**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 | Indicate whether the CA is operated by a private or public corporation, government agency, international organization, academic institution or consortium, NGO, etc. Note that in some cases the CA may be of a hybrid type, e.g., a corporation established by the government. For government CAs, the type of government should be noted, e.g., national, regional/state/provincial, or municipal. |
| 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.<br>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<br>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<br>Faidon Tsikliropoulos, Head of PKICA Services F.Tsikliropoulos@helex.gr, +30 210 3366283<br>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<br>O = Athens Exchange S.A.<br>C = GR |
| Certificate Summary | |
| 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) | No OCSP URI in the AIA of the end-entity or intermediate certs.<br><br>OCSP URI in the AIA of end-entity certs<br>Maximum expiration time of OCSP responses<br>Testing results<br>a) Browsing to test website with OCSP enforced in Firefox browser<br>b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version<br><br>BR #13.2.2: "The CA SHALL update information provided via an Online Certificate Status Protocol..."<br>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" |
| Requested Trust Bits | Websites (SSL/TLS)<br>Email (S/MIME)<br>Code Signing<br><br>Why do you need the websites trust bit set? What types of domains to you expect to issue SSL certificate for? Will there be more domains than *.helex.gr? |
| SSL Validation Type | DV |
| EV Policy OID(s) | Are you requesting EV-treatment for this CA hierarchy? |
| Non-sequential serial numbers and entropy in cert | http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html<br>"9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ...<br>- all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."<br><br>The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration.<br>This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn't an acceptable hash algorithm for certificates in this hierarchy. |

**CA Hierarchy information for each root certificate**

| | |
|---|---|
| CA Hierarchy | List, description, and/or diagram of all intermediate CAs signed by this root.<br>Identify which subCAs are internally-operated and which are externally operated. |
| Externally Operated SubCAs | If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist<br>If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors. |
| Cross-Signing | List all other root certificates for which this root certificate has issued cross-signing certificates.<br>List all other root certificates that have issued cross-signing certificates for this root certificate.<br>If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not. |
| Technical Constraints on Third-party Issuers | Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate |

**Verification Policies and Practices**

| | |
|---|---|
| Policy Documentation | Language(s) that the documents are in:<br>CP:<br>CPS:<br>Relying Party Agreement:<br><br>Mozilla policy requires that policy documentation be publicly available on the CA's website. Please provide links to the document repository with this information. |
| Audits | Audit Type:<br>Auditor: Ernst & Young (Panagiotis.Papagiannakopoulos@gr.ey.com)<br>URL to Audit Report and Management's Assertions:<br><br>If the audit statement is available on your website or the webtrust website, please provide the link. Otherwise, please attach the audit statement to the bug. |
| Baseline Requirements (SSL) | 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.<br><br>Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results. |
| SSL Verification Procedures | If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices |
| Organization Verification Procedures | |
| Email Address Verification | If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available |

| | |
|---|---|
| Procedures | documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices |
| Code Signing Subscriber Verification Procedures | If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices |
| Multi-factor Authentication | 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 | |
| CA Hierarchy | |
| Audit Criteria | |
| Document Handling of IDNs in CP/CPS | |
| Revocation of Compromised Certificates | |
| Verifying Domain Name Ownership | |
| Verifying Email Address Control | |
| Verifying Identity of Code Signing Certificate Subscriber | |
| DNS names go in SAN | |
| Domain owned by a Natural Person | |
| OCSP | |

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

| | |
|---|---|
| Long-lived DV certificates | |
| Wildcard DV SSL certificates | |
| Email Address Prefixes for DV Certs | If DV SSL certs, then list the acceptable email addresses that are used for verification. |
| Delegation of Domain / Email validation to third parties | |
| Issuing end entity certificates directly from roots | |
| Allowing external entities to operate subordinate CAs | |
| Distributing generated private keys in PKCS#12 files | |
| Certificates referencing hostnames or private IP addresses | |
| Issuing SSL Certificates for Internal Domains | |

| | |
|---|---|
| OCSP Responses signed by a certificate under a different root | |
| CRL with critical CIDP Extension | |
| Generic names for CAs | |
| Lack of Communication With End Users | |
| Backdating the notBefore date | |