HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A.

In order to participate in the Mozilla CA Root Certification Program we send you all the necessary information about the requirements of the program.

Organizational type:

HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. which is operating the CA is a private company.

Requested Trust Bits:

We issue ssl certificates for our web sites accessible from our clients register companies etc. These web sites have different domain names than *helex.gr for example https://www.inbroker.com/IBH/default/content/home/index.asp or https://www.axiaweb.gr

EV Policy OID(s):

We request EV-treatment for our CA hierarchy.

Non-sequential serial numbers and entropy in cert:

HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. is going 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.

CA Hierarchy:

The ATHEX Root CA signed two sub ca's the list is above:

CN=***ATHEX Root CA*** O=**Athens Exchange S.A.** C=***GR***
Thumbprint (SHA-1) = ***DB 2B 7B 43 4D FB 7F C1 CB 59 26 EC 5D 95 21 FE 35 0F F2 79***

CN= ***ATHEX General Certificates CA*** O= **Athens Exchange S.A.** C=***GR***
Thumbprint (SHA-1)= ***9C 72 BB 4D 9C 02 D7 1E 2E 98 F4 3F E2 90 C2 77 4A 87 53 1B***
issuing non-qualified certificates to the end users.

CN=***ATHEX Qualified Certificates CA*** O= **Athens Exchange S.A.** C=***GR***
Thumbprint (SHA-1)= ***04 A2 83 8B 61 7A 31 78 FF A4 4A DA 7C A2 73 43 34 F7 3F 31***
issuing qualified certificates to the end users.

Link to the certificates: http://www.helex.gr/documents/10180/681760/Certificates.zip

Externally Operated SubCAs:

We don't have any.

Cross Signing:

We have not issue any Cross Signing certificates from our CA.

Technical Constraints on Third-Party Issuers:

HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. has not issue any CA or Sub Ca's for Third-Party Issuers and is not going to do it.

Policy Documentation:

HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A. CP/CPS/ Relying Party Agreement is in Greek under the link: http://www.helex.gr/web/guest/digital-certificates-pki-regulations

OCSP URL:

The verification of the validity of the end user or CA certificates via the OSCP protocol is not currently available..

Email Address Verification:

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

110, Athinon Ave., 104 42 Athens, Greece, tel +30-210 3366800 fax +30-210 3366610, www.helex.gr

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.

Revocation of Compromised Certificates:

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.

Verifying Domain Name Ownership:

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.

DNS names go in SAN:

Server certificates that are issued by ATHEX General Certificates CA contain primary DNS name in the Subject Common Name field of certificate.

Domain owned by a Natural Person:

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).

Long-lived DV certificates:

No long-lived DV certificates exist, HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A only issues OV server certificates (SSL/TLS).

Document Handling of IDNs in CP/CPS:

We don’t allow the use of internationalized domain names (IDNs).

110, Athinon Ave., 104 42 Athens, Greece, tel +30-210 3366800 fax +30-210 3366610, www.helex.gr

Baseline Requirements (SSL):

At the time that audit report issued we haven't decide to issue ssl certificates, that's way the report does not include the verification of compliance with the CA/Browser Forum Baseline Requirements. Now he 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.

SSL Verification Procedures:

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.

Email Trust Bit:

We request Email Trust Bit. The verification process is: 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

The regulation is in Greek language as we are official member of EU. We are in process to translate it in English.

Wildcard DV SSL certificates:

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.

110, Athinon Ave., 104 42 Athens, Greece, tel +30-210 3366800 fax +30-210 3366610, www.helex.gr

Email Address Prefixes for DV Certs:

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:

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:

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:

Both subordinate CAs ATHEX General Certificates CA and ATHEX Qualified Certificates CA. are operated by the same subject as the root CA ATHEX Root CA.

Distributing Generated Private Keys in PKCS#12 Files:

The subscribers generate their own key pairs.

110, Athinon Ave., 104 42 Athens, Greece, tel +30-210 3366800 fax +30-210 3366610, www.helex.gr

Certificates Referencing Hostnames or Private IP Addresses:

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:

HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A currently not issue SSL Certificates for internal domains.

OCSP Responses Signed by a Certificate under a Different Root:

The verification of the validity of the end user or CA certificates via the OSCP protocol is not currently available in HELLENIC EXCHANGES – ATHENS STOCK EXCHANGE S.A.

CRL with Critical CIDP Extension:

"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:

Generic names for CAs are not used.

CN=***ATHEX Root CA*** O=**Athens Exchange S.A.** C=***GR***
Thumbprint (SHA-1) = ***DB 2B 7B 43 4D FB 7F C1 CB 59 26 EC 5D 95 21 FE 35 0F F2 79***

CN= ***ATHEX General Certificates CA*** O= **Athens Exchange S.A.** C=***GR***
Thumbprint (SHA-1)= ***9C 72 BB 4D 9C 02 D7 1E 2E 98 F4 3F E2 90 C2 77 4A 87 53 1B***
issuing non-qualified certificates to the end users.

CN=***ATHEX Qualified Certificates CA*** O= **Athens Exchange S.A.** C=***GR***
Thumbprint (SHA-1)= ***04 A2 83 8B 61 7A 31 78 FF A4 4A DA 7C A2 73 43 34 F7 3F 31***
issuing qualified certificates to the end users.

Lack of Communication With End Users:

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:

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.

If you have any question or if you need any additional information please contact us.

110, Athinon Ave., 104 42 Athens, Greece, tel +30-210 3366800 fax +30-210 3366610, www.helex.gr