Athens Stock Exchange, Qualified Trust Service Provider

ATHEX PKI Disclosure Statement

Version 1.5 - 30/05/2024

Contents

Revision History

Issue	Date	Changes in this Revision
1.0	22/07/2019	Initial version and Release
1.2	13/08/2019	Several corrections, clarifications and enrichments according to external audit comments.
1.3	26/03/2021	Enriched with CA/Browser Requirements
1.4	13/12/2021	Several corrections in order to be aligned with the CA/Browser Forum Requirements,
1.5	30/05/2024	Several corrections in order to be aligned with the CP/CPS v1.8.6

1 Introduction

Athens Stock Exchange (hereafter referred to as ATHEX) acts as Qualified Trust Service Provider (QTSP) which operates its own Root and Subordinate Certification Authorities (CA) and also its own Time-Stamping Authority (TSA).

This Disclosure Statement document is a supplemental and simplified instrument of disclosure and notice of ATHEX TSP. This document is not intended to replace or add any policy or practice that is described in ATHEX RSA Root CA R2 CP/CPS. ATHEX CP/CPS takes precedence over this Disclosure Statement.

2 ATHEX TSP contact info

The organization administering this PKI Disclosure Statement is ATHENS STOCK EXCHANGE S.A..
Inquiries should be addressed as follows:

ATHENS STOCK EXCHANGE S.A.
Digital Certificates Services (PKI-CA)
110 Athinon Ave.
GR 104 42, Athens
GREECE

Address inquiries about the PKI Disclosure Statement and CP/CPS to:

pkica-services@athexgroup.gr
Tel +30 210 336 6300

For revocation reporting or any other issue related to certificates the email address and phone number are:

pkica-services@athexgroup.gr
Tel +30 695 100 7878

PKI participants can find additional documents at the following URL:
https://repo.athexgroup.gr/

3 Certificate Types, Validation Procedures and Usage

All ATHEX Certificates have a policy object identifier (OID) which identifies their use.

ATHEX PKI issues Qualified Certificates according to ETSI EN 319 411-2 and eIDAS Regulation (EU No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market). Furthermore, ATHEX PKI provides either local or remote Qualified Signature Creation Devices (QSCD), used by Certificate Holder for signing.

3.1 Certificate Types

Certificate type	**ATHEX Certificate Policy OID 1.3.6.1.4.1.29402.1.5** {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) HELEX(29402) PKI-Organization-Unit(1) RSA-Root-CA-R2(5)}	**End entity Certificate asserts adherence to and compliance with:**
Server Authentication - EU Qualified OV Website	1.3.6.1.4.1.29402.1.5.100.1.4 {ServerAuth(100) Validation-Type(1) QNCP-w(4)}	• CA/Browser Extended Validation (OID 2.23.140.1.2.2) • ETSI 319 411-2, QNCP-w (OID 0.4.0.194112.1.5)

