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

Certificate Policy and Certificate Practices Statement for ATHEX Root CA G3 and ATHEX RSA Root CA G4 R1 Certificates

Version 1.8 – 26/3/2021

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.
1.6	17/9/2020	Change the CRL distribution points of end entities certificates, add LRAs, update the profile of EU qualified certificates.
1.7	22/12/2020	Update the contact info and add provision of testing certificates
1.7.1	5/1/2021	Add third-party remote QSCD
1.7.2	13/1/2021	Update Registration Procedure and Certificate Profile for Qualified eSign
1.7.3	18/1/2021	Remove the term LRA
1.8	26/3/2021	Add ATHEX RSA Root CA G4 R1 hierarchy and enrich the policy in order to comply with browser vendors root store programs, move procedures from Appendix to corresponding chapters, add new subordinate CAs at G3 hierarchy.

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 and ATHEX RSA Root CA G4 R1of 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 and ATHEX RSA Root CA G4 R1 CP/CPS approved by Policy Management Committee (PMC). The Object Identifier assigned to the Root CA G3 and ATHEX RSA Root CA G4 R1, covered by this CP/CPS, is 1.3.6.1.4.1.29402.1.3.0.1.7.3 (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(7) Third-Digit-of-Version(3)}) and 1.3.6.1.4.1.29402.1.4.0.1.7.4 (in details: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) HELEX(29402) PKI-Organization-Unit(1) Root-CA-G4(4) CP/CPS(0)

First-Digit-of-Version(1) Second-Digit-of-Version(7) Third-Digit-of-Version(4)}) .

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 General Certificates CA G3
  - ATHEX RSA Qualified Timestamp Certificates CA G3 R11
  - ATHEX RSA Qualified WEB CA G3 R11
  - ATHEX RSA Qualified eSeal CA G3 R11
  - ATHEX RSA Qualified eSign CA G3 R11

- ATHEX RSA Root CA G4 R1
  ATHEX RSA Root CA G4 R1 has signed the following subordinate CAs:
  - ATHEX RSA Timestamping CA G4 R11
  - ATHEX RSA EV TLS CA G4 R11
  - ATHEX RSA TLS CA G4 R11
  - ATHEX RSA Code Signing CA G4 R11
  - ATHEX RSA Client CA G4 R11
  - ATHEX RSA EV Code Signing CA G4 R11
  - ATHEX RSA SMIME CA G4 R11

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)}	**ATHEX Certificate Policy OID 1.3.6.1.4.1.29402.1.4** {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) HELEX(29402) PKI-Organization-Unit(1) Root-CA-G4(4)}	**End entity Certificate asserts adherence to and compliance with:**
Server Authentication - Domain validation		1.3.6.1.4.1.29402.1.4.100.1.1 {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		1.3.6.1.4.1.29402.1.4.100.1.2 {ServerAuth(100) Validation-Type(1) Organization -	• CA/Browser Baseline Requirements –

validation		Validation(2)}	Organization Validated (OID 2.23.140.1.2.2) • ETSI EN 319 411-1 OVCP (OID 0.4.0.2042.1.7) • CA/Browser Baseline Requirements – Individual Validated (OID 2.23.140.1.2.3) • ETSI EN 319 411-1 IVCP OID 0.4.0.2042.1.8
Server Authentication - EV Certificates		1.3.6.1.4.1.29402.1.4.100.1.3 {ServerAuth(100) Validation-Type(1) EV-Certificates(3)}	• CA/Browser Extended Validation (OID 2.23.140.1.1) • ETSI EN 319 411-1, EVCP OID 0.4.0.2042.1.4
Server Authentication - Qualified Website Authentication	1.3.6.1.4.1.29402.1.3.100.1.4 {ServerAuth(100) Validation-Type(1) QWAC(4)}		• CA/Browser Extended Validation (OID 2.23.140.1.1) • 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	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)

QSCD			
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)
Document Signing – Qualified Certificates for remote Qualified Electronic Signatures with QSCD	1.3.6.1.4.1.29402.1.3.200.1.6 {DocumentSigning(200) Validation-Type(1) QCP-n-qscd remote(6)}		• ETSI 319 411-2, QCP-n-qscd (OID 0.4.0.194112.1.2)
Document Signing – Qualified Certificates for Qualified remote Electronic Seals with QSCD	1.3.6.1.4.1.29402.1.3.200.1.7 {DocumentSigning(200) Validation-Type(1) QCP-l-qscd remote(7)}		• ETSI 319 411-2, QCP-l-qscd (OID 0.4.0.194112.1.3)
Code Signing		1.3.6.1.4.1.29402.1.4.300.1.1 {CodeSigning(300) Validation-Type(1) CodeSigning(1)}	• CA/B Forum OID 2.23.140.1.4.1 • Organization Validation (OV-NCP) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.1 • Organization Validation (OV-NCP+) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.2

			• Individual Validation (IV-NCP) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.1 • Individual Validation (IV-NCP+) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.2
Extended Validation Code Signing		1.3.6.1.4.1.29402.1.4.300.1.2 {CodeSigning(300) Validation-Type(1) EVCodeSigning(2)}	• CA/Browser Extended Validation Code Signing (OID 2.23.140.1.3) • ETSI EN 319 411-1, (NCP+) OID 0.4.0.2042.1.2
General – Simple S/MIME		1.3.6.1.4.1.29402.1.4.400.1.1 {General(400) Validation-Type(1) Simlpe-S/MIME(1)}	• ETSI EN 319 411-1 LCP (OID 0.4.0.2042.1.3) • Individual Validation (IV-NCP) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.1 • Individual Validation (IV-NCP+) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.2
General – Organizational S/MIME		1.3.6.1.4.1.29402.1.4.400.1.2 {General(400) Validation-Type(1) Organizational-S/MIME(2}	• ETSI EN 319 411-1 LCP (OID 0.4.0.2042.1.3) • Organization Validation (OV-NCP) compatible

			with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 • Organization Validation (OV-NCP+) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
Client Authentication	1.3.6.1.4.1.29402.1.3.400.2.1	1.3.6.1.4.1.29402.1.4.400.2.1	• ETSI EN 319 411-1 LCP (OID 0.4.0.2042.1.3) • Individual Validation (IV-NCP) compatible with ETSI EN 319 411-1 OID 0.4.0.2042.1.1 • Individual Validation (IV-NCP+) compatible with ETSI EN 319 411-1 0.4.0.2042.1.2
Timestamping		1.3.6.1.4.1.29402.1.4.500.1.1 {Timestamping(500) Validation-Type(1) QTimestamp(1)}	• ETSI EN 319 421 (OID 0.4.0.2023.1.1)
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/G4 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.

Third parties, who enter into a contractual relationship with ATHEX, may act as Registration Authorities on behalf of ATHEX. These third parties can also authorize the issuance of Qualified Electronic Signatures and Seals under subordinate CAs of ATHEX QTSP. Third-party RAs must abide by all the requirements of this CP/CPS.

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 and ATHEX RSA Root CA G4 R1. 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.

1.3.5 Other Participants

Third-party remote QSCD Providers may enter into a contractual relationship with ATHEX, in order to provide remote QSCD activities under this CP/CPS. This third-party provider must be a QTSP and properly audited under the eIDAS regulation and in conformity with the requirements of Article 20 of Regulation (EU) 910/2014 (eIDAS).

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 and APPENDIX C 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

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.

ATHEX should notify the National Supervisory Body (EETT) if any changes or updates occur in the CP/CPS.

1.6 Definitions & Acronyms

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

1.6.1 Definitions

Advanced Electronic Seal: An electronic signature that meets the requirements of Article 36 of Regulation (EU) 910/2014.

Advanced Electronic Signature: An electronic signature that meets the requirements of Article 26 of Regulation (EU) 910/2014.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Applicant Representative: A natural person acting on behalf of the Applicant, in a legally binding manner, who is employed either by the Applicant or an agent duly authorized to represent the Applicant:

- who signs and submits, or approves a certificate request on behalf of the Applicant, and/or
- who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or
- who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of ATHEX

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Identity Information is correct written by a lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. The coverage rules and maximum length of audit periods are described in Section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of audited standards listed in section 8.4.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a base domain name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public ATHEX Public Key Infrastructure Certificate Policy and Certification Practice Statement. For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements (BR): An integrated set of technologies, protocols, identity- proofing, lifecycle management, and auditing requirements issued by the CA/Browser Forum and available at cabforum.org.

Business Entity: Any entity that is not a Private Organization, Government Entity, or noncommercial entity as defined in the EV Guidelines. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CA Certificate: A Certificate in which the basic Constraints field has the cA attribute set to TRUE.

CAA: From RFC 8659 (http://tools.ietf.org/html/rfc8659): “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a

public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

CA/Browser Forum (CAB Forum): A consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of digital certificates. Details are available at: cabforum.org.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certificate Application: a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.

Certificate Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certificate Authority Authorization (CAA): The CAA record is used to specify which Certificate Authorities are allowed to issue Certificates for a domain.

Certificate Data: Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: A complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Request: Communications described in Section 10 of the Baseline Requirements requesting the issuance of a Certificate.

Certificate Requester: 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.

Certificate Revocation List: A regularly updated timestamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate Signing Request (CSR): a message sent to the certification authority containing the information required to issue a digital certificate.

Certification Authority (CA): an entity or organization that is responsible for the authorization, issuance, revocation, and management of a certificate. The term equally applies to Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Transparency: An "append-only" public logging Certificate system as described by RFC 6962.

Code Signing Certificate: A digital certificate that contains a code Signing EKU and is trusted in an Application Software Provider's root store to sign software objects.

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Compromise: A violation of a security policy that results in loss of control over sensitive information.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the ATHEX but is authorized by ATHEX, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of ATHEX's requirements found herein.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

Distinguished Name (DN): a globally unique identifier representing a Subject that is used on Certificates and in the Repository.

DNS CAA Email Contact: The email address defined in Appendix B.1.1. of the CA/B Forum Baseline Requirements.

DNS CAA Phone Contact: The phone number defined in Appendix B.1.2. of the CA/B Forum Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Appendix B.2.1. of the CA/B Forum Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Appendix B.2.2. of the CA/B Forum Baseline Requirements.

DNS Operator: An entity responsible for running DNS servers. For a zone's authoritative servers, the registrant may act as their own DNS operator, or their registrar may do it on their behalf, or they may use a third-party operator. For some zones, the registry function is performed by the DNS operator plus other entities who decide about the allowed contents of the zone.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Name System: An Internet service that translates Domain Names into IP addresses.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

eIDAS Regulation: REGULATION (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 and repealing Directive 1999/93/EC.

Electronic Seal: Data in electronic form, which is attached to or logically associated with other data in

electronic form to ensure the latter's origin and integrity.

Electronic Signature: Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Enterprise RA: An employee or agent of an organization unaffiliated with ATHEX who authorizes issuance of Certificates to that organization.

EV Certificate: A certificate that contains subject information specified in, and which has been validated in accordance with the EV Guidelines. There are EV Certificates for TLS and for Code Signing. Both certificate types follow the same practices for validation Subject Information related to the Identity of the Applicant.

