Print this page

Mozilla - CA Program

Case Information

Case Number	00000242	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Athens Exchange S.A. (Athex)	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include ATHEX Root CA G2	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1407921

General information about CA's associated organization

CA Email Alias 1	pkica-services@athexgroup.gr		
CA Email Alias 2			
Company Website	http://www.helex.gr/digital-certificates	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Greece, Europe	**Verified?**	Verified
Primary Market / Customer Base	Athens Stock Exchange (ATHEX) is the Operator of the Greek Cash, Bonds & Derivatives market.	**Verified?**	Verified
Impact to Mozilla Users	Athens Stock Exchange is a major player in Greece's financial sector.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices	NEED: CAs response to each of the items listed in https://wiki.mozilla.org/CA/Required_or_Recommended_Practices 1. Publicly Available CP and CPS: ??? Could not find Root CP/CPS document 2. Audit Criteria: ??? Need Root CP/CPS document and section where this is stated. 3. Revocation of Compromised Certificates: WebAuthCP-CPS section 4.9.1 4. Verifying Domain Name Ownership: WebAuthCP-CPS section 3.2.2 5. Verifying Email Address Control: ??? 6. DNS names go in SAN: ??? 7. OCSP: WebAuthCP-CPS section 7.3 8. Network Security Controls: ???	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	NEED: CA's response to each of the items listed in https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices 1. Long-lived Certificates: WebAuthCP-CPS section 6.2.2 (note typos in section heading, and that the description does not state the maximum allowed validity) -- PROBLEM 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: WebAuthCP-CPS section 3.2.2 3. Issuing End Entity Certificates Directly From Roots: ??? Need CP/CPS for root level. 4. Distributing Generated Private Keys in PKCS#12 Files: WebAuthCP-CPS section section 3.2.1 5. Certificates Referencing Local Names or Private IP Addresses: WebAuthCP-CPS section section 1.4.1 6. Issuing SSL Certificates for .int Domains: WebAuthCP-CPS section 1.4.1. 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: ??? Key size info for end-entity certs not found in WebAuthCP-CPS 9. Delegation of Domain / Email Validation to Third Parties: ??? Where is it documented in a CP/CPS that this is	**Verified?**	Need Response From CA

not allowed?

Root Case Record # 1

Root Case Information

Root Certificate Name	ATHEX Root CA G2	**Root Case No**	R00000457
Request Status	Information Verification In Process	**Case Number**	00000242

Certificate Data

Certificate Issuer Common Name	ATHEX Root CA G2
O From Issuer Field	ATHENS STOCK EXCHANGE
OU From Issuer Field	
Valid From	2016 Mar 15
Valid To	2036 Mar 14
Certificate Serial Number	3ecf
Subject	CN=ATHEX Root CA G2, OU=null, O=ATHENS STOCK EXCHANGE, C=GR
Signature Hash Algorithm	sha384WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	89:2A:1B:D4:C8:B0:F8:AA:9A:65:ED:4C:B9:D3:BF:48:40:B3:4B:C1
SHA-256 Fingerprint	C1:72:7F:3B:67:3E:6A:E7:F1:2F:23:D7:89:A7:BE:38:B9:18:22:3E:F6:91:1C:59:2D:A1:F5:83:44:4A:54:7E
Certificate ID	55:B6:0A:DE:7C:9A:99:D0:28:7A:9C:51:34:ED:A1:D1:F0:B0:79:CB:A9:28:5A:A9:B9:ED:74:0C:F6:2B:39:D4
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root has internally-operated intermediate certificates. The request is to turn on the Email and	**Verified?**	Verified

