Bugzilla ID: 581901
Bugzilla Summary: Add HARICA root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	HARICA -- Hellenic Academic and Research Institutions Certification Authority / Greek Universities Network
Website URL	http://www.harica.gr/
Organizational type	HARICA is a non profit activity operated by the Greek Universities Network (www.gunet.gr).
Primary market / customer base	The main goal of HARICA is the deployment of an infrastructure for secure communication between the collaborating members of the Greek Academic and Research Institutions. HARICA's main web site, www.harica.gr , has been operating since 2006. All HARICA certificates have a clear mark indicating that "This certificate is subject to Greek laws and their CPS. This Certificate must only be used for academic, research or educational purposes". This is also included in the comments and policy fields of each certificate.
CA Contact Information	CA Email Alias: ca-admin@harica.gr CA Phone Number: +30-2310998483, +30-2310998438 Title/Department: AUTH Network Operations Center, Harica Administration

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	Hellenic Academic and Research Institutions RootCA 2006
Cert summary / comments	
Root Cert URL	http://www.harica.gr/certs/HaricaRootCA2006.der
SHA-1 fingerprint	EF:BE:64:58:33:41:8D:95:82:21:4F:35:00:C2:3B:A6:62:C6:25:77
Valid from	2006-07-25
Valid to	2026-07-20
Cert Version	3
Modulus length / key length	2048 -- MD5 With RSA Encryption; Need to switch to the next generation root before continuing with inclusion request.
Test Website	https://www.harica.gr/
CRL URL	ARL: http://crlv1.harica.gr/HaricaRootCA2006/crlv1.der.crl End-entity CRL: http://crlv1.harica.gr/HaricaAdministrationCAR2/crlv1.der.crl (Next Update 1 month) NextUpdate for end-entity certs should be less than 10 days.

OCSP Responder URL	http://ocsp.harica.gr When I enforce OCSP in my Firefox browser and browse to the test website, https://www.harica.gr/, I get the error sec_error_ocsp_invalid_signing_cert. Please see https://wiki.mozilla.org/CA:Recommended_Practices#OCSP
CA Hierarchy	CA Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=460450 Currently there are 13 subordinate CAs operated internally by HARICA Administration: * HaricaAdministrationCAR2 * HaricaEKTCAR2 * HaricaTeiCreteCAR2 * HaricaTeiEpirusCAR2 * HaricaTeiKalamataCAR2 * HaricaTeiLamiaCAR2 * HaricaTeiLarissaCAR2 * HaricaTeiMessolonghiCAR2 * HaricaTeiSerresCAR2 * HaricaUcgCAR2 * HaricaUocCAR2 * HaricaUopCAR2 * HaricaUthCAR2 All these CAs belong to different Academic or Research Institutions and are used to issue both user and server certificates.
Externally operated subCAs	The following CAs are operated by Aristotle University of Thessaloniki Network Operations Center: * AuthCentralCAR2 (only issues sub-CAs) * AuthNocCAR3 (issues user and server certificates for the Network Operations Center of the University) * AuthUsersCAR3 (issues user certificates for the rest of the University) * AuthServersCAR3 (issues server certificates for the rest of the University) Please see https://wiki.mozilla.org/CA:SubordinateCA_checklist and provide the corresponding information.
Cross-Signing	CPS section 1.1: The HARICA Certification Authority issues User Certificates, Network Device Certificates (e.g. Servers, routers etc.), and Subordinate Certification Authority Certificates and cross-certification certificates with other Root Certification Authorities. Please provide further information about which root certificates have been or will be cross-signed with this root.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) ? Code 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.

SSL Validation Type	OV
EV policy OID(s)	Not requesting EV
CP/CPS	Certificate Practices: http://www.harica.gr/procedures.php Certification Policy and Certification Practices Statement (English): http://www.harica.gr/documents/CPS-en.php
AUDIT	Please see sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/ We need a publishable statement or letter from an auditor (who meets the policy requirements) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of: • ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities
Organization Identity Verification	CPS section 3.2.2: The Registration Authority should confirm that the subscriber belongs to the Institution, the name of which is included in the certificate. The subscriber should: a) be registered in the official directory service of her/his Institution and her/his Institution must appear in this record, or b) possess an electronic mail address in the official mail service of the Institution and the administration of her/his Institution confirms its relation with the subscriber. CPS section 3.2.3.1: The Registration Authority relies on the control of identity performed by the institutions the subscriber belongs to and uses authentication ways of user identities that are available in the institutions in order to check the identity. The collaborating institutions are compelled to have certified the identity of a user by means of an official document that bears the photograph of the beneficiary (eg police identity, passport, driving license, student identity) and which is considered reliable by the familiar institution. Alternatively, the RA of HARICA can execute the above process of applicant identification. In case the familiar institution of the user, according to its policy, has already performed a procedure of physical identity verification in the past (e.g. for the provision of a user account or e-mail address) there is no need to repeat the procedure but a typical confirmation through the officially certified e-mail address of the user is sufficient. CPS section 3.2.3.2: The individual who is in charge of the operation of the device and its conformity to the Certification Policy should be a subscriber of a certificate which was issued by a CA that is conformed to the “HARICA Certification Practice Statement/ Certification Policy”. The subscriber prepares and submits the application for a certificate issuance where she/he must be authenticated presenting the personal certificate. The issuance of a certificate for a device owned by an institution different from the institution of its administrator is not allowed. CPS section 3.2.5: The Registration Authorities determine procedures according to which the subscriber’s status and his conventional relationship with the institution is being verified. This is possible either with electronic lists that assembles each RA from the qualified - for each category- sources (e.g. secretariats of departments /faculties, management of

	institution administration computerization etc.), or bringing verified written certifications where the relation of the subscriber with the institution is documented.
Domain Name Ownership / Control	Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership We rely on publicly available documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please provide the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber.
Email Address Ownership / Control	If email trust bit is to be enabled… Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control We rely on publicly available documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; Please provide the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber.
Identity of Code Signing Subscriber	If code signing trust bit is to be enabled… We rely on publicly available documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Please provide the sections of the CP/CPS documents that describe the identity verification procedures for code signing certs.

Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and pointers to the relevant secitons of the CP/CPS. • Long-lived DV certificates ○ • Wildcard DV SSL certificates ○ • Email Address Prefixes for DV SSL Certs ○ • Delegation of Domain / Email validation to third parties ○ • Issuing end entity certificates directly from roots ○ • Allowing external entities to operate unconstrained 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 ○