EV Certificate Renewal: The process whereby an Applicant who has a valid, unexpired and non-revoked EV Certificate issued by ATHEX, makes an application for a newly issued EV Certificate that includes the same organizational name and Domain Name as the existing EV Certificate, a new "valid to" date beyond the expiry of the current EV Certificate and the application is prior to the expiration of the Applicant's existing EV Certificate.

EV Certificate Request: A request from an Applicant requesting an EV Certificate whose valid request is authorized by the Applicant and signed by the Applicant Representative.

EV Code Signing Guidelines: The document "Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates", published and maintained by the CA/B Forum.

EV Guidelines: The document "Guidelines For The Issuance And Management Of Extended Validation Certificates", published by the CA/B Forum. This document mainly focuses on TLS Certificates but some of these requirements are referenced by EV Code Signing Guidelines and ETSI European Norms (e.g. ETSI EN 319 411-1).

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Extended Key Usage: An extension in an X.509 certificate to indicate the allowed purpose(s) for the use of the public key. Also referenced or known as "Enhanced Key Usage".

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a Country, or political subdivision within such Country (such as a state, province, city, county, etc.).

Hardware Security Module (HSM): A type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

High Risk Certificate Request: A Request that ATHEX flags for additional scrutiny by reference to internal criteria and databases maintained by ATHEX, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that ATHEX identifies using its own risk-mitigation criteria.

Incorporate by Reference: To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

Individual: A natural person.

IP Address: A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Key Compromise: A Private Key is said to be Compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Generation Script: A documented plan of procedures for the generation of the Key Pair to be associated with a CA Certificate.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Object Identifier (OID): A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

Penetration Test: A process that identifies and attempts to exploit openings and vulnerabilities on the Certificate System through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

Payment Services Directive (PSD2): European Union Directive (EU) 2015/2366 that regulates payment services and payment service providers throughout the European Union and European Economic Area.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

PSD2 Certificate: A Qualified Certificate that includes PSD2 Specific Attributes.

PSD2 Specific Attributes: Attributes that are specific to PSD2 Certificates which are:

- authorization number if it is issued by the NCA, or registration number recognized on national or European level or Legal Entity Identifier included in the register of credit institutions.
- role or roles of PSP
- NCA name (NCAName) and unique identifier (NCAId).

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure (PKI): A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/ Qualifications of Assessor).

Qualified Certificate: A Certificate that meets the qualification requirements defined by the eIDAS Regulation.

Qualified Certificate for Electronic Seals: A Certificate for Electronic Seals, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of eIDAS Regulation.

Qualified Certificate for Electronic Signature: A Certificate for Electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation.

Qualified Electronic Seals: An advanced Electronic Seal, which is created by a Qualified Electronic Seal Creation Device, and that is based on a Qualified Certificate for Electronic Seal.

Qualified Electronic Signature: An advanced Electronic Signature that is created by a Qualified Electronic Signature Creation Device, and which is based on a Qualified Certificate for Electronic Signatures.

Qualified Electronic Signature Creation Device (QSCD): An electronic signature creation device that meets the requirements as stipulated within Annex II of eIDAS Regulation.

Qualified Timestamping (QTS): The provisioning of time stamps that comply with Article 42 of the eIDAS Regulation.

Qualified Trust Service Provider (QTSP): A natural or legal person that is recognized by a European Union member state national supervisory body to provide (a subset of) qualified trust service as defined within the eIDAS Regulation.

Random Value: A value specified by ATHEX to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency may include, but is not limited to

- a State Department of Corporations or a Secretary of State;
- a licensing agency, such as a State Department of Insurance; or
- a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of

Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Registration Number: The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token: A value derived in a method specified by ATHEX which binds this demonstration of control to the certificate request.

- The Request Token SHALL incorporate the key used in the certificate request.
- A Request Token MAY include a timestamp to indicate when it was created.
- A Request Token MAY include other information to ensure its uniqueness.
- A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.
- A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.
- A Request Token that does not include a timestamp is valid for a single use and ATHEX SHALL NOT re-use it for a subsequent validation.
- The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by ATHEX.

Root CA: The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

SSL Certificate: Certificates intended to be used for authenticating servers accessible through the Internet.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Supervisory Body: A body responsible for the task of supervising the qualified trust service providers established in the territory of the Member State and to take action, if necessary, in relation to non-qualified trust service providers established in the territory of the Member State. Details are described in eIDAS Article 17.

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Time-Stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

Time-Stamp Token (TST): a data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.

Time-Stamping Authority (TSA): TSP providing time-stamping services using one or more time-stamping units.

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

Transport Layer Security (TLS)/Secure Socket Layer (SSL): a security protocol that is widely used in the Internet, for the purpose of authentication and establishing secure sessions.

Trusted Role: An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over CA Operations.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

UTC(k): time scale realized by the certified laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified by the Baseline Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

1.6.2 Acronyms

Acronym	Meaning
AND	Authorization Domain Name
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	CA/Browser as in “CAB Forum”
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DV	Domain Validated
DVCP	Domain Validation Certificates Policy
EBA	European Banking Authority
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	United States Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
QTSP	Qualified Trust Service Provider
QSCD	Qualified Signature/Seal Creation Device
QWAC	Qualified Website Authentication Certificate
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
NCA	National Competent Authority
NIST	National Institute of Standards and Technology

OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
OVCP	Organizational Validation Certificates Policy
PIN	Personal Identification Number (e.g. a secret access code)
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PMC	Policy Management Committee
PSD2	Payment Services Directive 2
PSP	Payment Service Provider
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider Issuing Card-based payment instruments
PSP_PI	Payment Initiation Service Provider
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
TSP	Trust Service Provider
TTL	Time to Live
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VAT	Value Added Tax
X.509	ITU-T standard for Certificates and their corresponding authentication framework

2 Publication and Repository Responsibilities

2.1 Repositories

The locations of ATHEX repositories are:

- https://www.athexgroup.gr/web/guest/digital-Certificates-pki-regulations
- https://repo.athexgroup.gr
  This location only includes in the CA certificates.

The revocation list for subscriber Certificates can be found in the below repository, which is publicly available 24 hours a day, 7 days a week:
https://crl.athexgroup.gr

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 Certificates that chain up to ATHEX Root CA. These sites are accessible at the following URLs:

- ATHEX Root CA G4 Valid: https://certdemo-valid-rsag4r1.athexgroup.gr/
- ATHEX Root CA G4 Expired: https://certdemo-expired-rsag4r1.athexgroup.gr/
- ATHEX Root CA G4 Revoked: https://certdemo-revoked-rsag4r1.athexgroup.gr/

2.3 Time or Frequency of Publication

ATHEX at least annually reviews this CP/CPS and compare it with the CAB Forum's Baseline Requirements, EV Guidelines and ETSI Standards for any modifications.

Updates are published at least annually, in accordance with Section 1.5, and the document version number is incremented to account for the annual review and potential content revisions.

New versions of this CP/CPS document will become effective immediately for all participants listed in Section 1.3.

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 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 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 and APPENDIX C.

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

For all Certificates that include an organization identity, 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.

ATHEX SHALL verify the identity of an organization or domain, and the Applicant's authority to request Certificates on behalf of the organization or domain, in accordance with procedures set forth in this CP/CPS and the CAB Forum's Baseline Requirements.

For Code Singing and EV Code Singing Certificates, prior to issuing a certificate ATHEX MUST determine whether the entity is identified as requesting a Code Signing Certificate from a High Risk Region of Concern. ATHEX MUST also maintain and check an internal database listing Certificates revoked due to Code Signatures on Suspect Code and previous certificate requests rejected by the CA.

If an Applicant requests an Extended Validation (EV) Certificate or an (EV) Code Signing Certificate, ATHEX SHALL conform to the CAB Forum's respective EV Guidelines.

EV Certificates will only be issued in accordance with the EV Guidelines to the following types of organizations:

- Private Organizations;
- Government Entities;
- Business Entities;
- Non-commercial Entities.

3.2.2.1 Identity

OV TLS and OV Code Signing Certificates and S/MIME Certificates

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

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

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

Note that in case of OV TLS and OV Code Signing Certificates and S/MIME Certificates provided to ATHEX, the above verification tasks are not followed.

EV Certificates

ATHEX is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements. 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.

ATHEX discloses the Incorporating or Registration Agencies used for validating Organization Identities at the ATEHX repository as described in section 2.1.

Note that in case of EV certificates provided to ATHEX, the above verification tasks are not followed.

Qualified Certificates

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

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

a. by the physical presence of an authorized representative of the legal person; or
b. using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which ATHEX can prove the equivalence according to Article 24 paragraph 1 of the Regulation (EU) No 910/2014.

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

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

For the QWAC certificates If the subscriber is a legal person the identity of the subscriber and its link with the domain name to be certified and, if applicable, any specific attributes of the person.

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

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

3.2.2.2 DBA/Tradename

OV TLS and OV Code Signing Certificates and S/MIME Certificates

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.

EV Certificates

ATHEX verifies DBA information, in accordance with procedures set forth in this CPS and the CAB Forum's Baseline Requirements.

3.2.2.3 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.

3.2.2.4 Validation of Domain Authorization and Control

ATHEX SHALL confirm that prior to issuance, ATHEX has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate as follows:

1. When the FQDN does not contain "onion" as the rightmost label, ATHEX SHALL validate the FQDN using at least one of the methods listed below; and

2. When the FQDN contains "onion" as the rightmost label, ATHEX SHALL validate the FQDN in accordance with the BR Appendix B.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

ATHEX SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.;

Note that for the FQDNs that belongs to ATHEX group and ENEX group the below validations methods are not followed.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method of domain validation is not used.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact. Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

ATHEX MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail. ATHEX MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the

communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. ATHEX MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

ATHEX SHALL NOT perform validations using this method after May 31, 2019. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.;

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by 1. Sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name; and 1. including a Random Value in the email; and 1. receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

This method of domain validation is not used.

3.2.2.4.6 Agreed-Upon Change to Website

This method of domain validation is not used.

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

Note: Once the FQDN has been validated using this method, ATHEX MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless ATHEX performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9 Test Certificate

This method of domain validation is not used.

3.2.2.4.10 TLS Using a Random Number

This method of domain validation is not used.

3.2.2.4.11 Any Other Method

This method of domain validation is not used.

3.2.2.4.12 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if ATHEX is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.13 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.14 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The

same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.15 Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, ATHEX MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, ATHEX may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to ATHEX to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names..

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

ATHEX MAY NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, ATHEX may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned ATHEX to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number

and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3.

ATHEX MUST NOT be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, ATHEX may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to ATHEX to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, ATHEX MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.18 Agreed-Upon Change to Website v2

This method of domain validation is not used.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

This method of domain validation is not used.

3.2.2.4.20 TLS Using ALPN

This method of domain validation is not used.

3.2.2.5 Authentication for an IP address

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.

