General Information about the CA's associated organization	
CA Company Name	MULTICERT S.A., Serviços de Certificação Eletrónica S.A. Lagoas Park, Edifício 3, Piso 3 - 2740-266 Porto Salvo – Oeiras
Website URL	www.multicert.com http://pkiroot.multicert.com → MULTICERT Root CA http://pki.multicert.com → MULTICERT CA nnn http://ec2pki.multicert.com → MULTICERT CA nn http://ts4pki.multicert.com → MULTICERT TS CA
Organizational type	Private Organization
Primark Market / Customer Base	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 will be 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.

CA Contact Information **CA Email Alias**	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 CA
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.
Root Cert URL	http://pkiroot.multicert.com/cert/index_en.html
SHA1 Fingerprint	46 af 7a 31 b5 99 46 0d 46 9d 60 41 14 5b 13 65 1d f9 17 0a
Valid From	4 de abril de 2014 09:59:47
Valid To	4 de abril de 2039 09:59:47
Certificate Version	X.509 V3
Certificate Signature Algorithm	sha256RSA
Signing key parameters	RSA Keys, 4096 bits
CRL URL	http://pkiroot.multicert.com/crl/root_mc_crl.crl
OCSP URL	http://ocsp.multicert.com/ocsp
Requested Trust Bits	Server Authentication Client Authentication Secure E-mail Code Signing Time stamping OCSP Encrypting File System IPsec Document Signing

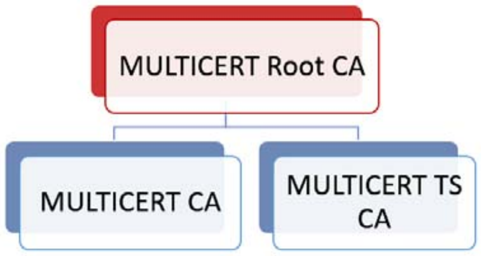
SSL Validation Type	OV, DV. For each of these policies exists a correspondent CA.

CA hierarchy Information for each root certificate	
CA Hierarchy	MULTICERT Root CA only issues certificate for subordinates Certification Authorities. There are, for now, 2 Certificate Authorities subordinate to MULTICERT Root CA: - MULTICERT Trust Services Certification Authority 001; - MULTICERT Certification Authority 002;
Externally Operated SubCAs	- MULTICERT doesn't have external subordinate CA's
Cross-Signing	N.A.
Technical Constraints or Audits of Third-Party Issuers	N.A.

Verification Policies and Practices	
Policy Documentation	Language(s) that the documents are in: CP: Portuguese, English CPS: Portuguese, English - > section 2.1 → Overview : "Commitment to Comply" Relying Party Agreement: Portuguese
Audits	Audit Type: Audit According with CabForum, ETSI TS 101 456, ETSI TS 102 042 Auditor: Paulo Jorge Martins Borges 19/2014 AuditorWebsite:http://www.gns.gov.pt/media/4311/listagemdeas.pdf URL to Audit Report and Management's Assertions: In attachement.
Baseline Requirements (SSL)	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
Organization Verification Procedures	https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf --> actually we only have a Portuguese Version MULTICERT is responsible for the authentication of the identity of the clients candidates for obtaining a certificate. The ways to proceed to this authentication include: →Ensure that the client exists and that he authorized the issuing of the certificate;

	→Ensure that MULTICERT's legal representatives accepted the client in question inside its hierarchy. The registration and authentication process shall be ensured by the following: it is the responsibility of the RA to correctly register the final users of the certificate, using the means necessary to positively identify them in a legal way. Among the operations to be performed to reach this objective are: → Verify in documents officially acknowledged by the State where the subscriber (individual or organization) is registered: a. Full name; b. Contact data, including the contact address; c. Its legal unique identification.
Domain Verification Procedures And Email Address Verification Procedures	For each Fully-Qualified Domain Name listed in a Certificate, MULTICERT confirms that, as of the issuante 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
Code Signing Subscriber Verification Procedures	https://pki.multicert.com/pol/cp/MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf --> actually we only have a Portuguese Version MULTICERT is responsible for the authentication of the identity of the clients candidates for obtaining a certificate. The ways to proceed to this authentication include: • Ensure that the client exists and that he authorized the issuing of the certificate; • Ensure that MULTICERT's legal representatives accepted the client in question inside its hierarchy. The registration and authentication process shall be ensured by the following: it is the responsibility of the RA to correctly register the final users of the certificate, using the means necessary to positively identify them in a legal way. Among the operations to be performed to reach this objective are:

	➔ Verify in documents officially acknowledged by the State where the subscriber (individual or organization) is registered: a. Full name; b. Contact data, including the contact address; c. Its legal unique identification.
Multi-factor Authentication	For certificate issuance directly on the CA two-factor authentication is required. Username+password and digital certificate authentication.
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	
Publicly Available CP and CPS	http://pkiroot.multicert.com/pol/index_en.html for both CP and CPS
CA Hierarchy	 MULTICERT Root CA is the top of the hierarchy working as an offline CA. MULTICERT CA is responsible for qualified certificate issuance. MULTICERT TS CA is responsible for services certificate issuance as TSL service, TSA service, etc.

<table>
<tr><td></td><td>Al this 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</td></tr>
<tr><td><b>Audit Criteria</b></td><td>
<table>
<tr><th>[redacted]</th><th>[redacted]</th></tr>
<tr><td>MULTICERT EC CA 001 e 002</td><td>DR 25/2004
Notas Técnicas GNS NT 02 e NT 03
ETSI 101 456
ETSI 102 042</td></tr>
<tr><td>MULTICERT Root Certification Authority 01</td><td>CabForum – Requisitos de Root CA
ETSI TS102 042
ETSI TS 101 456</td></tr>
<tr><td>MULTICERT Trust Services Certification Authority</td><td>ETSI TS 102 042</td></tr>
</table>
</td></tr>
<tr><td><b>Revocation of Compromised Certificates</b></td><td>The new state of certificate revocation is published in the maximum in 24 hours after the revocation request.</td></tr>
<tr><td><b>Verifying Domain Name Ownership</b></td><td>The same as ‘Domain Verification Procedures
And Email Address Verification Procedures’</td></tr>
<tr><td><b>Verifying Email Address Control</b></td><td>The MULTICERT clients have an account which is created only after email confirmation.</td></tr>
</table>

Verifying Identity of Code Signing Certificate Subscriber	The same as ‘Domain Verification Procedures And Email Address Verification Procedures’
DNS names go in SAN	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	N.A.
OCSP	ocsp.multicert.com/ocsp. This is a multiCA service.

Response to Mozilla's list of Potentially Problematic Practices	
Long-lived DV certificates	N.A.
Wildcard DV SSL certificates	N.A.
Email Address Prefixes for DV Certs	N.A.
Delegation of Domain / Email validation to third parties	N.A.
Issuing end entity certificates directly from roots	N.A.
Allowing external entities to operate subordinate CAs	N.A.
Distributing generated private keys in PKCS#12 files	N.A.
Certificates referencing hostnames or private IP addresses	N.A.
Issuing SSL Certificates for Internal Domains	N.A.
OCSP Responses signed by a certificate under a different root	N.A.
CRL with critical CIDP Extension	N.A.
Generic names for CAs	N.A.

Lack of Communication With End Users	MULTICERT has several channels of communication with the customer, either by email or by phone. There is also a process for managing complaints and satisfaction where customers can leave their complaints or compliments.
Backdating the notBefore date	N.A.

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.

Assinado de forma digital por [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
DN: c=PT, o=MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A., ou=Certificado para pessoa colectiva - Assinatura Qualificada, title=Procurador com poderes indicados na procuração emitida em 16/10/2013 - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, serialNumber=505767457, cn=[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
Dados: 2014.07.10 17:23:02 +01'00'