HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA, Qualified Trust Service Provider

Certificate Policy and Certificate Practices Statement for ATHEX Root CA G3 Certificates

Version 1.5 - 20/1/2020

Contents

Revision History

Version	Date	Changes in this Revision
0.9	26/06/2019	Initial version and Release
1.0	22/07/2019	Several corrections, clarifications and enrichments according to external audit comments.
1.1	01/08/2019	Small typo corrections
1.2	13/08/2019	Certificate Profile corrections
1.3	19/12/2019	Substitute eIDAS specific subordinate CAs with new ones which satisfy the eIDAS ANNEX I (b) requirement. Correction at a reference of a standard. Clarifications for the OCSP, CRL and OID of this document.
1.4	23/12/2019	Add BasicConstraints at qualified certificates
1.5	20/01/2020	Correct policy identifier of PSD2 eSeal, the profile of TSU certificate and subject public keys.

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).

1.1 Overview

This Certificate Policy and Certification Practice Statement (hereinafter "CP/CPS") presents the rules, processes and procedures related to management and operation of Digital Certificates chained to Root CA G3 of ATHEX QTSP.

The Digital Certificates in this CP/CPS 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; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366", for EU qualified website Certificates supporting PSD2 transactions (hereinafter "EU PSD2 QWAC"),
- 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, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates"
- CA/Browser Forum, "Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates"
- CA/Browser Forum, "Network and Certificate System Security Requirements"

Furthermore ATHEX as 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,
- No 813/1B of Hellenic Telecommunications & Post Commission (the Greek Supervisory Body), of 14 December 2017 on Greek Trust Service Providers
- (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.

This CP/CPS follows the structure defined in RFC 3647 Certificate Policy and Certification Practices Framework.

1.2 Document Name and Identification

The document is the ATHEX Root CA G3 CP/CPS approved by Policy Management Committee (PMC). The Object Identifier assigned to the Root CA G3, covered by this CP/CPS, is 1.3.6.1.4.1.29402.1.3. 0.1.3 (in details: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) HELEX(29402) PKI-Organization-Unit(1) Root-CA-G3(3) CP/CPS(0) First-Digit-of-Version(1) Second-Digit-of-Version(5)})

1.3 PKI Participants

1.3.1 Certification Authorities

ATHEX QTSP includes the following hierarchy of CAs which adhere to this CP/CPS:

- ATHEX Root CA G3
  ATHEX Root CA G3 has signed the following subordinate CAs:
  - ATHEX Qualified eSign Certificates CA-G3
  - ATHEX Qualified eSeal Certificates CA-G3
  - ATHEX Qualified WEB Certificates CA-G3
  - ATHEX Qualified Timestamp Certificates CA-G3
  - ATHEX Extended Validation Certificates CA G3
  - ATHEX General Certificates CA G3
  - ATHEX SSL Certificates CA G3
  - ATHEX Code Signing Certificates CA G3

The mapping between ATHEX Certificate Policy OID in the CertificatePolicies extension of an end entity Certificate and the Guidelines / Standard to which the Certificate asserts adherence, is specified at the following table:

Certificate type	**ATHEX Certificate Policy OID 1.3.6.1.4.1.29402.1.3** {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) HELEX(29402) PKI-Organization-Unit(1) Root-CA-G3(3)}	**End entity Certificate asserts adherence to and compliance with:**
Server Authentication - Domain validation	1.3.6.1.4.1.29402.1.3.100.1.1 {ServerAuth(100) Validation-Type(1) Domain-Validation(1)}	• CA/Browser Baseline Requirements – Domain validated (OID 2.23.140.1.2.1) • ETSI EN 319 411-1 DVCP (OID 0.4.0.2042.1.6)
Server Authentication - Organization validation	1.3.6.1.4.1.29402.1.3.100.1.2 {ServerAuth(100) Validation-Type(1) Organization - Validation(2)}	• CA/Browser Baseline Requirements – Organization Validates (OID 2.23.140.1.2.2) • ETSI EN 319 411-1 OVCP (OID 0.4.0.2042.1.7)
Server Authentication - EV Certificates	1.3.6.1.4.1.29402.1.3.100.1.3 {ServerAuth(100) Validation-Type(1) EV-Certificates(3)}	• CA/Browser Extended Validation (OID 2.23.140.1.1)
Server Authentication - Qualified Website Authentication	1.3.6.1.4.1.29402.1.3.100.1.4 {ServerAuth(100) Validation-Type(1) QWAC(4)}	• ETSI 319 411-2, QCP-w (OID 0.4.0.194112.1.4)
Server Authentication - Qualified Website Authentication for PSD2	1.3.6.1.4.1.29402.1.3.100.1.5 {ServerAuth(100) Validation-Type(1) QWAC-PSD2(5)}	• ETSI TS 119 495, QCP-w-psd2 (OID 0.4.0.19495.3.1)
Document Signing – Qualified Certificates for Advanced Electronic Signatures	1.3.6.1.4.1.29402.1.3.200.1.1 {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	1.3.6.1.4.1.29402.1.3.200.1.2 {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	1.3.6.1.4.1.29402.1.3.200.1.3 {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	1.3.6.1.4.1.29402.1.3.200.1.4 {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	1.3.6.1.4.1.29402.1.3.200.1.5 {DocumentSigning(200) Validation-Type(1) QCP-l-PSD2(5)}	• ETSI TS 119 495, QCP-l supporting PSD2 (OID 0.4.0.194112.1.1)
Code Signing	1.3.6.1.4.1.29402.1.3.300.1.1 {CodeSigning(300) Validation-Type(1) CodeSigning(1)}	• Code Signing Working Group, "Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates"
Extended Validation Code Signing	1.3.6.1.4.1.29402.1.3.300.1.2 {CodeSigning(300) Validation-Type(1) EVCodeSigning(2)}	• CA/Browser Extended Validation Code Signing (OID 2.23.140.1.3)
General – Simple S/MIME	1.3.6.1.4.1.29402.1.3.400.1.1 {General(400) Validation-Type(1) Simlpe-S/MIME(1)}	• ETSI EN 319 411-1 LCP (OID 0.4.0.2042.1.3)
General – Organizational S/MIME	1.3.6.1.4.1.29402.1.3.400.1.2 {General(400) Validation-Type(1) Organizational-S/MIME(2}	• ETSI EN 319 411-1 LCP (OID 0.4.0.2042.1.3)
Qualified Timestamping	1.3.6.1.4.1.29402.1.3.500.1.1 {Timestamping(500) Validation-Type(1) QTimestamp(1)}	• ETSI EN 319 421 (OID 0.4.0.2023.1.1)

ATHEX Root CA G3 and its underlying Issuing CAs issue Digital Certificates to Subscribers in accordance with this CP/CPS.

1.3.2 Registration Authority

ATHEX QTSP acts as RA for its Digital Certificates according to this CP/CPS. Some of the functions that are performed by an RA are:

- Process all Digital Certificate application requests ;

- Maintain and process all supporting documentation related to Digital Certificate applications;
- Process all Digital Certificate Revocation requests;
- Follow the privacy policy in accordance with this CP/CPS
- Deliver the Qualified Signature Creation Device (QSCD);
- Authenticate credentials in case of Remote Qualified Certificate to the Subscriber or Subject.

1.3.3 Subscribers

Subscribers use the ATHEX QTSP's services and PKI to support transactions and communications. Subscribers request Digital Certificates issued by a Subordinate CA under the ATHEX Root CA G3. Depending on the Digital Certificate type subscriber may be, but not limited to:

- An Individual responsible for a website
- An Individual responsible for distributing software
- An Individual signing documents
- A Payment Service Provider as defined in ETSI TS 119 495
- An Individual to whom a time-stamp is issued

1.3.4 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 this CP/CPS and all applicable laws and regulations.

Before relying on or using a ATHEX Certificate, Relying Parties are advised to: (i) read this 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.

1.4 Certificate Usage

Subscribers are required to utilize Certificates in accordance with this CP/CPS and all applicable laws and regulations.

1.4.1 Appropriate Certificate Usages

Digital Certificates may be used for identification, providing data confidentiality and data integrity, encryption, authentication and for digital signatures purposes, as designated by the key usage and extended key usage fields found within the Certificate.

The use of Certificates supported by this CP/CPS is restricted to parties authorised by contract to do so. Persons and entities other than those authorised by contract may not use Certificates for any purpose. No reliance may be placed on a Certificate by any person unless that person is an Authorised Relying Party.

Sea also APPENDIX A for the purpose of each Certificate type.

1.4.2 Prohibited Certificate Uses

The ATHEX CA shall not issue any Certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the Subscriber does not legitimately own or control. Such Certificate usage is expressly prohibited.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

ATHEX Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

In particular, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware,

bugs, or other problems.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization administering this CP/CPS 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

1.5.2 Contact Person

Address inquiries about the CP/CPS to:

pkica-services@athexgroup.gr
Tel +30 210 336 6300
Fax +30 210 336 6301

For revocation reporting the email address and phone number are:

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

1.5.3 Person determining CPS suitability for the policy

The ATHEX PMC determines the suitability of this CP/CPS to the functions and uses of Participants in the ATHEX PKI.

1.5.4 CP/CPS Approval Procedure

Approval of this CP/CPS and any amendments hereto is by the ATHEX Policy Management Committee (PMC).

The Policy Management Committee (PMC) is composed of ATHEX'S senior executives with the participation of experienced /specialized technical and legal advisers and constitutes the body that is responsible for policy making and designing the Digital Certificate Services offered by ATHEX.

Once the PMC takes into consideration the technological developments, the regulatory framework, the trade and transactional requirements of ATHEX and/or subscribers and ATHEX'S business plans, PMC approves ATHEX'S current CP/CPS.

1.6 Definitions & Acronyms

For the Definitions & Acronyms contained herein please refer to the standards listed at section 1.1.

2 Publication and Repository Responsibilities

2.1 Repositories

The location of ATHEX repository is:
https://www.athexgroup.gr/web/guest/digital-Certificates-pki-regulations

The revocation list for subscriber Certificates can be found in the above repository, which is publicly available 24 hours a day, 7 days a week.

2.2 Publication of Certificate Information

This CP/CPS, Subscriber Agreements (which includes in Terms and Conditions) can be found at the location of ATHEX repository.

ATHEX publishes Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) resources to allow Relying Parties to determine the validity of an ATHEX Certificate. Each CRL contains entries for all revoked un-expired Certificates issued. ATHEX maintains revocation entries on its CRLs, or makes Certificate status information available via OCSP, until after the expiration date of the revoked Certificate.

ATHEX shall host test Websites that allow Application Software Suppliers to test their software with Subscriber TLS/SSL Certificates that chain up to ATHEX Root CA. These sites are accessible at the following URLs:

- ATHEX Root CA G3 Valid: https://certdemo-valid-3.athexgroup.gr/
- ATHEX Root CA G3 Expired: https://certdemo-expired-3.athexgroup.gr/
- ATHEX Root CA G3 Revoked: https://certdemo-revoked-3.athexgroup.gr/

2.3 Time or Frequency of Publication

For CRL see Section 4.9.7.

ATHEX also provides an OCSP resource that is updated at least every twenty-four (24) hours.
.

2.4 Access Controls on Repository

Information published in the repository portion of the ATHEX website is publicly and internationally available. Read only access to such information is available twenty-for hours per day, seven day per week, except for reasonable maintenance requirements, where access is deemed necessary. ATHEX is the only entity that has write access to Repositories.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

All Subscribers require a distinguished name that is in compliance with the ITU X.500 standard for Distinguished Names (DN).

TLS/SSL Certificates are issued using the Fully Qualified Domain Name (FQDN) name of the server, service, or application that has been confirmed with the Subscriber. The Distinguished Names of a Code Signing Certificate must identify the legal entity that intends to have control over the use of the Private Key when signing code. The Baseline Requirements contain provisions prohibiting Certificates containing Internal Server Names or Reserved IP Addresses.

Wildcard TLS/SSL Certificates have a wildcard asterisk character for the server name in the Subject field. Wildcard EV Certificates may not be issued under the EV Guidelines.

The FQDN or authenticated domain name is placed in the Subject Alternative Name extension.

The Subject Name of all Digital Certificates issued to Individuals shall be the authenticated common name of the Subscriber. The Distinguished Name may include the following fields:

- Common Name (CN)
- Organisational Unit (OU)
- Organisation (O)
- Locality (L)
- State or Province (S)
- Country (C)
- Email Address (E)

3.1.2 Need for Names to be Meaningful

The subject of the Certificate which identifies the entity (i.e. person, organization, device or object), is meaningful and unambiguous.

The contents of the Digital Certificate Subject Name fields must have a meaningful association with the name of the Individual, Organization, or Device. In the case of Individuals, the name should consist of the first name, last name, and any middle initial. In the case of Organizations, the name shall meaningfully reflect the legal name or registered domain name of the Organization or the trading or business name of that Organization. In the case of a Device, the name shall state the name of the Device and the legal name or registered domain name of the Organization responsible for that Device.

3.1.3 Anonymity or Pseudonymity of Subscribers

ATHEX does not issue pseudonymous or anonymous Certificates pursuant to this CP/CPS.

3.1.4 Rules for Interpreting Various Name Forms

Fields contained in Digital Certificates are in compliance with this CP/CPS. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs. Digital Certificate Profiles are described in APPENDIX A.

3.1.5 Uniqueness of Names

The Subject Name of each Digital Certificate issued by an Issuing CA shall be unique within each class of Digital Certificate issued by that Issuing CA and shall conform to all applicable X.500 standards for the uniqueness of names. The Issuing CA may, if necessary, insert additional numbers or letters to the Subscriber's Subject Common Name, or other attribute such as subject serialNumber, in order to distinguish between two Digital Certificates that would otherwise have the same Subject Name.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. ATHEX, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. ATHEX is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another ATHEX -approved method. This requirement does not apply where a Key Pair is generated on behalf of a Subscriber.

3.2.2 Authentication of Organization and Domain Identity

Authentication of Organization and Domain Validity is specified at APPENDIX A.

