Print this page

Mozilla - CA Program

Case Information

Case Number	00000069	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	HARICA	**Request Status**	Need Information from CA

Additional Case Information

Subject	Add HARICA SHA256 Root CA Certificates	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1201423

General information about CA's associated organization

CA Email Alias 1	ca-admin@harica.gr		
CA Email Alias 2			
Company Website	http://www.harica.gr/	**Verified?**	Verified
Organizational Type	Consortium	**Verified?**	Verified
Organizational Type (Others)	Non profit activity operated by the Greek Universities Network (www.gunet.gr).	**Verified?**	Verified
Geographic Focus	Greece Greek Academic and Research Institutions	**Verified?**	Verified
Primary Market / Customer Base	HARICA is a non-profit organization serving the Greek Academic and Research Community	**Verified?**	Verified
Impact to Mozilla Users	Root renewal	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* Document Handling of IDNs in CP/CPS: HARICA does not use IDNs in certificates * Revocation of Compromised Certificates: CPS section 4.9 * DNS names go in SAN: HARICA follows the BR section 9.2.2 and includes DNS names in SAN.	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially	https://wiki.mozilla.org	**Problematic**	I have reviewed Mozilla's list

Problematic Practices	/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Practices Statement**	of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* HARICA issues DV certificates valid for up to 36 months. CPS section 6.3.2 * HARICA does not currently issue Wildcard DV certificates and Wildcard OV certificates. * Email Address Prefixes for DV Certs: CPS section 3.2.3.2 * 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 as per Mozilla's Inclusion Policy. * HARICA does not issue end entity certificates directly from root CAs except for OCSP purposes (CPS section 1.3.1) * When HARICA issues subordinate CA certificates to external entities they are either technically constrained or publicly disclosed and audited as per Mozilla's Inclusion Policy. * 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. * CPS 3.1.1.2: “The certification of IP addresses or hostnames instead of the FQDNs is not allowed.” * HARICA does not issue certificates for internal domains. Only internet domains are allowed. * HARICA does not sign OCSP Responses using a certificate under a different root. * HARICA has clear names for CN and O fields in all subCAs, including the ROOTCA. * 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. * We have issued 24 SHA1 SSL certificates that are valid beyond January 1, 2017. We have already contacted the owners to replace them with new SHA256 and plan to revoke them by 31/8/2016.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Hellenic Academic and Research Institutions RootCA 2015	**Root Case No**	R00000096
Request Status	Need Information from CA	**Case Number**	00000069

Additional Root Case Information

Subject	Include Hellenic Academic and Research Institutions RootCA 2015

Technical Information about Root Certificate

O From Issuer Field	Hellenic Academic and Research Institutions Cert. Authority	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified

Certificate Summary	This SHA256 “Hellenic Academic and Research Institutions RootCA 2015” root certificate will eventually replace the SHA--1 “Hellenic Academic and Research Institutions RootCA 2011” root certificate that was included via Bugzilla Bug #581901.	**Verified?**	Verified
Root Certificate Download URL	http://www.harica.gr/certs /HaricaRootCA2015.der	**Verified?**	Verified
Valid From	2015 Jul 07	**Verified?**	Verified
Valid To	2040 Jun 30	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www2.harica.gr	**Verified?**	Verified
CRL URL(s)	http://crlv1.harica.gr/HaricaRootCA2015 /crlv1.der.crl http://crlv1.harica.gr /HaricaAdministrationCAR5/crlv1.der.crl CPS section 4.9.7: For end-user/device certificates ... the CRL will be in effect for a maximum time of ten (10) days.	**Verified?**	Verified
OCSP URL(s)	http://ocsp.harica.gr For Subscriber Certificates: OCSP responses have a maximum expiration time of two (2) days.	**Verified?**	Verified
Revocation Tested	https://certificate.revocationcheck.com /www2.harica.gr no errors	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not Requesting EV Treatment	**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla now has the ability to constrain root certificates to certain domains. Should this root be constrained to certain domains? If yes, which? e.g. *.gr, *.eu, *.edu, *.org	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	01:0C:06:95:A6:98:19:14:FF:BF:5F:C6:B0:B6:95:EA:29:E9:12:A6	**Verified?**	Verified
SHA-256 Fingerprint	A0:40:92:9A:02:CE:53:B4:AC:F4:F2:FF:C6:98:1C:E4:49:6F:75:5E:6D:45:FE:0B:2A:69:2B:CD:52:52:3F:36	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	“Hellenic Academic and Research Institutions RootCA 2011” currently has	**Verified?**	Verified