ATHEX SHALL confirm that prior to issuance, ATHEX has validated each IP Address listed in the Certificate using at least one of the methods specified in this section.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

After July 31, 2019, ATHEX SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

1. Note: IP Addresses verified in accordance with this section 3.2.2.5 may be listed in Subscriber Certificates as defined in section 7.1.4.2 or in Subordinate CA Certificates via iPAddress in permittedSubtrees within the Name Constraints extension. CAs are not required to verify IP Addresses listed in Subordinate CA Certificates via iPAddress in excludedSubtrees in the Name Constraints extension prior to inclusion in the Subordinate CA Certificate. or

3.2.2.5.1 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested 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/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by ATHEX via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, ATHEX SHALL provide a Random Value unique to the certificate request and

SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of this document).;

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

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. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

ATHEX MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail. The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.5.3 Reverse Address Lookup

Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.2.4.

3.2.2.5.4 Any Other Method

This method is not used.

3.2.2.5.5 Phone Contact with IP Address Contact

Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. ATHEX MUST place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to a single number.

In the event that someone other than an IP Address Contact is reached, ATHEX MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, ATHEX may leave the Random Value and the IP Address(es) being validated. The Random Value MUST be returned to ATHEX to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.5.6 ACME "http-01" method for IP Addresses

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 under Section 3.2.2.5.6;

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

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 under Section

3.2.2.5.7.

3.2.2.6 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”.

3.2.2.7 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.

ATHEX considers the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

Databases maintained by ATHEX, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.2.8 CAA Records

As part of the issuance process, ATHEX MUST check 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 8659. If ATHEX issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, ATHEX MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. ATHEX MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this 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.

3.2.3 Authentication of Individual Identity

If an Applicant is a natural person, then the ATHEX SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

OV TLS and OV Code Signing Certificates

The Applicant is required to demonstrate control of certain identity attributes included in the request, such as his/her email address or domain name to which the Certificate relates if included in the Certificate Request.

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

Client Authentication Certificates

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

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

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

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

S/MIME Certificates

If the digitally signing or encrypting email messages (S/MIME Certificate) is operated by a natural person ATHEX shall take reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf, as specified in section 3.2.2.:

- ATHEX requesting the Applicant to enter the email address at the initial certificate request form and a verification email is sent back with a Random Value. Once the Applicant returns this Random Value back to ATHEX, the email address is validated;
- ATHEX requesting the Applicant to perform a validation for the domain portion of an email address as an Authorization Domain Name, using any of the allowed domain validation methods described in section 3.2.2.4.

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

Qualified Certificates

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

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

a) by the physical presence of the natural person; or

b) using identity verification methods which provide equivalent assurance in terms of reliability to the physical presence and for which ATHEX can prove the equivalence according to Article 24 paragraph 1 of the Regulation (EU) No 910/2014.

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

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

Validation of authority (i.e. the determination of whether an Applicant or Subscriber has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate) is the responsibility of the CA or CA-appointed Registration Authority (RA).

If the Applicant for a Certificate containing Subject Identity Information is an organization, ATHEX shall use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

ATHEX uses the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication. Provided that ATHEX uses a Reliable Method of Communication, ATHEX will establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source

within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that ATHEX deems appropriate.

In addition, ATHEX allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then ATHEX will not accept any certificate requests that are outside this specification. ATHEX will provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

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 may be electronic, which includes all registration information as described by this CP/CPS (see APPENDIX A and APPENDIX C) and the relevant Subscriber Agreement which may be electronic 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:

1. Identify the Applicant or Device in accordance with APPENDIX A and APPENDIX C,
2. Generate a Key Pair for the Digital Certificate in a secure fashion, and
3. 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.

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.

4.2 Certification Application Processing

4.2.1 Performing Identification and Authentication Functions

Prior to the issuance of a Certificate, ATHEX SHALL obtain the documentation from the processing and the verification of the certificate applications that is outlined in section 3.2. All certificate applications are checked for validity.

Section 6.3.2 limits the validity period of Subscriber Certificates. ATHEX MAY use the documents and data provided in Section 3.2 to verify certificate information, provided that ATHEX obtained the data or document from a source specified under Section 3.2 no more eight hundred and **twenty five (825) days** prior to issuing the Certificate.

Effective September 1, 2020, reuse of previous validations is limited to no more than 398 days for all server Certificates.

Except for reissuance of an EV Certificate under Section 11.14.2 and except when permitted otherwise in Section 11.14.1, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

(A) Legal existence and identity – thirteen months;

(B) Assumed name – thirteen months;

(C) Address of Place of Business – thirteen months;

(D) Verified Method of Communication – thirteen months;

(E) Operational existence – thirteen months;

(F) Domain Name – thirteen months;

(G) Name, Title, Agency, and Authority – thirteen months, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

The thirteen-month period set forth above SHALL begin to run on the date the information was collected by ATHEX.

ATHEX MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under Sections 11.9 and 11.10 of the EV Guidelines.

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 and APPENDIX C. 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.

Only for QWAC and QCP-l for supporting PSD2, ATHEX notifies NCA for Certificate issuance.

ATHEX refrains from issuing a server Certificate until the entire corpus of information and documentation assembled in support of the server Certificate Request is such that issuance of the server 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 server Certificate Request and notify the Applicant accordingly.

Especially for the EV and QWAC Certificate requests ATHEX requires a minimum of two (2) separate Validation Specialists for approval. The second Validation Specialist requires additional documentation and/or verification before approving the issuance an EV and QWAC certificate.

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The ATHEX Root CA G3 and ATHEX RSA Root CA G4 R1 has been self-generated and self-signed. ATHEX Root CA G3 and ATHEX RSA Root CA G4 R1 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, ATHEX issues the Digital Certificate to the Applicant or Device. ATHEX provides the capability to allow third parties (e.g., Application Software Suppliers) and auditors to check and test all the certificate types that it issues and chain up to each publicly trusted Root certificate. Any test certificates should clearly indicate that they are for testing purposes by the information at the subject (e.g. "Demo" at subject common name) and by the "User Notice" policy qualifier, at the certificate policy extension, explicitly declaring the following statement "This certificate is only for testing purposes".

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificates

ATHEX notifies the Subscribers via an email or another agreed upon method, with information about the issued Certificate.

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 to the Subscriber with the same Public Key (same key pair) and verified information in the Certificate. A renewed Certificate has a new serial number and an expiration date ending after the expiration date of the Certificate being renewed..

4.6.1 Circumstances for Certificate Renewal

Subscribers are responsible for the renewal of Certificates to maintain service continuity.

4.6.2 Who May Request Renewal

Certificate Renewals MAY be requested by the Subscriber or an authorized agent, providing the Renewal Request meets the requirements set forth in this CPS, the governing CP, and the CA/Browser Forum's Baseline Requirements and EV Guidelines published at www.cabforum.org.

4.6.3 Processing Certificate Renewal Requests

Renewal requests follow the same validation and authentication procedures as a new Certificate Request and MAY re-use the information provided with the original Certificate Request, for means of verification. If for any reason re-verification fails, the certificate SHALL not be renewed and be subject to new key generation, in accordance with Section 6.1.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

Certificate Renewals SHALL follow the same notification method as a new certificate, in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Certificate Renewals SHALL follow the same acceptance method as a new certificate, in accordance with Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Certificate Renewals SHALL follow the same publication method as a new certificate, in accordance with Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate notifications to other entities SHALL follow the same entity notification method as a new certificate, in accordance with Section 4.4.3

4.7 Certificate Re-Key

Certificate re-key means the issuance of a new Certificate to the Subscriber with a new Public Key (new key-pair) and same verified information in the Certificate. A re-keyed Certificate has a new serial number and same expiration date in the Certificate being re-keyed..

4.7.1 Circumstances for Certificate Re-Key

Certificate re-keying is the re-issuance of a certificate using the same subject information and expiration date ("validTo" field) but with a new key-pair. Furthermore, everything listed in section 1.3.3 applies. Reasons for re-keying may be (this list is not restrictive):

1. The discovery of a vulnerability in a key algorithm or key size
2. The loss or compromise or suspicion of compromise of a private key
3. The deprecation of a key algorithm or key size

4.7.2 Who May Request Certification of a New Public Key

ATHEX, the Applicant, or an authorized Certificate Requestor may submit re-key requests.

4.7.3 Processing Certificate Re-Keying Requests

Re-key requests generally follow the process used for renewals After successful email validation, the new certificate is issued.

4.7.4 Notification of New Certificate Issuance to Subscriber

Certificate Re-keying SHALL follow the same notification method as a new certificate, in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Certificate Re-keying SHALL follow the same acceptance method as a new certificate as a new certificate, in accordance with Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Certificate Re-keying SHALL follow the same publication method as a new certificate, in accordance with Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

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.

4.8.1 Circumstances for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

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

ATHEX SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that ATHEX revoke the Certificate;
2. The Subscriber notifies ATHEX that the original certificate request was not authorized and does not retroactively grant authorization. In addition, this applies for Qualified Certificates for electronic seals where there is a change in Legal representation and the former Legal representative is no longer authorized to create Electronic Seals.
3. ATHEX obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. ATHEX is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
5. ATHEX obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

ATHEX SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. ATHEX obtains evidence that the Certificate was misused;
3. ATHEX is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. 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);

5. ATHEX is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. ATHEX is made aware of a material change in the information contained in the Certificate;
7. ATHEX is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. ATHEX determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. ATHEX's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
11. ATHEX is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

ATHEX MUST revoke S/MIME certificates upon the occurrence of any of the following events:

1. The Subscriber notifies ATHEX that the original certificate request was not authorized and does not retroactively grant authorization.
2. ATHEX obtains reasonable evidence that the certificate has been used for a purpose outside of that indicated in the certificate or in ATHEX's subscriber agreement or terms of use;
3. ATHEX obtains reasonable evidence that the subscriber's private key (corresponding to the public key in the certificate) has been compromised or is suspected of compromise;
4. ATHEX receives notice or otherwise becomes aware that a subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use;
5. ATHEX receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted;
6. ATHEX receives notice or otherwise becomes aware of a material change in the information contained in the Certificate
7. ATHEX a determination that the certificate was not issued in accordance with ATHEX's CP/CPS;
8. ATHEX ceases operations for any reason and has not arranged for another CA to provide revocation support for the certificate;
9. ATHEX private key used in issuing the certificate is suspected to have been compromised;
10. ATHEX determines that any of the information appearing in the certificate is not accurate;

ATHEX MUST revoke a Code Signing Certificate in any of the following circumstances:

1. The Application Software Supplier requests revocation,
2. The subscriber requests revocation,
3. A third party provides information that leads ATHEX to believe that the certificate is compromised or is being used for Suspect Code, or
4. 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;
5. ATHEX otherwise decides that the certificate should be revoked.

ATHEX SHALL revoke a Qualified Certificate/Seal if any of the following event occurs:

1. The certificate is no longer compliant with the CP/CPS under which it has been issued; or

2. ATHEX becomes aware of changes which impact the validity of the certificate;
3. For which the used cryptography is no longer ensuring the binding between the subject and the public key;
4. ATHEX obtains evidence that the Subscriber's Private Key corresponding to a Qualified Certificate/Seal suffered a Key Compromise;
5. ATHEX becomes aware that the Subscriber no longer has the signing right, is declared non-existent, is deceased, otherwise is not available to be contacted, taking into account that Qualified Certificates for electronic signatures are in all cases non-transferable;
6. The National Supervisory Body, during its surveillance duties, rules that a Qualified Certificate/Seal contains false or inaccurate information, not-conformant to the eIDAS Regulation;

   Especially for the PSD2 Certificates, ATHEX shall follow the requirements of the ETSI TS 119 495 and based on an authentic request from an NCA, ATHEX shall revoke the certificate in a timely manner if any of the following conditions:

7. the authorization of the PSP has been revoked;
8. any PSP role included in the certificate has been revoked.