3.2.2.1 Validation of Domain Authorization and Control

For the validation of each FQDN listed in a Certificate, ATHEX follows the procedures specified at Section 3.2.2.4 of CA/Browser Baseline Requirement v.1.6.5, by

1. Validating the Applicant as a Domain Contact with BR section 3.2.2.4.1;
2. Communicating directly with the Domain Name Registrant via email, fax or postal mail provided by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.2 using a Random Value (valid for no more than 30 days from its creation);
3. Communicating directly with the Domain Name Registrant by calling their phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The phone number used must be the number listed by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.3;
4. Communicating with the Domain's administrator using a constructed email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorization Domain Name. Performed in accordance with BR section 3.2.2.4.4;
5. Confirming the Applicant's control over the requested FQDN by confirming the presence of an agreed-upon Random Value under the "/.well-known/pkivalidation" directory. Performed in accordance with BR section 3.2.2.4.6;
6. Confirming the Applicant's control over the requested Authorization Domain Name (which may be prefixed with a label that begins with an underscore character) by confirming the presence of an agreed-upon Random Value in a DNS record. Performed in accordance with BR section 3.2.2.4.7;
7. Confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8;
8. Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12;
9. Confirming the Applicant's control over the FQDN by sending a Random Value via email to a DNS CAA Email Contact and then receiving a confirming response utilizing the Random Value. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 performed in accordance with BR Section 3.2.2.4.13;
10. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR

Section 3.2.2.4.14;

11. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15; and
12. Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.16.

3.2.2.2 Authentication for an IP address

For the validation of each IP address, ATHEX follows the processes described at Section 3.2.2.5 of CA/Browser Baseline Requirements, by:

1. Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pkivalidation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;
2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;
4. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;
5. Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietfacme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or
6. Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietfacme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

3.2.2.3 Wildcard Domain Validation

Before issuing a Certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, ATHEX follows a procedure that determines that the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix".

3.2.2.4 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, ATHEX evaluates the source for its reliability, accuracy, and resistance to alteration or falsification.

3.2.3 Authentication of Individual Identity

Authentication of Individual Identity is described in APPENDIX A.

3.2.4 Non-verified subscriber information

ATHEX accepts non-verified subscriber information into the Digital Certificate only for demonstration

or testing purposes.

3.2.5 Validation of Authority

Validity of authority is specified in APPENDIX A.

3.2.6 Criteria for interoperation

No stipulation

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication for routine re-key

Key Pairs must always expire at the same time as the associated Certificate. The procedures that are followed for re-key are described at Section 4.7.

3.3.2 Identification and authentication for re-key after revocation

After revocation, Subscriber must submit a new Certificate application.

3.4 Identification and Authentication for Revocation Request

Identification and Authentication is specified at Section 4.9.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit A Certificate Application?

An application in a form prescribed by ATHEX must be completed by Applicants, which includes all registration information as described by this CP/CPS (see APPENDIX A) and the relevant Subscriber Agreement or other terms and conditions upon which the Digital Certificate is to be issued. All applications are subject to review, approval, and acceptance by the ATHEX in its discretion.

ATHEX maintains internal database of all previously revoked Certificates and previously rejected Certificate requests due to suspected phishing or other fraudulent usage or concerns and use this information to identify subsequent suspicious Certificate requests.

4.1.2 Enrollment Process and Responsibilities

Certain information concerning Certificate applications is set out in this CP/CPS.

The following steps are required by CA in any application for a Digital Certificate:

- Identify the Applicant or Device in accordance with APPENDIX A,
- Generate a Key Pair for the Digital Certificate in a secure fashion, and
- ATHEX shall enter into contractual relations with the Certificate Applicant for the use of that Digital Certificate and the ATHEX PKI.

All Subscriber Agreements concerning the use of, or reliance upon, Digital Certificates issued within the ATHEX PKI must incorporate by reference the requirements of this ATHEX CP/CPS as it may be amended from time to time.

4.2 Certification Application Processing

4.2.1 Performing Identification and Authentication Functions

The Identification and Authentication Requirements per Certificate Type are described in APPENDIX A.

4.2.2 Approval or Rejection of Certificate Applications

ATHEX will approve a Certificate Application based upon the Certificate Applicant meeting the requirements of this CP/CPS and the Digital Certificate Profiles contained in APPENDIX A. ATHEX, in its sole discretion, may refuse to accept an application for a Certificate or for the renewal of a Certificate, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. ATHEX reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

ATHEX may change the above requirements related to the application information requested. These changes must follow potential changes to relevant ETSI standards, EV Code Signing, EV Guidelines, Baseline Requirements or any relevant law.

4.2.3 Time to Process Certificate Applications

ATHEX makes reasonable efforts to confirm Certificate application information and issue a Certificate within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner. Upon the receipt of the necessary details and / or documentation, ATHEX aims to confirm submitted application data and to complete the validation process and issue / reject a Certificate application within five working days for all other Certificate types, except EV Certificates that may require up to ten working days.

Events outside of the control of ATHEX may delay the issuance process, however ATHEX will make every reasonable effort to meet issuance times and to make Applicants aware of any factors that may affect issuance times in a timely manner.

ATHEX rejects a Certificate application related to a Remote QSCD when the relevant Subscriber account

is not created and no other actions are needed from Subscriber

4.2.4 Certificate Authority Authorization (CAA)

As part of the issuance process, ATHEX checks for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the Certificate to be issued, as specified in RFC 6844 as amended by Errata 5065 (Appendix A). If the ATHEX Digital Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, ATHEX processes the issue, issuewild, and iodef property tags as specified in RFC 6844, although ATHEX is not required to act on the contents of the iodef property tag. ATHEX will not issue a Certificate if an unrecognized property is encountered with the critical flag set.

CAA checking is optional:

- for Certificates for which a Certificate Transparency pre-Certificate was created and logged in at least two public logs, and for which CAA was checked;
- for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant; and
- if ATHEX or an Affiliate of ATHEX is the DNS Operator (as defined in RFC 7719) of the domain's DNS

ATHEX is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure;
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

ATHEX documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances, and will dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The ATHEX Root CA G3 has been self-generated and self-signed. ATHEX Root CA G3 issues the CA Digital Certificates to ATHEX Subordinate CAs.

Upon the Applicant’s acceptance of the Subscriber Agreement or other terms and conditions, the successful completion of the application process and final approval of the application by ATHEX, ATHEX issues the Digital Certificate to the Applicant or Device.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificates

ATHEX may notify Subscriber about the Certificate Issuance.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon the availability of Digital Certificate to Applicant, he or she must install and verify the correctness of information in the Certificate within 30 days. Applicant must notify ATHEX that he or she accepts the Digital Certificate, in order ATHEX to proceed with is activation.

By accepting a certificate, the subscriber and subject of the certificate acknowledges that they agree to the terms and conditions contained in this CP/CPS and the applicable subscriber agreement. By accepting a certificate, the subscriber and subject of the certificate assumes a duty to retain control of the certificate’s private key, to use a trustworthy system and to take reasonable precautions to prevent its loss, exclusion, modification or unauthorized use.

4.4.2 Publication of the Certificate by the CA

All Certificates issued within ATHEX PKI may be available in public repositories except where the Subscriber has requested that the Certificate not be published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Usage

The Certificate shall be used by Subscriber lawfully in accordance with ATHEX's Subscriber Agreement and the terms of this CP/CPS. By accepting the Digital Certificate, Subscriber unconditionally agrees to use it in a manner consistent with the KeyUsage field extensions included in the Digital Certificate Profile.

4.5.2 Relying Party Public Key and Certificate Usage

With regard to ATHEX Digital Certificates, Relying Parties must verify that the Certificate is valid by examining the CRL or OCSP before initiating a transaction involving such Certificate. Furthermore, Relying Parties must assess the appropriateness of the use of Digital Certificate for any given purpose and that the Digital Certificate is being used in accordance with its key-usage filed extensions. ATHEX does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL or OCSP, or for use of Certificate which is not in accordance with its KeyUsage field extensions.

In addition, Relying Party must get informed about the limits of liability, the disclaimers, the limitation of guarantees and the limitation of usage of the Certificate that the ATHEX has stated, as well as about the time period of record keeping of the evidence listed herein and any other precautions prescribed in the ATHEX Subscriber Agreement and which the Relying Party must accept before making use of the services.

ATHEX and its authorized partners involved in the provision of the Certification services assume no liability to any user of its Certificates in the event that such user has failed to perform the above obligations and such failure has caused damages to the user in any way whatsoever.

4.6 Certificate Renewal

Certificate Renewal means the issuance of a new Certificate without changing the Public Key.

Certificate renewal is not offered and so the Subscriber is required to generate a new Public Key and complete a new Certificate request prior to the expiration of an existing Subscriber's Certificate. The process and cost for obtaining the new Certificate upon expiration of a previous Certificate will be the same as if the Subscriber is simply buying a Certificate for the first time.

4.7 Certificate Re-Key

Re-keying a Certificate means to request a new Certificate with the same contents except for a new key pair.

Identification and Authentication procedures for re-key are the same as for a new application.

4.8 Certificate Modification

ATHEX does not offer Certificate modification. Instead, ATHEX will revoke the old Certificate and issue a new Certificate as a replacement.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period.

A Digital Certificate will be revoked in the following instances:

- ATHEX determines that any of the information appearing in the Certificate is inaccurate or misleading;
- ATHEX obtains reasonable evidence that there has been loss, theft, modification, unauthorised disclosure, or other compromise of the Private Key corresponding to the Public Key within the Certificate, or that the Certificate has otherwise been misused;
- The Subscriber has failed to meet his, her or its obligations under this ATHEX CP/CPS or any other agreement, regulation, or law that may be in force with respect to that Digital Certificate;
- The Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the Subscriber provided inaccurate, false or misleading information;
- The Private Key corresponding to the Certificate has been used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, or other content, for phishing, or conduct that is harmful, malicious, hostile or to download malicious content onto a user's system without their consent;
- The Subscriber is a denied party or prohibited person on a government issued blacklist, or is operating from a prohibited destination;
- Where a Subscriber's employer or company that operates the Nominating Registration Authority, or its respective Subsidiaries, Holding Companies or Counterparties requests revocation because:
    - Of a change in the employment relationship with the Subscriber
    - The Subscriber is no longer authorised to act on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
    - The Subscriber otherwise becomes unsuitable or unauthorised to hold a Digital Certificate on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
- Affiliation change
- Cessation of operation
- Subscriber bankruptcy
- Subscriber liquidation
- Subscriber death
- Breach of Subscriber Agreement with ATHEX
- The Subscriber requests in writing the revocation of their Certificate;
- The Subscriber indicates that the original Certificate Request was not authorised and does not retroactively grant authorization;
- ATHEX receives notice or otherwise becomes aware that a Subscriber has breached a material obligation under the Subscriber Agreement or other contractual obligations;
- ATHEX receives a lawful and binding order from a government or regulatory body to revoke the Certificate;
- ATHEX is made aware of any circumstance indicating that use of a Fully Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- ATHEX is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- ATHEX determines, in its sole discretion, that the Certificate was not issued in accordance with the terms and conditions of ATHEX CP/CPS;
- ATHEX receives notice or otherwise becomes aware that there has been some other

modification of the information pertaining to the Subscriber that is contained within the Certificate;

- The Subscriber fails or refuses to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity;
- ATHEX determines, in its sole discretion, that the Private Key corresponding to the Certificate was used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, phishing, or other content, or that is harmful, malicious, hostile or downloaded onto a user's system without their consent;
- Either the Subscriber's or ATHEX's obligations under this CP/CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- ATHEX CA Private Key used to issue that Certificate has been compromised;
- Revocation is required by the ATHEX CP/CPS;
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);
- ATHEX' right to issue and manage Certificates under the EV Guidelines, the Baseline Requirements, or the Code Signing Minimum Requirements expires or is revoked or terminated (unless arrangements have been made to continue maintaining the CRL/OCSP Repository); or
- ATHEX ceases operations for any reason and has not arranged for another suitable CA to provide revocation support for the Certificate.

In the event that an ATHEX determines that its Digital Certificates or the ATHEX PKI could become compromised and that revocation of Digital Certificates is in the interests of the PKI, following remedial action, ATHEX will authorise the reissue of Digital Certificates to Subscribers at no charge, unless the actions of the Subscribers were in breach of the ATHEX CP/CPS or other contractual documents.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation of or revoke a Certificate issued by ATHEX is the Subscriber (including designated representatives) and ATHEX at its sole discretion.

Additionally Relying Parties, Application Software Suppliers, Greek Supervisory Body, National Competent Authority (only for PSD2 certificates) and other third parties may submit Certificate Problem Reports informing ATHEX of reasonable cause to revoke the Certificate.

ATHEX shall be entitled to revoke and shall revoke, a Digital Certificate at any time for any of the reasons set forth in section 4.9.1.

4.9.3 Procedure for Revocation Request

The steps of the procedure for Revocation Request when the Subscriber triggers the revocation are:

1. Subscriber must contact ATHEX, either by phone, e-mail message, a national/regional postal service, fax, or overnight courier, and request revocation of a Certificate.
2. Upon receipt of a revocation request, ATHEX will verify that the revocation request has been made by the organization or individual entity that has made the Certificate application and has been authenticated by the procedures in Section 3.2 of this CP/CPS
3. Then ATHEX seeks confirmation of the request by e-mail message to the administrative and technical contacts provided by the Subscriber at the time the Certificate was issued. The message will state that upon confirmation of the revocation request, ATHEX will revoke the Certificate and that posting the revocation to the appropriate CRL and OCSP will constitute notice to the Subscriber that the Certificate has been revoked. ATHEX will require a confirming e-mail message back from either the administrative or technical contact authorizing

revocation (or by other means acceptable to ATHEX).

4. Upon receipt of the confirming e-mail message, the Certificate will be revoked and the revocation will be posted to the appropriate CRL and OCSP.

Notification will not be sent to others than the Certificate Subscriber and the Subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and ATHEX shall revoke such Certificate within the next business day and post the revocation to the next published CRL and OCSP.

In the event of Compromise of ATHEX's Private Key used to sign a Certificate; ATHEX will send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates will be revoked by the next business day and that posting the revocation to the appropriate CRL and OCSP will constitute notice to the Subscriber that the Certificate has been revoked.

ATHEX maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

4.9.4 Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. ATHEX will revoke Digital Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5 Time within Which CA Must Process the Revocation Request

ATHEX takes commercially reasonable steps to process revocation requests within 24 hours.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely, prior to relying information featured in Certificate. Failure to do so negates the ability of the Relying Party to claim that it acted on a Certificate with reasonable reliance.

4.9.7 CRL Issuance Frequency

ATHEX shall post the CRL online daily and immediately after revocation of a Certificate. If a Certificate listed in a CRL expires, it will remain in the CRL after the Certificate's expiration.

4.9.8 Maximum Latency for CRLs

The maximum latency for the CRL is 10 minutes.

