Mozilla - CA Program

Case Information

Case Number	00000029	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	MULTICERT	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	New Owner/Root inclusion requested	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1040072

General information about CA's associated organization

CA Email Alias 1	ca.forum@multicert.com		
CA Email Alias 2			
Company Website	https://www.multicert.com/pt/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Portugal	**Verified?**	Verified
Primary Market / Customer Base	Multicert is one of the biggest Portuguese CAs issuing digital qualified certificates for general public.	**Verified?**	Verified
Impact to Mozilla Users	90% of Multicert customers are Mozzilla users. They use their certificate for home banking, online shops and other kind of electronic transactions. Having Multicert Root CA globally recognized and installed by default, acting as a relying party, will significantly enhance the user experience of e-signature and e-authentication services for Mozzilla customers.	**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	* Reasons for Revocation: Root CPS section 5.7.5 * DNS names go in SAN: SSL CP section 3.1.2: DNS = <full qualified domain name of the Web server>, Maximum 7 Domains.	**Verified?**	Verified

	This extension contain at least one entry. Each entry is either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server.

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list 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	* SSL certs are OV. * We are no longer issuing SHA-1 SSL certificates that chain up to our roots in Mozilla's program. We have issued about 4 SHA-1 SSL certificates that are valid beyond January 1, 2017, that we have not yet revoked, and we plan to have them revoked by July 31, 2016.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	MULTICERT Root Certification Authority 01	**Root Case No**	R00000033
Request Status	Ready for Public Discussion	**Case Number**	00000029

Additional Root Case Information

Subject	Include MULTICERT Root Certification Authority 01 root cert

Technical Information about Root Certificate

O From Issuer Field	MULTICERT - Serviços de Certificação Electrónica S.A.	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	The MULTICERT root CA will issue certificates for subordinate CAs under MULTICERT PKI, and will also issue certificates for managed subordinate CAs of large organizations and governmental bodies.	**Verified?**	Verified
Root Certificate Download URL	http://pkiroot.multicert.com/cert/MCRootCA.cer	**Verified?**	Verified
Valid From	2014 Apr 04	**Verified?**	Verified
Valid To	2039 Apr 04	**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://promotor.teste.multicert.com/	**Verified?**	Verified
CRL URL(s)	http://pkiroot.multicert.com/crl/root_mc_crl.crl http://ec2pki.multicert.com/crl/crl_mca002.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.multicert.com/ocsp	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/promotor.teste.multicert.com lists error: NextUpdate not set (RFC 5019, section 2.2.4). According to rfc6960 the nextUpdate value is optional, but according to rfc5019 (OCSP Profile for High-Volume Environments) it's required. The revocationcheck site is tuned CA's for high volume environments. MULTICERT response: We don't perform caching at all, at least until we have more intermediate CA's that justifies.	**Verified?**	Verified
CA/Browser Forum Lint Test	Tested. no errors.	**Verified?**	Verified
Test Website Lint Test	Tested. No errors	**Verified?**	Verified
EV Tested	Not requesting EV treatment	**Verified?**	Not Applicable

Digital Fingerprint Information

SHA-1 Fingerprint	46:AF:7A:31:B5:99:46:0D:46:9D:60:41:14:5B:13:65:1D:F9:17:0A	**Verified?**	Verified
SHA-256 Fingerprint	60:4D:32:D0:36:89:5A:ED:3B:FE:FA:EB:72:7C:00:9E:C0:F2:B3:CD:FA:42:A1:C7:17:30:E6:A7:2C:3B:E9:D4	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	MULTICERT Root CA will issue certificates for subordinate CAs under MULTICERT PKI, and will also issue certificates for managed subordinate CAs of large organizations and governmental bodies. There are, for now, 2 Certificate Authorities subordinate to MULTICERT Root CA: 1) MULTICERT CA is responsible for qualified certificate issuance and SSL OV. 2) MULTICERT TS CA is responsible for services certificate issuance as TSL	**Verified?**	Verified

	service, TSA service, etc. All these CA's are accredited by GNS (Gabinete Nacional de Segurança - http://www.gns.gov.pt/) or http://www.gns.gov.pt/media/1891/TSLPTHR.pdf.		
Externally Operated SubCAs	MULTICERT will also issue certificates for managed subordinate CAs of large organizations and governmental bodies. These subordinate CAs, in turn, issue the following end entity certificate types: Qualified Signature, Authentication, Advanced Signature, SSL Certificates for web server (CAs issuing SSL certificates are separated from CAs issuing Timestamping or Code Signing certificates), Application Certificates (e.g., e-Invoice, WS-Security), OCSP online validation, Code Signing, Timestamping. CPS section 9: In the case of certificate authorities belonging to MULTICERT's PKI but operated by other entities, MULTICERT may, whenever it sees fit, conduct internal audits to them. These entities are also required to annually deliver to MULTICERT the annual audit report, or a statement of compliance, conducted by an independent and recognized for that purpose.	**Verified?**	Verified
Cross Signing	For now, MULTICERT CA 001 and 002 are signed by both MULTICERT and Baltimore Root CA's	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Where MULTICERT has a External RA, a procedure is established in order to comply with all our requirements. All the documentation is store by MULTICERT, training is in place as well as all member (Registration Administrator) are dully identified. MULTICERT provided a web interface, where the Registration Administrator need to be authenticate for a new subject registration. External RA's are audited on an annual basis. In the case of External RA's issuing qualified certificates, they are dully registered in the supervisory body (www.gns.gov.pt). > The subordinate CAs who are not part of the MULTICERT organization... Are there any technical constraints on them? It depends on the kind of contract established and the audience of our costumer. They are all obliged to meet our CPS requirements. We don't have, for now, any Subordinate CA which is not part of MULTICERT Organization.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Portuguese, with some translated into English. Documents in Portuguese: Root CPS: http://pkiroot.multicert.com	**Verified?**	Verified