Server Authentication - EU Qualified OV Website supporting PSD2	1.3.6.1.4.1.29402.1.5.100.1.5 {ServerAuth(100) Validation-Type(1) QCP-w-PSD2(5)}	• CA/Browser Extended Validation (OID 2.23.140.1.2.2) • ETSI TS 119 495, QCP-w-psd2 (OID 0.4.0.19495.3.1)
Document Signing – Qualified Certificates for Advanced Electronic Signatures	1.3.6.1.4.1.29402.1.5.200.1.1 {DocumentSigning(200) Validation-Type(1) QCP-n(1)}	• ETSI 319 411-2, QCP-n, (OID 0.4.0.194112.1.0)
Document Signing – Qualified Certificates for Qualified Electronic Signatures with QSCD	1.3.6.1.4.1.29402.1.5.200.1.2 {DocumentSigning(200) Validation-Type(1) QCP-n-qscd(2)}	• ETSI 319 411-2, QCP-n-qscd (OID 0.4.0.194112.1.2)
Document Signing – Qualified Certificates for Advanced Electronic Seals	1.3.6.1.4.1.29402.1.5.200.1.3 {DocumentSigning(200) Validation-Type(1) QCP-l(3)}	• ETSI 319 411-2, QCP-l (OID 0.4.0.194112.1.1)
Document Signing – Qualified Certificates for Qualified Electronic Seals with QSCD	1.3.6.1.4.1.29402.1.5.200.1.4 {DocumentSigning(200) Validation-Type(1) QCP-l-qscd(4)}	• ETSI 319 411-2, QCP-l-qscd (OID 0.4.0.194112.1.3)
Document Signing – Qualified Certificates for Advanced Electronic Seal supporting PSD2 transaction	1.3.6.1.4.1.29402.1.5.200.1.5 {DocumentSigning(200) Validation-Type(1) QCP-l-PSD2(5)}	• ETSI TS 119 495, QCP-l supporting PSD2 (OID 0.4.0.194112.1.1)
Document Signing – Qualified Certificates for remote Qualified Electronic Signatures with QSCD	1.3.6.1.4.1.29402.1.5.200.1.6 {DocumentSigning(200) Validation-Type(1) QCP-n-qscd remote(6)}	• ETSI 319 411-2, QCP-n-qscd (OID 0.4.0.194112.1.2)
Document Signing – Qualified Certificates for Qualified remote Electronic Seals with QSCD	1.3.6.1.4.1.29402.1.5.200.1.7 {DocumentSigning(200) Validation-Type(1) QCP-l-qscd remote(7)}	• ETSI 319 411-2, QCP-l-qscd (OID 0.4.0.194112.1.3)
General – Simple Client	1.3.6.1.4.1.29402.1.5.400.2.1	• ETSI EN 319 411-1 LCP (OID 0.4.0.2042.1.3)

Authentication		• Individual Validation (IV-NCP) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.1 • Individual Validation (IV-NCP+) compatible with ETSI EN 319 411-1 0.4.0.2042.1.2
General – Organizational Client Authentication	1.3.6.1.4.1.29402.1.5.400.2.1	• ETSI EN 319 411-1 LCP (OID 0.4.0.2042.1.3) • Organization Validation (OV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 • Organization Validation (OV-NCP+) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
Qualified Timestamping	1.3.6.1.4.1.29402.1.5.500.1.1 {Timestamping(500) Validation-Type(1) QTimestamp(1)}	• ETSI EN 319 421 (OID 0.4.0.2023.1.1)

3.2 Certificate Usage

Certificate Type	Key Usages
Server Authentication - EU Qualified OV Website	KU: Digital Signature, Key Encipherment EKU: Server Authentication, Client Authentication
Server Authentication - EU Qualified OV Website	KU: Digital Signature, Key Encipherment EKU: Server Authentication, Client Authentication
Document Signing – Qualified Certificates for Advanced Electronic Signatures	KU: Non-Repudiation EKU: Document Signing, Email Protection (optional)
Document Signing – Qualified Certificates for Qualified Electronic Signatures with QSCD	KU: Non-Repudiation EKU: Document Signing, Email Protection (optional)
Document Signing – Qualified Certificates for Advanced Electronic Seals	KU: Non-Repudiation EKU: Document Signing, Email Protection (optional)
Document Signing – Qualified Certificates for Qualified Electronic Seals with QSCD	KU: Non-Repudiation EKU: Document Signing, Email Protection (optional)
Document Signing – Qualified Certificates for	KU: Non-Repudiation EKU: Document Signing, Email Protection (optional)

Advanced Electronic Seal supporting PSD2 transaction	
Document Signing – Qualified Certificates for remote Qualified Electronic Signatures with QSCD	KU: Non-Repudiation EKU: Document Signing, Email Protection (optional)
Document Signing – Qualified Certificates for Qualified remote Electronic Seals with QSCD	KU: Non-Repudiation EKU: Document Signing, Email Protection (optional)
General – Simple Client Authentication	KU: Digital Signature, Key Encipherment EKU: Client Authentication
General – Organizational Client Authentication	KU: Digital Signature, Key Encipherment EKU: Client Authentication
Qualified Timestamping	KU: Digital Signature, Non-Repudiation EKU: Time Stamping

3.3 Certificate Procedures

3.3.1 ATHEX EU Qualified OV Certificates for Website Authentication

Purpose

EU Qualified OV Website Certificates

Certificates are aimed to support website authentication based on EU qualified website certificates (QNCP-w).

