Bugzilla ID: 967387
Bugzilla Summary: Add Athens Exchange root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A.
Website URL	http://www.helex.gr/digital-certificates
Organizational type	HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. which is operating the CA is a private company.
Primark Market / Customer Base	Public sector, bank sector, corporate sector.
Impact to Mozilla Users	HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. is the organizer and operator of the Greek Stock & Derivatives Market. Also develops PKI/CA services to fit business needs. Specifically, our company is developing a PKI infrastructure for issuing digital certificates used in smart card applications that require digital signatures such as signing document, emails and financial transactions.
Inclusion in other major browsers	Microsoft Explorer http://social.technet.microsoft.com/wiki/contents/articles/19217.windows-and-windows-phone-8-ssl-root-certificate-program-may-2013.aspx
CA Primary Point of Contact (POC)	PKICA-Services@helex.gr Faidon Tsikliropoulos, Head of PKICA Services F.Tsikliropoulos@helex.gr, +30 210 3366283 John Balafas, Deputy Director of Applications' Management, HW & SW Management, Users' Technical Support & PKICA Services J.Balafas@helex.gr, +30 210 3366155

Technical information about each root certificate

Certificate Name	ATHEX Root CA

Certificate Issuer Field	CN = ATHEX Root CA
	O = Athens Exchange S.A.
	C = GR

Certificate Summary	This root has two internally-operated subordinate CAs; one subCA issues qualified certificates, and the other subCA issues non-qualified certificates.
Root Cert URL	http://www.helex.gr/documents/10180/681760/Certificates.zip/b95d8bc0-7d4f-4239-9e02-b7695d6500c6
SHA1 Fingerprint	DB:2B:7B:43:4D:FB:7F:C1:CB:59:26:EC:5D:95:21:FE:35:0F:F2:79
Valid From	2010-10-18
Valid To	2030-10-17
Certificate Version	3
Certificate Signature Algorithm	SHA-1

Signing key parameters	2048
Test Website URL (SSL)	https://trs.helex.gr/
CRL URL	CRL URI in end-entity cert only, and it is LDAP
OCSP URL (Required now)	Comment #4: The verification of the validity of the end user or CA certificates via the OSCP protocol is not currently available. BR #13.2.2: "The CA SHALL update information provided via an Online Certificate Status Protocol..." BR Appendix B regarding authorityInformationAccess in Subordinate CA Certificate and Subscriber Certificate: "With the exception of stapling .... this extension MUST be present ... and it MUST contain the HTTP URL of the Issuing CA's OCSP responder" Need: - OCSP URI in the AIA of end-entity certs - Maximum expiration time of OCSP responses - Testing results of browsing to test website with OCSP enforced in Firefox browser, as per https://wiki.mozilla.org/CA:Recommended_Practices#OCSP
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing Comment #4: We issue ssl certificates for our web sites accessible from our clients register companies etc. These web sites have different domain names other than *helex.gr, for example https://www.inbroker.com/IBH/default/content/home/index.asp or https://www.axiaweb.gr
SSL Validation Type	OV, EV
EV Policy OID(s)	If EV treatment is being requested, then need: - EV Policy OID - EV Audit statement - Screen shot showing successful completion of EV testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Non-sequential serial numbers and entropy in cert	Comment #4: HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. may enforce uniqueness within the DN or by requiring that each certificate include a unique non sequential serial number with at least 20 bits of entropy. Where is this documented in the CP or CPS?

CA Hierarchy information for each root certificate

CA Hierarchy	ATHEX Root CA has signed two internally-operated subCAs: - ATHEX General Certificates CA -- issuing CA for non-qualified certificates - ATHEX Qualified Certificates CA -- issuing CA for qualified certificates
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on Third-party Issuers	Comment #4: HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. has not issue any CA or Sub CAs for Third-Party Issuers and is not going to do it.