4.9.9 On-Line Revocation/Status Checking Availability

ATHEX provides OCSP. The URL of OCSP is specified at Authority Information Access extension of the Certificate.

4.9.10 On-Line Revocation Checking Requirements

A Relying Party must check the status of a Certificate on which he/she/it wishes to rely.

ATHEX supports an OCSP capability using the GET method for Certificates issued in accordance with the Baseline Requirements.

Where required by the Baseline Requirements (all TLS/SSL Certificates) or other industry requirements, if ATHEX OCSP responder receives a request for status of a Certificate that has not been issued, then the responder will not respond with a "good" status.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

When the Private Key of an End-Entity Certificate is compromised, then it must immediately be revoked.

When the Private Key of a CA is compromised, then all Certificates chained to this CA must immediately be revoked.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of Certificates is available either via CRL or OCSP. The URL of CRL and the URL of OCSP is specified in the Certificate.
The revoked Certificates are not removed from CRL and OCSP after their expiration date.

4.10.2 Service Availability

Certificate status services are available 24X7. ATHEX also maintains controls to provide reasonable assurance that it operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

A subscriber may end a subscription for an ATHEX Certificate by:

- Allowing his/her/its Certificate to expire without renewing or re-keying that Certificate
- Revoking of his/her/its Certificate before Certificate expiration without replacing the Certificates.

4.12 Key Escrow and Recovery

ATHEX PKI does not support key escrow or recovery of Subscriber's Private Key.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

ATHEX CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt. The secure datacenter is located in Athens, Greece.
ATHEX CAs are physically located in a highly secure facility which includes the following:

- Electronic control access systems
- Alarmed doors and video monitoring
- Security logging and audits
- Card key access for specially approved employees with defined levels of management approval required

5.1.2 Physical Access

Entry to the PKI infrastructure areas is protected with security doors bearing a locking mechanism. Every access to these areas is supervised and controlled by the control mechanisms that operate on an ongoing basis. The security areas are monitored even during non-working hours with sensor detection and alarm systems. Unauthorized personnel and any visitors that must enter the secure areas must be accompanied by authorized personnel throughout the duration of their stay therein. Access to all security areas requires the use of control techniques such as passwords, magnetic cards and/or a reception desk. All access rights in specific areas, security lockers and sensitive documents, and distributed access tools, such as keys, magnetic cards and tabs-badges are recorded in special 'access control lists'.

Every visit to the secure areas by visitors, external system maintenance and supply crews as well as authorized personnel outside of working hours is entered in an 'Access Control Log'. These entries include the following details:

- Identity and status (personnel or partner) of the incoming individual,
- Specific areas that may be visited,
- Exact time of entry and exit,
- Identity of entry supervisor

ATHEX securely stores the Cryptographic Signing Units (CSU) used to generate and store the Subscribers Private Keys for remote signature. Access to the rooms used for key storage and key generation activities is controlled and logged by the building access card system. Access card logs and video records are reviewed on a regular basis.

5.1.3 Power and Air Conditioning

ATHEX secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating/air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

5.1.4 Water Exposures

The ATHEX CA facility is not susceptible to flooding or other forms of water damage. ATHEX has taken reasonable precautions to minimize the impact of water exposure to ATHEX systems.

5.1.5 Fire Prevention and Protection

ATHEX has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. ATHEX fire prevention and protection measures have been designed to comply with local fire safety regulations.

Fire prevention for ATHEX's CA facility is by strict building fire prevention protocol. Detection is by

centralized and 24 hour a day/7 day a week monitored smoke, heat, and ionization detection. Fire suppression is by FM 200 in all computing areas and by dry pipe water in all office areas.

5.1.6 Media Storage

Data media and their copies, which are used to operate the system, are stored in secure cabinets that protect them from environmental threats such as temperature, humidity and magnetic fields. Backups do not include the users' qualified Certificates.

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with ATHEX normal waste disposal requirements.

5.1.8 Off-Site Backup

ATHEX performs routine backups of critical system data, audit log data, and other sensitive information. Critical CA facility backup media are stored in a physically secure manner at an offsite facility, which is available to authorised personnel 24 hours per day seven days per week and has appropriate levels of physical security in place.

5.2 Procedural Controls

5.2.1 Trusted Roles

It is designated for the purposes of this text that all employees, contractual partners and consultants of ATHEX TSP that have access to or control cryptographic operations related to Certificates lifecycle, and the management of published directories including repository, serve 'trusted roles'.

Included in the personnel of 'trusted roles' are the system and network administrators, technician and other operators as well as those persons that are assigned to supervise the operations of ATHEX's PKI infrastructure.

5.2.2 Number of Persons Required per Task

To ensure that the security regulations are not circumvented by a person acting alone, the administration and operations of ATHEX TSP are distributed to multiple 'trusted roles' and corresponding individuals. At least two people are assigned to each trusted role to ensure adequate support at all times. Every access account to the ATHEX system will have limited capabilities taking into consideration the 'role' of the individual holding that account. For this reason, every ATHEX TSP personnel will be subject to verification of their identity and powers, before:

- being included in the lists of individuals with access to secure areas,
- gaining an access account to the system and equipment,
- receiving the necessary Certificate to perform their role.

All the system Administrators' rights are controlled and certified with the issuance of special administrator Certificates which are required for access to the administrative operations of ATHEX TSP.

Such a Certificate (and related access account) has the following features:

- it is directly associated with a specific natural person,
- use by anyone else is prohibited,
- its use is restricted to acts permitted by the specific roles of the holder, the operating system and the procedural controls with the use of special software.

These administrator Certificates are installed in special tokens (e.g. smart cards) that require an 'activation code', thus ensuring the utmost security of ATHEX TSP operations.

CA key pair generation and initialisation of each CA (Root and Issuing) requires the active participation of at least two trusted individuals in each case.

5.2.3 Identification and Authentication for Each Role

Each individual performing any of the trusted roles shall use ATHEX issued Digital Certificate (i.e., a Utility Certificate) stored on a cryptographic smart card to identify themselves to the Digital Certificate server and repository.

5.2.4 Roles Requiring Separation of Duties

No Trusted Roles can assume any other role.

5.3 Personnel Controls

Access to the secure parts of ATHEX facilities is limited using physical and logical access controls and is only accessible to appropriately authorized individuals filling trusted roles for which they are properly qualified and to which they have been appointed by management.

ATHEX requires that all personnel filling trusted roles are properly trained and have suitable experience before being permitted to adopt those roles.

5.3.1 Qualifications, Experience, and Clearance Requirements

ATHEX requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background Check Procedures

All trusted personnel have background checks before access is granted to ATHEX systems. These checks may include, but are not limited to, verification of the individual's identity using a government issued photo ID, credit history, employment history, education and character references.

5.3.3 Training Requirements

Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached. CA Administrators are trained in the operation and installation of CA software. Operators are trained in the maintenance, configuration, and use of the specific software, operating systems, and hardware systems used by PKI.

RA Officers are trained in ATHEX validation and verification policies and procedures.

5.3.4 Retraining Frequency and Requirements

ATHEX provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Any personnel who, knowingly or negligently, violate ATHEX's security policies, exceed the use of their authority, use their authority outside the scope of their employment, or allow personnel under their supervision to do so may be liable to disciplinary action up to and including termination of employment. Should the unauthorized actions of any person reveal a failure or deficiency of training, sufficient training or retraining will be employed to rectify the shortcoming.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to ATHEX employees in a comparable position. Independent contractors and consultants who have

completed or passed the background check procedures specified in Section 5.3.2 are permitted access to ATHEX's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times. Once the independent contractor completes the work for which it was hired, or the independent contractor's employment is terminated, physical access rights assigned to that contractor are removed at once.

5.3.8 Documentation Supplied to Personnel

ATHEX provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

For audit purposes, ATHEX maintains electronic or manual logs of the following events for core functions.

5.4.1 Types of Events Recorded

CA Key and Certificate Lifecycle Management Events:

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber Certificate lifecycle management, including successful and unsuccessful Certificate applications, Certificate issuances, Certificate re-issuances and Certificate renewals , Certificate revocation requests including revocation reason
- CRL updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a private key
- Certificate Application Information:
    - The documentation and other related information presented by the Applicant as part of the application validation process
    - Storage locations, whether physical or electronic, of presented documents

Security Related Events:

- System downtime
- Software crashes, hardware failures and other anomalies
- System actions including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful access attempts
- Secure facility visitor entry and exit
- Remote QSCD facility access entry/exit
-

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

5.4.2 Frequency of Processing Log

Logs are archived by the system administrator on a monthly basis and reviewed by CA management.

5.4.3 Retention Period for Audit Log

ATHEX audit logs relating to the Certificate lifecycle are retained as archive records for seven (7) years.

Certain high volume system generated logs may be retained for less than seven years based on a risk assessment.

5.4.4 Protection of Audit Log

The relevant audit data collected is regularly analyzed for any attempts to violate the integrity of any element of the ATHEX PKI.

Only certain ATHEX Trusted Roles and auditors may view audit logs in whole. ATHEX decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction.

5.4.5 Audit Log Backup Procedures

All logs are backed up on removable media on a daily basis.

5.4.6 Audit Collection System

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

A vulnerability is a weakness in the organization or in an information system that might be exploited by a threat, with the possibility of causing harm to assets. In order to mitigate the risk or possibility of causing harm to assets, ATHEX performs regular vulnerability assessment by taking a two-pronged approach. ATHEX assesses vulnerabilities by (1) making an assessment of the threats to, impacts on, and the vulnerabilities of assets and the likelihood of their occurrence, and (2) by developing a process of selecting and implementing security controls in order to reduce the risks identified in the risk assessment to an acceptable level.

Furthermore, ATHEX undergoes periodic penetration tests.

5.5 Records Archival

ATHEX implements a backup standard for all business critical systems located at its data centers. ATHEX retains records in electronic or in paper-based format in conformance with this subsection of this CP/CPS.

5.5.1 Types of Records Archived

For each Certificate, the records will address creation, issuance, use, revocation, expiration, and renewal activities.

These records will include all relevant evidence in the Issuing CA's possession including:

- Audit logs;
- Certificate Requests and all related actions;
- Evidence produced in verification of Applicant details;
- Contents of issued Certificates;
- Evidence of Certificate acceptance and signed (electronically or otherwise) Subscriber Agreements;
- Certificate renewal requests and all related actions;
- Revocation requests and all related actions;
- CRL lists posted; and
- Audit Results.

5.5.2 Retention Period for Archive

See Section 5.4.3.

5.5.3 Protection of Archive

ATHEX protects the archive so that only authorized Trusted Persons are able to obtain access to the

archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CP/CPS.

5.5.4 Archive Backup Procedures

Administrators at each ATHEX location are responsible for carrying out and maintaining backup activities. ATHEX employs both scheduled and unscheduled backups. Scheduled backups are automated using approved backup tools. Scheduled backups are monitored using automated tools. Unscheduled backups occur before carrying out major changes to critical systems and are part of any change request that has a possible impact on data integrity or security. All backup media is labeled according to the information classification, which is based on the backup information stored on the media.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

ATHEX CA key pairs are retired from service at the end of their respective maximum lifetimes and so there is no key changeover. Towards the end of the CA Private Key's lifetime, ATHEX ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs and OCSP responder Certificates associated with that key. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with this CP/CPS.

5.7 Compromise and Disaster Recovery

Organizations are regularly faced with events that may disrupt their normal business activities or may lead to loss of information and assets. These events may be the result of natural disasters, accidents, equipment failures, or deliberate actions. This section details the procedures ATHEX employs in the event of a compromise or disaster.

5.7.1 Incident and Compromise Handling Procedures

ATHEX monitors system activities continuously in order to detect any abnormal system activity which may indicate potential security violation. ATHEX has an Incident Management procedure with the main purpose of limiting the impact of breaches of security. This procedure adheres to the requirements specified in ETSI standards and to the Regulations of Greek Supervisory Body.

Backup copies of essential business and CA information are made routinely. In general, backups are performed daily on-site but may be performed less frequently in ATHEX discretion according to production schedule requirements. ATHEX ensures that backup copies can be recovered following a disaster.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to ATHEX Security. Appropriate escalation, incident investigation, and incident response will

ensue.

5.7.3 Entity Private Key Compromise Procedures

In the event of the compromise of ATHEX Issuing CA Private Key, ATHEX shall:

- promptly notify all Subscribers, Relying Parties and Greek Supervisory Body via e-mail or any other method that has been reporter to us.;
- post a relevant notice at www.athexgroup.gr ; and
- revoke all Certificates signed with that ATHEX's Issuing CA

5.7.4 Business Continuity Capabilities after a Disaster

Hellenic Exchanges – Athens Stock Exchange has successfully completed the certification according to the international standard ISO 22301:2012 of the Business Continuity Management System, that has already implemented and put into operation.

The Business Continuity Management System, refers to the mechanism and the organization of all the need procedures ensuring the continuity of critical business functions and operations in case of a catastrophic event, of events that could cause prolonged interruption of normal business operation. Athens Exchange Group of companies obtained the Certification ISO22301:2012 for Business Continuity activities related to all business operation and provided products & services (www.athexgroup.gr/athexgroup-business-continuity)

5.8 CA or RA Termination

In the event that ATHEX decides on the termination of CA or RA activities as TSP the following steps will take place:

In the context of a scheduled termination:

- Cessation of the issuance of any new Certificate;
- Termination notification to the Greek Supervisory Body and Relying Parties within 3 months before the effective termination and no later than 2 months before the effective termination;
- Dissemination of relevant information (Communication Management Team upon written formal request from the Policy Management Committee);
- Preservation and transfer of auditing and archival records to the arranged custodian for the required period of time;
- Revocation of unexpired and unrevoked Subjects' Qualified Certificates (performed by Security officers when officially informed by the Policy Management Committee);
- Creation of a last CRL (performed by Security officers when officially informed by the Policy Management Committee);
- When applicable, decommissioning of the CA keys.

In the context of an unscheduled termination, as far as it is possible, the plan for expected termination as described in section above will be followed with the following potential significant differences:

- Shorter or even no delay for the notification of the interested parties;
- Shorter or no delay for the revocation of Certificates.