In addition, EU Qualified OV Website Certificates offer at a minimum the "Organization Validated" level of assurance as defined by the CA/Browser Forum and the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates used in support of websites authentication:

- The requirements for QNCP-w include all the NCP requirements for certificates issued to natural or legal persons, plus either the IVCP or the OVCP requirements, plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014

EU Qualified OV Website Certificates for PSD2 (or QCP-w-psd2)

EU Qualified OV Website Certificates for PSD2 are EU Qualified OV Website Certificates used only for Open Banking.

Commitment to Comply with Standards

EU Qualified OV Website Certificates conform to the current version of the ETSI 319 411-2 standard and to the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document, the ETSI standard and Baseline Requirements, the Baseline Requirements take precedence over this document and ETSI standard.

Identity Validation Process

Authentication of Organization

Identity validation procedures for these Digital Certificates meet the relevant requirements at Section 6.2.2 of ETSI EN 319 411-2 and the Regulation (EU) No 910/2014.

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

a. by the physical presence of an authorized representative of the legal person; or
b. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which ATHEX can prove the equivalence according to Article 24 paragraph 1 of the Regulation (EU) No 910/2014; or
c. by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a); or
d. remotely using video conference or asynchronous video with final human decision.

If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence shall be provided of:

a. Full name of the organizational entity (private organization, government entity, business entity or non-commercial entity) consistent with the national or other applicable identification practices.
b. When applicable, the association between the legal person and the other organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices.

For the EU Qualified OV Website Certificates, the identity of the subscriber and its link with the domain name to be certified and, if applicable, any specific attributes of the person. Furthermore, the organization's address is verified in the same manner as it is for OV Client Authentication and OV S/MIME certificates.

Only for the EU Qualified OV Website certificates supporting PSD2 transaction (i.e., QCP-w-psd2), the specific PSD2 attributes at public or EBA register are verified.

3.3.2 ATHEX Qualified Certificate for eSignature, eSeal and eSeal supporting PSD2

Purpose

Qualified eSignature (QCP-n-qscd)
Certificates issued under these requirements are aimed to support qualified electronic signatures such as defined in article 3 (12) of the Regulation (EU) No 910/2014,

Qualified eSeal (QCP-l-qscd)
Certificates issued under these requirements are aimed to support qualified electronic seals such as defined in article 3 (27) of the Regulation (EU) No 910/2014.

Advanced eSignatures based on a qualified Certificate (QCP-n)
Certificates issued under these requirements are aimed to support the advanced electronic signatures based on a qualified Certificate defined in articles 26 and 27 of the Regulation (EU) No 910/2014,

Advanced eSeals based on a qualified Certificate (QCP-l)
Certificates issued under these requirements are aimed to support the advanced electronic seals based on a qualified Certificate defined in articles 36 and 37 of the Regulation (EU) No 910/2014,

Qualified eSeal for supporting PSD2 transaction
A Qualified eSeal Certificate for supporting PSD2 transaction allows the Relying Party to validate the identity of the subject of the Certificate, as well as the authenticity and integrity of the sealed data, and also prove it to third parties. The electronic seal provides strong evidence, capable of having legal effect, that given data is originated by the legal entity identified in the Certificate.

Commitment to Comply with Standards

The ATHEX Qualified and Advanced Certificates for eSignature and eSeal from ATHEX RSA Root CA R2 conform to the current version of the ETSI 319 411-2 standard. In the event of any inconsistency between this document and standard, the standard takes precedence over this document.

Who can apply

ATHEX Qualified or Advance eSignatures are issued only to natural persons. Note that the applicant can be natural or legal entity.

ATHEX Qualified or Advance eSeals are issued only to legal persons.

ATHEX Qualified eSeal for supporting PSD2 transaction are issued only to PSPs registered by NCA.

Identity Validation Process

Authentication of Organization

Identity validation procedures for these Digital Certificates meet the relevant requirements at Section 6.2.2 of ETSI EN 319 411-2 and the Regulation (EU) No 910/2014.

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

a. by the physical presence of an authorized representative of the legal person; or
b. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which ATHEX can prove the equivalence according to Article 24 paragraph 1 of the Regulation (EU) No 910/2014; or
c. by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a); or
d. remotely using video conference or asynchronous video with final human decision.

If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence shall be provided of:

a. Full name of the organizational entity (private organization, government entity, business entity or non-commercial entity) consistent with the national or other applicable identification practices.
b. When applicable, the association between the legal person and the other organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices.