Verification Policies and Practices

Policy Documentation	Documents are in Greek. Document Repository: http://www.helex.gr/web/guest/digital-certificates-pki-regulations CPS for Non-Qualified Certs: http://www.helex.gr/documents/10180/681762/KP_NON-Q.pdf CP for Non-Qualified Certs: http://www.helex.gr/documents/10180/681762/CP_NON-Q.pdf CPS for Qualified Certs: http://www.helex.gr/documents/10180/681762/KP_Q.pdf CP for Qualified Certs: http://www.helex.gr/documents/10180/681762/CP_Q.pdf
Audits	Audit Type: WebTrust for CA Auditor: Ernst & Young (Panagiotis.Papagiannakopoulos@gr.ey.com) URL to Audit Report: https://bug967387.bugzilla.mozilla.org/attachment.cgi?id=8380545 (2013.07.31) Kathleen: Need to confirm authenticity of audit statement.
Baseline Requirements (SSL)	Comment #4: At the time that audit report issued we haven't decide to issue ssl certificates, that's why the report does not include the verification of compliance with the CA/Browser Forum Baseline Requirements. Now we have decide to issue ssl certificates and is going to be mention in this year audit report (June 2014). Is this going to be a problem? Please advice us accordingly. If the SSL trust bit is being requested, then we cannot proceed with the inclusion process until I receive an audit statement that SSL certificate issuance is in compliance with the CA/Browser Forum's Baseline Requirements. Need the document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.
SSL Verification Procedures	Comment #4: During the registration process the subscriber must present the verification of the legal identity together with an affidavit of ownership of the domain name. This procedure is described in the certification policy for non-qualified certificates. The link http://www.helex.gr/documents/10180/681762/KP_NON-Q.pdf paragraph 3. Comment #4: The procedures for verifying that the domain name referenced in a server certificate (SSL/TLS) is owned/controlled by the subscriber. A description of this process will be added to the new version of the Certificate Practice Statement. Please provide translations (into English) of section 3 of the CPS for Non-Qualified Certs.
Organization Verification Procedures	Please provide translations (into English) of the sections of the CPS/CP that address organization verification procedures for SSL and Code Signing certificates.
Email Address Verification Procedures	Comment #4: The current practice of HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A is that the email address is verified by send email to the email address declared by the customer. This is in accordance with the certification policies. The subscriber's identity is verified against valid legal documents (valid ID card, passport, etc.), which are specified in the particular certification policy. **The link is http://www.helex.gr/documents/10180/681762/KP_Q.pdf paragraph 3.** In the Regulations tab under the Digital Certificates section of our site http://www.helex.gr/web/guest/digital-certificates-pki-regulations is the application form with title "Application-contract Subscriber for the procurement and use of personal electronic signature certificates" under the link: http://www.helex.gr/documents/10180/681762/Smart-Sign+v1.0+- +%CE%A3%CF%85%CE%BD%CE%B4%CF%81%CE%BF%CE%BC%CE%B7%CF%84%CE%B9%CE%BA%CE%AE%20%CE%