The conditions and effect resulting from termination ATHEX Services will be communicated via the ATHEX website (http://www.athexgroup.gr/digital-Certificates-pki-regulations) upon termination. That communication will outline the provisions that may survive termination and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

6 Technical Security Controls

The ATHEX Certification Authority Private Keys are protected within a hardware security module meeting at least Federal Information Processing Standard-140-2 level 3. Access to the modules within the ATHEX environment, including the Root and Operational Digital Certification Authorities' Private Keys, are restricted by the use of token/smartcards and associated pass phrases. These smartcards and pass phrases are allocated among the multiple members of the ATHEX management team. Such 2-of-N allocation ensures that no one member of the team holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

The Private keys of EU Remote Qualified Certificates, are operated by ATHEX using exclusively devices certified specifically in accordance with the applicable requirements per Article 30.3 of the eIDAS and, thus included in the list of qualified devices maintained by the European Commission in compliance with Articles 30, 31 and 39 of eIDAS.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

ATHEX Root CA G3 key pair generation fell under a Special Root Key Generation Ceremony for Certification Authority, witnessed by a Qualified Auditor and followed a formal key generation script. CA private keys are generated in a physically secure environment within cryptographic modules that are validated to Federal Information Processing Standard-140-2 level 3. CA Certificate signing keys are only used within this secure environment. Access to the modules within the ATHEX environment, including the private keys, is restricted by the use of token/smart cards and associated pass phrases. These smartcards and pass phrases are allocated among multiple members of the ATHEX management team. Such allocation ensures that no one member of the team holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

For relevant European Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Subscriber Private Keys are generated and stored on a Qualified Electronic Signature/ Seal Creation Device (QSCD) which meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 and is certified to the appropriate standards.

In case of Remote Signature Service, ATHEX generates and manages private keys on behalf of the Subscriber.

6.1.2 Private Key Delivery to Subscriber

As regards TLS/SSL Certificates Certificate Subscribers are solely responsible for the generation of the private keys used in their Certificate Requests. ATHEX does not provide SSL key generation, escrow, recovery or backup facilities.

As regards EU Qualified Certificates following QCP-n-qscd or QCP-l-qscd, the Qualified Signature Creation Device (QSCD) is sent via registered mail or courier; or is delivered directly to Subscriber at ATHEX premises. QSCD is maintained and used under Subscriber's sole control.

6.1.3 Public Key Delivery to Certificate Issuer

As regards TLS/SSL Certificates Certificate Subscribers send the public key to ATHEX through a structured Certificate Signing Request (PKCS#10).

6.1.4 CA Public Key Delivery to Relying Parties

ATHEX Public Keys are securely delivered to software providers to serve as trust anchors in commercial browsers and operating system root stores, or may be specified in a Certificate validation or path discovery policy file. Relying Parties may also obtain ATHEX self-signed CA Certificates containing the

Public Key from the ATHEX website.

Furthermore, ATHEX delivers the Root Certificates and Subordinates CA Certificates to the Greek Supervisory Body which is also responsible to inform the EU Trusted List of Greek QTSPs.

6.1.5 Key Sizes

Key sizes for Digital Certificates are disclosed in APPENDIX A.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes

The Private Key of ATHEX Root CA G3 has been used to sign only the following Certificates:

- Certificates for Subordinate CAs
- Certificates for infrastructure purposes (administrative role Certificates, internal CA operational device Certificates).

Keys may be used for the purposes and in the manner as described in APPENDIX A.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The ATHEX CA Infrastructure uses trustworthy systems to provide Certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

6.2.1 Cryptographic Module Standards and Controls

The generation and maintenance of ATHEX Root CA G3 and its Issuing CA Private Keys are facilitated through the use of an advanced cryptographic device known as a Hardware Security Module. The Hardware Security Module used by Issuing CAs in the ATHEX PKI are designed to provide at least Federal Information Processing Standard-140-2 Level 3 in both the generation and the maintenance in all Root and Issuing CA Private Keys.

For relevant European Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Certificate Subscriber Private Keys are generated and stored on a Qualified Electronic Signature/ Seal Creation Device (QSCD) which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards.

6.2.2 Private Key (m of n) Multi-Person Control

The procedure control at Section 5.2.2 is followed.

6.2.3 Private Key Escrow

Private keys are not escrowed.

6.2.4 Private Key Backup

ATHEX creates backup copies of CA key pairs and Subscriber key pairs generated and stored by a Remote QSCD, for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices.

6.2.5 Private Key Archival

ATHEX does not support private key archive.

6.2.6 Private Key Transfer Into or From Cryptographic Module

CA Private key transfer into or from a cryptographic module is performed in secure fashion in

accordance to manufacturing guidelines of module.

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.1.

6.2.8 Method of Activating Private Key

An EU Qualified Certificate Subscriber of type QCP-n-qscd or QCP-lqscd must be authenticated to the QSCD before the activation of the Private Key. This Authentication may be a specific PIN.

The Subscriber Private Keys on Remote QSCD are protected by username, password and OTP codes. The following rules apply:

- Subscriber needs to enter the username, password and OTP code to the QSCD for each transaction;
- In case the Subscriber enters a wrong username, password and OTP code 8 times in a row, the Remote QSCD account is locked;
- Remote QSCD account cannot be password reset;
- User may change the password.

6.2.9 Method of Deactivating Private Key

Issuing CA Private Keys are not usually deactivated, but are kept in locked computer cabinets with appropriate physical and logical security controls.

6.2.10 Method of Destroying Private Key

Procedural controls will prevent expired CA Key Pairs from being returned to production use. Furthermore, the CA private key is destroyed by deleting and overwriting the data (e.g., via re-initialization or zeroization) or physical destruction (e.g., with a metal shredder or hammer),in accordance to the guidelines of HSM manufacturer.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are part of Digital Certificates that will be archived in the Repository.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Usage periods for Public Keys and Private Keys shall match the usage periods for the Digital Certificate that binds the Public Key to an Individual, Organization, or Device.

The validity period is specified in APPENDIX A.

6.4 Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys. Examples of activation data include, but are not limited to, Personal Identification Numbers (PINs), passphrases, and portions of private keys used in a key-splitting regime.

6.4.1 Activation Data Generation and Installation

Activation data is generated in accordance with the specifications of the HSM. This hardware is certified by FIPS 140-3.

6.4.2 Activation Data Protection

If activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptographic Module (e.g. QSCD). PINs may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third-party interception of the PIN. Activation Data should be memorized, not written down. Activation Data must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g., a Certificate Subscriber's personal information.

Subscribers of Remote QSCD are required to safeguard their remote QSCD Secret Shares and sign an agreement acknowledging their Subscribers responsibilities. The Subscriber shall memorize the activation credentials (PIN, PUK, username, password, OTP) and not share them with anyone else.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

ATHEX has a formal Information Security Policy that documents the ATHEX policies, standards and guidelines relating to information security. This Information Security Policy has been approved by management and is communicated to all employees.

6.5.1 Specific Computer Security Technical Requirements

Computer security technical requirements are achieved utilizing a combination of hardened security modules and software, operating system security features, PKI and CA software and physical safeguards, including security Policies and Procedures that include but are not limited to:

- Access controls to ATHEX PKI infrastructure;
- Segregation of duties for PKI roles and regular review of privileged accounts at ATHEX PKI
- Identification and Authentication of personnel that fulfil roles of responsibility in the ATHEX PKI;
- Use of cryptographic smart cards and x.509 Certificates for all accounts capable of directly causing Certificate issuance.
- Archive of CA history and audit data

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

According to ATHEX Information Security Policy, the change management procedure is followed for the development and implementation of new system from the network layer up to the application layer. At the design phase, an analysis of security requirements is carried out.

6.6.2 Security Management Controls

Formal procedures and controls are in place to relating to the security-related configurations of ATHEX PKI according to ATHEX Information Security Policy.

6.6.3 Life Cycle Security Controls

ATHEX employs periodic internal procedures for verifying the CA software and monitoring the configuration of the CA systems.

All PKI changes follow the change management procedure, where at the design phase security analysis is performed.

6.7 Network Security Control

PKI infrastructure reside in highly segmented networks constrained from both the Internet and the ATHEX corporate network via multiple levels of firewalls. Firewalls have been configured to allow access only to those ports and IP addresses that are required for Issuing CA functions and monitoring systems.

All systems associated with certification authority activities shall be hardened with services restricted to only those necessary for certification authority operations strictly. Root CA equipment is kept in an offline state.

6.8 Time Stamping

The ATHEX Time-stamping Authority uses PKI and trusted time sources to provide reliable standards-based time-stamps. ATHEX TSA service is provided in accordance with ETSI EN 319 421.

The private keys and the TSU meet the technical specifications of ETSI EN 319 422. The TSU has a single time-stamp signing key active at a time. This key is sued exclusively for this purpose.

The time-stamps shall be issued securely and shall include the correct time. In particular:

- The time values the TSU uses in the time-stamp shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.
- The time included in the time-stamp shall be synchronized with within the accuracy defined in the policy and, if present, within the accuracy defined in the time-stamp itself.
- If the time-stamp provider's clock is detected as being out of the stated accuracy then time-stamps shall not be issued.
- The time-stamp shall be signed using a key generated exclusively for this purpose.
- The time-stamp generation system shall reject any attempt to issue time-stamps when the end of the validity of the TSU private key has been reached.

The TSU clock shall be synchronized with at least the following particular requirements:

- The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.
- 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 time-stamp issuance.
- The clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The Digital Certificate profile issued by ATHEX conforms to the specifications contained in IETF RFC 5280.

7.1.1 Version Number(s)

See APPENDIX A.

7.1.2 Certificate Extensions

See APPENDIX A.

7.1.3 Algorithm Object Identifiers

See APPENDIX A.

7.1.4 Name forms

See APPENDIX A.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

See APPENDIX A.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

See APPENDIX A.

7.1.9 Processing semantics for the critical Certificate Policies extension

7.2 CRL Profile

The profile for Certificate Revocation List (CRL) issued by ATHEX conforms to the specifications contained in IETF RFC 5280.

7.2.1 Version Number(s)

Version 2.

7.2.2 CRL and CRL Entry Extensions

- CRL Number (monotonically increasing integer - never repeated)
- Authority Key Identifier (same as Authority Key Identifier in Certificates issued by CA)
- CRL Entry Extensions
    - Invalidity Date (UTC - optional)
    - Reason Code (optional)

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) responder conforms to RFC 6960.

7.3.1 Version Number(s)

Version 1.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

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 this 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.

8.2 Identity/Qualifications of Assessor

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. Audits are performed by a public accounting firm that:

- Demonstrates proficiency in conducting these certifications
- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function

8.3 Assessor's Relationship to Assessed Entity

The Qualified and Accredited Auditor is independent of ATHEX, and does not have a financial interest, business relationship, or course of dealing that would create a conflict of interest or create a significant bias (for or against) ATHEX.

8.4 Topics Covered by Assessment

The scope of ATHEX annual audit includes the following Services:

- Against the regulation eIDAS and the supporting ETSI European Norms
  - Qualified Certificates for Electronic Signatures
  - Qualified Certificates for Electronic Seals
  - Qualified Certificates for Electronic Timestamps
  - Qualified Certificates for Website Authentication
  - Qualified Certificates for Website Authentication supporting PSD2 transactions
- Against the CA/Browser Forum
  - Certificates adhered to Baseline Requirements
  - Extended Validation Certificates
  - Extended Validation for Code Signing

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of ATHEX's operations, significant exceptions or deficiencies identified during the audit will result in a determination of actions to be taken. This determination is made by ATHEX management with input from the auditor. ATHEX management is responsible for developing and implementing a corrective action plan. If ATHEX determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the Certificates issued under this CP/CPS, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, ATHEX management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communications of Results

The results of these audits may be released at the discretion of ATHEX management.

ATHEX submits this audit report to Greek Supervisory Body.

8.7 Self-Audits

The self-audit monitors adherence to this CP/CPS and strictly controls ATHEX's service quality against a randomly selected sample of the greater of one Certificate or at least 3% of the TLS/SSL Certificates (EV Certificates, Standard TLS/SSL Certificates and EV Code Signing Certificates) issued by ATHEX during the period commencing immediately after the previous self-audit sample was taken.

Results of the Periodic audits are presented to ATHEX's PKI Policy Authority with a description of any deficiencies noted and corrective actions taken.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

ATHEX is entitled to charge Subscribers for verification, issuance, management, and renewal of Certificates. The fees charged will be as stated on ATHEX website or in any applicable contract at the time the Digital Certificate is issued or renewed, and may change from time to time without prior notice.

9.1.2 Certificate Access Fees

ATHEX does not charge a fee as a condition of making a Digital Certificate available in a repository or otherwise making Digital Certificates available to Relying Parties

9.1.3 Revocation or Status Information Access Fees

ATHEX does not charge a fee as a condition of making the CRL required by this CP/CPS available in a repository or otherwise available to Relying Parties. ATHEX may, however, charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

ATHEX will refund fees and will revoke a Certificate upon request by the Subscriber within seven days of issuance or renewal of the Certificate. To request a refund, please contact the person who is referred by section 1.5.2.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

ATHEX currently maintains commercially reasonable insurance.

9.2.2 Other Assets

Customers shall maintain adequate financial resources for their operations and duties, and shall be able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

ATHEX encourages customers, Subscribers, End-Entities, Relying Parties, and all other entities to maintain adequate insurance to protect against errors and omissions, professional liability, and general liability.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered confidential:

- All private keys
- Business Continuity Plan
- Termination Plan
- Security practices, measures or mechanisms used to protect confidentiality, integrity or availability of information
- Any information specified in Section 9.4.4.
- Audit logs and archive records

9.3.2 Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data and information appearing in Certificates is public information.

9.3.3 Responsibility to Protect Confidential Information

ATHEX PKI Participants are responsible for protecting Confidential Business Information in their possession, control or custody.

9.4 Privacy of Personal Information

9.4.1 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.

9.4.2 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.

9.4.3 Information Not Deemed Private

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

9.4.4 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.

9.4.5 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.

9.4.6 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.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

ATHEX owns all intellectual property rights associated with its databases, websites, Digital Certificates and any other publication originating from ATHEX including this CP/CPS.

9.6 Representations and Warranties

9.6.1 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 and 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.

For further obligations and warranties please refer to APPENDIX A.

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.

9.6.2 RA Representations and Warranties

ATHEX as RA, performs its functions by Complying with this CP/CPS in all material aspects.

For RA Warranties see Section 9.6.1.

9.6.3 Subscriber Representations and Warranties

See APPENDIX A.

9.6.4 Relying Party Representations and Warranties

Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP/CPS and any other precautions prescribed in the ATHEX Subscriber Agreement.

9.6.5 Representations and Warranties of other Participants

No stipulation

9.7 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 and throughout the entire period of Certificate validity may not be cumulatively less than 2000 $.