Authentication of Individual Identity

Identity validation procedures for these Digital Certificates meet the relevant requirements at Section 6.2.2 of ETSI EN 319 411-2 and the Regulation (EU) No 910/2014.

The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:

a. by the physical presence of the natural person; or
b. using identity verification methods which provide equivalent assurance in terms of reliability to the physical presence and for which ATHEX can prove the equivalence according to Article 24 paragraph 1 of the Regulation (EU) No 910/2014; or
c. by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a); or
d. remotely using video conference or asynchronous video with final human decision.

If the Subject is a natural person, evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national

identification practices); and

- Date and place of birth, reference to a nationally recognized identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence shall be provided of:

- full name (including surname and given names, consistently with the national or other applicable identification practices) of the subject;
- date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which can be used to, as far as possible, distinguish the person from others with the same name;
- full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber);
- any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity identified in association with the legal person, consistent with the national or other applicable identification practices;
- affiliation of the natural person to the legal person consistent with national or other applicable identification practices;
- when applicable, the association between the legal person and any organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices; and
- approval by the legal person and the natural person that the subject attributes also identify such organization.

If the e-mail address is included into the Digital Certificate, ATHEX shall take reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate. Specifically, ATHEX requests the Applicant to enter the email address at the initial certificate request form and a verification email is sent back with a Random Value. Once the Applicant returns this Random Value back to ATHEX, the email address is validated.

3.3.3 ATHEX Client Authentication

Purpose

A Certificate intended to be issued to individuals (as well as devices not acting in the capacity of a server), solely for the purpose of identifying that the holder of the Private Key is in fact the individual or device named in the Certificate's subject field.

Commitment to Comply with Guidelines

The Client Authentication Certificates from ATHEX Root CA G4 conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org, In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Identity Validation Process

Authentication of Organization

ATHEX verifies the identity and address of the organization and that the address is the Applicant's address of existence or operation. ATHEX verifies the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

- A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
- A third party database that is periodically updated and considered a Reliable Data Source;

- A site visit by ATHEX or a third party who is acting as an agent for the CA; or
- An Attestation Letter.

Authentication of Individual Identity

The initial application for the client authentication Certificate shall be requested by employees of an organization such that they meet the requirements of section 3.2.2 Authentication of Organization and Domain Identity. The Applicant's employer is required to demonstrate the validity of the Applicant employee or contractor legal name and determine that an Applicant is an employee or contractor of the organization through correlation with Human Resources and contractor records before the issuance of the certificate.

Acceptable means of correlation shall include, but is not limited to the following:

- ATHEX verifies the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). ATHEX SHALL inspect the copy for any indication of alteration or falsification.
- ATHEX verifies the Applicant's address using a form of identification that ATHEX determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. ATHEX MAY rely on the same government-issued ID that was used to verify the Applicant's name.
- ATHEX verifies the certificate request with the Applicant using a Reliable Method of Communication.

3.3.4 ATHEX Qualified Timestamping Certificates

Purpose

ATHEX Time-Stamp Certificate is used for trusted time-stamping services.

4 Reliance Limits

Refer to Section 9.7 and 9.8 of ATHEX RSA Root CA R2 CP/CPS for reliance limits.

Audit logs are retained for at least two years.

ATHEX Timestamp accuracy is one (1) second. If it is detected that the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC, TSU shall stop timestamp issuance.

5 Obligation of Subscribers

Each Applicant must enter into a Subscriber Agreement with ATHEX which specifically names both the Applicant and the individual Contract Signer signing the Agreement on the Applicant's behalf, and contains provisions imposing on the Applicant the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to ATHEX, both in the Certificate request and as otherwise requested by ATHEX in connection with the issuance of the Certificate(s) to be supplied by ATHEX;
- Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- Use of Certificate: An obligation and warranty to install the Certificate only on servers that are

accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;

- Reporting and Revocation: An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- Responsiveness: An obligation to respond to ATHEX's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- Acknowledgment and Acceptance: An acknowledgment and acceptance that ATHEX is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if ATHEX discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

In addition to the above, the subscriber's obligations include:

1. an obligation to provide ATHEX with accurate and complete information in accordance with the requirements of the ETSI 319 411-1, particularly with regards to registration;
2. an obligation for the key pair to be only used in accordance with any limitations notified to the subscriber;
3. prohibition of unauthorized use of the subject's private key;
4. if the subscriber generates the subject's keys:
    - an obligation or recommendation to generate the subject keys using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP; and
    - an obligation or recommendation to use key length and algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP during the validity time of the Certificate;
5. an obligation to notify ATHEX without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the Certificate:
    - the subject's private key has been lost, stolen, potentially compromised;
    - control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
    - inaccuracy or changes to the Certificate content, as notified to the subscriber;
6. an obligation to only use the subject's private key(s) for cryptographic functions within the secure cryptographic device;
7. an obligation, following compromise of the subject's private key, to immediately and permanently discontinue the use of this key, except for key decipherment; and
8. an obligation, in the case of being informed that the subject's Certificate has been revoked, or that ATHEX has been compromised, to ensure that the private key is no longer used by the subject.

If the subject and subscriber are separate entities, the subject's obligations shall comply with the above points 2, 3, 5, 6, 7 and 8.

6 Certificate status checking obligations of relying parties

A Relying Party is an individual or entity that acts in reliance of valid Certificates issued by ATHEX in accordance with the terms and conditions of ATHEX RSA Root CA R2 CP/CPS and all applicable laws and regulations.

Before relying on or using a ATHEX Certificate, Relying Parties are advised to: (i) read the CP/CPS in its entirety; (ii) visit the ATHEX Repository to determine whether the Certificate has expired or been

revoked and to find out more information concerning the Certificate; and (iii) make their own judgment as to whether and to what degree to rely upon a Certificate.

The status of Certificates is published in a Certificate Revocation List located at:
http://crl.athexgroup.gr
Furthermore, it can be retrieved via Online Certificate Status Protocol Checking
http://ocsp.athexgroup.gr/ATHEXRSARootCAR2.

7 Limited warranty and disclaimer/Limitation of liability

7.1 CA Representations and Warranties

By issuing a Digital Certificate, ATHEX represents and warrants that, during the period when the Digital Certificate is valid, ATHEX has complied with this CP/CPS in issuing and managing the Digital Certificate to ATHEX PKI Participants (Subscriber, Relying Parties and Application Software Suppliers).

ATHEX performs its functions by:

- Providing the operational infrastructure and certification services, including the Repository, OCSP responders and CRLs;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation;
- Maintaining this CP/CPS and enforcing the practices described within it and in all relevant collateral documentation;
- Retaining overall responsibility for conformance with the procedures prescribed in its information security policy; and
- Investigating any suspected compromise which may threaten the integrity of the ATHEX PKI.

ATHEX hereby warrants (i) it has taken reasonable steps to verify that the information contained in any Certificate is accurate at the time of issue (ii) Certificates shall be revoked if ATHEX believes or is notified that the contents of the Certificate are no longer accurate, or that the key associated with a Certificate has been compromised in any way. Furthermore, ATHEX ensures the access to the private keys on the Remote QSCD to the authorized Subscriber of the keys and the proper management and compliance of the Remote QSCD.

When ATHEX issues a Certificate, ATHEX warranties to ATHEX PKI Participants, during the period while the Certificate is Valid, that ATHEX has followed the requirements of the Guidelines, the Standards and its Regulations in issuing and managing the Certificate and in verifying the accuracy of the information contained in the Certificate.

The ATHEX Certificate Warranties specifically include, but are not limited to, the following:

- Right to Use Domain Name: That, at the time of issuance, ATHEX (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

- Authorization for Certificate: That, at the time of issuance, ATHEX (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

- Accuracy of Information: That, at the time of issuance, ATHEX (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in ATHEX's Certificate Policy and/or Certification Practice Statement;

- No Misleading Information: That, at the time of issuance, ATHEX (i) followed the procedure when issuing the Certificate; and (ii) accurately described the procedure in the ATHEX's

Certificate Policy and/or Certification Practice Statement;

- Identity of Applicant: That, if the Certificate contains Subject Identity Information, ATHEX (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the ATHEX's Certificate Policy and/or Certification Practice Statement;
- Subscriber Agreement: That, if ATHEX and Subscriber are not Affiliated, the Subscriber and ATHEX are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if ATHEX and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- Status: That ATHEX maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all Certificates; and
- Revocation: That ATHEX will revoke the Certificate for any of the reasons specified in these Requirements.

