**General information about the ATHEX Root CA G2**

1. **Name:**

**ATHEX Root CA G2**

2. **Website URL:**

[**http://www.athexgroup.gr**](http://www.athexgroup.gr)

3. **Organizational type:**

**The CA is operated by a private corporation (ATHENS STOCK EXCHANGE – ATHEX)**

4. **Primary market / customer base:**

 Which types of customers does the CA serve:

The inclusion of these certificate authorities will enable Mozilla’s consumers to authenticate to ATHEX products and services.

 Are there particular vertical market segments in which it operates:

 Financial services

 Does it focus its activities on a particular country or other geographical region:

**No, the CA is global, and has already been included in the European List of Trusted Lists (LOTL) (**[**https://webgate.ec.europa.eu/tl-browser/#/tl/EL**](https://webgate.ec.europa.eu/tl-browser/#/tl/EL) **).**

5. **Impact to Mozilla users:**

**Any user or individual who is using any of ATHEX secured web based services.**

**Athens Stock Exchange is a major player in Greece's financial sector, providing a full range of certificates for use by individuals and companies.**

**Our Digital signing, Web SSL certificates are already used in governmental and private sector companies. Timestamping services, are provided as well. Also E-Seal services will be provided soon (during next couple of months). The need of listing our Root CA is essential for a hassle free user experience in the involved services and activities.**

**CA Contact Information:**

|  |  |  |
| --- | --- | --- |
| **Athens Stock Exchange S.A.****Post Code : 10442****Athens Greece**  | **John Balafas****J.Balafas@ATHEXgroup.gr****(+30) 2103366155** | **Stamatis Vamvakeris****S.Vamvakeris@ATHEXgroup.gr****(+30) 2103366280** |

**Technical information about the ATHEXGroup Root CA certificate**

1. **Certificate Name:**

**ATHEX Root CA G2**

1. **Certificate Issuer Field**

**CN = ATHEX Root CA G2**

**O = ATHENS STOCK EXHANGE**

**C = GR**

1. **Certificate Summary**

A summary about this root certificate, it's purpose, and the types of certificates that are issued under it.

**Athens Stock Exchange (ATHEX) has established a system of "public key Infrastructure" (PKI Public Key Infrastructure) in order to work as "volunteer accredited" certification-service-provider (provider Certification Authority CA) in accordance with the Presidential Decree 150/2001. According to the regulations of (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 Athens Exchange has filed a compliance report (Conformity Assessment Report) please see** [**http://www.ATHEXgroup.gr/documents/10180/681762/ATHEX+-+Conformity+Assessment+Report+-+Webauth\_vFINAL.pdf/de20f234-fff0-4325-898f-b2e8bf48ebe5**](http://www.athexgroup.gr/documents/10180/681762/ATHEX%2B-%2BConformity%2BAssessment%2BReport%2B-%2BWebauth_vFINAL.pdf/de20f234-fff0-4325-898f-b2e8bf48ebe5) **for each type of certificate provided and is already registered in the European Trusted List service providers, please see,** [**https://webgate.ec.europa.eu/tl-browser/#/tl/EL**](https://webgate.ec.europa.eu/tl-browser/#/tl/EL) **concurrently registered at the Registered Certification-Service Providers established in Greece, please see** [**https://www.eett.gr/tsl/EL-TSL.xml**](https://www.eett.gr/tsl/EL-TSL.xml)**.**

**The official establishment of the PKI infrastructure of ATHEX, through the creation and storage of cryptographic keys of certification authorities of the Athens Stock Exchange (ATHEX) (both the Root CA and the five Subordinate CAs), was held under special "ceremony to create cryptographic keys (Key Generation Ceremony"), in the presence of specialized Auditors Ernst & Young. The ceremony took place in a secure physical environment, it was shot and held under the project (script) in which ATHEX described in great detail all the necessary steps, from the initial installation of the operating system, installing the PKI applications, creating and saving of encrypted keys to secure signature-creation device FIPS 140-2 Level 2, placing copies of cryptographic keys in safe Bank box. The compliance audit successfully carried out by Ernst & Young, was in accordance with the requirements of the AICPA/CICA WebTrust template Program for Certification Authorities, the relevant requirements of Microsoft Corporation for the recognition of certification service providers, as well as instructions of the group "Internet Engineering Task Force-IETF (RFC 2527-PKIX framework).**

**The Athens Stock Exchange (ATHEX) as a Certification Service Provider (CSP) was evaluated, up to a certain time, by standard WebTrust for Certification Authorities and currently by EIDAS according to ETSI standards.**