	20 internally operated and technically-constrained subCAs.		
Externally Operated SubCAs	There is currently one externally-operated subordinate CA: - Aristotle University of Thessaloniki - http://www.auth.gr, http://it.auth.gr - http://www.pki.auth.gr/certs/AuthCentralCAR3.pem, (to be decommissioned by Sep 2015) - http://www.pki.auth.gr/certs/AuthCentralCAR4.pem - http://www.pki.auth.gr/certs/AuthCentralCAR5.pem - AuthCentralCAR4 and AuthCentralCAR5 issue sub-CAs and end user/server certificates - http://www.pki.auth.gr/documents/CPS-EN.pdf - 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 - For all certificates chaining up to these Sub-CA, both the organization and the ownership/control of the domain are verified. - This CA is currently operated by the same administration team as the HARICA Root CA. - OCSP: http://ocsp.pki.auth.gr - Audit: http://pki.auth.gr/documents/AUTH-ETSI_CERTIFICATE_AUTH_W_ANNEX	**Verified?**	Verified
Cross Signing	This Root will be cross-signed by “Hellenic Academic and Research Institutions RootCA 2011” to assist the rollover.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	HARICA has implemented technical restrictions (at the RA and CA level) allowing only specific domains affiliated with their 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	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	All documents are in Greek and English.	**Verified?**	Verified
CA Document Repository	http://www.harica.gr/procedures	**Verified?**	Verified
CP Doc Language			
CP		**Verified?**	Not Applicable

CP Doc Language			
CPS	http://www.harica.gr/documents/CPS-EN.pdf	**Verified?**	Verified
Other Relevant Documents	Qualified Certificates (under GUnet): http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/EsignProviders.html	**Verified?**	Verified
Auditor Name	QMSCERT	**Verified?**	Verified
Auditor Website	http://www.qmscert.com	**Verified?**	Verified
Auditor Qualifications	http://www.esyd.gr/eped/1.179906_en.doc	**Verified?**	Verified
Standard Audit	https://www.harica.gr/documents/HARICA-ETSI_CERTIFICATE_AUTH_W_ANNEX.pdf	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	6/5/2015	**Verified?**	Verified
BR Audit	http://pki.auth.gr/documents/AUTH-ETSI_CERTIFICATE_AUTH_W_ANNEX.pdf	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	6/5/2015	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.5.4	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.3.2: For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certifiate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by: - Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar, - Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; - Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; - Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name.... CPS section 3.2.4: The certificates that are issued do not include non-verified subscriber information. Each server certificate is manually verified.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	HARICA MoU http://www.harica.gr/documents/MoU-EN.pdf. Only Institutions currently registered as Academic or Research Institutions and their affiliates in Greece are allowed to join HARICA CPS sections 3.2.2 and 3.2.3	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.3.1: HARICA central RA uses three methods for e-mail ownership and control verification: - The first method uses simple e-mail verification. The user	**Verified?**	Verified

	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. - 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 third method uses a Single Sign On (SSO) architecture based on the SAML specification. The user enters the personal e-mail address at the initial request form and is then redirected to the appropriate web page of the Identity Provider. The Identity Provider verifies the user and returns the real name and the email address..		
Code Signing Subscriber Verification Pro	CPS sections 3.2.2 and 3.2.3	**Verified?**	Verified
Multi-Factor Authentication	HARICA uses multi-factor authentication for the issuance of server certificates, and to access the RA and CA engines. CPS section 6.5.1.	**Verified?**	Verified
Network Security	HARICA has performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices CPS section 6.7.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.harica.gr/rep_dyn.php	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	Hellenic Academic and Research Institutions ECC RootCA 2015	**Root Case No**	R00000097
Request Status	Need Information from CA	**Case Number**	00000069

Additional Root Case Information

Subject	Include Hellenic Academic and Research Institutions ECC RootCA 2015

Technical Information about Root Certificate

O From Issuer Field	Hellenic Academic and Research Institutions Cert. Authority	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified

Certificate Summary	This “Hellenic Academic and Research Institutions ECC RootCA 2015” root certificate is the ECC version of the “Hellenic Academic and Research Institutions RootCA 2015”	**Verified?**	Verified
Root Certificate Download URL	http://www.harica.gr/certs /HaricaECCRootCA2015.der	**Verified?**	Verified
Valid From	2015 Jul 07	**Verified?**	Verified
Valid To	2040 Jun 30	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www3.harica.gr	**Verified?**	Verified
CRL URL(s)	http://crlv1.harica.gr /HaricaECCRootCA2015/crlv1.der.crl http://crlv1.harica.gr /HaricaECCAdministrationCAR1 /crlv1.der.crl CPS section 4.9.7: For end-user/device certificates ... the CRL will be in effect for a maximum time of ten (10) days.	**Verified?**	Verified
OCSP URL(s)	http://ocsp.harica.gr For Subscriber Certificates: OCSP responses have a maximum expiration time of two (2) days.	**Verified?**	Verified
Revocation Tested	NEED: Resolve errors https://certificate.revocationcheck.com /www3.harica.gr - OCSP response expired	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not Requesting EV Treatment	**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla now has the ability to constrain root certificates to certain domains. Should this root be constrained to certain domains? If yes, which? e.g. *.gr, *.eu, *.edu, *.org	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	9F:F1:71:8D:92:D5:9A:F3:7D:74:97:B4:BC:6F:84:68:0B:BA:B6:66	**Verified?**	Verified
SHA-256 Fingerprint	44:B5:45:AA:8A:25:E6:5A:73:CA:15:DC:27:FC:36:D2:4C:1C:B9:95:3A:06:65:39:B1:15:82:DC:48:7B:48:33	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	“Hellenic Academic and Research	**Verified?**	Verified

	Institutions ECC RootCA 2015" currently has the following internally operated subCAs: - Hellenic Academic and Research Institutions ECC AdminCA R1 We plan to issue the following internally operated subCAs for specific usages: - ECC Client Authentication and SecureEmail - ECC Code Signing - ECC SSL (DV/OV) Server Certificates		
Externally Operated SubCAs	There are currently no externally operated subCAs issued from this root. According to our CP/CPS and the Mozilla RootCA program, in case of externally operated CAs, they will either be technically constrained or publicly disclosed and audited.	**Verified?**	Verified
Cross Signing	This Root will be cross-signed by "Hellenic Academic and Research Institutions RootCA 2011" to assist the rollover.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	HARICA has implemented technical restrictions (at the RA and CA level) allowing only specific domains affiliated with their 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	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	All documents are in Greek and English.	**Verified?**	Verified
CA Document Repository	http://www.harica.gr/procedures	**Verified?**	Verified
CP Doc Language			
CP		**Verified?**	Not Applicable
CP Doc Language			
CPS	http://www.harica.gr/documents/CPS-EN.pdf	**Verified?**	Verified
Other Relevant Documents	Qualified Certificates (under GUnet): http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/EsignProviders.html	**Verified?**	Verified
Auditor Name	QMSCERT	**Verified?**	Verified
Auditor Website	http://www.qmscert.com	**Verified?**	Verified
Auditor Qualifications	http://www.esyd.gr/eped/1.179906_en.doc	**Verified?**	Verified
Standard Audit	https://www.harica.gr/documents/HARICA-ETSI_CERTIFICATE_AUTH_W_ANNEX.pdf	**Verified?**	Verified

Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	6/5/2015	**Verified?**	Verified
BR Audit	http://pki.auth.gr/documents/AUTH-ETSI_CERTIFICATE_AUTH_W_ANNEX.pdf	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	6/5/2015	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.5.4	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.3.2: For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certifiate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by: - Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar, - Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; - Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; - Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name.... CPS section 3.2.4: The certificates that are issued do not include non-verified subscriber information. Each server certificate is manually verified.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	HARICA MoU http://www.harica.gr/documents/MoU-EN.pdf. Only Institutions currently registered as Academic or Research Institutions and their affiliates in Greece are allowed to join HARICA CPS sections 3.2.2 and 3.2.3	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.3.1: HARICA central RA uses three 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. - 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	**Verified?**	Verified

	acceptable official photo-id document. - The third method uses a Single Sign On (SSO) architecture based on the SAML specification. The user enters the personal e-mail address at the initial request form and is then redirected to the appropriate web page of the Identity Provider. The Identity Provider verifies the user and returns the real name and the email address..		
Code Signing Subscriber Verification Pro	CPS sections 3.2.2 and 3.2.3	**Verified?**	Verified
Multi-Factor Authentication	HARICA uses multi-factor authentication for the issuance of server certificates, and to access the RA and CA engines. CPS section 6.5.1.	**Verified?**	Verified
Network Security	HARICA has performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices CPS section 6.7.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.harica.gr/rep_dyn.php	**Verified?**	Verified