9.8 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.

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.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

Unless otherwise set forth in this CP/CPS and/or Subscriber Agreement, Subscriber, as applicable, hereby agrees to indemnify and hold, ATHEX (including, but not limited to, its officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of a Certificate and that arises from:

- any false or misleading statement of fact by the Subscriber (or any person acting on the behalf of the Subscriber
- any failure by the Subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive;
- any failure on the part of the Subscriber to protect its Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of Certificate; or
- any failure on the part of the Subscriber to promptly notify ATHEX, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Certificate once the Subscriber has constructive or actual notice of such event.

9.10 Term and Termination

9.10.1 Term

The CP/CPS becomes effective upon publication in the ATHEX repository. Amendments to this CP/CPS become effective upon publication in the ATHEX repository.

9.10.2 Termination

This CP/CPS, including all amendments remain in force until it is replaced by a newer version.

9.10.3 Effect of Termination and Survival

Upon termination of this CP/CPS, ATHEX PKI Participants are nevertheless bound by its terms

- for Digital Certificates issued for the remainder of the validity periods of such Certificates; and
- for protecting business confidential and private personal information.

9.11 Individual Notices and Communications with Participants

PKI Participants can provide their notices required pursuant to this CP/CPS either by e-mail, postal mail or fax (see Section 1.5).

ATHEX provides notices required by this CP/CPS to Participants either by e-mail, postal mail or fax

9.12 Amendments

9.12.1 Procedure for Amendment

This CP/CPS undergoes a regular review process and is subject to amendment on at least an annual basis as prescribed by the ATHEX PMC. Amendments may be made by updating the entire document or by addendum.

The approval procedure that is followed is described in section 1.5.4.

The reasons that can cause amendments may be technological developments, regulatory framework changes, trade and transactional requirements of ATHEX and/or subscribers and ATHEX business plans.

9.12.2 Notification Mechanism and Period

The CP/CPS and any amendments thereto are available through http://www.athexgroup.gr/el/web/guest/digital-Certificates-pki-regulations .

ATHEX submits to the Greek Supervisory Body the updated version of this CP/CPS.

9.12.3 Circumstances under which OID must be changed

The ATHEX PMC reserves the right to amend this CP/CPS without notification for amendments that are not material, including clerical changes. The decision to designate amendments as material or non-material to this CP/CPS is at the sole discretion of the ATHEX PMC. Tshe last digits of Object Identifier to this CP/CPS represent the version of this document.

9.13 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.

9.14 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.

9.15 Compliance with Applicable Law

Subscribers and Relying Parties acknowledge and agree to use Certificates in compliance with all applicable laws and regulations, ATHEX may refuse to issue or may revoke Certificates if in the reasonable opinion of ATHEX such issuance or the continued use of such Certificates would violate applicable laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

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

No stipulation.

9.16.5 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.

9.17 Other Provisions

No stipulation.

10 APPENDIX A

10.1 ATHEX TLS/SSL Certificates CA G3

10.1.1 Purpose

The purposes of a TLS/SSL Certificate are to:

- Identify the legal entity that controls a website;
- Enable encrypted communications with a website.

10.1.2 Commitment to Comply with Guidelines

The TLS/SSL Certificates from ATHEX Root CA G3 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.

10.1.3 Who can apply

Incorporated entities, government entities, general partnerships, unincorporated associations, and individual entrepreneurship

10.1.4 Subscriber Agreement

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' 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, following compromise of the subject's private key, to immediately and permanently discontinue the use of this key, except for key decipherment; and
7. 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.

10.1.5 ATHEX TLS/SSL Certificates Warranties

When ATHEX issues an TLS/SSL Certificate, ATHEX warranties to ATHEX PKI Participants, during the period when the TLS/SSL Certificate is Valid, that ATHEX has followed the requirements of TLS/SSL Guidelines and its TLS/SSL Policies in issuing and managing the TLS/SSL Certificate and in verifying the accuracy of the information contained in the TLS/SSL Certificate.

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

- Right to Use Domain Name or IP Address: 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) and IP address(es) listed in the TLS/SSL 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 TLS/SSL Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;
- Authorization for TLS/SSL Certificate: That, at the time of issuance, ATHEX (i) implemented a procedure for verifying that the Subject authorized the issuance of the TLS/SSL Certificate and that the Applicant Representative is authorized to request the TLS/SSL Certificate on behalf of the Subject; (ii) followed the procedure when issuing the TLS/SSL Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;
- 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 TLS/SSL Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the TLS/SSL Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;
- No Misleading Information: That, at the time of issuance, ATHEX (i) implemented a procedure for reducing the likelihood that the information contained in the TLS/SSL Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the TLS/SSL Certificate; and (iii) accurately described the in

ATHEX CA G3 CP/CPS;

- Identity of Applicant: That, if the TLS/SSL Certificate contains Subject Identity Information, ATHEX (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2 of CA/Browser Forum Baseline Requirements; (ii) followed the procedure when issuing the TLS/SSL Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;
- 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 unexpired TLS/SSL Certificates; and
- Revocation**:** That ATHEX will revoke the TLS/SSL Certificate for any of the reasons specified in these Requirements.

10.1.6 Verification Process

Before issuing a Business SSL Certificate, ATHEX performs limited procedures to verify that all Subject information in the Certificate is correct, and that the Applicant is authorized to use the domain name and has accepted a Subscriber Agreement for the requested Certificate.

ATHEX shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA of ATHEX shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

Identity:
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 the CA or a third party who is acting as an agent for the CA; or
- An Attestation Letter.

DBA/Tradename:
If the Subject Identity Information is to include a DBA or tradename, ATHEX verifies the Applicant's right to use the DBA/tradename using at least one of the following:

- Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
- A Reliable Data Source; 3. Communication with a government agency responsible for the management of such DBAs or tradenames;
- An Attestation Letter accompanied by documentary support; or
- A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

Verification of Country:
ATHEX verifies the country associated with the Subject using one of the following:

- the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;
- the ccTLD of the requested Domain Name;
- information provided by the Domain Name Registrar; or

- a method identified in “Identity” above.

Note that in case of SSL certificates provided to ATHEX the above verification process is not followed.

10.1.7 Application Process

The steps of the application process are:

1. The Applicant provides:
   - PCKCS#10 CSR
   - Signed Subscriber Agreement ATHEX verifies information using a variety of sources.
3. ATHEX obtains and documents further explanation or clarification as necessary to resolve discrepancies or details requiring further explanation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, ATHEX will decline the Certificate Request and notify the Applicant accordingly.
4. ATHEX issues the TLS/SSL Certificate, which is placed in Hold status.
5. The TLS/SSL Certificate is delivered to the Applicant.
6. The Applicant accepts Certificate issuance.
7. ATHEX activates the TLS/SSL Certificate.

Field	**CONTENTS**
Version	V3
Serial Number	Unique system generated random number assigned to each Certificate, containing at least 64 bits of output.
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX SSL Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	1, 2 or 3 years
Subject Distinguished Name • TLS/SSL Certificates for DV must include FQDN or IP address at subjectAltName • TLS/SSL Certificates for OV must also include at least the following attributes: o Organization o Country o Locality or stateOrProvinceName	
Organization Name	Must not be present at DV Certificates Mandatory for OV Certificates Subject Organization Name is verified in accordance with Section 3.2.2 of BR
Organization Unit	Must not be present at DV Certificates Optional for OV Certificates Subject Organizational Unit
Common Name	Optional for DV and OV Certificates It must contain at least one FQDN or an IP address that is one of the values contained in the subjectAltName extension.
Locality	Must not be present at DV Certificates Locality or stateOrProvinceName must be present for OV Certificates

State or province (if any)	Must not be present at DV Certificates Locality or stateOrProvinceName must be present for OV Certificates It is verified in accordance with Section 3.2.2 of BR
Country	Must not be present at DV Certificates Mandatory for OV Certificates Subject Country is verified in accordance with Section 3.2.2 of BR
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Mandatory for DV and OV Certificates Critical Digital Signature, Key Encipherment
Extended Key Usage	Mandatory for DV and OV Certificates Not Critical Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Mandatory for DV and OV Certificates Not Critical
Certificate Policies	Mandatory for DV and OV Certificates For TLS/SSL Certificates for DV: Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.3.100.1.1} [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations [2]Certificate Policy: Policy Identifier= 0.4.0.2042.1.6 For TLS/SSL Certificates for OV: Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.3.100.1.2} [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.7
Authority Info Access	Mandatory for DV and OV Certificates Not Critical [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

	Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXSSLCertificatesCAG3.crt
Authority Key Identifier	Mandatory for DV and OV Certificates Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Mandatory for DV and OV Certificates Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXSSLCertificatesCAG3.crl
Basic Constraints	Mandatory for DV and OV Certificates For TLS/SSL Certificates for DV: Not Critical Subject Type=End Entity For TLS/SSL Certificates for OV: Critical Subject Type=End Entity
Subject Alternative Name	Mandatory for DV and OV Certificates Not Critical FQDN of Device It is verified in accordance with Section 3.2.2 of BR
Certificate Transparency	Optional for DV and OV Certificates This field may include two or more Certificate Transparency proofs from approved CT Logs

10.2 ATHEX Extended Validation (EV) SSL Certificates CA G3

10.2.1 Purpose

Extended Validation (EV) Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols.

The purposes of a EV Certificate are to:

- Identify the legal entity that controls a website;
- Enable encrypted communications with a website
- EV Certificates also help establish the legitimacy of a business claiming to operate a website or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:
    - Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;
    - Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
    - Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

ATHEX EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject.

ATHEX EV Certificates are not intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;
- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is “safe” to do business with the Subject named in the EV Certificate.

10.2.2 Commitment to Comply with Guidelines

The EV Code Signing Certificates from ATHEX Root CA G3 conform to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

10.2.3 Who can apply

Private Organizations, Government Entities, Business Entities and Non-Commercial Entities.

An Applicant qualifies as a Private Organization if:

- The entity’s legal existence is created or recognized by a by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a Certificate of incorporation, registration number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);
- The entity designated with the Incorporating or Registration Agency a Registered Agent, a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration), or an equivalent facility;
- The entity is not designated on the records of the Incorporating or Registration Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;
- The entity has a verifiable physical existence and business presence;
- The entity’s Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place

of Business is not in any country where the CA is prohibited from doing business or issuing a Certificate by the laws of the CA's jurisdiction; and EV Guidelines, v. 1.6.9 9
- The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

An Applicant qualifies as a Government Entity if:
- The entity's legal existence was established by the political subdivision in which the entity operates;
- The entity is not in any country where the CA is prohibited from doing business or issuing a Certificate by the laws of the CA's jurisdiction; and
- The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

An Applicant qualifies as a Business Entity if:
- The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, Certificate, or license, and the entity's existence can be verified with that Registration Agency;
- The entity has a verifiable physical existence and business presence;
- At least one Principal Individual associated with the entity is identified and validated by the CA;
- The identified Principal Individual attests to the representations made in the Subscriber Agreement;
- the CA verifies the entity's use of any assumed name used to represent the entity pursuant to the requirements of Section 11.3 of EV Guidelines;
- The entity and the identified Principal Individual associated with the entity are not located or residing in any country where the CA is prohibited from doing business or issuing a Certificate by the laws of the CA's jurisdiction; and
- The entity and the identified Principal Individual associated with the entity are not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

An Applicant qualifies as a Non-Commercial Entity if:
- The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of Applicants who qualify as an International Organization for EV eligibility; and
- The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a Certificate by the laws of the CA's jurisdiction; and
- The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- Subsidiary organizations or agencies of an entity that qualifies as a Non-Commercial Entity also qualifies for EV Certificates as a Non-Commercial Entity.

10.2.4 Subscriber Agreement

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' 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.

10.2.5 ATHEX EV Certificate Warranties

When ATHEX issues an EV Certificate, ATHEX warranties to ATHEX PKI Participants, during the period when the EV Certificate is Valid, that ATHEX has followed the requirements of EV Guidelines and its EV Policies in issuing and managing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate.

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

- Legal Existence: ATHEX has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- Identity: ATHEX has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- Right to Use Domain Name: ATHEX has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the right to use all the Domain Name(s) listed in the EV Certificate;
- Authorization for EV Certificate: ATHEX has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
- Accuracy of Information: ATHEX has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
- Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with ATHEX that satisfies the requirements of EV Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
- Status: ATHEX follows the requirements of EV Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and

- Revocation**:** ATHEX follows the requirements of EV Guidelines and revoke the EV Certificate for any of the revocation reasons specified in these Guidelines.

10.2.6 Applicant roles

EV Guidelines specify the following Applicant roles for the issuance of an EV Certificate:

1. Certificate Requester: The EV Certificate Request is submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.
2. Certificate Approver: The EV Certificate Request is approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
3. Contract Signer: A Subscriber Agreement applicable to the requested EV Certificate is signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
4. Applicant Representative: In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate is acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any of these roles.

10.2.7 Verification Requirements

Before issuing an EV Certificate, the ATHEX ensures that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, EV Guidelines and matches the information confirmed and documented by ATHEX pursuant to its verification processes. Such verification processes are intended to accomplish the following:

- Verify Applicant's existence and identity, including;
    - Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 of EV Guidelines),
    - Verify the Applicant's physical existence (business presence at a physical address), and
    - Verify the Applicant's operational existence (business activity).
- Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;
- Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;
- Verify the Applicant's authorization for the EV Certificate, including;
    - Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
    - Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
    - Verify that a Certificate Approver has signed or otherwise approved the EV

Certificate Request.

As a general rule, ATHEX is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subsections below. The Acceptable Methods of Verification set forth in each of Sections 11.2 through 11.14 of EV Guidelines (which usually include alternatives) are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, ATHEX is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

10.2.8 Application Process

Two ATHEX Validation Specialists are involved in the Application Process.

The steps of the application process are:

1. The Certificate Requester provides:
    a. PCKCS#10 CSR
    b. The contacts info of Applicant Roles
    c. Subscriber Agreement signed by Contract SignerATHEX First Validation Specialist reviews and verifies all information that is required to be verified by the EV Guidelines.
3. All signatures by Certificate Requesters and Certificate Approvers are verified
4. ATHEX obtains and documents further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, and/or other sources of information as necessary to resolve discrepancies or details requiring further explanation. ATHEX Second Validation Specialist who is not responsible for the collection and review of information reviews all of the information and documentation assembled in support of the EV Certificate and looks for discrepancies or other details requiring further explanation. ATHEX Second Validation Specialist approves the issuance of EV Certificate.
5. ATHEX issues the EV Certificate, which is placed in Hold status.
6. The Certificate Approver is contacted to obtain approval of Certificate issuance.
7. The Certificate Approver accepts Certificate issuance.
8. ATHEX activates the EV Certificate.