ATHEX MAY revoke any Certificate in its sole discretion, including if ATHEX believes that:

1. 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.
2. The Subscriber is a denied party or prohibited person on a government issued blacklist, or is operating from a prohibited destination;
3. ATHEX receives a lawful and binding order from a government or regulatory body to revoke the Certificate;
4. 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;
5. 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 ceases operations for any reason and has not arranged for another suitable CA to provide revocation support for the Certificate.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

ATHEX SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

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

4.9.3.1 Certificate revocation by the Subscriber

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, 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. 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.

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.

4.9.3.2 Revocation Based on an Application Software Supplier's Request

If the Application Software Supplier requests ATHEX revoke because the Application Software Supplier

believes that a Certificate attribute is deceptive, or that the Certificate is being used for malware, bundle ware, unwanted software, or some other illicit purpose, then the Application Software Supplier may request that ATHEX revoke the certificate.

Within two (2) business days of receipt of the request, ATHEX MUST either revoke the certificate or inform the Application Software Supplier that it is conducting an investigation.

If ATHEX decides to conduct an investigation, it MUST inform the Application Software Supplier whether or not it will revoke the Certificate, within two (2) business days.

If the CA decides that the revocation will have an unreasonable impact on its customer, then ATHEX MUST propose an alternative course of action to the Application Software Supplier based on its investigation.

4.9.3.3 Revocation request by the eIDAS National Supervisory Body

If the National Supervisory Body (EETT) believes that a Qualified Certificate includes information that is incorrect or misleading, or that the Certificate is Compromised or being used to sign falsified data, or some other illicit purpose, then the Supervisory Body may request that ATHEX suspends or revokes the Qualified Certificate. The Supervisory Body must specify a revocation reason based on Article 11 of the Trust Service Providers National regulation (FEK 4396-B, 2017).

In such a case, ATHEX must authenticate the revocation request and execute the request within two (2) business days. In all cases, the Subscriber shall be notified prior to any status change of their Certificate.

4.9.3.4 Revocation request by a National Competent Authority

ATHEX allow the NCA, as the owner of the PSD2 specific information, to request certificate revocation. The NCA must specify a reason, which can be descriptive rather than in a standard form, for the revocation.

If the NCA as the owner of the PSD2 specific information notifies ATHEX, that information has changed which can affect the validity of the certificate, but without a properly authenticated request with an acceptable reason for why the certificate should be revoked, ATHEX shall investigate this notification regardless of its content and format, and shall revoke the affected certificate(s) if necessary. This notification need not be processed within 24 hours.

ATHEX will process such requests, and validate their authenticity. If it is not clearly indicated or implied why the revocation is requested or the reason is not in the area of responsibility of the NCA then ATHEX may decide to not take action. Based on an authentic request from an NCA, ATHEX shall revoke the certificate in a timely manner if any of the following conditions:

- the authorization of the PSP has been revoked;

- any PSP role included in the certificate has been revoked.

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

Within 24 hours after receiving a Certificate Problem Report, ATHEX SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, ATHEX SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which ATHEX will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST

NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by ATHEX SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
5. Relevant legislation.

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.

ATHEX updates and reissues CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

For Subordinate CA Certificates, CRL is updated at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

The maximum latency for the CRL is 10 seconds under normal network operating conditions.

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.

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

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 as described in RFC 6960 and/or RFC 5019. Where required by the Baseline Requirements (all TLS 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.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

1. OCSP responses MUST have a validity interval greater than or equal to eight hours;

2. OCSP responses MUST have a validity interval less than or equal to ten days;

3. For OCSP responses with validity intervals less than sixteen hours, then ATHEX SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then ATHEX SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates:

ATHEX SHALL update information provided via an Online Certificate Status Protocol (i) at least every twelve months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

For the status of Subordinate CA Certificates:

ATHEX SHALL update information provided via an Online Certificate Status Protocol (i) at least every twelve months; and (ii) within 24 hours after revoking a Subordinate CA Certificate. If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder MUST NOT respond with a "good" status for such requests.

ATHEX SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or

2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or

3. "unused" if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

As defined in Section 4.9.1.

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.

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

Certificate suspension is only allowed for Qualified certificates (eSign and eSeal) and S/MIME certificates and Code Signing certificates. Certificate suspension is not allowed for any other types of end entity Certificates.

4.9.14 Who can Request Suspension

ATHEX shall accept authenticated requests for suspension. Authorization for suspension shall be accepted if the suspension request is received from either the Subscriber or an affiliated organization named in the Certificate. ATHEX may also at their own discretion suspend Certificates including Certificates that are issued to other cross signed Issuing CAs.

4.9.15 Procedure for Suspension Request

Certification suspension may be requested via a revocation request. ATHEX will record each request for suspension and authenticate the source, taking appropriate action to suspend the Certificate if the request is authentic and approved.

Once suspended, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason code “on hold” will be included. CRLs may be published immediately or they may be published as defined within this CP/CPS.

4.9.16 Limits on Suspension Period

Certificate suspension may last as long as the validity period of Certificate.

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

4.12.1 Key Escrow and Recovery Policy and Practices

ATHEX shall not escrow CA’s Private Keys. ATHEX may escrow Subscriber key management keys to provide key recovery services for S/MIME certificates. ATHEX shall encrypt and protect escrowed Private Keys with at least the level of security used to generate and deliver the Private Key.

Subscribers and other authorized entities may request recovery of an escrowed (decryption) Private Key. Entities escrowing Private Keys shall have personnel controls in place that prevent unauthorized access to Private Keys. Key recovery requests can only be made for one of the following reasons:

1. The Subscriber has lost or damaged the private-key token,

2. The Subscriber is not available or is no longer part of the organization that contracted with ATHEX for Private Key escrow,

3. The Private Key is part of a required investigation or audit,

4. The requester has authorization from a competent legal authority to access the communication that is encrypted using the key,

5. If key recovery is required by law or governmental regulation, or

6. If the entity contracting with ATHEX for escrow of the Private Key indicates that key recovery is mission critical or mission essential.

An entity receiving Private Key escrow services shall:

1. Notify Subscribers that their Private Keys are escrowed,

2. Protect escrowed keys from unauthorized disclosure,

3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys,

4. Release escrowed keys only for properly authenticated and authorized requests for recovery, and

5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

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. TSU private signing keys stored on TSU cryptographic module shall be erased upon device retirement in a way that it is practically impossible to recover them. 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. ATHEX enforces rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV and QWAC Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in Section 11.13 of the EV Guidelines, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV or the QWAC Certificate.

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. Validation Specialists are trained and tested to the EV Certificate validation criteria.

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

ATHEX and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. ATHEX SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

ATHEX SHALL record at least the following events:

CA Key and Certificate Lifecycle Management Events:

- CA Root signing key functions, including key generation, backup, recovery, archival and destruction;
- Certificate requests, renewal, and re-key requests, and revocation;
- Approval and rejection of certificate requests;
- Cryptographic device lifecycle management events;
- Generation of Certificate Revocation Lists and OCSP entries;
- Introduction of new Certificate Profiles and retirement of existing Certificate Profiles;
- 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.

Subscriber Certificate lifecycle management events, including:

- Certificate requests, renewal, and re-key requests, and revocation;
- All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
- Approval and rejection of certificate requests;
- Issuance of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries.

Security Related Events:

- System downtime;
- System crashes, hardware failures and other anomalies;
- Installation, update and removal of software on a Certificate System;
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement;
- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- Firewall and router activities;
- Secure facility visitor entry and 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;
- Description of the 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.

ATHEX SHALL retain, for at least two years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
    a. the destruction of the CA Private Key; or
    b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the revocation or expiration of the Subscriber Certificate;
3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

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

ATHEX performs an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

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 a vulnerability assessment at least once a quarter by taking a two-pronged approach. In addition, ATHEX will perform a vulnerability scan after any system or network changes that ATHEX determines are significant and within one week of receiving a request from the CA/Browser Forum.

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 at least annually and after infrastructure or application upgrades that ATHEX determines are significant.

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 has an Incident Response Plan and a Disaster Recovery Plan. ATHEX documents business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

ATHEX is not required to publicly disclose its business continuity plans but it will make its business continuity plan and security plans available to ATHEX's CA auditors upon request.

ATHEX annually tests, reviews, and updates these procedures.

For incidents relating to Qualified Certificates for electronic signatures/seals, all provisions of article 19 of Regulation (EU) No. 910/2014 apply for the notification of the National supervisory body.

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).

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.

The business continuity plan includes:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
    Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

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 and ATHEX RSA Root CA G4 R1 key pair generation or TSU certificate issuance 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. In addition, the generation of the TSU's signing key(s) shall be undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control.

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 server Certificates Certificate Subscribers are solely responsible for the generation of the private keys used in their Certificate Requests. ATHEX does not provide server 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.

ATHEX creates private keys on behalf of subscribers only when sufficient security is maintained within the key generation process to the Subscriber. For S/MIME and Client Certificates, this is achieved through the use of PKCS#12 (.pfx) files containing private Keys and Certificates encrypted by at least eight (8) character password. For Code Signing, this is achieved through the use of PKCS#12 (.pfx) files containing private Keys and Certificates encrypted by at least sixteen (16) character password.

6.1.3 Public Key Delivery to Certificate Issuer

As regards server 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 ATHEX's repository.

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

For RSA key pairs ATHEX SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

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 and ATHEX RSA Root CA G4 R1 has been used to sign only the following Certificates:

- Certificates for Subordinate CAs
- Certificates for OCSP Response verification.

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 ATHEX RSA Root CA G4 R1 and its Issuing CA and TSU 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

ATHEX shall not escrow its signature keys. Subscribers may not escrow their private signature keys. ATHEX may escrow Subscriber Private Keys for S/MIME certificates used for encryption in order to provide key recovery as described in section 4.12.1.

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. The CA and TSU Private Keys are backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

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 and TSU private keys are 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.

ATHEX Certificates and renewed Certificates shall have a maximum validity period of:

Root CA: 25 years,

Subordinate CA: 15 years,

Client Authentication and S/MIME and Qualified Certificates for Electronic Signatures and Seals: 3 years,

Code Signing Certificates: 2 years,

TLS Certificates and QWAC certificates: 397 days, (Valid Certificates issued prior 1 September 2020 have a longer validity Period of up to 825 days).

Time-Stamping Unit or EV Timestamp Certificate: 10 years, (For the Time-Stamping Unit, a new Timestamp Certificate with a new private key must be created no later than every 15 months).

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.
- The declared accuracy is 1 second or better.
- 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.

- The clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record is maintained of the exact time (within the declared accuracy) when this change occurred.

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)

Certificates MUST be of type X.509 v3.

7.1.2 Certificate Extensions

This section specifies the additional requirements for Certificate content and extensions for Certificates.

