Bugzilla ID: 1040072
Bugzilla Summary: Add MULTICERT Root Certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	MULTICERT S.A., Serviços de Certificação Eletrónica S.A.
Website URL	https://www.multicert.com/pt/
Organizational type	Private Organization
Primark Market / Customer Base	Which types of customers does the CA serve? **Any costumer who need a qualified signature or need to identify his enterprise website.** Are there particular vertical market segments in which it operates? **No** Does the CA focus its activities on a particular country or other geographic region? **No** **MULTICERT pretends to have full control of its trust certification path, up to the root. This will allow an improved value offer to our large organization and governmental customers.** **The root CA will issue certificates for subordinate CAs under MULTICERT PKI. MULTICERT will also issue certificates for managed subordinate CAs of large organizations and governmental bodies.** **These subordinate CAs, in turn, will 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.** **Actually Multicert is one of the biggest Portuguese CAs issuing digital qualified certificates for general public.**

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.**
Inclusion in other major browsers	**Actually we are recognized by Microsoft and Adobe. We are also working on the Oracle and Apple Root Certificate Program.**
CA Primary Point of Contact (POC)	CA Email Alias: sara.nunes@multicert.com CA Phone Number: +351961959273 Title: Chief Information Security Officcer

Technical information about each root certificate

Certificate Name	MULTICERT Root Certification Authority 01

Certificate Issuer Field	CN = MULTICERT Root Certification Authority 01
	O = MULTICERT - Serviços de Certificação Electrónica S.A.
	C = PT

Certificate Summary	**MULTICERT ROOT CA is the top of the hierarchy, and issues only certificates for subordinate CA's. Subordinate CA's issue other kinds of certificates, including digital qualified certificates, ssl certificates, certificates for timestamping signatures, etc.**
Mozilla Applied Constraints	Mozilla has the ability to apply Domain Name Constraints at the root level, such that Mozilla products would only recognize SSL certificates in the CA's hierarchy with domains in the listed constraints. Constraints may be at the country level such as *.us; and can include a list such as (*.gov.us, *.gov, *.mil). Please consider the types of SSL certificates that need to be issued within this CA hierarchy, and if applicable provide a list of names to constrain the CA hierarchy to. **No constraints. MULTICERT CA will have his own constraints for ssl certificate issuance depending on information validation for ssl certificate request.**
Root Cert URL	http://pkiroot.multicert.com/cert/

SHA1 Fingerprint	46:AF:7A:31:B5:99:46:0D:46:9D:60:41:14:5B:13:65:1D:F9:17:0A
Valid From	2014-04-04
Valid To	2039-04-04
Certificate Version	3
Certificate Signature Algorithm	SHA-256
Signing key parameters	4096
Test Website URL (SSL)	https://promotor.teste.multicert.com/ An error occurred during a connection to promotor.teste.multicert.com. The OCSP server experienced an internal error. (Error code: sec_error_ocsp_server_error) **Please try again** Please test with OCSP enforced in Firefox: https://wiki.mozilla.org/CA:Recommended_Practices#OCSP
CRL URL	http://pkiroot.multicert.com/crl/root_mc_crl.crl NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS. **http://pkiroot.multicert.com/crl/root_mc_crl.crl** **CRL's are issued every 4 months.** **"MULTICERT Root CA shall publish a new CRL in its repository whenever there is a revocation. When there are no changes to the validity status of the certificates, i.e. if no revocation is produced, MULTICERT Root CA makes a new CRL available every 4 months. "**
OCSP URL	http://ocsp.multicert.com/ocsp **Maximum expiration time of OCSP responses, for now, is 0ms.**
Requested Trust Bits	One or more of: **Server Authentication** **Client Authentication** **Secure E-mail** **Code Signing** **Time stamping** **OCSP** **Encrypting File System** **IPsec** **Document Signing**
SSL Validation Type	**Organizational Validation Certificates Policy**
EV Policy OID(s)	Not Applicable. Not requesting EV treatment at this time.

Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html “9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: … - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number).” The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration. This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn’t an acceptable hash algorithm for certificates in this hierarchy. **Serial Number is Represented with 6 hexadecimal digit (MULTICERT Root CA serial number - 54 4d a5 bc 40 35 56 5a). All certificates in MULTICERT Root Hierarchy are issued with, at least, SHA256 signature algorithm. You can find this information in the CP’s, f.g: https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0002_pt.pdf.**
Response to Recent CA Communication(s)	https://wiki.mozilla.org/CA:Communications Action 1 - Primary Point of Contact (POC) – sara.loja@multicert.com/nuno.ponte@multicert.com Action 2 - Audit Statement do BR is attached Action 3 - C) 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. Action 4 – None of the Above Action 5 - We do not support IPv6, and have no plans to do so.