In lieu of the warranties set forth above, ATHEX has followed its Certification Practice Statement in issuing and managing the Certificate and in verifying the accuracy of the information contained in the EU Qualified OV Website Certificate.

ATHEX makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

7.2 Disclaimers of Warranties

Where despite the above disclaimers and the limitations to the guarantees it offers, ATHEX becomes liable to any third party or Subscriber for a genuine error or inaction, condition violation, malfunction or inaccuracy in the services it offers, the maximum limit of liability assumed by ATHEX and the entire network of its services for each Certificate is outlined in the following Section.

7.3 Limitation of Liability

As regards the above, ATHEX shall not be liable to any injured third party where there has been no fault on the part of ATHEX with regards to the malfunction or failure that caused the damage to the third party or where ATHEX has acted in compliance with the provisions of the Certificate Practice Statement and the Policy of its Certificate or where the injured party themselves or such other party —outside the ATHEX services provision network— has caused the damage by violating the terms and conditions of the respective Certificate Policy or has caused the damage through an incorrect, inappropriate or illegal act.

ATHEX shall also not be liable (and thus neither shall be the third parties working with it in providing certification services) for any malfunctioning of its services in cases of force majeure, including but not limited to earthquakes, floods, fires, etc., including cases of black-out, problems in network communication and in general in cases of all outside obstacles that may prevent the smooth delivery of services and are not attributed to it.

Unless otherwise provided for in this CP/CPS, ATHEX shall not guarantee nor be liable for the appropriateness, quality, lack of error or fitness for a particular purpose, of all related services, products and documentation provided or offered by it. The services and products offered to its Subscribers and third parties are provided by ATHEX and its network on an "as-is" basis and responsibility about whether they are suitable for the desired purpose or whether the subscriber should or should not rely on them shall lie exclusively with the ATHEX Subscriber or the third party who decides to rely on them.

To the extent ATHEX has issued and managed the certificate in accordance with the Baseline Requirements and this CP/CPS, ATHEX shall not be liable to the subscriber, Relying Party or any third parties for any losses suffered as a result of use or reliance on such certificate. Otherwise, ATHEX liability to the subscriber, Relying Party or any third parties for any such losses shall in no event exceed two thousand euro (2.000€) per certificate, for EU Qualified Certificate (in accordance with Regulation EU No 910/2014) and a total maximum of claims of 1.000.000€, regardless of the nature of the liability and the type, amount or extent of any damages suffered.

Lastly, ATHEX shall not be liable for any indirect or consequential damages, criminal or disciplinary action or punishment, foregone profits or any other indirect consequences suffered by any party on the occasion of the use of or his reliance on a certain Certificate.

7.4 Force Majeure

ATHEX 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 ATHEX. See also Section 9.8 of the CP/CPS.

7.5 Insurance Coverage

ATHEX currently maintains commercially reasonable insurance.

ATHEX SHALL maintain the following insurance related to their respective performance and obligations:

(A) Commercial General Liability insurance (occurrence form) with policy limits of at least two million EURO in coverage; and

(B) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million EURO in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EU Qualified OV Website Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Such insurance MUST be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

ATHEX MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that it has at least five hundred million EURO in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

8 Applicable agreements, CPS, CP

The following documents are available online at http://repo.athexgroup.gr/ :

- Certificate Policy/Certificate Practice Statement
- Subscriber Agreements

9 Privacy Policy

9.1 Privacy Plan

ATHEX implements the General Data Protection Regulation ("GDPR"), Regulation (EU) 2016/689 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

In any case the Subscriber is entitled to contact the Data Protection Officer of ATHEX to make use of his

rights of information and access.

9.2 Information Treated as Private

Personal information obtained from an Applicant during the application or identity verification process is considered private information if this information is not included in the issued Digital Certificate, Digital Certificate directories or online Repositories.

9.3 Information Not Deemed Private

The contents of Digital Certificates and Certificate Revocation List are deemed not private. The CP/CPS is a public document.

9.4 Responsibility to Protect Private Information

ATHEX will not provide any private personal information to any third party for any reason, unless compelled to do so by law or competent regulatory authority.

