Print this page

Mozilla - CA Program

Case Information

Case Number	00000029	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	MULTICERT	**Request Status**	Information Verification In Process

Additional Case Information

Subject	MULTICERT Root Certification Authority 01	**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	**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	Multicert customers use their certificate for home banking, online shops and other kind of electronic transactions.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_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	1. Publicly Available CP and CPS: CP/CPS section 2 NEED: There is a Confidentiality clause at the top of both of the CP and CPS documents. This is problematic, since Mozilla requires the CA's CP/CPS to be publicly disclosed. Note that the CP and CPS are published on the CA's website: https://pki.multicert.com/index.html So I recommend that the CA remove the confidentiality clauses. 1.1 Revision Table, updated annually: CP/CPS page 2 1.2 CAA Domains listed in CP/CPS: CPS section 3.2.5 1.3 BR Commitment to Comply statement in CP/CPS: CP/CPS section 1.1 2. Audit Criteria: ETSI EN 319 411 3. Revocation of Compromised Certificates: CP/CPS section 4.9.1 4. Verifying Domain Name Ownership: CP/CPS section 3.2.2 5. Verifying Email Address Control: NEED: If requesting the Email (S/MIME) trust bit, then the CP and/or CPS must explain how the CA confirms that the certificate requester owns/controls the email address to be included in the certificate. https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control 6. DNS names go in SAN: CP/CPS section 7.1 7. OCSP: CP/CPS section 7.3 - OCSP SHALL NOT respond "Good" for unissued certs: 8. Network Security Controls: CP/CPS section 6.7	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_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	1. Long-lived Certificates: CP/CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CP section 3.2.2 3. Issuing End Entity Certificates Directly From Roots: CPS section 1.3 4. Distributing Generated Private Keys in PKCS#12 Files: CPS section 3.2.1.3 5. Certificates Referencing Local Names or Private IP Addresses: CP section 3.2.2.2 6. Issuing SSL Certificates for .int Domains: CP section 3.2.2 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: CP section 7.1 9. Delegation of Domain / Email Validation to Third Parties: CP/CPS section 1.3.2	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	MULTICERT Root Certification Authority 01	**Root Case No**	R00000033
Request Status	Information Verification In Process	**Case Number**	00000029

Certificate Data

Certificate Issuer Common Name	MULTICERT Root Certification Authority 01
O From Issuer Field	MULTICERT - Serviços de Certificação Electrónica S.A.
OU From Issuer Field	
Valid From	2014 Apr 04
Valid To	2039 Apr 04
Certificate Serial Number	544DA5BC4035565A
Subject	CN=MULTICERT Root Certification Authority 01; OU=; O=MULTICERT - Serviços de Certificação Electrónica S.A.; C=PT
Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	46AF7A31B599460D469D6041145B13651DF9170A
SHA-256 Fingerprint	604D32D036895AED3BFEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4
Subject + SPKI SHA256	005AB8B5CE2CE45FBC8BD466F5B9DEB8146627E4ECDFDB1CAC81A21962E75972
Certificate Version	3

Technical Information about Root Certificate

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
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
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified

SSL Validation Type	OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://demo.mtrust.online/	**Verified?**	Need Response From CA
Test Website - Expired	https://expired.mtrust.online/		
Test Website - Revoked	https://revoked.mtrust.online/		
Example Cert			
Test Notes	The intermediate cert, MULTICERT Certification Authority 002, is cross-certified by Baltimore CyberTrust Root. I was unable to browse to https://demo.mtrust.online/ when I disabled the Baltimore CyberTrust Root.		

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

Revocation Tested	https://certificate.revocationcheck.com/demo.mtrust.online	**Verified?**	Not Verified
CA/Browser Forum Lint Test	NEED: Please explain the Lint testing errors: https://crt.sh/?caid=5842&opt=cablint,zlint,x509lint&minNotBefore=2014-04-04 https://crt.sh/?caid=1602&opt=cablint,zlint,x509lint&minNotBefore=2014-04-04	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: Please explain the Lint testing errors: https://crt.sh/?caid=84368&opt=cablint,zlint,x509lint&minNotBefore=2014-04-04 https://crt.sh/?caid=15339&opt=cablint,zlint,x509lint&minNotBefore=2014-04-04	**Verified?**	Need Response From CA
EV Tested	Not requesting EV treatment	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CPS section 1.3 MULTICERT Root CA will issue certificates for subordinate CAs under	**Verified?**	Verified

	MULTICERT PKI, and will also issue certificates for managed subordinate CAs of large organizations and governmental bodies.		
Externally Operated SubCAs	NEED: It appears that MULTICERT CA allows for externally-operated subordinate CAs. However, I did not find text in the CP or CPS stating that such externally-operated subCAs must follow the rules of the CP/CPS and must be externally-audited (as per the BRs and Mozilla's requirements), or must be technically constrained, etc.	**Verified?**	Need Response From CA
Cross Signing	For now, MULTICERT CA 001 and 002 are signed by both MULTICERT and Baltimore Root CAs	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	External RAs are allowed per rules listed in CP/CPS section 1.3.2	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Portuguese, with some translated into English.	**Verified?**	Verified
CA Document Repository	https://pki.multicert.com/index.html	**Verified?**	Verified
CP Doc Language	English		
CP	https://pki.multicert.com/docs/EN/MULTICERT_PJ.ECRAIZ_426_en.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pki.multicert.com/docs/EN/MULTICERT_PJ.ECRAIZ_427_en.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor	Associação Portuguesa de Certificação (APCER)	**Verified?**	Verified
Auditor Location	Portugal	**Verified?**	Verified
Standard Audit	https://bug1040072.bmoattachments.org/attachment.cgi?id=8998564	**Verified?**	Verified
Standard Audit Type	ETSI EN 319 411	**Verified?**	Verified
Standard Audit Statement Date	2/7/2018	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8746964	**Verified?**	Verified
BR Audit Type	ETSI EN 319 411	**Verified?**	Verified
BR Audit Statement Date	2/7/2018	**Verified?**	Verified
EV SSL Audit	Not requesting EV treatment	**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable

EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CP/CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bug1040072.bmoattachments.org/attachment.cgi?id=8966648	**Verified?**	Verified
SSL Verification Procedures	CP/CPS section 3.2.2	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS section 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	NEED: If requesting the Email (S/MIME) trust bit, then the CP and/or CPS must explain how the CA confirms that the certificate requester owns/controls the email address to be included in the certificate. https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	N/A	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 5	**Verified?**	Verified
Network Security	CP/CPS section 6.7	**Verified?**	Verified