ATHEX refrains from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate Request is such that issuance of the EV Certificate will not communicate factual information that ATHEX knows, or the exercise of due diligence should discover from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, ATHEX will decline the EV Certificate Request and notify the Applicant accordingly.

10.2.9 Age of Validated Data

The age of all data used to support issuance of an EV Certificate (before revalidation is required) shall not exceed thirteen months.

In the case of outdated information, ATHEX repeats the verification processes required by the EV Guidelines.

Field	**CONTENTS**
Version	V3
Serial Number	Unique system generated random number assigned to each Certificate, containing at least 64 bits of output.
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens

	CN = ATHEX Extended Validation Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	1 or 2 years
Subject Distinguished Name	
Organization Name	Mandatory This field must contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organization name will be used
Organization Unit	Optional Subject Organizational Unit
Common Name	Optional It must contain at least one FQDN or an IP address that is one of the values contained in the subjectAltName extension.
City or Town of Incorporation	May be required subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1) Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the city or town level, including both country and state or province information as follows
State/Province of Incorporation	May be required subject:jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the state or province level, including country information as follows, but not city or town information above
Country of Incorporation	Mandatory subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) Jurisdiction of Incorporation for an Incorporating or Registration Agency at the country level would include country information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code
Registration Number	Mandatory Subject:serialNumber (2.5.4.5) For Private Organizations and Business Entities, this field MUST contain the unique Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation. If the Incorporating or Registration Agency does not provide Registration Numbers, then the field will contain the date of incorporation or registration. For Government Entities, that do not have a Registration Number or verifiable date of creation, the field will contain the label "Government Entity".

Business Category	Mandatory Subject:businessCategory (2.5.4.15) This field must contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity", depending on which section of the EV Guidelines applies to the Subject
Number & street	Optional subject:streetAddress (2.5.4.9)
Locality	Locality or stateOrProvinceName must be present subject:localityName (2.5.4.7)
State or province	Locality or stateOrProvinceName must be present subject:stateOrProvinceName (2.5.4.8)
Country	Mandatory subject:countryName (2.5.4.6)
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Mandatory Critical Digital Signature, Key Encipherment
Extended Key Usage	Mandatory Not Critical Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Mandatory Not Critical
Certificate Policies	Mandatory Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.3.100.1.3} [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations [2]Certificate Policy: Policy Identifier=2.23.140.1.1
Authority Info Access	Mandatory Not Critical [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr.gr/pki/-/file/ATHEXExtendedValidationCertificatesCAG3.crt

Authority Key Identifier	Mandatory Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Mandatory Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/- /file/ATHEXExtendedValidationCertificatesCAG3.crl
Basic Constraints	Mandatory Critical Subject Type=End Entity
Subject Alternative Name	Mandatory Not Critical FQDN of Device It is verified in accordance with Section 9.2 of EV Guidelines Wildcard domain names are prohibited for EV Certificates
Certificate Transparency	Optional This field MAY include two or more Certificate Transparency proofs from approved CT Logs

10.3 ATHEX Extended Validation (EV) Code Signing Certificates CA G3

10.3.1 Purpose

ATHEX EV Code Signing Certificates and signatures are intended to be used to verify the identity of the Subscriber and the integrity of its code. They provide assurance to a user or platform provider that code verified with the Certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. EV Code Signing Certificates may help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware.

No particular software object is identified by an EV Code Signing Certificate, only its distributor is identified.

ATHEX EV Code Signing Certificates are not intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Code Signing Certificate is actively engaged in doing business;
- That the Subject named in the EV Code Signing Certificate complies with applicable laws;
- That the Subject named in the EV Code Signing Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is "safe" to do business with the Subject named in the EV Code Signing Certificate.

10.3.2 Commitment to Comply with Guidelines

The EV Code Signing Certificates from ATHEX Root CA G3 conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

10.3.3 Who can apply

Private Organizations, Government Entities, Business Entities and Non-Commercial Entities.

10.3.4 Subscriber Agreement

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 not knowingly sign software that contains Suspect Code and use the EV Code Signing Certificate as follows:
    - only to sign code that complies with the requirements set forth in the EV Code Signing Guidelines;
    - solely in compliance with all applicable laws;
    - solely for authorized company business; and
    - solely in accordance with the Subscriber Agreement;

- Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request ATHEX to revoke the Certificate, in the event that:
    - there is evidence that the Certificate was used to sign suspect code;
    - any information in the Certificate is, or becomes, incorrect or inaccurate; or
    - there is any actual or suspected misuse or compromise of either the key activation data or the Subscriber's Private Key associated with the Public Key included in the Certificate;
- 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.

10.3.5 ATHEX EV Code Signing Certificate Warranties

When ATHEX issues an EV Code Signing Certificate, ATHEX warranties to ATHEX PKI Participants, during the period when the EV Code Signing Certificate is Valid, that ATHEX has followed the requirements of EV Code Signing Guidelines and its EV Policies in issuing and managing the EV Code Signing Certificate and in verifying the accuracy of the information contained in the EV Code Signing Certificate.

Similarly, when a Signing Authority provides an EV Signature, the Signing Authority represents and warrants to the ATHEX PKI Participants, during the period when the EV Signature is Valid, that ATHEX has followed the requirements in providing the EV Signature to the Subscriber.

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

- Legal Existence: ATHEX has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Code Signing Certificate was issued, the Subject named in the EV Code Signing Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- Identity: ATHEX has confirmed that, as of the date the EV Code Signing Certificate was issued, the legal name of the Subject named in the EV Code Signing Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- Authorization for EV Code Signing Certificate: ATHEX has taken all steps reasonably necessary to verify that the Subject named in the EV Code Signing Certificate has authorized the issuance of the EV Code Signing Certificate;
- Accuracy of Information: ATHEX has taken all steps reasonably necessary to verify that all of the other information in the EV Code Signing Certificate is accurate, as of the date the EV Certificate was issued;
- Subscriber Agreement: The Subject named in the EV Code Signing Certificate has entered into a legally valid and enforceable Subscriber Agreement with ATHEX that satisfies the requirements of EV Code Signing Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
- Status: ATHEX follows the requirements of EV Code Signing Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Code

Signing Certificate as Valid or revoked; and

- Revocation**:** ATHEX follows the requirements of EV Code Signing Guidelines and revoke the EV Code Signing Certificate for any of the revocation reasons specified in these Guidelines.

10.3.6 Verification Requirements

Before issuing an EV Code Signing Certificate, the ATHEX ensures that all Subject organization information to be included in the EV Code Signing Certificate conforms to the requirements of, and is verified in accordance with the EV Guidelines and matches the information confirmed and documented by ATHEX pursuant to its verification processes. Such verification processes are intended to accomplish the following:

- Verify Applicant's existence and identity, including;
    - Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 of EV Code Signing Guidelines),
    - Verify the Applicant's physical existence (business presence at a physical address), and
    - Verify the Applicant's operational existence (business activity).
- Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Code Signing Certificate;
- Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;
- Verify the Applicant's authorization for the EV Code Signing Certificate, including;
    - Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
    - Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
    - Verify that a Certificate Approver has signed or otherwise approved the EV Code Signing Certificate Request.

An EV Timestamp Authority is not required to validate in any way data submitted to it for time-stamping. It simply adds the time to the data that are presented to it, signs the result and appends its own Certificate.

10.3.7 Application Process

Two ATHEX Validation Specialists are involved in the Application Process.

The steps of the application process are:

1. The Certificate Requester provides:
    a. PCKCS#10 CSR
    b. The contacts info of Applicant Roles
    c. Subscriber Agreement signed by Contract SignerATHEX First Validation Specialist reviews and verifies all information that is required to be verified by the EV Code Signing Guidelines.
3. All signatures by Certificate Requesters and Certificate Approvers are verified
4. ATHEX obtains and documents further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, and/or other sources of information as necessary to resolve discrepancies or details requiring further explanation. ATHEX Second Validation Specialist who is not responsible for the collection and review of information reviews all of the information and documentation assembled in support of the EV Code Signing Certificate and looks for discrepancies or other details requiring further explanation. ATHEX Second Validation Specialist approves the issuance of EV Certificate.
5. ATHEX issues the EV Code Signing Certificate, which is placed in Hold status.
6. The EV Code Signing Certificate is delivered to the Certificate Approver.
7. The Certificate Approver is contacted to obtain approval of Certificate issuance.

8. The Certificate Approver accepts Certificate issuance.
9. ATHEX activates the EV Code Signing Certificate.

ATHEX refrains from issuing an EV Code Signing Certificate until the entire corpus of information and documentation assembled in support of the EV Code Signing Certificate Request is such that issuance of the EV Code Signing Certificate will not communicate factual information that ATHEX knows, or the exercise of due diligence should discover from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, ATHEX will decline the EV Code Signing Certificate Request and notify the Applicant accordingly.

10.3.8 Age of Validated Data

The age of all data used to support issuance of an EV Code Signing Certificate (before revalidation is required) shall not exceed thirteen months.

In the case of outdated information, ATHEX repeats the verification processes required by the EV Guidelines.

Field	**CONTENTS**
Version	V3
Serial Number	Unique system generated random number assigned to each Certificate, containing at least 64 bits of output.
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Code Signing Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	1 or 2 years
Subject Distinguished Name	
Organization Name	Mandatory This field must contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organization name will be used
Organization Unit	Optional Subject Organizational Unit
Common Name	Mandatory The Subject's verified legal name
City or Town of Incorporation	May be required subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1) Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the city or town level, including both country and state or province information as follows

State/Province of Incorporation	May be required subject:jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the state or province level, including country information as follows, but not city or town information above
Country of Incorporation	Mandatory subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) Jurisdiction of Incorporation for an Incorporating or Registration Agency at the country level would include country information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code
Registration Number	Mandatory Subject:serialNumber (2.5.4.5) For Private Organizations and Business Entities, this field MUST contain the unique Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation. If the Incorporating or Registration Agency does not provide Registration Numbers, then the field will contain the date of incorporation or registration. For Government Entities, that do not have a Registration Number or verifiable date of creation, the field will contain the label “Government Entity”.
Business Category	Mandatory Subject:businessCategory (2.5.4.15) This field must contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity", depending on which section of the EV Guidelines applies to the Subject
Number & street	Optional subject:streetAddress (2.5.4.9)
Locality	Locality or stateOrProvinceName must be present subject:localityName (2.5.4.7)
State or province (if any)	Locality or stateOrProvinceName must be present subject:stateOrProvinceName (2.5.4.8)
Country	Mandatory subject:countryName (2.5.4.6)
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Mandatory Critical Digital Signature
Extended Key Usage	Mandatory Not Critical id-kp-codeSigning
Subject Key Identifier	Mandatory Not Critical
Certificate Policies	Mandatory

	Not Critical [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.300.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=2.23.140.1.3
Authority Info Access	Mandatory Not Critical [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXCodeSigningCertificatesCAG3.crt
Authority Key Identifier	Mandatory Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Mandatory Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXCodeSigningCertificatesCAG3.crl
Basic Constraints	Mandatory Critical Subject Type=End Entity

10.4 ATHEX QWAC and QWAC for PSD2

10.4.1 Purpose

ATHEX Qualified Website Authentication Certificates (QWAC) are aimed to support website authentication based on a qualified Certificate defined in articles 3 (38) and 45 of the Regulation (EU) No 910/2014.

Certificates issued under these requirements endorse the requirement of EV Certificates whose purpose is specified in clause 5.5 of ETSI EN 319 411-1 [2]. In addition, EU qualified Certificates issued under this policy may be used to provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website as specified in Regulation (EU) No 910/2014.

ATHEX QWAC for PSD2 Certificates make it possible to establish a Transport Layer Security channel with the subject of the Certificate, which secures data transferred through the channel.

10.4.2 Commitment to Comply with Standards

The ATHEX QWAC from ATHEX Root CA G3 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 take precedence over this document.

10.4.3 Who can apply

ATHEX QWAC are issued only to legal persons who operate website.

ATHEX QWAC for PSD2 are issued only to PSPs registered by NCA.

10.4.4 Subscriber Agreement

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' 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.

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 or to the subject;
6. 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
7. 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.

10.4.5 ATHEX Qualified Certificate Warranties

When ATHEX issues an QWAC Certificate, ATHEX warranties to ATHEX PKI Participants, during the period when the QWAC Certificate is Valid, that ATHEX has followed the requirements of QWAC Guidelines and its QWAC Policies in issuing and managing the QWAC Certificate and in verifying the accuracy of the information contained in the QWAC Certificate.

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

- Right to Use Domain Name or IP Address: 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) and IP address(es) listed in the QWAC 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 QWAC Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;
- Authorization for QWAC Certificate: That, at the time of issuance, ATHEX (i) implemented a procedure for verifying that the Subject authorized the issuance of the QWAC Certificate and that the Applicant Representative is authorized to request the QWAC Certificate on behalf of the Subject; (ii) followed the procedure when issuing the QWAC Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;
- 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 QWAC Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure

when issuing the QWAC Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;

- No Misleading Information: That, at the time of issuance, ATHEX (i) implemented a procedure for reducing the likelihood that the information contained in the QWAC Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the QWAC Certificate; and (iii) accurately described the in ATHEX CA G3 CP/CPS;
- Identity of Applicant: That, if the QWAC Certificate contains Subject Identity Information, ATHEX (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2 of CA/Browser Forum Baseline Requirements; (ii) followed the procedure when issuing the QWAC Certificate; and (iii) accurately described the procedure in ATHEX CA G3 CP/CPS;
- 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 unexpired QWAC Certificates; and
- Revocation**:** That ATHEX will revoke the QWAC Certificate for any of the reasons specified in these Requirements.