	Websites trust bits, and to enable EV treatment.		
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8967569	**Verified?**	Verified
CRL URL(s)	http://www.helex.gr/pki/-/file/AthexRootCAG2.crl http://www.athexgroup.gr/pki/-/file/AthexSSLCAG2.crl WebAuthCP-CPS section 4.9.7	**Verified?**	Verified
OCSP URL(s)	http://ocsp.athexgroup.gr/AthexRootCAG2 http://ocsp.athexgroup.gr/AthexSSLCAG2	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	1.3.6.1.4.1.29402.1.1.5.1.1.0	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://certdemo-valid.athexgroup.gr	**Verified?**	Verified
Test Website - Expired	https://certdemo-expired.athexgroup.gr		
Test Website - Revoked	https://certdemo-revoked.athexgroup.gr		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/certdemo-valid.athexgroup.gr NEED to fix errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	https://crt.sh/?caid=60855&opt=cablint,zlint,x509lint&minNotBefore=2016-03-15 OK	**Verified?**	Verified
Test Website Lint Test	See above.	**Verified?**	Verified

EV Tested	https://tls-observatory.services.mozilla.com/static/ev-checker.html ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root cert signs internally-operated intermediate certs, which are listed here: https://www.athexgroup.gr/digital-certificates-repository The ATHEX Root CA G2 has five subordinate Issuing CAs: 1) ATHEX SSL Certificates CA G2 2) ATHEX Qualified Certificates CA G2 3) ATHEX General Certificates CA G2 4) ATHEX TSA 5) ATHEX Code Signing Certificates CA G2	**Verified?**	Verified
Externally Operated SubCAs	ATHEX Stock Exchange (ATHEX) does not permit sub CAs operated by 3rd parties. NEED: The CP/CPS document and section where this is stated If Mozilla included this root certificate, the all of the subordinate CA certificates it signs or has signed will also be trusted, so it is important that we understand the full impact or potential impact of including this root certificate. https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy#intermediate-certificates	**Verified?**	Need Response From CA
Cross Signing	ATHEX Stock Exchange (ATHEX) does not permit cross signing Certificate Authorities. NEED: The CP/CPS document and section where this is stated	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external Registration Authorities. References: - section 7.1.5 of the CA/Browser Forum's Baseline Requirements - Mozilla's Root Store Policy	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	Some documents are in Greek, and others are in English.	**Verified?**	Verified

	Some of the sites referred to have an SSL cert than chains up to the Athex Root CA, which can be imported from here: https://bugzilla.mozilla.org/attachment.cgi?id=8967570		
CA Document Repository	https://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.athexgroup.gr/documents/10180/681762/WebAuthCP-CPS_EN.pdf/a0c9ce95-d8cf-4533-bf3d-1f433d44760e	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.athexgroup.gr/documents/10180/681762/WebAuthCP-CPS_EN.pdf/a0c9ce95-d8cf-4533-bf3d-1f433d44760e	**Verified?**	Verified
Other Relevant Documents	There are separate CP documents for each type of cert issuance. See the full list here: https://www.athexgroup.gr/web/guest/digital-certificates-pki-regulations The CP/CPS linked to above is the WebAuthCP-CPS_EN.pdf file with title "CP/CPS for EU Qualified Certificates for Website Authentication"	**Verified?**	Verified
Auditor (New)		**Verified?**	Not Verified
Auditor Location (New)		**Verified?**	Not Verified
Standard Audit	NEED: Public (not marked as confidential) audit statements meeting the requirements of Mozilla's Root Store Policy. https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy#audits	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: BR audit as per Mozilla's Root Store Policy. See also https://www.mozilla.org/en-US/about/governance/policies	**Verified?**	Need Response From CA

	/security-group/certs/policy#public-audit-information		
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
EV SSL Audit Type		**Verified?**	Need Response From CA
EV SSL Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	WebAuthCP-CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8946984	**Verified?**	Verified
SSL Verification Procedures	WebAuthCP-CPS section 3.2.3	**Verified?**	Verified
EV SSL Verification Procedures	WebAuthCP-CPS section 3.2.2	**Verified?**	Verified
Organization Verification Procedures	WebAuthCP-CPS sections 3.2.2, 3.2.4	**Verified?**	Verified
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	WebAuthCP-CPS section 5.2, 5.3	**Verified?**	Verified
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	**Verified?**	Need Response From CA