7.1.2.1 Root CA Certificate

- basicConstraints This extension MUST appear as a critical extension. The cA field MUST be set true. ThepathLenConstraint field SHOULD NOT be present.
- keyUsage This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- certificatePolicies This extension SHOULD NOT be present.
- extendedKeyUsage This extension MUST NOT be present.

7.1.2.2 Subordinate CA Certificate

- certificatePolicies This extension MUST be present and SHOULD NOT be marked critical.

  certificatePolicies:policyIdentifier (Required)

  The following fields MAY be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

  - certificatePolicies:policyQualifiers:policyQualifierId (Optional) id-qt 1 [RFC5280].
  - certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

  HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.
- cRLDistributionPoints This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- authorityInformationAccess
  This extension SHOULD be present. It MUST NOT be marked critical.

  It SHOULD contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). It MAY contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).
- basicConstraints

  This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.
- keyUsage

  This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

- nameConstraints (optional)

  If present, this extension SHOULD be marked critical.

- extKeyUsage (optional/required)

  For Subordinate CA Certificates that will be used to issue TLS certificates, the value id-kp-serverAuth [RFC5280] MUST be present. The value id-kp-clientAuth [RFC5280] MAY be present. The values id-kp-emailProtection [RFC5280], id-kp-codeSigning [RFC5280], id-kp-timeStamping [RFC5280], and anyExtendedKeyUsage [RFC5280] MUST NOT be present. Other values SHOULD NOT be present.

  For Subordinate CA Certificates that are not used to issue TLS certificates, then the value id-kp-serverAuth [RFC5280] MUST NOT be present. Other values MAY be present, but SHOULD NOT combine multiple independent key purposes (e.g. including id-kp-timeStamping [RFC5280] with id-kp-codeSigning [RFC5280]). This extension MUST be present and SHOULD NOT be marked critical.

Other values MAY be present.

If present, this extension SHOULD be marked non-critical.

7.1.2.3 Subscriber Certificate

- certificatePolicies

  This extension MUST be present and SHOULD NOT be marked critical.

  – certificatePolicies:policyIdentifier (Required) A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

  The following extensions MAY be present:

  – certificatePolicies:policyQualifiers:policyQualifierId (Recommended) id-qt 1 [RFC 5280].

  – certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

  HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

- cRLDistributionPoints

  This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.

- authorityInformationAccess

  This extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

  It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

- basicConstraints (optional)

  The cA field MUST NOT be true.

- keyUsage (optional)

  If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

- extKeyUsage (required)

  Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present.

Other values SHOULD NOT be present. The value anyExtendedKeyUsage MUST NOT be present.

- authorityKeyIdentifier (required)

  This extension MUST be present and MUST NOT be marked critical. It MUST contain a keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.

7.1.2.3.1 Special Extensions for Qualified Certificates

If the Certificate is used in compliance with Regulation (EU) No. 910/2014, the following extensions must be added:

- **Qualified Certificates for Electronic Signatures**

Qualified Certificates for Electronic Signatures contain following qcStatements:

- id-etsi-qcs-QcCompliance
- id-etsi-qct-esign

If the Private Key related to the certified Public Key resides in a QSCD "id-etsi-qcs-QcSSCD" is included.

- **Qualified Certificates for Electronic Seals**

Qualified Certificates for Electronic Seals contain following qcStatements:

- id-etsi-qcs-QcCompliance
- id-etsi-qct-eseal

If the Private Key related to the certified Public Key resides in a QSCD "id-etsi-qcs-QcSSCD" is included.

Qualified certificates for Electronic Seals which are issued for PSD2 use include "id-etsi-psd2-qcStatement".

- **Qualified Web Authentication Certificates**

Qualified Web Authentication Certificates contain the following qualified statements:

- id-etsi-qcs-QcCompliance
- id-etsi-qct-web

Qualified Web Authentication Certificates which are issued for PSD2 use include "id-etsi-psd2-qcStatement".

If the Certificate is used in compliance with Regulation (EU) No. 2018/389 and Directive (EU) 2015/2366, the following extensions must be added.

- Qualified Certificates following the PSD2 contain the following qcStatements:
  - The role of the payment service provider, which maybe one or more of the following:

    i) account servicing (PSP_AS);

    ii) payment initiation (PSP_PI);

    iii) account information (PSP_AI);
  - the name of the competent authority where the payment service provider is registered.

7.1.2.4 All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. ATHEX SHALL NOT issue a Certificate that contains a keyUsage flag, extKeyUsage value, Certificate extension, or other data not

specified in section 7.1.2.1, 7.1.2.2, or 7.1.2.3 unless ATHEX is aware of a reason for including the data in the Certificate.

ATHEX SHALL NOT issue a Certificate with:

a. Extensions that do not apply in the context of the public Internet (such as an extKeyUsage value for a service that is only valid in the context of a privately managed network), unless:

   i. such value falls within an OID arc for which the Applicant demonstrates ownership, or

   ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

b. semantics that, if included, will mislead a Relying Party about the certificate information verified by ATHEX (such as including an extKeyUsage value for a smart card, where ATEHX is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5 Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 - Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under these Baseline Requirements.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the subjectPublicKeyInfo field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

ATHEX SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL. ATHEX SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the AlgorithmIdentifier for RSA keys MUST be byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by ATHEX Private Key MUST conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

• The signatureAlgorithm field of a Certificate or Precertificate.

• The signature field of a TBSCertificate (for example, as used by either a Certificate or

Precertificate).

• The signatureAlgorithm field of a CertificateList

• The signature field of a TBSCertList

• The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

ATHEX SHALL use one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:

  Encoding: 300d06092a864886f70d01010b0500.

- RSASSA-PKCS1-v1_5 with SHA-384:

  Encoding: 300d06092a864886f70d01010c0500.

- RSASSA-PKCS1-v1_5 with SHA-512:

  Encoding: 300d06092a864886f70d01010d0500.

- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:

  Encoding:

  304106092a864886f70d01010a3034a00f300d060960864801650304020 1
  0500a11c301a06092a864886f70d010108300d060960864801650304020 1 0500a203020120

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:

  Encoding:

  304106092a864886f70d01010a3034a00f300d060960864801650304020 2
  0500a11c301a06092a864886f70d010108300d060960864801650304020 2 0500a203020130

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

  Encoding:

  304106092a864886f70d01010a3034a00f300d06096086480165030402030500a11c301a060
  92a864886f70d010108300d060960864801650304020 3 0500a203020140

7.1.4 Name forms

Each Certificate includes a unique serial number. As of the issuance date, all Subject information is accurate, and all attributes present in the Subject field of a certificate have been verified.

TLS Certificates MUST NOT contain metadata such as '.', '-', and ' 'characters or any indication that a value or field is absent, incomplete, or not applicable.

TLS Certificates MUST NOT contain underscore characters ("_") in dNSName entries.

OU fields are restricted to Subscriber information that has been verified in accordance with section 3 of this CP/CPS.

CA certificates contain a commonName attribute that uniquely identifies and distinguishes it from other CAs; and

Certificates SHALL be issued with name forms in accordance with RFC 5280 and Section 3 of this CP/CPS.

See APPENDIX A and APPENDIX C for more details.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

See APPENDIX A and APPENDIX C.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

See APPENDIX A and APPENDIX C.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

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).

Especially for the **reasonCode (OID 2.5.29.21)** effective 2020-09-30, all of the following requirements MUST be met:

If present, this extension MUST NOT be marked critical. If a CRL entry is for a Root CA or Subordinate CA Certificate, this CRL entry extension MUST be present. If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit reasonCode entry extension, if allowed by the previous requirements. If a CRL entry is for a Certificate not subject to these Requirements and was either issued on-or-after 2020-09-30 or has a notBefore on-or-after 2020-09-30, the CRLReason MUST NOT be certificateHold (6). If a CRL entry is for a Certificate subject to these Requirements, the CRLReason MUST NOT be certificateHold (6). See section 4.9.15 for more information.

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 Certificates (EV Certificates, Standard TLS 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.

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

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

- Right to Use Domain Name 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 Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- Authorization for Certificate: That, at the time of issuance, ATHEX (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- Accuracy of Information: That, at the time of issuance, ATHEX (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in ATHEX's Certificate Policy and/or Certification Practice Statement;
- No Misleading Information: That, at the time of issuance, ATHEX (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the ATHEX's Certificate Policy and/or Certification Practice Statement;

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

In lieu of the warranties set forth above, ATHEX has followed the Guidelines and its Certification Practice Statement in issuing and managing the Certificate and in verifying the accuracy of the information contained in the EV TLS Certificate and/or EV Code Signing 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: For EV Certificates only, 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 EV Guidelines and/or Baseline Requirements for Code Signing or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
- Status: ATHEX will follow the requirements of EV Guidelines and/or Baseline Requirements for Code Signing 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 will follow the requirements of EV Guidelines and/or Baseline Requirements for Code Signing and revoke the EV Certificate for any of the revocation reasons specified in the EV Guidelines and/or Baseline Requirements for Code Singing.

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

RAs represent that:

1. The RA's certificate management services conform to this CP/CPS,

2. Information provided by the RA does not contain any false or misleading information,

3. Translations performed by the RA are an accurate translation of the original information, and

4. All Certificates requested by the RA meet the requirements of this CP/CPS.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

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); Especially for the code signing certificates to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
- 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 and specifically for the Code Signing certificates c) there is evidence that the Certificate was used to sign Suspect Code.
- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- Responsiveness: An obligation to respond to ATHEX's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- Acknowledgment and Acceptance: An acknowledgment and acceptance that ATHEX is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if ATHEX discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

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

1. an obligation to provide ATHEX with accurate and complete information in accordance with the requirements of the ETSI 319 411-1, particularly with regards to registration;
2. an obligation for the key pair to be only used in accordance with any limitations notified to the subscriber;
3. prohibition of unauthorized use of the subject's private key;
4. if the subscriber generates the subject's keys:
    - an obligation or recommendation to generate the subject keys using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP; and
    - an obligation or recommendation to use key length and algorithm as specified in ETSI

TS 119 312 for the uses of the certified key as identified in the CP during the validity time of the Certificate;

5. an obligation to notify ATHEX without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the Certificate:
    - the subject's private key has been lost, stolen, potentially compromised;
    - control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
    - inaccuracy or changes to the Certificate content, as notified to the subscriber;
6. an obligation, 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.

In lieu of the warranties set forth above, ATHEX has followed the Guidelines and its Certification Practice Statement in issuing and managing the Certificate and in verifying the accuracy of the information contained in the EV TLS Certificate and/or EV Code Signing Certificate:

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

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.

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.

To that extent ATHEX has issued and managed the certificate in accordance with the Baseline Requirements and this CP/CPS, ATHEX shall not be liable to the subscriber, relaying party or any third parties for any losses suffered as a result of use or reliance on such certificate. Otherwise, ATHEX liability to the subscriber, relaying party or any third parties for any such losses shall in no event exceed two thousand euro (2.000€) per certificate, for an EV certificate for EV TLS and EV Code Singing

certificate and a total maximum of claims of 1.000.000€, regardless of the nature of the liability and the type, amount or extent of any damages suffered.

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

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 or postal mail (see Section 1.5).

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

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. The 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 QWAC and QWAC for PSD2

10.1.1 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.

10.1.2 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.