10.4.6 Verification Requirements

ATHEX shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA of ATHEX shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

Before issuing a QWAC, the ATHEX ensures that all Subject organization information to be included in the QWAC conforms to the requirements of, and is verified in accordance with the EV Guidelines and matches the information confirmed and documented by ATHEX pursuant to its verification processes. Such verification processes are intended to accomplish the following:

- Verify Applicant's existence and identity, including;
    - Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 of EV Guidelines),
    - Verify the Applicant's physical existence (business presence at a physical address), and
    - Verify the Applicant's operational existence (business activity).
- Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;
- Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;
- Verify the Applicant's authorization for the QWAC, including;
    - Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
    - Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
    - Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.
- Only for QWAC for supporting PSD2 transaction, verify the specific PSD2 attributes at public or EBA register

As a general rule, ATHEX is responsible for taking all verification steps reasonably necessary to satisfy

each of the Verification Requirements set forth in the subsections below. The Acceptable Methods of Verification set forth in each of Sections 11.2 through 11.14 of EV Guidelines (which usually include alternatives) are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, ATHEX is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

Furthermore, evidence shall be provided of:

- identifier of the device by which it can be referenced (e.g. Internet domain name);
- full name of the organizational entity;
- assumed name (according to 11.3.2 clause of EV Guidelines)
- any relevant existing registration information (e.g. company registration) of the legal person or other organizational entity identified in association with the legal person that would appear in the organization attribute of the Certificate, consistent with the national or other applicable identification practices;
- a nationally recognized identity number, or other attributes which can be used to, as far as possible, distinguish the organizational entity from others with the same name;
- 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; and
- the identity of the subscriber and its link with the domain name to be certified and, if applicable, any specific attributes of the person shall be verified either by physical presence or 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.

Note that in case of QWAC certificates provided to domains which belong to ATHEX, the above verification tasks are not followed.

10.4.7 Application Process

Two ATHEX Validation Specialists are involved in the Application Process.

The steps of the application process are:

1. The duly mandated subscriber provides:
    a. PCKCS#10 CSR
    b. Signed Subscriber AgreementATHEX First Validation Specialist reviews and verifies all information that is required to be verified by QWAC.
3. The duly mandated subscriber is contacted to obtain approval of Certificate issuance.
4. All signatures by Subscriber are verified
5. ATHEX obtains and documents further explanation or clarification from the duly mandated subscriber, and/or other sources of information as necessary to resolve discrepancies or details requiring further explanation. ATHEX Second Validation Specialist who is not responsible for the collection and review of information reviews all of the information and documentation assembled in support of the QWAC and looks for discrepancies or other details requiring further explanation. ATHEX Second Validation Specialist approves the issuance of QWAC.
6. ATHEX creates the QWAC which is placed in Hold status.
7. The QWAC is delivered to the Subscriber.
8. The Subscriber accepts Certificate issuance
9. ATHEX activates the QWAC Certificate.
10. Only for QWAC for supporting PSD2, ATHEX notifies NCA for Certificate issuance. ATHEX refrains from issuing an QWAC until the entire corpus of information and documentation assembled in support of the QWAC Request is such that issuance of the QWAC will not communicate factual information that ATHEX knows, or the exercise of due diligence should discover from the assembled information and documentation,. If satisfactory explanation

and/or additional documentation are not received within a reasonable time, ATHEX will decline the QWAC Request and notify the Applicant accordingly.

10.4.8 Age of Validated Data

The age of all data used to support issuance of QWAC (before revalidation is required) shall not exceed thirteen months.

In the case of outdated information, ATHEX repeats the verification processes required.

Field	**CONTENTS**
Version	V3
Serial Number	Unique system generated random number assigned to each Certificate, containing at least 64 bits of output.
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX Qualified WEB Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 or 2 years
Subject Distinguished Name	
Organization Name	Mandatory This field must contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organization name will be used.
Organization Unit	Optional Subject Organizational Unit
OrganizationIdentifier	Mandatory for QWAC and QWAC for PSD2 Its structure for QWAC is: • 3 character legal person identity type reference (e.g. VAT) • 2 character ISO 3166-1 [8] country code • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); • identifier (according to country and identity type reference) Its structure for QWAC supporting PSD2: PSD2 Authorization Number recognized by the NCA. For Bank of Greece this Authorization Number has the following structure: • "PSD" as 3 character legal person identity type reference; • 2 character ISO 3166-1 [8] country code representing the NCA country; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); • 2-8 character NCA identifier without country code (A-Z

	uppercase only, no separator); • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • PSP identifier (authorization number as specified by the NCA. There are no restrictions on the characters used).
Common Name	Optional It must contain at least one FQDN or an IP address that is one of the values contained in the subjectAltName extension.
City or Town of Incorporation	May be required subject:jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1) Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the city or town level, including both country and state or province information as follows
State/Province of Incorporation	May be required subject:jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) Full name of Jurisdiction of Incorporation for an Incorporating or Registration Agency at the state or province level, including country information as follows, but not city or town information above
Country of Incorporation	Mandatory subject:jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) Jurisdiction of Incorporation for an Incorporating or Registration Agency at the country level would include country information but would not include state or province or city or town information. Country information MUST be specified using the applicable ISO country code
Business Category	Mandatory Subject:businessCategory (2.5.4.15) This field must contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity", depending on which section of the EV Guidelines applies to the Subject
Number & street	Optional subject:streetAddress (2.5.4.9)
Locality	Locality or stateOrProvinceName must be present subject:localityName (2.5.4.7)
State or province	Locality or stateOrProvinceName must be present subject:stateOrProvinceName (2.5.4.8)
Country	Mandatory subject:countryName (2.5.4.6)
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Mandatory Critical Digital Signature, Key Encipherment
Extended Key Usage	Mandatory

	Not Critical Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Mandatory Not Critical
Certificate Policies	Mandatory Not Critical For QWAC: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.100.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4 For QWAC supporting PSD2: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.100.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.19495.3.1
Authority Info Access	Mandatory Not Critical [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAQualifiedG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXQualifiedCertificatesCAG3.crt
Authority Key Identifier	Mandatory Not Critical Issuer's Subject Key Identifier
Basic Constraints	Mandatory Critical Subject Type=End Entity
CRL Distribution Point	Mandatory Not Critical [1]CRL Distribution Point Distribution Point Name:

	Full Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXQualifiedCertificatesCAG3.crl
Subject Alternative Name	Mandatory Not Critical FQDN of Device It is verified in accordance with Section 9.2 of EV Guidelines Wildcard domain names are prohibited for QWAC
Certificate Transparency	Optional This field MAY include two or more Certificate Transparency proofs from approved CT Logs
qcStatements	
id-etsi-qcs- QcCompliance	Mandatory esi4-qcStatement-1: Claim that the Certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014
id-etsi-qcsQcType	Mandatory esi4-qcStatement-6 : Type of Certificate id-etsi-qcs-QcType 3 = Certificate for website authentication as defined in Regulation EU No 910/2014
id-etsi-qcsQcPDS	Optional esi4-qcStatement-5: URL=https: https://www.athexgroup.gr/pki/-/file/ATHEX_PDS_EN.pdf Language = EN
id-qcs-pkixQCSyntax-v2	Mandatory id-etsi-qcs-SemanticsId-Legal
id-etsi-psd2-qcStatement	Must not be present for QWAC Mandatory for QWAC supporting PSD2 etsi-psd2-qcStatement PSD2QcType : { rolesOfPSP NCAName NCAId } The RolesofPSP can be any combination of the following roles: PSP_AS, PSP_PI, PSP_AI or PSP_IC.

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

10.5.1 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 (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 (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.

10.5.2 Commitment to Comply with Standards

The ATHEX Qualified and Advanced Certificates for eSignature and eSeal from ATHEX Root CA G3 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 take precedence over this document.

10.5.3 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 by legal persons.

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

10.5.4 Subscriber and Subject Obligations

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 and the subject if the subject is a natural or legal person;
3. prohibition of unauthorized use of the subject's private key;
4. if the subscriber or subject 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. if the subscriber or subject generates the subject's keys:
    - when the subject is a natural person: an obligation for the subject’s private key to

be maintained under the subject's sole control;
    - when the subject is a legal person: an obligation for the subject's private key to be maintained under the subject's control;
6. an obligation to only use the subject's private key for cryptographic functions within the secure cryptographic device;
7. if the subject's keys are generated under control of the subscriber or subject: an obligation to generate the subject's keys within the secure cryptographic device;
8. 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 or to the subject;
9. 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
10. 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, 8, 9 and 10.

10.5.5 Verification Process

Identity validation procedures for these Digital Certificates meet the relevant requirements at Section 6.2.2 of ETSI EN 319 411-2.

ATHEX shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA of ATHEX shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

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

- by the physical presence of the natural person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence and for which ATHEX can prove the equivalence. The proof of equivalence can be done according to the Regulation (EU) N° 910/2014.

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

Evidence may be provided on behalf of the subject by the RA. However, the subject remains responsible for the content of the Certificate.

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

- 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.
- 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.

If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence of the identity, shall be checked against a duly mandated subscriber either directly, by physical presence of a person allowed to represent the legal person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

Only for QCP-l for supporting PSD2 transaction, verify the specific PSD2 attributes at public or EBA register.

Note that in case of Qualified Certificates for eSeal and eSignature provided to ATHEX, the above verification tasks are not followed.

10.5.6 Application Process

The steps of the application process QCP-n, QCP-l, QCP-n-qscd when qscd is local, QCP-l-qscd when qscd is local and PSD2 QCP-l are:

1. The Subscriber provides signed Subscriber AgreementATHEX Validation Specialist reviews and verifies all information that is required to be verified by Qualified and Advanced Certificate.
3. It issues the certificate, which is placed in Hold status. If QSCD is required, ATHEX prepares the QSCD.
4. The certificate is delivered to the Subscriber. If QSCD is required, it is delivered to the Subscriber.
5. The Subscriber accepts Certificate issuance
6. ATHEX activates the Certificate.
7. Only for QCP-l for supporting PSD2, ATHEX notifies NCA for Certificate issuance. The steps of the application process for Remote Signature QCP-n-qscd and QCP-l-qscd are:

1. The Subscriber provides signed Subscriber AgreementATHEX First Validation Specialist reviews and verifies all information that is required to be verified by Qualified Certificate.
3. ATHEX First Validation Specialist creates Remote Signature Account.
4. ATHEX PKI Manager approves the creation of the Account.
5. Subscriber activates the accounts using two-factor authentication method. Furthermore, key pairs and certificates are automatically created.

Field	CONTENTS
Version	V3
Serial Number	Unique system generated random number assigned to each Certificate, containing at least 64 bits of output.
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	For QCP-n and QCP-n-qscd: OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX Qualified eSign Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR For QCP-l, QCP-l-qscd and PSD2 QCP-l OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX Qualified eSeal Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 or 2 years
Subject Distinguished Name	
Organization Name	Must not be present for QCP-n, QCP-n-qscd when subject and subscriber are the same entities and it is a natural person. Mandatory for QCP-n, QCP-n-qscd when subscriber is a legal person and the subject is a natural person, i.e., when the subject is a natural person who is identified in association with a legal person. Mandatory for QCP-l, QCP-l-qscd, PSD2 QCP-l This field must contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters as defined by RFC 5280, only the full legal organization name will be used.
Organization Unit	Optional Subject Organizational Unit
OrganizationIdentifier	Must not be present for QCP-n, QCP-n-qscd when subject and subscriber are the same entities and it is a natural person. Mandatory for QCP-n, QCP-n-qscd when subscriber is a legal person and the subject is a natural person, i.e., when the subject is a natural person who is identified in association with a legal person. Mandatory for QCP-l, QCP-l-qscd, PSD2 QCP-l Its structure for QCP-l, QCP-n, QCP-n-qcscd and QCP-l-qscd is: • 3 character legal person identity type reference (e.g. VAT) • 2 character ISO 3166-1 [8] country code • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));

	• identifier (according to country and identity type reference) Its structure for PSD2 QCP-l is: PSD2 Authorization Number recognized by the NCA. For Bank of Greece this Authorization Number has the following structure: • "PSD" as 3 character legal person identity type reference; • 2 character ISO 3166-1 [8] country code representing the NCA country; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); • 2-8 character NCA identifier without country code (A-Z uppercase only, no separator); • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • PSP identifier (authorization number as specified by the NCA. There are no restrictions on the characters used).
Common Name	Mandatory Subject's Common Name
givenName	Mandatory for QCP-n and QCP-n-qscd Must not be present for QCP-l, QCP-l-qscd and PSD2 QCP-l Represantation of the Subject's given name
Surname	Mandatory for QCP-n and QCP-n-qscd Must not be present for QCP-l, QCP-l-qscd and PSD2 QCP-l Represantation of the Subject's surname
Locality	Locality or stateOrProvinceName must be present subject:localityName (2.5.4.7)
State or province	Locality or stateOrProvinceName must be present subject:stateOrProvinceName (2.5.4.8)
Country	Mandatory Subject Country Name (2.5.4.6)
email	Optional Subject email
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Serial Number	Must not be present for QCP-l, QCP-l-qscd and PSD2 QCP-l. Must be present for QCP-n and QCP-n-qscd. The is structure is: • 3 character natural identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).
Extensions	
Key Usage	Mandatory Critical Non Repudiation
Extended Key Usage	Mandatory Not Critical

	Document Signing E-mail protection
Subject Key Identifier	Mandatory Not Critical
Certificate Policies	Mandatory Not Critical For QCP-n: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.200.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 For QCP-n-qscd: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.200.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 For QCP-l: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.200.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 For QCP-l-qscd: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.200.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 For QCP-l supporting PSD2: [1]Certificate Policy:

	Policy Identifier=1.3.6.1.4.1.29402.1.3.200.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.1
Authority Info Access	Mandatory Not Critical For QCP-n and QCP-n-qscd: [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAQualifiedG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXQualifiedCertificatesCAG3.crt For QCP-l, QCP-l-qscd and PSD2 QCP-l: [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAQualifiedG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXeSealCertificatesCAG3.crt
Basic Constraints	Mandatory Critical Subject Type=End Entity
Authority Key Identifier	Mandatory Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Mandatory Not Critical For QCP-n and QCP-n-qscd: [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXQualifiedCertificatesCAG3.crl For QCP-l, QCP-l-qscd and PSD2 QCP-l:

	1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXeSealCertificatesCAG3.crl
Subject Alternative Name	Must not be present for QCP-l, QCP-l-qscd and PSD2 QCP-l. Optional for QCP-n and QCP-n-qscd: Email Address (RFC 822 Name)
Card Serial Number 1.2.752.34.2.1	Must not be present for QCP-l, PSD2 QCP-l and QCP-n Must be present for QCP-n-qscd and QCP-l-qscd It is the number of hard token
qcStatements	
id-etsi-qcs- QcCompliance	Mandatory esi4-qcStatement-1: Claim that the Certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014
id-etsi-qcsQcType	Mandatory For QCP-n, QCP-n-qscd: esi4-qcStatement-6 : Type of Certificate id-etsi-qcs-QcType 1 = Certificate for electronic signature as defined in Regulation EU No 910/2014 For QCP-l, QCP-l-qscd, QCP-l supporting PSD2 esi4-qcStatement-6 : Type of Certificate id-etsi-qcs-QcType 2 = Certificate for electronic Seals as defined in Regulation EU No 910/2014
id-etsi-qcsQcPDS	Optional esi4-qcStatement-5: URL=https: https://www.athexgroup.gr/pki/-/file/ATHEX_PDS_EN.pdf Language = EN
id-etsi-qcs-QcSScd	Must not be present for QCP-l, QCP-n and PSD2 QCP-l Mandatory for QCP-n-qscd, QCP-l-qscd esi4-qcStatement-4
id-qcspkixQCSyntax -v2	Mandatory For QCP-n, QCP-n-qscd id-etsi-qcs-SemanticsId-Natural For QCP-l, QCP-l-qscd and PSD2 QCP-l id-etsi-qcs-SemanticsId-Legal
id-etsi-psd2-qcStatement	Only for QCP-l supporting PSD2 etsi-psd2-qcStatement PSD2QcType : { rolesOfPSP NCAName NCAId } The RolesofPSP can be any combination of the following roles: PSP_AS, PSP_PI, PSP_AI or PSP_IC.