**The Athens Stock Exchange (ATHEX) is registered in the registers kept by the EETT, EETT according to Regulation 248/71/2002, as "electronic signature Certification service provider issuing qualified certificates" and as "electronic signature Certification service provider" (under REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014).**

**The main objective of the Athens Stock Exchange (ATHEX), via PKI/CA infrastructure that has been developed and the relevant know-how acquired, is providing:**

* **WebSites (SSL/TLS) for web site authentication that chain to a HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE (ATHEX) Trusted Root. Facilitating secure communication by providing limited authentication of a Subscriber's server and permitting SSL encrypted transactions between a Relying Party's browser and the Subscriber's server.**
* **Digital certificate services (Certification Authority-CA services) to authorized users of applications (e.g. B2b/B2c applications users group, etc.) by using "smart cards" and “usb token”.**
* **Remote Document Signing to integrate services with applications (application integration services).**
* **Time-stamps use electronic signatures, incorporating the time from an accurate source, to confirm WHAT happened WHEN. Individual signatures may be used independently – or together with time-stamps – to increase the trustworthiness of electronic records and transactions.**

**In addition, the necessary consulting services are also supplied for the integration of the above services (PKI/CA) with e-business applications (e-business applications) and the best possible strengthening of our security mechanisms (authentication, authorization, data confidentiality, data integrity, non-repudiation).**

1. **Root Certificate URL**
	* **http://www.athexgroup.gr/digital-certificates-repository**
2. **SHA1 fingerprint**

**89 2A 1B D4 C8 B0 F8 AA 9A 65 ED 4C B9 D3 BF 48 40 B3 4B C1**

1. **Valid from (YYYY-MM-DD)**

**Tuesday, March 15, 2016 13:14:32 GMT +2**

1. **Valid to (YYYY-MM-DD)**

**Saturday, March 15, 2036 12:00:00 GMT +2**

1. **Certificate Version (should be 3)**

**V3**

1. **Certificate Signature Algorithm**

**Sha384RSA**

1. **Signing key parameters**

**2048 bits**

1. **Test website URL -- if you are requesting to enable the Websites (SSL/TLS) trust bit**
	* + **https://certdemo-valid.athexgroup.gr/**
2. **Example certificates**
	* If this root does not issue certificates for SSL, then provide example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s).

**Athens Stock Exchange issues certificates for SSL.**

1. **Certificate Revocation Lists (CRLs)**
	* URL(s) at which the CRL(s) may be obtained -- for end-entity certs and for intermediate CAs.

**http://www.athexgroup.gr/digital-certificates-repository http://www.athexgroup.gr/pki/-/file/ATHEXSSLCAG2.crl**

* + The value that nextUpdate is set to in the CRLs for end-entity certificates.

**For end-entity certificates under the issuing sub CA, nextUpdate is 7 days.**

* + The sections of your CP/CPS documentation that state the requirements about frequency of updating CRL.

**For Certificate Revocation List (CRL) Frequency of updating, please check :** [**http://www.athexgroup.gr/documents/10180/681762/WebAuthCP-CPS\_EN.pdf/a0c9ce95-d8cf-4533-bf3d-1f433d44760e**](http://www.athexgroup.gr/documents/10180/681762/WebAuthCP-CPS_EN.pdf/a0c9ce95-d8cf-4533-bf3d-1f433d44760e)

**Certification Practice Statement, Chapter 4.9.7,.**

Note the [CA/Browser Forum's EV guidelines:](http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf) CRLs MUST be updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days.

1. **OCSP (OCSP is required for the SSL trust bit enabled)**
* The OCSP URI that is in the AIA of your subscriber certificates.

**http://ocsp.athexgroup.gr/ATHEXSSLCAG2**

* The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation.

**ATHENS STOCK EXCHANGE (ATHEX) posts the CRL online daily and immediately after revocation of a Certificate.**

* The sections of your CP/CPS specifying availability and update requirements for the OCSP service.

