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 2011
Cert summary / comments	This root is the SHA1 version of the HARICA root. HARICA currently has an MD5 root that has several internally operated, and one externally operated, subordinate CAs, where each subCA is used for a different academic or research institution. Eventually all of the hierarchy under the MD5 root will be transitioned to this SHA1 root. There is one externally-operated subCA.
Root Cert URL	http://www.harica.gr/certs/HaricaRootCA2011.der (see Comment #31)
SHA-1 fingerprint	FE:45:65:9B:79:03:5B:98:A1:61:B5:51:2E:AC:DA:58:09:48:22:4D
Valid from	2011-12-06
Valid to	2031-12-01
Cert Version	3
Modulus length / key length	2048
Test Website	https://www2.harica.gr
CRL URL	http://crlv1.harica.gr/HaricaRootCA2011/crlv1.der.crl http://crlv1.harica.gr/HaricaAdministrationCAR3/crlv1.der.crl (NextUpdate: 5 days) CPS section 4.9.7: The CRL must be updated and published at least every five (5) days.
OCSP Responder URL	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	There is one externally-operated subCA: 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-EN.pdf 6. Sections in CP/CPS demonstrating the measures to verify: * Ownership of domain name: 3.2.2, 3.2.3.2 and 3.2.5 * Ownership of e-mail: 3.2.2, 3.2.3.1 and 3.2.5 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 noticed. 9. This CA is operated by the same administration team as the HARICA Root CA. 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. 12: Audit Statement: http://www.trust-it.gr/userfiles/AUTH.2011.03.18.Rev1.7.English.pdf
Cross-Signing	None.
Technical Constraints on Third-party issuers	Comment #22: HARICA has implemented technical restrictions (at the RA and CA level) allowing only specific domains affiliated with our constituency to be included in certificates. HARICA has implemented technical controls to restrict issuance to a specific set of domain names which have been confirmed. These controls check the dNSName, E-mail and the CN of the certificate requests. CPS section 7.1.5: Each subCA MUST be constrained to the Institution's domain name that the subCA signs for. For example, Aristotle University of Thessaloniki subCA will be limited to the "auth.gr" domain, using the name constraints extension.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
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.pdf
AUDIT	Audit Type: ETSI TS 101 456 Auditor: Deventum Auditor Website: http://deventum.com Audit Report: http://www.trust-it.gr/userfiles/Harica.2011.03.18.Rev1.2.ENG.pdf (2011. 03.18) Note that this audit report is posted on the Trust-IT website.
Organization Identity Verification	See CPS sections 3.2.2, 3.2.3, and 3.2.5. Also, see the audit report.

Domain Name Ownership / Control	CPS section 3.2.3.2: "HARICA central RA uses the following methods for device ownership verification. First of all, issuance of an SSL/TLS certificate is only allowed for domains belonging to each institution. Secondly, in order for a user to apply for an SSL/TLS device certificate he must own a user certificate which proves his identity. Then a verification e-mail is sent to an institution's network operations center designated administrator who verifies the validity of the FQDN of the certificate request. He also checks that the person who applied for the certificate is the rightful owner of the FQDN according to the institution's database of users / servers." CPS section 3.2.4: The certificates that are issued do not include non-verified subscriber information. Comment #22: Each server certificate is manually verified.
Email Address Ownership / Control	CPS section 3.2.3.1: HARICA central RA uses 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. Certificates of Class A are recommended to include an extra organizational unit (OU) in the subject field with the value 'Class A – Private Key created and stored in hardware CSP'. Certificates of Class B are recommended to include an extra organizational unit (OU) in the subject field with the value 'Class B – Private Key created and stored in software CSP'.
Identity of Code Signing Subscriber	See CPS sections 3.2.2 and 3.2.3.
Multi-factor Authentication	Comment #22: We confirm multi-factor authentication for server certificates, and multi-factor authentication to access the RA and CA engines.
Network Security	Comment #22: HARICA has recently (Apr 2011) passed a security audit at the same time as the ETSI TS 101 456 audit.

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.
	  ○ CPS section 9.16.3 requires that external RAs confirm the ownership of the email address and domain name to be included in the certificate, and that the RA be audited.

	• Issuing end entity certificates directly from roots
	  ○ No. The root only signs intermediate CAs.
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ CPS section 9.16.2 requires sub-CAs to have a CP/CPS that is at least as strict and binding as HARICA's CPS, and the subCA must be audited according to the ETSI TS 101 456 (or equivalent) requirements.
	• Distributing generated private keys in PKCS#12 files
	  ○ Comment #5: The CP/CPS discourages 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
	  ○ CPS section 3.1.1.2 states that IP addresses or hostnames are not allowed. Only FQDNs are 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.