Bugzilla ID: 438825
Bugzilla Summary: Add CA Root certificate (Brazil's National PKI)

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil) Instituto Nacional de Tecnologia da Informação (ITI)
Website URL	https://www.icpbrasil.gov.br/ http://www.iti.gov.br/
Organizational type	National Government CA The ITI (Instituto Nacional de Tecnologia da Informação), a Federal organization linked to the Presidency of the Republic of Brazil with the principal attribution of being the Root Certification Authority (CA-Root) and supervising to many Certification Authority (CA). The ITI, between other attributions, is the Root Certification Authority (CA Root) of ICP Brasil (Infra-Estrutura de Chaves Públicas Brasileira) or Brazil's National PKI created by the law (Medida Provisória nº 2.200-2 / 2001). As such is the first authority of the chain of certification, executioner of the Politics of Certificates and technical and operational standards approved by the Committee of ICP-Brasil. Hierarchical structure of ICP-Brasil: https://bugzilla.mozilla.org/attachment.cgi?id=333737
Primary market / customer base.	ICP Certificates are used in all secure Brazilian government sites (and several financial too). ICP-Brazil is not exclusively used by the government but the entire Brazilian society. The ICP-Brazil has the only (V0 and V1) chain operated by the ITI.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data - Old Root	Data - New Root
Certificate Name	Autoridade Certificadora Raiz Brasileira	Autoridade Certificadora Raiz Brasileira v1
Cert summary / comments	Root cert used to secure Brazilian government and financial sites.	The next version of the root.
Root CA certificate URL	http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt	http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt
SHA-1 fingerprint.	8E:FD:CA:BC:93:E6:1E:92:5D:4D:1D:ED:18:1A:43:20:A4:67:A1:39	70:5D:2B:45:65:C7:04:7A:54:06:94:A7:9A:F7:AB:B8:42:BD:C1:61
Valid from	11/30/2001	7/29/2008
Valid to	11/30/2011	7/29/2021

Cert Version	3	3
Modulus length	2048	2048
Test Websites	https://internetbanking.caixa.gov.br/SIIBC/index.processa	https://ccd.serpro.gov.br/certificados/index.htm In order to see the full chain, I also had to install these subCAs: https://ccd.serpro.gov.br/acserpro/docs/serprov2.crt https://ccd.serpro.gov.br/acserpro/docs/serprofinalv2.crt
CRL	http://acraiz.icpbrasil.gov.br/LCRacraiz.crl	http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl
	In page 27 of CP from 2006: Frequency of update for CRL 6 hours for all certificates	
OCSP Responder URL	Not Applicable	Not Applicable
List or description of subordinate CAs operated by the CA organization associated with the root CA.	The ITI operates only the CA root (V0 and V1 chains) Complete CA Hierarchy: http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_completa.pdf Comment #67: The blue boxes indicates the RA (registry authority) linked with sub-CAs (2º level) High-level CA Hierarchy: https://bugzilla.mozilla.org/attachment.cgi?id=342297 http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_da_ICP-Brasil_-_site22-08.pdf	
For subordinate CAs operated by third parties, if any:	See 438825-subCA-review.pdf List of all of the Subordinate CA's operated by third parties: http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp Cert Hierarchy: https://bugzilla.mozilla.org/attachment.cgi?id=342297 The 8 CAs (1º level) are externally operated by other organizations: CAIXA (www.caixa.gov.br), SERPRO (www.serpro.gov.br), SERASA (http://www.serasa.com.br/) , Certisign – a affiliate Verisign (http://www.certisign.com.br/), Secretaria da Receita Federal (http://www.receita.fazenda.gov.br/), Presidência da República (http://www.presidencia.gov.br/ingles/), Imprensa Oficial do Estado de São Paulo (http://www.imprensaoficial.com.br/PortalIO/Certificacao/Sobre/Apresentacao_7_0.aspx), Poder Judiciário Brasileiro (http://www.acjus.gov.br/) . The ITI authorizes, supervises and audits the operations of CAs (1º level) like table https://bugzilla.mozilla.org/attachment.cgi?id=342298	
List any other root CAs that have issued cross-signing certificates for this root CA	none	none
Requested Trust Bits Websites, Email, and/or	Websites	