10.1.3 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.

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
	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX RSA Qualified WEB CA G3 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	397 days (current) , 1 or 2 years (only for Certificates prior 1 September 2020)
Subject Distinguished Name	
Organization Name	Required

	subject:organizationName (OID 2.5.4.10) 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 *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
OrganizationIdentifier	Required for QWAC and QWAC for PSD2 *subject:organizationIdentifier (OID: 2.5.4.97)* 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 *subject:commonName (OID 2.5.4.3)* 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 (OID: 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 (OID: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	Required *subject:jurisdictionOfIncorporationCountryName (OID: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	Required *Subject:businessCategory (OID: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 (OID:2.5.4.9)*
Locality	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent.
State or province	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent. Optional if the subject:localityName field and the subject:organizationName field, the subject:givenName field, or the subject:surname field are present. subject:stateOrProvinceName (OID: 2.5.4.8)
Country	Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent. subject:countryName (OID: 2.5.4.6)

Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Required Critical Digital Signature, Key Encipherment
Extended Key Usage	Required 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	Required Not Critical
Certificate Policies	Required 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 [3]Certificate Policy: Policy identifier=2.23.140.1.1 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	Required 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=https://www.athexgroup.gr/pki/-

	/file/ATHEXQualifiedWEBCertificatesCAG3.crt
	Required 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://repo.athexgroup.gr/ATHEXRSAQualifiedWEBCAG3R11.crt
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier
Basic Constraints	Required Critical Subject Type=End Entity
CRL Distribution Point	Required Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXQualifiedWEBCertificatesCAG3R1.crl
	Required Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSAQualifiedWEBCAG3R11.crl
Subject Alternative Name	Required 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	Required esi4-qcStatement-1: Claim that the Certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014
id-etsi-qcsQcType	Required 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-etsi-psd2-qcStatement	Must not be present for QWAC Required 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.

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

10.2.1 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.

10.2.2 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.

10.2.3 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 to legal persons.

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

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
	For QCP-n and QCP-n-qscd: OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX RSA Qualified eSign CA G3 R11 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 CA G3 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 or 2 or 3 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. Required 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. Required for QCP-l, QCP-l-qscd, PSD2 QCP-l *subject:organizationName (OID 2.5.4.10)* 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 *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
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. Required 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. Required 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) *subject:organizationIdentifier (OID: 2.5.4.97)* 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	Required *subject:commonName (OID 2.5.4.3)* It must contain at least one FQDN or an IP address that is one of the values contained in the subjectAltName extension.
givenName	Required for QCP-n and QCP-n-qscd Must not be present for QCP-l, QCP-l-qscd and PSD2 QCP-l *subject:givenName (2.5.4.42)* If present, the subject:givenName field MUST contain a natural person Subject's name as verified under Section 3.2.3.Represantation of the Subject's given name.
Surname	Required for QCP-n and QCP-n-qscd Must not be present for QCP-l, QCP-l-qscd and PSD2 QCP-l *subject:surname (2.5.4.4)* If present, the subject:surname field MUST contain a natural person Subject's name as verified under Section 3.2.3Optional
Locality	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present. *subject:localityName (OID: 2.5.4.7)*

State or province	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent. Optional if the subject:localityName field and the subject:organizationName field, the subject:givenName field, or the subject:surname field are present. Prohibited if the subject:organizationName field, the subject:givenName field, or subject:surname field are absent. *subject:stateOrProvinceName (OID: 2.5.4.8)*
Country	Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent *subject:countryName (OID: 2.5.4.6)* Subject Country is verified in accordance with Section 3.2.2 of BR
email	Optional Subject email
Subject public Key Info	RSA with **key length 2048 bits** when the key pair is located at soft token or at ATHEX's remotely accessed QSCD. This applies to QCP-n-qscd, QCP-n, QCP-l-qscd, QCP-l and PSD2 QCP-l. RSA with **key length 3072 bits** when the key pair is located at personal QSCD. This applies to QCP-n-qscd and QCP-l-qscd.
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 and must be unique identifier for each subject. *Subject:serialNumber (OID: 2.5.4.5)* When RA is in ATHEX, the structure depends on whether it is used for HERMES application of ATHEX or not. Specifically: • When it is not used for HERMES application, the 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). • When it is used for HERMES application, the structure is: o 16 digit number which is unique identifier for each subject. When RA is not in ATHEX, it may have other structure, following the requirement to be unique.
Extensions	
Key Usage	For QCP-l, QCP-l-qscd and QCP-l supporting PSD2: Required Critical Non Repudiation

	For QCP-n and QCP-n-QSCD: Required Critical Non Repudiation
Extended Key Usage	Required Not Critical Document Signing and/or E-mail protection
Subject Key Identifier	Required Not Critical
Certificate Policies	Required 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 at hard token: [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-n-qscd at remote token: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.200.1.6 [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-qscd remote: [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.3.200.1.7 [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	Required 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
	Required 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://repo.athexgroup.gr/ATHEXRSAQualifiedeSignCAG3R11.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://repo.athexgroup.gr/ATHEXRSAQualifiedeSealCAG3R11.crt
Basic Constraints	Required Critical Subject Type=End Entity
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Required Not Critical For QCP-n and QCP-n-qscd: [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXQualifiedeSignCertificatesCAG3.crl

	For QCP-l, QCP-l-qscd and PSD2 QCP-l: 1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXQualifiedeSealCertificatesCAG3.crl
	Required Not Critical For QCP-n and QCP-n-qscd: [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSAQualifiedeSignCAG3R11.crl For QCP-l, QCP-l-qscd and PSD2 QCP-l: 1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSAQualifiedeSealCAG3R11.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	Required esi4-qcStatement-1: Claim that the Certificate is an EU Qualified Certificate in accordance with Regulation EU No 910/2014
id-etsi-qcsQcType	Required 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 Required for QCP-n-qscd, QCP-l-qscd esi4-qcStatement-4

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.

10.3 ATHEX Qualified Timestamping Certificates

10.3.1 Purpose

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

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
	OrganizationIdentifier= VATEL-099755108 L = Athens CN = ATHEX RSA Qualified Timestamp Certificates CA G3 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 year
Subject Distinguished Name	
Organization Name	Required subject:organizationName (OID 2.5.4.10) 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 Identifier	Required 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) *subject:organizationIdentifier (OID: 2.5.4.97)*
Common Name	Required *subject:commonName (OID 2.5.4.3)* .

Country	Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. *subject:countryName (OID: 2.5.4.6)*
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Required Critical Digital Signature
Extended Key Usage	Required Critical Time Stamping (id-kp-timeStamping)
Subject Key Identifier	Required 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	Required 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/ATHEXTimestampCertificatesCAG3.crt
	Required 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://repo.athexgroup.gr/ATHEXRSAQualifiedTimestampCAG3R11
	Required

CRL Distribution Point	Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXTimestampCertificatesCAG3.crl
	Required Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.athexgroup.gr/ATHEXRSAQualifiedTimestampCAG3R11.crl
Basic Constraints	Required Critical Subject Type=End Entity
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier
qcStatements	
id-qc-pkixQCSyntax-v1	Required id-etsi-qcs-SemanticsId-Legal
esi4-qtstStatement-1 0.4.0.19422.1.1	Required Claims to be a qualified electronic time-stamp as per Regulation (EU) No 910/2014

10.4 ATHEX Client Authentication CA G3

10.4.1 Purpose

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

10.4.2 Commitment to Comply with Guidelines

The Client Authentication 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.

10.4.3 Who can apply

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

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 = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 or 2 or 3 years
Subject Distinguished Name	
Organization Name	Optional *subject:organizationName (OID 2.5.4.10*) If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 3.2.2.2.
Organization Unit	Optional Subject Organizational Unit *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Common Name	Optional *subject:commonName (OID 2.5.4.3)* It must contain at least one FQDN or an IP address that is one of the values contained in the subjectAltName extension.
Locality	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present. *subject:localityName (OID: 2.5.4.7)*
State or province (if any)	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent. Optional if the subject:localityName field and the subject:organizationName field, the subject:givenName field, or the subject:surname field are present. Prohibited if the subject:organizationName field, the subject:givenName field, or subject:surname field are absent.

	subject:stateOrProvinceName (OID: 2.5.4.8)
Country	Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent *subject:countryName (OID: 2.5.4.6)* 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	Required Critical Digital Signature, Key Encipherment
Extended Key Usage	Required Not Critical Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Required Not Critical
Certificate Policies	Required Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.3.400.2.1} [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations For LCP: [2]Certificate Policy: Policy Identifier= 0.4.0.2042.1.3 For IV-NCP: [2]Certificate Policy: Policy Identifier= 0.4.0.2042.1.1 For IV-NCP+: [2]Certificate Policy: Policy Identifier= 0.4.0.2042.1.2
Authority Info Access	Required 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/ATHEXGeneralCertificatesCAG3.crt
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Required Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXGeneralCertificatesCAG3.crl
Basic Constraints	Required Not Critical Subject Type=End Entity
Subject Alternative Name	Required Not Critical Email
Certificate Transparency	Optional This field may include two or more Certificate Transparency proofs from approved CT Logs

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 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

11.2.2 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

11.2.3 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

11.2.4 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

11.2.5 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

11.2.6 ATHEX RSA Qualified Timestamp Certificates CA G3 R11

Field	**Value**
Version	V3
Serial Number	7ef6180c4891f9e300dbd5a31167bdee
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: February 26, 2021 12:05:11 PM GMT NotAfter: February 26, 2021 00:00:00 AM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX RSA Qualified Timestamp Certificates CA G3 R11 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 (06)
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)
Subject Key Identifier	4f77b533eeaae1355d82343b5a22bb2fc82c62c1

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

11.2.7 ATHEX RSA Qualified WEB Certificates CA G3 R11

Field	**Value**
Version	V3
Serial Number	21124c0b1cb87c0a07a36159eeef7112
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: February 26, 2021 12:01:28 PM GMT NotAfter: February 26, 2021 00:00:00 AM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = RSA Qualified WEB Certificates CA G3 R11 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)
Subject Key Identifier	5e6b5fa9d6f12fdb69615f3ef4b23e90ad0ff2ff
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 RSA Qualified eSeal Certificates CA G3 R11

Field	**Value**
Version	V3
Serial Number	35a8d4254120b59ba28b96360ea50587
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: February 26, 2021 11:55:55 PM GMT NotAfter: February 26, 2021 00:00:00 AM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108 L = Athens CN = ATHEX RSA Qualified eSeal Certificates CA G3 R11 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)
Subject Key Identifier	4b411e96cbdd621f5f0ef340b4ecd7c89e69e144
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

11.2.9 ATHEX RSA Qualified eSign Certificates CA G3 R11

Field	**Value**
Version	V3
Serial Number	402cc5db1b16e09f667e8e35a40e0ba5
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: February 26, 2021 11:51:45 PM GMT NotAfter: February 26, 2021 00:00:00 AM GMT
Subject Distinguished Name	OrganizationIdentifier = VATEL-099755108

	L = Athens CN = ATHEX RSA Qualified eSign Certificates CA G3 R11 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)
Subject Key Identifier	d3e0ca4c7ad154aa259fda58797a4e30684cfada
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