10.6 ATHEX S/MIME Certificates

10.6.1 Purpose

The purposes of a S/MIME Certificate are to:

- Identify the subscriber entity that controls the MIME data;
- Enable encryption of MIME data.

10.6.2 Who can apply

Individuals (natural persons), Incorporated entities, government entities, general partnerships, unincorporated associations, and individual entrepreneurship

10.6.3 Subscriber and Subject Obligations

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 or subject 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 or to the subject;
6. 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
7. 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.

10.6.4 Verification Process

If the MIME data is operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person (e.g. business e-mail), evidence shall be provided of:

- identifier of the MIME data by which it can be referenced;
- full name of the organizational entity;
- any relevant existing registration information (e.g. company registration) of the legal person or other organizational entity identified in association with the legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices; and

- a nationally recognized identity number, or other attributes which can be used to, as far as possible, distinguish the organizational entity from others with the same name.

If the MIME data (e.g. e-mail) is operated by a natural person, evidence shall be provided of:

- being the holder of MIME data;
- a nationally recognized identity number, or other attributes which can be used to, as far as possible, distinguish the natural person from others with the same name.

Note that in case of S/MIME certificates provided to ATHEX and to its employee the above verification process is not followed.

10.6.5 Application Process

The steps of the application process are:

1. The Applicant provides signed Subscriber Agreement.
2. ATHEX verifies information using a variety of sources.
3. ATHEX issues the S/MIME Certificate which is placed in Hold status.
4. The S/MIME Certificate is delivered to the Applicant.
5. The Applicant accepts Certificate issuance.
6. ATHEX activates the S/MIME Certificate.

Field	**CONTENTS**
Version	V3
Serial Number	Unique system generated random number assigned to each Certificate, containing at least 64 bits of output.
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX General Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	1 or 2 years
Subject Distinguished Name	
Organization Name	Must not be present if subscriber is a natural person not associated with organization entity. Must be present if MIME data is operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person. This field must contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation.
Organization Unit	Optional Subject Organizational Unit
OrganizationIdentifier	Must not be present if subscriber is a natural person not associated with organization entity. Must be present if MIME data is operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person. Its structure is: • 3 character legal person identity type reference (e.g. VAT)

	• 2 character ISO 3166-1 [8] country code • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); • identifier (according to country and identity type reference)
Common Name	Optional Subject's Common Name
givenName	Optional Represantation of the Subject's given name
Surname	Optional Represantation of the Subject's surname
Locality	Optional
State or province	Optional
Country	Mandatory Subject Country Name (2.5.4.6)
email	Optional Subject email
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Mandatory Critical Digital Signature, Key Encipherment
Extended Key Usage	Mandatory Not Critical Secure Email
Subject Key Identifier	Mandatory Not Critical
Certificate Policies	Mandatory Not Critical For S/MIME certificates without Organization [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.400.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.helex.gr/el/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3 For S/MIME certificates with Organization [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.400.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.helex.gr/el/web/guest/digital-certificates-pki-

	regulations [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXGeneralCertificatesCAG3.crt
Authority Key Identifier	Mandatory Not Critical
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXGeneralCertificatesCAG3.crl
Basic Constraints	Mandatory Not Critical Subject Type=End Entity
Subject Alternative Name	Mandatory e-mail address rfc822name

10.7 ATHEX Qualified Timestamping Certificates

10.7.1 Purpose

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

10.7.2 Role and Obligations of the ATHEX Time-stamping Authority:

ATHEX undertakes the following obligations to TSA Subscribers:

- To operate in accordance with this ATHEX 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, loss of time synchronization, and causes outlined in relevant section of the ATHEX CP/CPS.

10.7.3 Who can apply

Either natural or legal person

Field	**CONTENTS**
Version	V3
Serial Number	Unique system generated random number assigned to each Certificate, containing at least 64 bits of output.
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	OrganizationIdentifier= VATEL-099755108 L = Athens CN = ATHEX Qualified Timestamp Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 year
Subject Distinguished Name	
Organization Name	ATHENS STOCK EXCHANGE
Organization Identifier	VATEL-099755108
Common Name	TSUATHEXG3
Country	GR
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Mandatory Critical Digital Signature
Extended Key Usage	Mandatory Critical Time Stamping (id-kp-timeStamping)
Subject Key Identifier	Mandatory

	Not Critical
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.500.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=0.4.0.2023.1.1
Authority Info Access	Mandatory Not Critical [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXTimestampCertificatesCAG3.crt
CRL Distribution Point	Mandatory Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/ATHEXTimestampCertificatesCAG3.crl
Basic Constraints	Mandatory Critical Subject Type=End Entity
Authority Key Identifier	Mandatory Not Critical Issuer's Subject Key Identifier
qcStatements	
id-qc-pkixQCSyntax-v1	Mandatory id-etsi-qcs-SemanticsId-Legal
esi4-qtstStatement-1 0.4.0.19422.1.1	Mandatory Claims to be a qualified electronic time-stamp as per Regulation (EU) No 910/2014

11 APPENDIX B

11.1 Root CA G3 Certificate Profile

Field	Value
Version	V3
Serial Number	7e a2 77 bc b2 97 1d 9d fd c9 7b e2 00 39 76 63
Issuer Signature Algorithm	sha384WithRSAEncryption (1.2.840.113549.1.1.12)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: Mar 15 14:38:32 2019 GMT NotAfter: Mar 15 01:00:00 2039 GMT
Subject Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Subject public Key Info	RSA (4096 bits) 30 82 02 0a 02 82 02 01 00 a6 3f ad ee 99 46 52 57 ba 11 28 71 1d bf 1d e8 02 65 e2 a5 8a 10 9e 00 4f 45 0e 5b 0b b9 ec 12 77 68 9c 11 c5 1f 6d 78 08 9d 57 7f 1e 33 9d 45 6c 2d e8 42 79 7c 71 1f 7f a4 15 63 e4 4e 37 0c 99 ee b0 82 c6 e8 8d 23 96 21 f0 5e 05 c3 9b 0f 97 41 d0 1a 9c 61 93 50 d5 c4 73 42 04 d4 e4 4a c5 b9 a0 e0 aa 25 69 04 2d 63 a9 b5 7c 30 43 d7 ac b0 e6 ec 83 f7 a6 f5 b4 91 5c 78 5e 77 c6 64 71 a4 5e fc a8 d7 ed e2 dd 2f 07 71 ba be 63 d6 b3 48 25 c2 06 8e e0 f1 d3 2b 93 8f 1a 97 e2 32 e5 01 87 36 d3 81 6f df 5d 0d d9 ba 8a 27 33 3e 07 93 21 ed cb 43 75 8c a9 52 46 e2 17 f5 c4 a1 40 c8 e4 33 82 87 e3 99 c6 0e 98 f0 f0 9a 2d b0 e0 a1 e1 86 6f ca 2d 40 fb d3 89 0c 89 d3 ba 4b 68 c9 9a 04 67 1e 87 95 bd a2 6e 62 9b 69 4c 4d a2 01 1c 1a 59 19 55 cb fe 0f 62 ff 3f 34 6b dc 10 8d ea b8 df 67 37 c6 e3 66 22 d9 e7 b0 12 04 74 55 2a 7a c0 43 df 88 76 cf b8 a2 fe 81 6c 2f 12 0b d9 31 e1 b6 44 be 7f 8c db a2 94 2a 91 3e a3 a9 54 d6 f6 c8 1c 2c 26 ed f7 21 37 78 e3 32 98 0a ab 3d 0e 16 fd a4 20 9a 43 0c ae ca 7f 1e 38 8b f3 93 02 66 10 12 37 ec 30 e3 26 54 1b fb 46 0e 35 2f d1 26 34 68 78 d7 4c 8c cb 33 14 22 ab e4 93 19 4b a5 fb 9b ce 31 12 59 27 83 c5 2a 2f 2c 9c 1e b7 bc 9b de 7a d3 1e ca 44 56 5a ee 3d 29 e5 00 4c 58 32 60 ff da b7 d6 b3 90 1b 27 41 08 24 c0 fb 18 f3 e2 38 cf 5a f8 a5 ac 5d f7 71 4b 20 93 e2 fd 6b 87 56 c2 a0 06 11 ee 2e 63 83 a0 85 20 0a e0 66 07 ea 5f 12 1b 16 b1 2a ca d7 ae e1 29 72 87 97 8a 91 11 ca 4e bf b7 fe 30 75 24 5f 23 cb b1 32 d7 29 b1 c0 94 b9 5a 4b b6 43 98 88 5c c9 2c ef 58 db 7a f0 b4 ba 63 4c 95 02 03 01 00 01
Extensions	
Key Usage	Critical Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	43 e2 28 d1 30 60 b4 4f
Basic constraints	Critical Subject Type=CA Path Length Constraint=None

11.2 SUB CAs

11.2.1 ATHEX Extended Validation Certificates CA G3

Field	Value
Version	V3
Serial Number	08 ce 5e 19 ba bf 9d 4f 93 88 76 96 1a ff 22 3a
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: Mar 22 13:28:04 2019 GMT NotAfter: Mar 22 01:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX Extended Validation Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Subject public Key Info	RSA (2048 bits)
Extensions	
Key Usage	Critical Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	47 47 57 7f 88 e2 b8 86
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt
Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl

11.2.2 ATHEX SSL Certificates CA G3

Field	Value
Version	V3
Serial Number	77 b3 c1 dc 93 35 02 04 34 f1 5d 75 3a 05 84 67
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: Mar 22 13:41:22 2019 GMT NotAfter: Mar 22 01:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX SSL Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Critical Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	48 4c e3 ba 45 3a c0 30
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt
Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl

11.2.3 ATHEX General Certificates CA G3

Field	Value
Version	V3
Serial Number	5f c5 fc 52 3c d2 3b 91 1e bf 82 7d 0c f5 19 3a
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: Mar 22 13:15:26 2019 GMT NotAfter: Mar 22 01:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX General Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Critical Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	4c 59 e7 54 f5 78 b6 b3
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt
Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl

11.2.4 ATHEX Qualified WEB Certificates CA-G3

Field	Value
Version	V3
Serial Number	68874639c8d052359dcda2c3a948ed58
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: December 19, 2019 11:06:13 AM GMT NotAfter: December 19, 2029 11:06:13 AM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX Qualified WEB Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Subject public Key Info	RSA (4096 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Critical Certificate Signing, Off-line CRL Signing, CRL Signing
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1) OCSP Signing (1.3.6.1.5.5.7.3.9)
Subject Key Identifier	22992457066c56758edbeb7d79659c5335a9d191
Basic constraints	Critical Subject Type=CA Path Length Constraint=0
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt
Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name:

	Full Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl

11.2.5 ATHEX Qualified eSeal Certificates CA-G3

Field	**Value**
Version	V3
Serial Number	41643d1140c39b5a3866204ce8807630
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: December 17, 2019 1:44:48 PM GMT NotAfter: December 17, 2029 1:44:48 PM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX Qualified eSeal Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Subject public Key Info	RSA (4096 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Critical Certificate Signing, Off-line CRL Signing, CRL Signing
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12) OCSP Signing (1.3.6.1.5.5.7.3.9)
Subject Key Identifier	27be139f8991c5ae8e53147767c8c3097a1dbd1d
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt

Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl

11.2.6 ATHEX Qualified eSign Certificates CA-G3

Field	**Value**
Version	V3
Serial Number	3dca7f8fb01fb9da960c166e34775b37
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: December 17, 2019 1:32:32 PM GMT NotAfter: December 17, 2029 1:32:32 PM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX Qualified eSign Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Subject public Key Info	RSA (4096 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Critical Certificate Signing, Off-line CRL Signing, CRL Signing
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12) OCSP Signing (1.3.6.1.5.5.7.3.9)
Subject Key Identifier	6f93d1f0e63735f588816fa587859b336684b2b9
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

	Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt
Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl

11.2.7 ATHEX Qualified Timestamp Certificates CA-G3

Field	**Value**
Version	V3
Serial Number	3541734f62b68277b23c0ce1953f2e10
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: December 17, 2019 1:51:09 PMGMT NotAfter: December 17, 2019 1:51:09 PM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX Qualified Timestamp Certificates CA-G3 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Subject public Key Info	RSA (4096 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Critical Certificate Signing, Off-line CRL Signing, CRL Signing
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8) OCSP Signing (1.3.6.1.5.5.7.3.9)
Subject Key Identifier	eb5d090ab2bd48e1454b19b145322142667bf4bb
Basic constraints	Critical Subject Type=CA Path Length Constraint=0
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-

	Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt
Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl

11.2.8 ATHEX Code Signing Certificates CA G3

Field	**Value**
Version	V3
Serial Number	10 d6 78 d0 7e 93 78 22 7e 42 27 f6 fd c7 66 db
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX Root CA G3 O = ATHENS STOCK EXCHANGE C = GR
Validity Period	NotBefore: Mar 22 14:24:30 2019 GMT NotAfter: Mar 22 01:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX Code Signing Certificates CA G3 O = ATHENS STOCK EXCHANGE C = GR
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Critical Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	42 98 13 08 f9 25 9b cc
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:

	http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.athexgroup.gr/AthexRootCAG3 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crt
Authority Key Identifier	KeyID=43 e2 28 d1 30 60 b4 4f
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.athexgroup.gr/pki/-/file/AthexRootCAG3.crl