Code Signing	
CP/CPS	CP (Portuguese): http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-04_-_v._3.0.pdf CPS of CA-root (Portuguese): http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-01_-_versao_4.0_retificada_em_15-01-09.pdf CPS Requirements for sub-CA (Portuguese): http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-05_-_versao_3.1_(REQUISITOS_MIN._PARA_AS_DPCs_DAS_ACs).pdf ICP-Brasil Documents: http://www.iti.gov.br/twiki/bin/view/Certificacao/DocIcp
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV: For SSL certs issued under this root both the Organization and the ownership/control of the Domain Name are verified. CP Section 3 declares that the CPS for each sub-CA must include the following sections: 3.1.8. Method to prove possession of private key 3.1.9. Authentication of the identity of an individual 3.1.9.1. Documents for identification of an individual 3.1.9.2. Information in the certificate issued to an individual 3.1.10. Authentication of the identity of an organization 3.1.10.1. General 3.1.10.2. Documents for identification of an organization 3.1.10.3. Information in the certificate issued to an organization 3.1.11. Authentication of the identity of equipment or application 3.1.11.1. General 3.1.11.2. Procedures for identification of equipment or application 3.1.11.3 - Information contained in the certificate issued to a device or application CPS of CA-root section 3.1.8, Identification of an organization: The identification of a CA by the CA Root is executed through the procedures described in the document CRITERIA AND PROCEDURES FOR ACCREDITATION BODIES OF MEMBERS OF ICPBRASIL [6]. CPS Requirements for sub-CA Section 3.1.9, Authentication of the identity of an individual To verify the identity of an individual, the CPS documents of the sub-CAs must include the following in section 3.1.9: This item should be defined the procedures employed by RA bound for the confirmation of identity of an individual. This confirmation should be performed by the physical presence of the person with based on the identification documents legally accepted. CPS Requirements for sub-CA Section 3.1.10, Authentication of the identity of an organization To verify Organization, the CPS documents of the sub-CAs must include the following in section 3.1.10: Confirmation of the identity of a legal person should be made by presentation of at least the following documents: a.i) “if legal person (company) established or authorized its creation by law, copy of act Establishing and CNPJ;” The CPS documents of the sub-CAs must also include the following in section 3.1.10.3: Should be made to confirm the identity

	of the organization and individuals in the following terms: a) submission of the list of documents listed in Section 3.1.10.2; b) submitting the list of documents listed in Section 3.1.9.1 (s) representative (s) legal (s) of the corporation and of the use of the certificate; c) physical presence of the use of the certificate and signature of the guarantee in respect of which item 4.1.1 and d) the physical presence of the representative (s) (s) legal (s) of the person and the signature of the legal term for ownership of which item 4.1.1. CPS Requirements for sub-CA section 3.1.11, Authentication of the identity of equipment or application To verify Domain Ownership, the CPS documents of the sub-CAs need to include the following in sections 3.1.11 and 3.1.11.2: For certified equipment or application using the URL field Common Name must be verified if the applicant holds the certificate of registration of domain name with the competent body, or has permission from the owner field to use that name. In this case must be presented documentation (term of authorization for use of domain or similar) signed by the holder of the domain. For example: in Brazil we consult WHOIS service E-mail is optional, except AC-SRF is mandatory. When mandatory or person asked for use e-mail address. It is also a part of the issuance of the certificate, the user to receive a PIN (PIN1) in RA and another PIN (PIN2) to be sent to e-mail. You can confirm in the CPS documents of the sub-CAs (item 3.1.10 and 3.1.11) AC-Caixa: https://icp.caixa.gov.br/repositorio/DPCACCAIXAPF.pdf AC-Certisign:http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_Certisign_Multipla_v3.0.pdf AC-Serpro:https://ccd.serpro.gov.br/serproacf/docs/dpcserproacf_v2.0.pdf AC-PR: https://ccd.serpro.gov.br/ACPR/docs/dpcacpr.pdf AC-SERASA: http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf AC-Imprensa-Oficial-Estado-SãoPaulo: http://www.imprensaoficial.com.br/PortalIO/Certificacao/downloads/pdf/RFB/DPC_AC_IMESP_RFB_v3.0.pdf AC-Jus (AC-CAIXA-Jus):https://icp.caixa.gov.br/repositorio/DPCACCAIXAJUS.pdf AC-SRF: http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf
EV policy OID(s)	Not EV
AUDIT	Audit Type: ETSI TS 101 456 and ETSI TS 102 042 Auditor: ICP-Brasil Management Committee Auditor Website: http://www.iti.gov.br/twiki/bin/view/Main/ComiteGestor Audit Report: confidential (Currently working on an independent audit, which will be funded and published in 2010. Request is to proceed with current info, and public audit report will be provided as soon as possible.) I understand that the audit report may be confidential, but could someone from the audit committee provide a statement that an audit was provided over a specific time frame, what criteria was used (including ETSI 101 456 and ETSI 102 042), and if any