**Please check :** [**http://www.ATHEXgroup.gr/documents/10180/681762/WebAuthCP-CPS\_EN.pdf/a0c9ce95-d8cf-4533-bf3d-1f433d44760e**](http://www.athexgroup.gr/documents/10180/681762/WebAuthCP-CPS_EN.pdf/a0c9ce95-d8cf-4533-bf3d-1f433d44760e) **Certification Practice Statement, Chapter 4.9.9 and 4.9.10.**

* + [CA/Browser Forum's EV Guidelines](https://cabforum.org/extended-validation/) Section 26(b): “If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.”
* You must test that your OCSP service is compatible with the Firefox browser.
	+ See: <https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#OCSP>

**Yes, OCSP Service is compatible with Firefox Browser but as it is expected “Error code: SEC\_ERROR\_UNKNOWN\_ISSUER” appears because of the not so far, inclusion of the *ATHEX Root CA G2* certificate in the Mozilla Root Certificate Program.**

* OCSP responders should be set up to listen on a standard port (e.g. port 80), because firewalls may block ports other than 80/443.
1. **Test!!!**
* If requesting to enable the Websites (SSL/TLS) trust bit, then you must perform all of the following tests
	+ Revocation: Browse to <https://certificate.revocationcheck.com/> and enter the Test Website URL. Make sure there are no errors listed in the output.
		- If certificate.revocationcheck.com does not know about the root cert, then use the 'Certificate Upload' tab to directly input the PEM for the certificates.
	+ The CA MUST check that they are not issuing certificates that violate any of the [CA/Browser Forum Baseline Requirements](https://cabforum.org/baseline-requirements-documents/) (BRs).
	+ Mozilla WILL check that the CA is not issuing certificates that violate any of the BRs by performing the following tests.
		- Browse to <https://crt.sh/>
		- Enter the SHA-1 or SHA-256 Fingerprint for the root certificate. Then click on the 'Search' button.
		- When the certificate information is shown, along the left column under Certificate, click on the "Run cablint" and "Run x509lint" links. Each of these will add a row to the table, showing the test results.
		- All errors must be resolved/fixed. Warnings should also be either resolved or explained.
	+ Alternatively, you may use the test code directly via Github:
		- BR Lint Test: <https://github.com/awslabs/certlint>
		- X.509 Lint Test: <https://github.com/kroeckx/x509lint>
		- All errors must be resolved/fixed. Warnings should also be either resolved or explained.
	+ [Test Errors](https://wiki.mozilla.org/CA%3ATestErrors) - Meaning and recommended solutions to errors that CAs have run into while doing the tests listed above.

If you are requesting to enable EV treatment, then you must also perform the [PSM EV Testing](https://wiki.mozilla.org/PSM%3AEV_Testing_Easy_Version)

* + You must provide successful output from the [EV Checking Tool](https://tls-observatory.services.mozilla.com/static/ev-checker.html).

	
1. **Requested Trust Bits**
	* State which of the three trust bits you are requesting to be enabled for this root. One or more of:
* Websites (SSL/TLS)
* Email (S/MIME)

Request Athens Stock Exchange requests the following trust bits :

* + - **Websites (SSL/TLS)**
		- **Server Authentication**
		- **Client Authentication**
		- **Secure E-mail**
		- **Timestamping**
		- **Document Signing**
	+ Mozilla’s standpoint is that we should operate the root program in terms of minimizing risk. One way that we can minimize risk is by not enabling more trust bits than CAs absolutely require.

1. **SSL Validation Type**
	* Indicate the levels of SSL validation that are used for certificates within this root's hierarchy. One or more of:
		+ OV -- In addition to verifying the domain ownership, you also validate the organization to be listed in the O field - making sure public record and government resources can verify the address, existence, and good legal standing of the organization itself. Verifying that the whois listed address matches the verified address, and any other additional checks that a given CA lists in its CPS.

**OV/EV**

1. **If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.**

**EV Policy OID :1.3.6.1.4.1.29402.1.1.5.1.1.0**

**CA hierarchy information for the ATHEXgroup Root CA certificate**

1. CA Hierarchy
	* A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate.
		+ List and/or describe all of the subordinate CAs that are signed by this root.
		+ Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.

It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do *not* require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements.

**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**

1. Sub CAs Operated by 3rd Parties
	* If this root has any subordinate CAs that are operated by external third parties, then provide the information listed in the [Subordinate CA Checklist](https://wiki.mozilla.org/CA%3ASubordinateCA_checklist)
	* 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.

**N/A. ATHEX Stock Exchange (ATHEX) does not permit sub CAs operated by 3rd parties.**

1. Cross-Signing
	* List all other roots for which this root CA has issued cross-signing certificates.
	* List all other root CAs that have issued cross-signing certificates for this root CA.
	* If any such roots exist, it is important to note whether the roots in question are already included in the Mozilla root store or not.

**N/A. ATHEX Stock Exchange (ATHEX) does not permit cross signing Certificate Authorities.**