12 Appendix C

12.1 ATHEX TLS Certificates CA G4

12.1.1 Purpose

The purposes of a TLS Certificate are to:

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

12.1.2 Commitment to Comply with Guidelines

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

12.1.3 Who can apply

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

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 RSA TLS CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	397 days
Subject Distinguished Name • TLS Certificates for DV must include FQDN or IP address at subjectAltName • TLS Certificates for OV must also include at least the following attributes: ○ Organization ○ Country ○ Locality or stateOrProvinceName	
Organization Name	Must not be present at DV Certificates Required for OV Certificates *subject:organizationName (OID 2.5.4.10)* 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:organizationalUnitName (OID: 2.5.4.11)* Subject Organizational Unit

	subject:organizationalUnitName (OID: 2.5.4.11) ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Common Name	Optional for DV and OV Certificates *subject:commonName (OID 2.5.4.3)* 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 *subject:localityName (OID: 2.5.4.7)*
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 *subject:stateOrProvinceName (OID: 2.5.4.8)*
Country	Must not be present at DV Certificates Required for OV Certificates *subject:countryName (OID: 2.5.4.6)* 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	Required for DV and OV Certificates Critical Digital Signature, Key Encipherment
Extended Key Usage	Required for DV and OV Certificates Not Critical Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	Required for DV and OV Certificates Not Critical
Certificate Policies	Required for DV and OV Certificates For TLS Certificates for DV: Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.4.100.1.1} [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 [3]Certificate Policy: Policy Identifier= 2.23.140.1.2.1 For TLS Certificates for OV: Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.4.100.1.2} [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 [3]Certificate Policy: Policy Identifier= 2.23.140.1.2.2 OR for IV: [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.8 [3]Certificate Policy: Policy Identifier= 2.23.140.1.2.3
Authority Info Access	Required 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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/ATHEXRSATLSCAG4R11.crt
Authority Key Identifier	Required for DV and OV Certificates Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Required for DV and OV Certificates Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSATLSCAG4R11.crl
Basic Constraints	Required for DV and OV Certificates

	For TLS Certificates for DV: Not Critical Subject Type=End Entity For TLS Certificates for OV: Critical Subject Type=End Entity
Subject Alternative Name	Required 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

12.2 ATHEX Extended Validation (EV) TLS Certificates CA G4

12.2.1 Purpose

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

12.2.2 Commitment to Comply with Guidelines

The EV Code Signing Certificates from ATHEX Root CA G4 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.

12.2.3 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.

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 RSA EV TLS CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	397 days
Subject Distinguished Name	
Organization Name	Required *organizationName (OID 2.5.4.10)* 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 *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Organization Identifier	Optional 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) *subject:organizationIdentifier (OID: 2.5.4.97)*
	Optional

	If the subject:organizationIdentifier is present, this field MUST be present. If present, this field MUST contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme. *cabfOrganizationIdentifier (OID: 2.23.140.3.1)*
Common Name	Optional *subject:commonName (OID: 2.5.4.3)* 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 (OID: 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 (OID: 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	Required *subject:jurisdictionOfIncorporationCountryName (OID: 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	Required *Subject:serialNumber (OID: 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	Required *Subject:businessCategory (OID: 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 (OID: 2.5.4.9)*
Locality	Locality or stateOrProvinceName must be present *subject:localityName (OID:2.5.4.7)*
State or province	Locality or stateOrProvinceName must be present *subject:stateOrProvinceName (OID: 2.5.4.8)*
Country	Required *subject:countryName (OID: 2.5.4.6)* This field MUST contain the address of the physical location of the Subject's Place of Business.
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Required Critical Digital Signature, Key Encipherment
Extended Key Usage	Required Not Critical Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	Required Not Critical
Certificate Policies	Required Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.4.100.1.3} [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 [3]Certificate Policy: Policy Identifier=0.4.0.2042.1.4
Authority Info Access	Required 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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/ ATHEXRSAEVTLSCAG4R11.crt
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Required Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSAEVTLSCAG4R11.crl
Basic Constraints	Required Critical Subject Type=End Entity
Subject Alternative Name	Required 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

12.3 ATHEX Extended Validation (EV) Code Signing Certificates CA G4

12.3.1 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.

12.3.2 Commitment to Comply with Guidelines

The EV Code Signing Certificates from ATHEX Root CA G4 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.

12.3.3 Who can apply

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

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 RSA EV Code Signing CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	397 days
Subject Distinguished Name	
Organization Name	Required *subject:organizationName (OID 2.5.4.10)* 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 *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Common Name	Required

	subject:commonName (OID: 2.5.4.3) The Subject's verified legal name
City or Town of Incorporation	May be required subject:jurisdictionOfIncorporationLocalityName (OID: 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 (OID: 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	Required *subject:jurisdictionCountryName (OID: 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	Required *Subject:serialNumber (OID: 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	Required *Subject:businessCategory (OID: 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 (OID: 2.5.4.9)*
Locality	Locality or stateOrProvinceName must be present *subject:localityName (OID:2.5.4.7)*
State or province (if any)	Locality or stateOrProvinceName must be present

	subject:stateOrProvinceName (OID: 2.5.4.8)
Country	Required *subject:countryName (OID: 2.5.4.6)* This field MUST contain the address of the physical location of the Subject's Place of Business.
Subject public Key Info	RSA (3072 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Required Critical Digital Signature
Extended Key Usage	Required Not Critical id-kp-codeSigning
Subject Key Identifier	Required Not Critical
Certificate Policies	Required Not Critical [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.4.300.1.2 [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 [3]Certificate Policy: Policy Identifier= 0.4.0.2042.1.2
Authority Info Access	Required 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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/ATHEXRSAEVCodeSigningCAG4R11.crl
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Required Not Critical

	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSAEVCodeSigningCAG4R11.crl
Basic Constraints	Required Critical Subject Type=End Entity

12.4 ATHEX Code Signing Certificates CA G4

12.4.1 Purpose

ATHEX 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 Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. 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 Code Signing Certificate, only its distributor is identified.

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

- That the Subject named in the Code Signing Certificate is actively engaged in doing business;
- That the Subject named in the Code Signing Certificate complies with applicable laws;
- That the Subject named in the 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 Code Signing Certificate.

12.4.2 Commitment to Comply with Guidelines

The Code Signing Certificates from ATHEX Root CA G4 conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of 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.

12.4.3 Who can apply

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

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 RSA Code Signing CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA

	C = GR
Validity Period	1 or 2 years
Subject Distinguished Name	
Organization Name	Required *subject:organizationName (OID 2.5.4.10)* 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 *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Common Name	Required *subject:commonName (OID: 2.5.4.3)* The Subject's verified legal name
City or Town of Incorporation	May be required subject:jurisdictionOfIncorporationLocalityName (OID: 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 (OID: 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	Required

	subject:jurisdictionCountryName (OID: 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	Required *Subject:serialNumber (OID: 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	Required *Subject:businessCategory (OID: 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 (OID: 2.5.4.9)*
Locality	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present. *subject:localityName (OID: 2.5.4.7)*
State or province (if any)	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent. Optional if the subject:localityName field and the subject:organizationName field, the subject:givenName field, or the subject:surname field are present. Prohibited if the subject:organizationName field, the subject:givenName field, or subject:surname field are absent. *subject:stateOrProvinceName (OID: 2.5.4.8)*
Country	 Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. Optional if the subject:organizationName field, subject:givenName

	field, and subject:surname field are absent *subject:countryName (OID: 2.5.4.6)* Subject Country is verified in accordance with Section 3.2.2 of BR
Subject public Key Info	RSA (3072 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Required Critical Digital Signature
Extended Key Usage	Required Not Critical id-kp-codeSigning
Subject Key Identifier	Required Not Critical
Certificate Policies	Required Not Critical [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.4.300.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/digital-certificates-pki-regulations [2]Certificate Policy: Policy Identifier=2.23.140.1.4.1 For OV NCP: [3]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 For OV NCP+: [3]Certificate Policy: Policy Identifier=0.4.0.2042.1.2
Authority Info Access	Required 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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/ATHEXRSACodeSigningCAG4R11.crt
Authority Key Identifier	Required

	Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Required Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSACodeSigningCAG4R11.crl
Basic Constraints	Required Critical Subject Type=End Entity

12.5 ATHEX S/MIME Certificates

12.5.1 Purpose

The purposes of a S/MIME Certificate are to:

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

12.5.2 Who can apply

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

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 RSA SMIME CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 or 2 or 3 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. *subject:organizationName (OID 2.5.4.10)* 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 *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Common Name	Optional *subject:commonName (OID 2.5.4.3)* It must contain at least one FQDN or an IP address that is one of the values contained in the subjectAltName extension
givenName	Optional *subject:givenName (2.5.4.42)* If present, the subject:givenName field MUST contain a natural person Subject's name as verified under Section 3.2.3.
Surname	Optional *subject:surname (2.5.4.4)* If present, the subject:surname field MUST contain a natural person Subject's name as verified under Section 3.2.3
Locality	Optional *subject:localityName (OID: 2.5.4.7)*
State or province	Optional *subject:stateOrProvinceName (OID: 2.5.4.8)*
Country	Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent. subject:countryName (OID: 2.5.4.6)
email	Optional Subject email
Subject public Key Info	RSA (2048 bits)
Signature Algorithm	sha256
Extensions	
Key Usage	Required Critical Digital Signature, Key Encipherment

Extended Key Usage	Required Not Critical Secure Email
Subject Key Identifier	Required Not Critical
Certificate Policies	Required Not Critical For S/MIME certificates without Organization [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.4.400.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.helex.gr/el/web/guest/digital-certificates-pki-regulations For LCP: [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3 For IV-NCP: [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 For IV-NCP+: [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 For S/MIME certificates with Organization [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.4.400.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.helex.gr/el/web/guest/digital-certificates-pki-regulations For LCP: [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3 For OV-NCP: [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 For OV-NCP+: [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.2
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/AthexRSARootCAG4R1

	[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/ATHEXRSASMIMECAG4R11.crt
Authority Key Identifier	Required Not Critical
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSASMIMECAG4R11.crl
Basic Constraints	Required Not Critical Subject Type=End Entity
Subject Alternative Name	Required *extensions:subjectAltName* This extension must contain at least one entry. Each entry must be an rfc822Name containing an email address of the Subscriber. It must not contain a Domain Name or IP Address.