	issues were found? Comment #63: We have 2 documents about this: a) http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/Resolucao_05.pdf b) http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/RESOLU__O_29_DE_29_01_2004.PDF The references are for the CPS (CA-root), in none of these public documents you are going to find reference the quoted standards. In the auditing to happen in 2010 we will have information of equivalences to the quoted standards. We'll proceed as per the queue for public discussion https://wiki.mozilla.org/CA:Schedule#Queue_for_Public_Discussion This will allow us to proceed through the approval process. However, it is likely that the actual inclusion will be postponed until an audit that meets the requirements of the Mozilla CA Certificate Policy has been provided. The document ICP DOC-ICP-08 v.2.0 defines the practices of auditing adopted (http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-08_-_v_2.0.pdf) The ITI also is responsible for the process of inspection of the Authorities subordinated according to document: http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-09_-_v_2.0.pdf And so, the CA subordinate of 1st level are audited by the ITI itself. The CA subordinate of 2nd level are audited by the ITI and independent auditing. The independent auditing accredited by the ITI previously. The RA also are audited by independent auditing accredited by the ITI. The independent accredited auditing is in http://www.iti.gov.br/twiki/bin/view/Certificacao/AuditoriaIndependente The accredited independent auditor follow the requisites of auditing predicted in the Resolution 44 of ICP-Brasil available in http://www.iti.gov.br/twiki/pub/Certificacao/AuditoriaIndependente/RESOLU__O_44_DE_18_04_2006II.pdf Statement about ICP-Brazil's auditing procedures: https://bug438825.bugzilla.mozilla.org/attachment.cgi?id=374501 Meantime due to operational questions of budget and planning, this auditing will be contracted and executed only in 2010. So, we will be able to ask the emission of declaration of agreement with the Brazilian standards of digital certification (CPS, PC and PS) and the equivalences to international standards, especially ETSI TS 101 456 V1.4.3 (2007-05) and ETSI TS 102 042 V1.3.4 (2007-12) demanded by the Mozilla Foundation. We are planning to launch the chain V2 this year. It is to prevent ICP Brazil of an eventual crash of the SHA-1 algorithm,

	according directions of the NIST.

Review CPS sections dealing with subscriber verification (section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - The CPS documents of the sub-CAs are required to have section 3.1.11.2: "For certified equipment or application using the URL field Common Name must be verified if the applicant holds the certificate of registration of domain name with the competent body, or has permission from the owner field to use that name. In this case must be presented documentation (term of authorization for use of domain or similar) signed by the holder of the domain."
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Not requesting email trust bit at this time.
- Verify identity info in code signing certs is that of subscriber
    - Not requesting code signing trust bit at this time

Flag Problematic Practices

http://wiki.mozilla.org/CA:Problematic_Practices

- Long-Lived Domain-Validated SSL certs
    - Not applicable within ICP-Brasil. For sub-CAs, see 438825-subCA-review.pdf.
- Wildcard DV SSL certs
    - Not applicable within ICP-Brasil. For sub-CAs, see 438825-subCA-review.pdf.
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA
    - The CA root is off-line. All certificates are issuing through a subordinate CA (2º level).
- Allowing external entities to operate subordinate CAs
    - The ITI authorizes, supervises and audits the operations of CAs (1º level) like table **https://bugzilla.mozilla.org/attachment.cgi?id=342298**
    - The completely document is here http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-08_-_v_2.0.pdf
    - Each CA (1º and 2º level) has CP/CPS approved by the ITI.
- Distributing generated private keys in PKCS#12 files
    - Not applicable within ICP-Brasil. For sub-CAs, see 438825-subCA-review.pdf.
- Certificates referencing hostnames or private IP addresses
    - Not applicable within ICP-Brasil. For sub-CAs, see 438825-subCA-review.pdf.