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 2010
Cert summary / comments	
Root Cert URL	New Root: http://www.harica.gr/certs/HaricaRootCA2010.der Old (MD5 Root): http://www.harica.gr/certs/HaricaRootCA2006.der
SHA-1 fingerprint	EF:FE:69:56:A4:00:13:09:52:79:6F:14:E7:08:59:24:0E:11:1F:48
Valid from	2010-09-19
Valid to	2030-09-14
Cert Version	3
Modulus length / key length	2048
Test Website	Please provide a url to a test website whose SSL cert chains up to the new root.
CRL URL	The new root will eventually have the same CRL support as the old MD5 root. The info here is for the MD5 root. ARL: http://crlv1.harica.gr/HaricaRootCA2006/crlv1.der.crl End-entity CRL: http://crlv1.harica.gr/HaricaAdministrationCAR2/crlv1.der.crl CPS section 4.9.7: NextUpdate for end-entity certs is 5 days.

OCSP Responder URL	The new root will eventually have the same OCSP support as the old MD5 root. The info here is for the MD5 root. http://ocsp.harica.gr
CA Hierarchy	CA Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=460450 The new root will eventually have the same hierarchy and sub-CAs as the old MD5 root, as described here. As shown in the diagram, the MD5 root has 13 subordinate CAs operated internally by HARICA Administration. Each of these subCAs is used for a different Academic or Research Institution and issue both user and server certificates.
Externally operated subCAs	Comment #4: According to https://wiki.mozilla.org/CA:SubordinateCA_checklist, here is the requested information: 1. Company Name: Aristotle University of Thessaloniki Network Operations Center 2. Corporate URL: http://noc.auth.gr 3. Certificate download URL: http://www.pki.auth.gr/certs/AuthCentralCAR2.pem 4. General CA hierarchy: * 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) 5. CP/CPS Link: http://www.pki.auth.gr/documents/CPS.php 6. Sections in CP/CPS demonstrating the measures to verify: * Ownership of domain name: 3.2.3.2 and 3.2.5 * Ownership of e-mail: 3.2.3.1 and 3.2.5 CP/CPS of the subCA also needs to have more information (see below) 7. For all certificates chaining up to this Sub-CA, both the organization and the ownership/control of the domain are verified. 8. No potentially problematic practices were found. 9. This CA is operated by the same administration team as the HARICA Root CA and a common audit will take place at Q1 2011. 10. Section 4.9.7 states that if a secret key is revealed to a third party then a new CRL is issued immediately. Regular updates will take place every 5 days (will be changed at the next CP/CPS update). 11. An OCSP responder operates and can be tested by connecting to the site https://ocsp.pki.auth.gr.
Cross-Signing	None. Comment #4: Cross-certification will be removed from the CP/CPS.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV
EV policy OID(s)	Not requesting EV
CP/CPS	The next version of the CP/CPS will incorporate the changes as listed in this document. Certificate Practices: http://www.harica.gr/procedures.php Certification Policy and Certification Practices Statement (English): http://www.harica.gr/documents/CPS-en.php

AUDIT	Comment #4: The audit will take place in Q1, 2011, and will include both the MD5 root and this new root. 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	Comment #4: Issuance of an SSL/TLS certificate is only allowed for a limited number of domains, the ones belonging to an institution. In order for a user to apply for an SSL/TLS certificate he must own a user certificate which proves his identity. Then an email is sent to the institution's network operations center pki administrator that requires his approval based on the fqdn in the certificate, the user that submitted the request and the institution's database of users / servers. The whole procedure is described at paragraphs 3.2.3.2 and 3.2.5. Since the CP/CPS is aimed at users with no technical background on protocols such as LDAP and mostly contains legal issues regarding the issuance and use of certificates, we haven't included any technical characteristics. However, we can include all this challenge-response information at the next version of our CP/CPS
Email Address Ownership / Control	Comment #4: HARICA users two methods for e-mail ownership and control verification: The first method uses simple e-mail verification. The user enters the e-mail address at the initial certificate request form and a verification e-mail is sent to the user with a link to a unique web page. After following this link, an e-mail is sent to the institution's network operation center mail administrator that requires an approval based on the full name entered by the user and the user's email. This approval requires the identification of the user with his/her physical presence and an acceptable official document. If this procedure took place before (e.g. for the creation of an e-mail account) then there is no reason to be repeated. The second method uses an LDAP server. The user enters the personal e-mail address at the initial certificate request form and the corresponding password. This information is verified against the institution's LDAP server. If the verification is successful, the RA queries the real name of the user and creates the certificate request. In order for a user to be listed in the Institutional Directory server, the institution must have verified the user with his/her physical presence and an acceptable official photo-id document. The whole procedure is described at paragraphs 3.2.3.1 and 3.2.5. Since the CP/CPS is aimed at users with no technical background on protocols such as LDAP and mostly contains legal issues regarding the issuance and use of certificates, we haven't included any technical characteristics. However, we can include all this challenge-response information at the next version of our CP/CPS
Identity of Code Signing Subscriber	Comment #4: The same procedure as the e-mail ownership/control is used.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices)
	• Long-lived DV certificates
	  ○ SSL certs are OV. End-entity certs have a 2-year maximum validity period.
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV. Wildcard SSL certs are not allowed.
	• Email Address Prefixes for DV SSL Certs
	  ○ SSL certs are OV. In order to request an SSL certificate the user must already own an S/MIME one in order to be authenticated.
	• Delegation of Domain / Email validation to third parties

	○ Comment #5: The main RA and CA is run by the HARICA Administration Team. In case an institution -within the HARICA constituency- wants to run its own RA, it must provide an official audit according to the mozilla CA requirements. ○ Please make sure the CP/CPS includes information about the requirements of the RA to follow the CP/CPS and how those RAs are regularly monitored/audited. • Issuing end entity certificates directly from roots ○ No. The root only signs intermediate CAs. • Allowing external entities to operate unconstrained subordinate CAs ○ Please make sure the CP/CPS includes information about the requirements of the RA to follow the CP/CPS and how those RAs are regularly monitored/audited. • Distributing generated private keys in PKCS#12 files ○ Comment #5: The CP/CPS discoureges key-pair generation on behalf of users and strongly advises only end user to be able to generate private keys. Section 6.1.2 of our CP/CPS mentions that there might be cases for batch key generation under a very strict procedure. • Certificates referencing hostnames or private IP addresses ○ Comment #5: Host certificates are only allowed to have FQDNs. Hostnames or IP addresses are not allowed. This is described in section 3.1.1.2. Our next CP/CPS revision will specifically mention that hostsnames or private IP Addresses are not allowed. • Issuing SSL Certificates for Internal Domains ○ Comment #5: Use of internal domains is not allowed. Only internet domains belonging to HARICA academic institutions are allowed. • OCSP Responses signed by a certificate under a different root ○ Comment #5: The OCSP responses are signed by the certificate of the Harica Administration SubCA, which is in turn signed by the Harica Root CA. • CRL with critical CIDP Extension ○ Comment #5: CRLs don't have a critical CIDP extension • Generic names for CAs ○ The CN has the full name of the CA. • Lack of Communication With End Users ○ Comment #5: Harica Administration uses e-mail and telephone support for end-users. Telephone support works 8 hours/day, working days. Furthermore, specific institutions, such as the Aristotle University of Thessaloniki, provide helpdesk visiting facilities for end users and on-site support at faculty members offices/computers.