:

• physical access to facilities concerned with time-stamping services is limited to properly authorised individuals;
• controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities; and
• controls are implemented to avoid compromise or theft of information and information processing facilities.

b) Access controls are applied to the cryptographic modules to meet the requirements of security of cryptographic modules as identified in clauses 8.2.1 and 8.2.2.
c) The following additional controls have been applied to time-stamping management:

• The time-stamping management facilities are operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

• Physical protection is achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the time-stamping management. Any parts of the premises shared with other organizations are outside this perimeter.
• Physical and environmental security controls are implemented to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The
ATHEX Information Security Policy addresses the physical access control, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), protection against theft, breaking and entering and disaster recovery.

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

8.4.5 Operations Management

The ATHEX-PKI maintains extensive operational controls in compliance with ETSI EN 319 421. This documentation is not publicly available. ATHEX undergoes internal and external reviews of compliance and the effectiveness of these controls. The operations management controls for the ATHEX-TSA are incorporated within the overall ATHEX-PKI operations management controls.

8.4.6 System Access Management

ATHEX maintains appropriate physical and logical access controls for affected facilities, hardware, systems, and information. The systems access management controls for the ATHEX-TSA are incorporated within the overall ATHEX-PKI systems access management controls.

8.4.7 Trustworthy Systems Deployment and Maintenance

The ATHEX-TSA uses trustworthy systems that are protected against modification. The systems deployment and maintenance controls for the ATHEX-TSA are incorporated within the overall ATHEX-PKI systems deployment and maintenance controls.

8.4.8 Compromise of TSA Services

In the event of compromise of a TSU private key, ATHEX will revoke the relevant Certificate and add it to the ATHEX CRL. The TSU will not issue time-stamps if its private key is not valid.

The TSU will not issue time-stamps if its clock is outside the declared accuracy from reference UTC, until steps are taken to restore calibration of time. As described in section 8.4.11 (Recording of Information Concerning Operation of Time-stamping Services) of this document, the ATHEX-TSA maintains audit trails to discriminate between genuine and backdated tokens.

8.4.9 TSA Termination

In the case of termination of the ATHEX-TSA, ATHEX will at a minimum inform Subscribers, revoking TSU Certificates, and transferring obligations to a reliable party for maintaining event log and audit archives as well as access to private keys.

8.4.10 Compliance with Legal Requirements

The ATHEX-TSA complies with applicable legal requirements, as well as the requirements of the European data protection Directive [Dir 95/46/EC]. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Information contributed by users to the TSA shall be completely protected from disclosure unless with their agreement or by court order or other legal requirement.

8.4.11 Recording of Information Concerning Operation of Time-stamping Services

ATHEX maintains records of all relevant information concerning the operation of the ATHEX-TSA for a period of 11 years, in accordance with the ATHEX business practices. Records are time-stamped to protect data integrity and moved to a protected server for storage and subsequent archiving. No personal data relating to Subscribers is transmitted between jurisdictions.

Records concerning the operation of time-stamping services are available at the request of Subscribers or if required by court order or other legal requirement. The ATHEX-TSA maintains records, including precise time, of:

• Time-stamp requests and created time-stamps
• Events related to TSA administration (including Certificate management, key management, and clock synchronisation).

• Events relating to the life-cycle of TSU keys and Certificates.

8.5 Organisational

The ATHEX organisational structure, policies, procedures and controls apply to the ATHEX-TSA. ATHEX organisational procedures fulfil the standards in section 2 (References) of this document, in particular ETSI EN 319 421. Important policy and practice documents for the ATHEX-PKI are available at http://www.athexgroup.gr/digital-certificates-pki-regulations.

8.6 Compliance with Applicable Law

Subscribers and Relying Parties acknowledge and agree to use Certificates in compliance with all applicable laws and regulations, HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. may refuse to issue or may revoke Certificates if in the reasonable opinion of HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. such issuance or the continued use of such Certificates would violate applicable laws and regulations.

8.7 Miscellaneous Provisions

8.7.1 Entire Agreement

Not Applicable

8.7.2 Assignment

8.7.3 Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

8.7.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not Applicable

8.7.5 Force Majeure

HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A..

8.8 Other Provisions

Not Applicable.