CA Hierarchy information for each root certificate

CA Hierarchy	MULTICERT Root CA is the top of the hierarchy working as an offline CA. 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 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. The OID's for each policy: MULTICERT CA: QC - 1.3.6.1.4.1.25070.1.1.1.1.0.1.2 SSL (OV) - 1.3.6.1.4.1.25070.1.1.1.1.0.1.5 MULTICERT TS CA: Timestamping - 1.3.6.1.4.1.25070.1.1.1.2.0.1.1 CodeSigning - 1.3.6.1.4.1.25070.1.1.1.2.0.1.2 MULTICERT Root CA CPS - 1.3.6.1.4.1.25070.1.1.1.0.7 MULTICERT CA CPS - 1.3.6.1.4.1.25070.1.1.1.1.0.7 MULTICERT TS CA CPS - 1.3.6.1.4.1.25070.1.1.1.2.0.7
Externally Operated SubCAs	MULTICERT doesn't currently have external subordinate CA's. The root CA will issue certificates for subordinate CAs under MULTICERT PKI. 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. Please provide the information listed in this checklist: https://wiki.mozilla.org/CA:SubordinateCA_checklist#CA_Policies_about_Third-Party_Subordinate_CAs Does MULTICERT operate as a Super-CA according to the description here? https://wiki.mozilla.org/CA:SubordinateCA_checklist#Super-CAs If yes, please explain. **It is a Super CA. This is a Offline SuperCA which issue certificates for the MULTICERT Subordinate CA's.**
Cross-Signing	None. Any planned? **No**
Technical Constraints on Third-party Issuers	Please translate into English the sections of the CP/CPS documents that explain the requirements placed on anyone external to MULTICERT who can cause a certificate to be issued within this CA hierarchy. External RAs count as third-party issuers. What technical constraints are place on them? Root CPS section 2.3.2: MULTICERT may … establish agreements with other entities … to perform this role. **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, and the managed subordinate CAs are all third-party issuers. 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.**

Verification Policies and Practices

Policy Documentation	**Root CPS (English):** **http://pkiroot.multicert.com/pol/CPS_MULTICERT_PJ.ECRAIZ_24.1.1_0001_en.pdf** **Root CPS (Portuguese):** **http://pkiroot.multicert.com/politicas/CP_MULTICERT_PJ_ECRAIZ_24_1_2_0001_pt.pdf** **Note: We are revewing these documents** **SSL CP (Portuguese): https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf** **Root CP (Portuguese): https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0001_pt.pdf** **Qualified Digital Signature CP (Portuguese):** **https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0002_pt.pdf** **Authentication CP (Portuguese):** **https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0003_pt.pdf**
Audits	**Audit Type: Audit According with CabForum, ETSI TS 102 042 and ETSI TS 101 456** **ETSI TS 101 456** **Auditor: Unisys** **AuditorWebsite: http://www.gns.gov.pt/media/4311/listagemdeas.pdf** **ETSI TS 102 042** **Auditor: SGS Portugal** **AuditorWebsite: http://www.european-accreditation.org/ea-members** **URL to Audit Report and Management's Assertions: Conformance Declarations in attachment** **"The Root CPS (English) says: "International hierarchy of trust with WebTrust accreditation**

	(http://www.webtrust.org/) and is present in the majority of the operating systems and Web bro wsers." **Please point me to the WebTrust audit statement"** **This does respect to our subordinates MULTICERT CA 002 and MULTICERT CA 001 wich are, for now, signed by Baltimore as well.**
Baseline Requirements (SSL)	Please carefully review: https://wiki.mozilla.org/CA:BaselineRequirements (also have your auditor carefully review this wiki page) Need the ETSI TS 102 042 PTC-BR audit statement/certificate, as per section 17 of the Baseline Requirements → **In Attachment.** The Subordinate CA responsible for SSL certificate issuance, for now we only issue OV, is compliant with the ETSI TS 102 042 and follows CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf --> actually we only have a Portuguese Version RootCPS (English) section 2.1: MULTICERT Root CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly--Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

SSL Verification Procedures	The Subordinate CA responsible for SSL certificate issuance, for now we only issue OV, is compliant with the ETSI TS 102 042 and follows CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Each Subordinate CA has to be audited according to section 17 of the Baseline Requirements, or Technically Constrained as per section 9.7 of the Baseline Requirements. Root CP (English) section 2.1: MULTICERT Root CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document. Need to compare with corresponding document in Portuguese. **Root CPS (Portuguese): A MULTICERT Root CA está de acordo com a versão atual dos requisitos básicos para a Emissão e Gestão de Certificados Publicly-Trusted, publicados pelo CA/Browser Forum no documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", disponibilizado em http://www.cabforum.org. No caso de qualquer inconsistência entre este documento e o descrito no documento de Baselines, o definido no documento emitido pelo CA/Browser Forum sobrepõe-se ao descrito neste documento.** SSL CP section 3.1: The profile of the Web Server is certified according to: - Recommendation X.5093 ITU.T; - RFC 5280 and - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA / Browser Forum 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 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` 4.2 Authorization for an IP Address (Used Google Translate) For each IP address listed in the certificate, the EC confirms that the date of issue of the certificate, the