9.5 Notice and Consent to Use Private Information

In the course of accepting a Certificate, Applicants have agreed to allow their personal data submitted in the course of registration to be processed by ATHEX, and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly accessible directories and be communicated to others.

9.6 Disclosure Pursuant to Judicial or Administrative Process

ATHEX reserves the right to disclose personal information if reasonably believes that:

- disclosure is required by law or regulation, or
- disclosure is necessary in response to judicial, administrative, or other legal process.

10 Refund policy

ATHEX will refund fees and will revoke a Certificate upon request by the Subscriber:

- within seven days of Certificate activation, when the Certificate is provided to Subscriber in suspended status; or
- within seven days of Certificate issuance, when the Certificate is not provided to Subscriber in suspended status.

To request a refund, please contact the person who is referred by section 2.

11 Applicable law, complaints and dispute resolution

11.1 Governing Law

Greek law shall be the applicable law and it is agreed that disputes related to the provision of the digital Certificates services described herein shall be subject to the exclusive jurisdiction of the Courts of Athens.

11.2 Dispute Resolution Provisions

Through the Complaint Handling and Dispute Resolution Committee (CHDRC), ATHEX offers its subscribers and third parties that rely on its Certificates reliable (both legally and technically) information and clarifications on the data of the relevant Certificates and tips for interpreting and resolving potential disputes related to certification and use of its electronic Certificates.

It consists of ATHEX'S executives and specialized technical and legal advisers and forwards queries to ATHEX'S PMC when in doubt.

The CHDRC meets whenever deemed necessary by circumstances, with the competency of checking compliance of the Certification Practice Statement and the handling of any complaints and/or the resolution of any differences related to ATHEX TSP.

The CHDRC has full access to the records and logs of ATHEX TSP and prepares an annual report addressed to the PMC with its activities and conclusions on an annual basis.

Should interested parties wish to use the mediation service of the CHDSC, they must submit their dispute to the Committee in writing, and the Committee must respond in writing within 30 days at the latest from the time it received the written request for mediation.

Where the dispute is turned against ATHEX or a third party member of ATHEX'S network in the provision of certification services (complaint), the Committee shall not be obligated to reply to the request of the interested party where the latter has initiated court or any other proceedings against them before the end of the aforementioned 30-day period and where appropriate, forwards such complaints to law enforcement.

These services must be provided free of charge to the interested party, at least where that party does not bring the case before the courts during that period of time.

12 TSP and repository licenses, trust marks, and audit

The Digital Certificates in ATHEX RSA Root CA R2 adhere to the latest version of the following guidelines and standards:

- ETSI EN 319 401, “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”
- ETSI EN 319 411-1, “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Certificates; Part 1: General requirements”,
- 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”,
- ETSI TS 119 495, “Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking”,
- ETSI EN 319 421, “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”,
- CA/Browser Forum, “Guidelines for the Issuance and Management of Extended Validation Certificates”,
- CA/Browser Forum, “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”
- CA/Browser Forum, “Network and Certificate System Security Requirements”

Furthermore, ATHEX as a Qualified Trust Service Provider follows the Regulations of:

- (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market,
- Ministerial Decree No 837/1B of Hellenic Telecommunications & Post Commission (the Greek Supervisory Body), of 14 December 2017 on Greek Trust Service Providers,
- Ministerial Decree 27499 of 10 August 2021 (Official Journal of the Hellenic Republic Number 3682) related to remote identification for natural persons,
- (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Pursuant to the provisions of the Hellenic Telecommunications & Post Commission, which is responsible for the supervision on all Greek Certification Authorities, in respect of the Certification services, ATHEX is subject to regular internal and external audits to verify its compliance with ATHEX RSA Root CA R2 CP/CPS.

Compliance Audits are conducted at least annually. Audits are conducted over unbroken sequences of

audit periods with each period no longer than one year duration.

The external compliance audits are conducted by Qualified and Accredited certification bodies for the certification of Trust Service Providers against the regulation (EU) 910/2014 – eIDAS and the supporting ETSI European Norms.

ATHEX is Qualified Trust Service Provider at https://webgate.ec.europa.eu/tl-browser/#/trustmark/EL/VATEL-099755108 for the following services: QCert for eSig, QCert for eSeal, QWAC and QTimestamp.