	A3%CF%8D%CE%BC%CE%B2%CE%B1%CF%83%CE%B7.pdf/520a67b4-a4ec-4b6b-8edc-50a035ebc4da With this form our costumers apply for issuing the certificates. According to Greek law should determine the personal identity of the person concerned after completing the form and send it to our offices. Following the discovery of her identity certificate is issued. The regulation is in Greek language as we are official member of EU. We are in process to translate it in English.
Code Signing Subscriber Verification Procedures	Please provide translations (into English) of the sections of the CPS/CP that describe verification procedures Code Signing certificates.
Multi-factor Authentication	Please provide translations (into English) of the sections of the CPS/CP that describe multi-factor authentication for anyone who can directly cause the issuance of a certificate. Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.
CA Hierarchy	See above.
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	Comment #4: We don't allow the use of internationalized domain names (IDNs).
Revocation of Compromised Certificates	Comment #4: Revocation of compromised certificates or certificates for which verification of subscriber information is known to be invalid is incorporated into HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. common practices (this issue is addressed in CP and CPS). **The link is http://www.helex.gr/documents/10180/681762/KP_Q.pdf paragraph 5.2.** Please provide translation (into English) of that section of the CPS.
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	Comment #4: Server certificates that are issued by ATHEX General Certificates CA contain primary DNS name in the Subject Common Name field of certificate. **Needs to be updated to become compliant with the Baseline Requirement #9.2.1 and #9.2.2.**
Domain owned by a Natural Person	Comment #4: If the domain is owned by a natural person, the server certificate issued by ATHEX General Certificates CA will have the following fields: · CN = DNS · OU= identifier of a natural person (internal identification code).
OCSP	See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	Comment #4: No long-lived DV certificates exist, HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A only issues OV server certificates (SSL/TLS).
Wildcard DV SSL certificates	Comment #4: HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A only issues OV server certificates. The legal identity of the subscriber is always verified prior to issuing the certificate. The link http://www.helex.gr/documents/10180/681762/KP_NON-Q.pdf paragraph 3.
Email Address Prefixes for DV Certs	Comment #4: HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A does not issue domain validating (DV) server certificates (SSL/TLS) that would use an email address to verify the domain ownership.
Delegation of Domain / Email validation to third parties	Comment #4: HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A does not delegate the validation of the subscriber's identity or domain/email ownership to third parties. In the Regulations tab under the Digital Certificates section of our site http://www.helex.gr/web/guest/digital-certificates-pki-regulations is the application form with title "Application-contract Subscriber for the procurement and use of personal electronic signature certificates" under the link: http://www.helex.gr/documents/10180/681762/Smart-Sign+v1.0+-+%CE%A3%CF%85%CE%BD%CE%B4%CF%81%CE%BF%CE%BC%CE%B7%CF%84%CE%B9%CE%BA%CE%AE%20%CE%A3%CF%8D%CE%BC%CE%B2%CE%B1%CF%83%CE%B7.pdf/520a67b4-a4ec-4b6b-8edc-50a035ebc4da With this form our costumers apply for issuing the certificates. According to Greek law should determine the personal identity of the person concerned after completing the form and send it to our offices. Following the discovery of her identity certificate is issued.
Issuing end entity certificates directly from roots	Comment #4: The root certification authority ATHEX Root CA only issues certificates to its subordinate certification authorities ATHEX General Certificates CA and ATHEX Qualified Certificates CA. The end entity certificates are issued only by these subordinate certification authorities.
Allowing external entities to operate subordinate CAs	No. See above.
Distributing generated private keys in PKCS#12 files	No.
Certificates referencing hostnames or private IP addresses	Comment #4: HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A currently issue server certificates that contain public DNS or private IP addresses.
Issuing SSL Certificates for Internal Domains	Comment #4: HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A currently not issue SSL Certificates for internal domains.
OCSP Responses signed by a	See above.

certificate under a different root	
CRL with critical CIDP Extension	Comment #4: “CRL Issuing Distribution Point” (CIDP) extensions in the CRLs are not flagged as critical. The link http://www.helex.gr/documents/10180/681762/KP_NON-Q.pdf paragraph 5.2.3 and the link http://www.helex.gr/documents/10180/681762/KP_Q.pdf paragraph 5.2.3
Generic names for CAs	CN in root and subCA certs include ATHEX
Lack of Communication With End Users	Comment #4: Subscribers and relying parties can contact HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. via: Hellenic Exchanges S.A. Digital Certificates Services (PKI-CA) 110, Athinon Ave. GR104 42 Athens GREECE +30 210 336 6300 +30 210 336 6301 PKICA-Services@helex.gr The link is: http://www.helex.gr/web/guest/digital-certificates-contact-info
Backdating the notBefore date	Comment #4: The validity range of the certificate and crl’s issued set by our CA. Our CA has accurate time and we can certify that the time of the issuing is correct.