12.6 ATHEX Client Authentication CA G4

12.6.1 Purpose

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

12.6.2 Commitment to Comply with Guidelines

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

12.6.3 Who can apply

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

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 RSA Client CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 or 2 or 3 years

Subject Distinguished Name	
Organization Name	Optional *subject:organizationName (OID 2.5.4.10*) If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 3.2.2.2.
Organization Unit	Optional Subject Organizational Unit *subject:organizationalUnitName (OID: 2.5.4.11)* ATHEX SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Common Name	Optional *subject:commonName (OID 2.5.4.3)* It must contain at least one FQDN or an IP address that is one of the values contained in the subjectAltName extension.
Locality	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present. *subject:localityName (OID: 2.5.4.7)*
State or province (if any)	Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent. Optional if the subject:localityName field and the subject:organizationName field, the subject:givenName field, or the subject:surname field are present. Prohibited if the subject:organizationName field, the subject:givenName field, or subject:surname field are absent. *subject:stateOrProvinceName (OID: 2.5.4.8)*
Country	 Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent *subject:countryName (OID: 2.5.4.6)*

	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	Required Critical Digital Signature, Key Encipherment
Extended Key Usage	Required Not Critical Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Required Not Critical
Certificate Policies	Required Not Critical [1]Certificate Policy: Certificate Policies; {1.3.6.1.4.1.29402.1.4.400.2.1} [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.athexgroup.gr/en/web/guest/digital-Certificates-pki-regulations For LCP: [2]Certificate Policy: Policy Identifier= 0.4.0.2042.1.3 For IV-NCP: [2]Certificate Policy: Policy Identifier= 0.4.0.2042.1.1 For IV-NCP+: [2]Certificate Policy: Policy Identifier= 0.4.0.2042.1.2
Authority Info Access	Required 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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/ATHEXRSAClientCAG4R11.crt
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier
CRL Distribution Point	Required Not Critical

	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSAClientCAG4R11.crl
Basic Constraints	Required Not Critical Subject Type=End Entity
Subject Alternative Name	Required Not Critical Email
Certificate Transparency	Optional This field may include two or more Certificate Transparency proofs from approved CT Logs

12.7 ATHEX Timestamping Certificates

12.7.1 Purpose

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

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 RSA Timestamping CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	1 year
Subject Distinguished Name	
Organization Name	Required subject:organizationName (OID 2.5.4.10) 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 Identifier	Required 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) *subject:organizationIdentifier (OID: 2.5.4.97)*
Common Name	Required *subject:commonName (OID 2.5.4.3)*
Country	Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. *subject:countryName (OID: 2.5.4.6)*
Subject public Key	RSA (2048 bits)

Info	
Signature Algorithm	sha256
Extensions	
Key Usage	Required Critical Digital Signature
Extended Key Usage	Required Critical Time Stamping (id-kp-timeStamping)
Subject Key Identifier	Required Not Critical
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29402.1.4.500.1.1 [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	Required 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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/ATHEXRSATimestampingCAG4R11.crt
CRL Distribution Point	Required Not Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/ATHEXRSATimestampingCAG4R11.crl
Basic Constraints	Required Critical Subject Type=End Entity
Authority Key Identifier	Required Not Critical Issuer's Subject Key Identifier

13 Appendix D

13.1 ATHEX Root CA G4 Certificate Profile

Field	**Value**
Version	V3
Serial Number	35692d3605d0c127a7e5972c299166c5
Issuer Signature Algorithm	sha384WithRSAEncryption (1.2.840.113549.1.1.12)
Issuer Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	NotBefore: Feb 25 12:03:51 2021 GMT NotAfter: Feb 25 00:00:00 2041 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Subject public Key Info	RSA (4096 bits) 30 82 02 0a 02 82 02 01 00 b6 07 2a c5 51 d0 51 2e db 9a 5c a6 b8 3c c0 92 34 dc 0d 91 22 b1 61 2a 13 26 d8 86 1d a8 45 aa 55 fe f4 2f 15 7a df 13 cd 66 18 07 9f a2 a8 92 1b f9 72 1b 5c 8c 92 15 03 90 93 3e 23 f9 07 e9 62 81 8b 61 1b aa d3 e0 fa 03 72 55 14 1f 11 9e e6 bb 95 b4 dc b2 8e 75 8d 64 f3 28 6c 02 39 b4 b5 ee b3 40 e7 1e f6 58 9f d1 5f 30 18 42 28 fe cc 7c c4 6c 47 65 1c c0 2c a4 35 2a a9 7b db 89 83 a2 7c 03 27 d3 79 2b 6d 06 06 3c 52 2d f3 62 6b 51 5b de 2e d9 c3 85 1d bd 30 2f 0d 86 6e c4 83 89 fe 09 e5 97 28 fc 0e 21 9c 52 fd 7f e1 a0 4d 7f 88 a1 d3 31 51 06 32 49 d3 7a 45 44 cc e3 e5 6d 21 1d 7a 9d 76 d9 cd 29 87 67 40 d0 f2 7c 36 02 8d 52 ef 95 5e 3c 0b 09 ec a4 eb b3 8e 35 a6 e6 58 4c 52 da 2d 5b 71 45 cf bc 7f f1 38 22 bb 2b 05 5f d5 ee a3 04 a7 a7 18 f7 5b df ed b5 24 59 f7 79 70 89 00 47 80 93 b6 d7 89 e8 de be 03 92 7b b0 cf d3 b1 60 21 65 15 45 5e f9 f2 77 7f 01 07 0c e4 6a 61 86 5c 50 27 89 36 37 41 d0 19 c2 fd f0 0e 5a 05 14 74 66 0e 50 38 e7 66 76 7e 74 6b fb b3 52 bd 98 2c 1d 5d 2f 9e 64 72 ce 0b 2f 1c f9 53 bd 18 34 5a de d4 96 72 7c e7 0c 8f 62 43 6d b0 76 96 27 03 52 c3 eb 17 ae 40 04 ab f8 a7 cb c5 e6 d2 7f a9 70 6c c9 00 cd 46 30 9a 2d fc 83 3b ac ab 02 f1 52 95 27 b4 2a b9 26 01 0a c9 fc ad 8f 45 52 f3 af be 3a 0e d8 9b 15 b6 e2 4a da ad 73 89 ce 9b 3c 65 2d 9b 1a 41 3a c5 d3 f1 40 05 29 fa 57 e5 bb 9a f2 c8 1d f6 1e 88 c3 6a 91 63 ed 88 ef 25 f7 64 d5 06 24 d5 47 7b eb b4 03 2c c7 20 a0 0c ab 2c 4d c0 88 ad 76 c6 77 30 e7 5e 1b 0e 85 c6 fb 17 89 a7 1b 81 25 b2 c2 eb b8 c7 ec b0 20 ca 90 a5 2f 6e 58 e4 4f 02 03 01 00 01
Extensions	
Key Usage	Critical Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	f82b4bb0de5c2bd19c8f88b06bce38833394ac26
Basic constraints	Critical Subject Type=CA Path Length Constraint=None

13.2 SUB CAs

13.2.1 ATHEX RSA EV TLS CA G4 R11

Field	Value
Version	V3
Serial Number	6a1800ba682e94841894ba0017b750d5
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	NotBefore: Feb 25 12:42:18 2021 GMT NotAfter: Feb 25 00:00:08 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA EV TLS CA G4 R11 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Subject public Key Info	RSA (4096 bits)
Extensions	
Key Usage	Critical Certificate Signing, Off-line CRL Signing, CRL Signing (06)
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)
Subject Key Identifier	87f63ec4ebe08b835e7c455a5cf2e562b1e5fe20
Basic constraints	Critical Subject Type=CA Path Length Constraint=0
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies
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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/AthexRSARootCAG4R1.crt
Authority Key Identifier	KeyID=f82b4bb0de5c2bd19c8f88b06bce38833394ac26
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/AthexRSARootCAG4R1.crl

13.2.2 ATHEX RSA TLS CA G4 R11

Field	Value
Version	V3

Serial Number	2f7e88fabf812b6e7c140ecaff6f35ed
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	NotBefore: Feb 25 12:40:38 2021 GMT NotAfter: Feb 25 00:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA TLS CA G4 R11 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 (06)
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)
Subject Key Identifier	1e184574bbd295f158576d6a8299ff043c918798
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies
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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/AthexRSARootCAG4R1.crt
Authority Key Identifier	KeyID=f82b4bb0de5c2bd19c8f88b06bce38833394ac26
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/AthexRSARootCAG4R1.crl

13.2.3 ATHEX RSA Code Signing CA G4 R11

Field	**Value**
Version	V3
Serial Number	793d75d3346b788fe0c08f2f6527735c
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens

	CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	NotBefore: Feb 25 12:44:30 2019 GMT NotAfter: Feb 25 00:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA Code Signing CA G4 R11 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 (06)
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
Subject Key Identifier	793d75d3346b788fe0c08f2f6527735c
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies
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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/AthexRSARootCAG4R1.crt
Authority Key Identifier	KeyID=f82b4bb0de5c2bd19c8f88b06bce38833394ac26
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/AthexRSARootCAG4R1.crl

13.2.4 ATHEX RSA EV Code Signing CA G4 R11

Field	**Value**
Version	V3
Serial Number	793d75d3346b788fe0c08f2f6527735c
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR

Validity Period	NotBefore: Feb 25 12:44:30 2019 GMT NotAfter: Feb 25 00:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA EV Code Signing CA G4 R11 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 (06)
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
Subject Key Identifier	793d75d3346b788fe0c08f2f6527735c
Basic constraints	Critical Subject Type=CA Path Length Constraint=0
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies
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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/AthexRSARootCAG4R1.crt
Authority Key Identifier	KeyID=f82b4bb0de5c2bd19c8f88b06bce38833394ac26
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/AthexRSARootCAG4R1.crl

13.2.5 ATHEX RSA Client CA G4 R11

Field	**Value**
Version	V3
Serial Number	4c4c0c4b67a2914841a08d965d964ae7
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	NotBefore: Feb 25 12:38:22 2021 GMT NotAfter: Feb 25 00:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA Client CA G4 R11 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 (06)
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	f28b5b129ab5f4a4be357c7c1e5a120fa2df7454
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies
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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/AthexRSARootCAG4R1.crt
Authority Key Identifier	KeyID=f82b4bb0de5c2bd19c8f88b06bce38833394ac26
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/AthexRSARootCAG4R1.crl

13.2.6 ATHEX RSA S/MIME CA G4 R11

Field	**Value**
Version	V3
Serial Number	0cda7aaa276a3ac025aa7f64cdacf93b
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	NotBefore: Feb 25 12:38:22 2021 GMT NotAfter: Feb 25 00:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA SMIME CA G4 R11 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 (06)
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)
Subject Key Identifier	a22b533c54c023724e307c18cf96931ed3439ffe
Basic constraints	Critical Subject Type=CA Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies
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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/AthexRSARootCAG4R1.crt
Authority Key Identifier	KeyID=f82b4bb0de5c2bd19c8f88b06bce38833394ac26
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/AthexRSARootCAG4R1.crl

13.2.7 ATHEX RSA Timestamping CA G4 R11

Field	**Value**
Version	V3
Serial Number	26a21e4680ac125351c6654a3964c118
Issuer Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer Distinguished Name	L = Athens CN = ATHEX RSA Root CA G4 R1 O = HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA C = GR
Validity Period	NotBefore: Feb 25 12:46:58 2021 GMT NotAfter: Feb 25 00:00:00 2029 GMT
Subject Distinguished Name	L = Athens CN = ATHEX RSA Timestamping CA G4 R11 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 (06)

Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)
Subject Key Identifier	a22b533c54c023724e307c18cf96931ed3439ffe
Basic constraints	Critical Subject Type=CA Path Length Constraint=0
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies
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/AthexRSARootCAG4R1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.athexgroup.gr/AthexRSARootCAG4R1.crt
Authority Key Identifier	KeyID=f82b4bb0de5c2bd19c8f88b06bce38833394ac26
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.athexgroup.gr/AthexRSARootCAG4R1.crl