	/pol/CPS_MULTICERT_PJ.ECRAIZ_24.1.1_0001_pt.pdf Root CP: http://pkiroot.multicert.com/politicas /CP_MULTICERT_PJ_ECRAIZ_24_1_2_0001_pt.pdf SSL CP: https://pki.multicert.com/pol/cp /MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf Qualified Digital Signature CP: https://pki.multicert.com /pol/cp/MULTICERT_PJ.CA3_24.1.2_0002_pt.pdf Authentication CP: https://pki.multicert.com/pol/cp /MULTICERT_PJ.CA3_24.1.2_0003_pt.pdf		
CA Document Repository	http://pkiroot.multicert.com/	**Verified?**	Verified
CP Doc Language	English		
CP	http://pkiroot.multicert.com/politicas /CP_MULTICERT_PJ_ECRAIZ_24_1_2_0001_en.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://pkiroot.multicert.com /pol/CPS_MULTICERT_PJ.ECRAIZ_24.1.1_0001_en.pdf	**Verified?**	Verified
Other Relevant Documents	Qualified Digital Signature CP (English): https://pki.multicert.com/pol/cp /MULTICERT_PJ.CA3_24.1.2_0002_en.pdf ETSI TS 101 456 Auditor: Unisys Auditor Website: http://www.gns.gov.pt/media /4311/listagemdeas.pdf	**Verified?**	Verified
Auditor Name	SGS Portugal	**Verified?**	Verified
Auditor Website	http://www.sgs.com/	**Verified?**	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap /ESI/TrustServiceProviders.aspx http://ipac.pt/pesquisa/ficha_ocf.asp?id=A0003	**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8651752	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	4/1/2015	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8651752	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	4/1/2015	**Verified?**	Verified
EV Audit	Not requesting EV treatment	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	Root CPS section 2.1 SSL CP section 3.1	**Verified?**	Verified
SSL Verification Procedures	SSL CP section 4.1: For each Fully-Qualified Domain Name listed in a Certificate, MULTICERT confirms that, as of the issuance date the - Confirmation that the certificate applicant has the domain name registration directly over the FQDN by: o Direct communication with the responsible domain name using the address, email or number of service provided by the domains registration Entity; o Direct communication with the responsible domain name using the contact information listed in the "registrant" field, "technical" or "administrative" records	**Verified?**	Verified

	the WHOIS o Communication with the domain administrator using the email address created with the prefix "Admin", "administrator", "webmaster", "hostmaster" and "postmaster", followed by "@" sign, and terminated by Domain Name; o An Authorization Document trusted domain Statement by the Applicant that has practical control over the Fully Qualified Domain Name, through the pre-agreement on an amendment to certain information contained in a Online Web page identified by a URI that contains the Fully Qualified Domain Name followed by the Domain Name; o Use of any other confirmation method (since that provides the same level of confidence that the test methods referred to above), and the EC will preserve record that will serve as evidence confirming that the Applicant is responsible for the Domain Name or has control over the Fully Qualified Domain Name` section 4.2 - Authorization for an IP Address		
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	Root CPS section 4.2	**Verified?**	Verified
Email Address Verification Procedures	Qualified Digital Signature CP section 4.1.1: Additionally, a validation is made to the email address which will include in certificate. This activitybegins after the submission of an application for a qualified digital signature, by sending a request for confirmation e-mail to the titleholder, by MULTICERT, to the address indicated therein. In this email, the titleholder is asked to confirm the email address by accessing the link provided for that purpose. The holder of a Qualified Digital Signature, issued by the MULTICERT CA, cannot activate the certificate if the confirmation e-mail is not made.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	The Code Signing trust bit is expected to be removed from Mozilla policy in 2016, so Mozilla is no longer enabling the Code Signing trust bit for any root certs.	**Verified?**	Not Applicable
Multi-Factor Authentication	MULTICERT Response: For certificate issuance directly on the CA two-factor authentication is required. Username+password and digital certificate authentication.	**Verified?**	Verified
Network Security	Root CPS section 6 and 7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://pki.multicert.com/index.html	**Verified?**	Verified