	Applicant has control over the IP address through: • Statement by the Applicant that has control over the IP address through préacordo on an amendment to certain information contained in a Web page online identified by a URI9 that contains the IP address; • Obtaining documentation on the assignment of the IP address from the Internet Assigned Numbers Authority (IANA) or Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC). • Conducting research on the IP address and then check the control over the Domain Name resultant; • Using any other method of confirmation (since that provides the same level of confidence that the verification methods mentioned above), and the EC will preserve record that will serve as evidence confirming that the Applicant is responsible for the IP address or have control over the IP address.
Organization Verification Procedures	Root CPS (English) section 4.2: The procedures for the identification and authentication of subscriber previously unknown shall follow the following rules: 1. The subscriber or its legal representative (in case of a collective person) shall present themselves physically to MULTICERT; 2. The physical identification shall be authenticated against identifying proofs that must be compliant with the following provisions: a. To be officially recognized in the jurisdiction where the subscriber is registered; b. To indicate the full name of the subscriber and its official address; c. To have at least one identity proof with a photograph of the subscriber (always applicable); d. To indicate a unique registration number inside of the jurisdiction where it was issued. 3. In case of certificates for non-human subscribers, the mentioned authentication processes shall apply to the people who are authorized to request certifications for the specified subscribers. 3. MULTICERT shall verify that each candidate for obtaining a certificate has the right to obtain that certificate and, in case obtaining that certificate also implies obtaining attributes or privileges of any kind, the candidate really has the right to those privileges and attributes; 4. When necessary, MULTICERT shall require the requesting entity of a certificate prepares and submits an appropriate logical request of certificate to the CA; 5. Also when necessary, MULTICERT shall verify the correctness of the information included in the logical request of certificate from the requesting entity.
Email Address Verification Procedures	The MULTICERT clients have an account which is created only after email confirmation. – where (in theCP/CPS) is this explained? See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control
Code Signing Subscriber Verification	Same text provided as above for Organization Verification Procedures
Procedures Multi-factor Authentication	Which CP/CPS sections actually talk about Code Signing certificates? For certificate issuance directly on the CA two-factor authentication is required. Username+password and digital certificate authentication. –Which document and sections describe this requirement? We have an internal document describing all this kind of procedures.

Network Security	We are compliant and comfortable with this items and regarding the Network and Certificate System Security Requirements from CA/BForum. CPS on the sections 6 and 7 describes Physical Safety, Management, and Operating Measures and TECHNICAL SAFETY MEASURES http://pkiroot.multicert.com/pol/CPS_MULTICERT_PJ%20ECRAIZ_24%20.1%20.1_0001_en.pdf However the MULTICERT Root CA is an offline CA.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)	
Publicly Available CP and CPS	See above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	Does MULTICERT allow this? Where is it documented?
Revocation of Compromised Certificates	Root CPS section 5.7.5 Please see Baseline Requirements section 13.1.5. MULTICERT PKI CPS's are under review.
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above
DNS names go in SAN	SSL CP section 3.1.2: DNS = <full qualified domain name of the Web server>, Maximum 7 Domains SAN: 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.
Domain owned by a Natural Person	Not Applicable
OCSP	See above
Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)	
Long-lived DV certificates	NA
Wildcard DV SSL certificates	What sections of the CP/CPS document whether wildcard SSL certs are allowed or not?
Email Address Prefixes for DV Certs	N.A.
Delegation of Domain / Email validation to third parties	See above.
Issuing end entity certificates directly from roots	No. See above.
Allowing external entities to operate subordinate CAs	See above.
Distributing generated private keys in PKCS#12 files	No

Certificates referencing hostnames or private IP addresses	SSL CP section 3.1.2: CN - <full qualified domain name of the Web server or IPAddress> Please see https://wiki.mozilla.org/CA:Problematic_Practices#Certificates_referencing_hostnames_or_private_IP_addresses
Issuing SSL Certificates for Internal Domains	Please see https://wiki.mozilla.org/CA:Problematic_Practices#Issuing_SSL_Certificates_for_Internal_Domains
OCSP Responses signed by a certificate under a different root	No. See above.
SHA-1 Certificates	Please see https://wiki.mozilla.org/CA:Problematic_Practices#SHA-1_Certificates We don’t issue SHA-1 Certificates.
Generic names for CAs	No. See above.
Lack of Communication With End Users	No
Backdating the notBefore date	No