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

A root with externally-operated sub-CAs needs to provide the following information in their CPS or contractually with the company operating the sub-CA.

Info Needed	Data
Root Name	Autoridade Certificadora Raiz Brasileira
List of all of the Subordinate CA's operated by third parties	http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp The 8 CAs (1º level) are externally operated by anothers 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/), Poder Judiciário Brasileiro (http://www.acjus.gov.br/). Imprensa Oficial do Estado de São Paulo (http://www.imprensaoficial.com.br/PortalIO/Certificacao/Sobre/Apresentacao_7_0.aspx),
Requirements (technical and contractual) for subordinate CAs in regards to whether or not subordinate CAs are constrained to issue certificates only within certain domains, and whether or not subordinate CAs can create their own subordinates.	Determined on a per-sub-CA basis. CP: http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-04_-_v_2.0.pdf CPS: http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-01_-_v_3.0.pdf Certification Practice Statement pointer: http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf
Requirements for sub-CAs to take reasonable measures to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	Currently only requesting the websites (SSL/TLS) trust bit. This is not specified in the ICP-Brasil CP/CPS. ICP-Brasil should add a section stating controls that sub-CAs must have in place in regards to verifying that the domain is owned/controlled by the subscriber.
Whether or not the root CA audit includes the sub-CAs. Audit requirements for subordinate CAs with regard to the frequency of audits and who can/should perform them, as per sections 8, 9, and 10 of	The sub-CAs are working on an independent audit, but it will not be available until 2010. The ITI authorizes, supervises and audits the operations of CAs (1º level) like table https://bugzilla.mozilla.org/attachment.cgi?id=342298 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 Mozilla CA policy.	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 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

The 8 CAs (1º level) are externally operated by other organizations:

Sub-CA	**Details provided below**	**Issues sub-CAs**	**Are SSL certs OV?**	**Verifies Domain Ownership / Control**	**Applicable Problematic Practices**	**Audited?**
CAIXA	Yes	Yes internal	Yes	Yes	None	?
SERPRO	Yes	Yes internal	Yes	Yes	None	Annually
SERASA	Yes	Yes 2 internal **1 external**	Yes	Yes	Delegation of Domain / Email validation to third parties. In Brazil, Registration Authorities (RA) perform such functions. Acording to ICP-Brasil regulation, RA contract and conduct their own audit process, but the audit reports are presented to the related CA.	Planned for this year
Certisign	Yes	No	Yes	Yes	Delegation of Domain / Email validation to third parties.	Annually

					Authentication procedures are defined in DPC_AC_Certisign_Multipla_v3.0.pdf	
Secretaria da Receita Federal	No	?	?	?	?	?
Presidência da República	No	?	?	?	?	?
Imprensa Oficial do Estado de São Paulo	No	?	?	?	?	?
Poder Judiciário Brasileiro	No	?	?	?	?	?

Details for each sub CA are provided in the following tables.

CAIXA

Info Needed	Data
Sub-CA Company Name	**CAIXA ECONOMICA FEDERAL (CAIXA)**
Sub-CA Corporate URL	http://www.caixa.gov.br
Cert Download URL	https://icp.caixa.gov.br/repositorio/ACCAIXA.cer
CA hierarchy under the sub-CA.	The CA CAIXA signs the CA CAIXA PF (certificates for individuals) and the CA CAIXA PJ (certificates for legal representatives of companies). These CA are part of Brazil´s official PKI (ICP-Brasil). The link http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/AC_CEF_-_site.pdf contains a chart that represents the CA CAIXA and its sub-CAs.
CP/CPS	http://icp.caixa.gov.br/asp/repositorio.asp (all documents) https://icp.caixa.gov.br/repositorio/DPCACCAIXA.pdf https://icp.caixa.gov.br/repositorio/DPCACCAIXAPF.pdf https://icp.caixa.gov.br/repositorio/DPCACCAIXAPJ.pdf https://icp.caixa.gov.br/repositorio/DPCACCAIXAJUS.pdf https://icp.caixa.gov.br/repositorio/PCACCAIXA.pdf https://icp.caixa.gov.br/repositorio/PCA1ACCAIXAPF.pdf https://icp.caixa.gov.br/repositorio/PCA3ACCAIXAPF.pdf https://icp.caixa.gov.br/repositorio/PCA1ACCAIXAPJ.pdf https://icp.caixa.gov.br/repositorio/PCA3ACCAIXAPJ.pdf https://icp.caixa.gov.br/repositorio/PCA1AC-CAIXAJUS.pdf https://icp.caixa.gov.br/repositorio/PCA2AC-CAIXAJUS.pdf https://icp.caixa.gov.br/repositorio/PCA3AC-CAIXAJUS.pdf https://icp.caixa.gov.br/repositorio/PCS1AC-CAIXAJUS.pdf https://icp.caixa.gov.br/repositorio/PCS2AC-CAIXAJUS.pdf https://icp.caixa.gov.br/repositorio/PCS3AC-CAIXAJUS.pdf

Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates. DV: Organization attribute is not verified. Only the Domain Name referenced in the certificate is verified to be owned/controlled by the subscriber. OV: Both the Organization and the ownership/control of the Domain Name are verified.	OV
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	domain ownership/control (Extract from https://icp.caixa.gov.br/repositorio/DPCACCAIXAPF.pdf) 3.1.11.2. Procedures for identification of equipment or application 3.1.11.2.1. For licenses to use equipment or application URL in the Common Name field must be verified if the applicant holds the certificate of registration of the domain name from the competent body, or has permission of the holder of the domain to use that name. In this case must be presented related documentation (term of authorization for use of domain or similar) duly signed by the holder of the domain. email address ownership/control Not applicable. The certs are used for signatures only. From CAIXA: And about e-mail certificate, there is a list below with the use purposes of our certificates, extracted from CA CAIXA PF CPS. (https://icp.caixa.gov.br/repositorio/DPCACCAIXAPF.pdf) 6.1.9. Use purposes of the key (as the "key usage" in X.509 v3) 6.1.9.1 The private keys of the holders of certificates issued by the CA CAIXA PF can be used for digital signature, as specified in its corresponding CP. 6.1.9.2 Certificates of signature are used in applications such as confirmation of identity on the web, email, online transactions, virtual private networks, cipher session keys and signature of electronic documents with verification of integrity of their information. 6.1.9.3 The private key of the CA CAIXA PF is only used for the signature of certificates issued by it and its LCR. digitally signing code objects The sub-CA CAIXA PF and the sub-CA CAIXA PJ doesn´t issue certificates for code-signing.

Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	Long-lived DV certificates Not applicable. CA CAIXA does not issue DV certificates. All certificates issued are OV. Wildcard DV SSL certificates Not applicable. CA CAIXA does not issue Wildcard certificates. Delegation of Domain / Email validation to third parties Domain and Email validation are incorporated into the issuing of CA CAIXA procedures. There are no third parties involved on these procedures. Issuing end entity certificates directly from roots Not applicable. CAIXA's hierarchy is composed by an Intermediate CA. Allowing external entities to operate unconstrained subordinate CAs Not applicable. All CAIXA's subordinated CAs is operated by its own IT infrastructure. Distributing generated private keys in PKCS#12 files Not applicable. Each subscriber must generate its own private key. 6.1.1. Generation of pair of keys 6.1.1.1 The key pair of the CA CAIXA PF generated in hardware cryptographic module to FIPS140-1 standard security level 2, using RSA algorithm to generate the key pair and 3-DES algorithm for their protection. 6.1.1.2 Pairs of keys are generated only by the holder of the certificate. Following the instructions contained on the website of the CA CAIXA PF, the applicant generates his pair of keys and request the PKCS # 10 format, which is submitted to the CA CAIXA. 6.1.1.3 The CP implemented by CA CAIXA PF defining the medium used to store the private key, based on requirements established by the document MINIMUM REQUIREMENTS FOR THE CERTIFICATE POLICIES OF ICPBRASIL (http://www.iti.gov.br). (Extract from https://icp.caixa.gov.br/repositorio/DPCACCAIXAPF.pdf) Certificates referencing hostnames or private IP addresses Not aplicable. In an Equipment or application certificate, the CN identifier contains the correspondent URL or application name. OCSP Responses signed by a certificate under a different root Not applicable. CAIXA doesn't permit Indirect OCSP Responses. CRL with critical CIDP Extension Not applicable. CAIXA doesn't issue certificates with CIDP extension. Generic names for CAs It's not a CPS requirement, but by internal procedure, CAIXA always includes the term "CAIXA" in their CAs. CAIXA ECONOMICA FEDERAL, or just CAIXA, is a very strong and known brand in Brazil. Founded in the year of 1861, CAIXA is one of the biggest banks in Brazil.
If the root CA audit does not include this sub-CA, then for this sub-CA provide a	

publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	
CRL update frequency for end-entity certificates.	

SERPRO

Info Needed	Data
Sub-CA Company Name	**SERPRO** – Serviço Federal de Processamento de Dados The Federal Service of Data processing - SERPRO is a public company, tied with the Treasury department.
Sub-CA Corporate URL	http://www.serpro.gov.br http://www.serpro.gov.br/servicos/certificacao_digital
Cert Download URL	https://ccd.serpro.gov.br/acserpro/docs/serprov2.crt https://ccd.serpro.gov.br/acserpro/docs/serprofinalv2.crt
CA hierarchy under the sub-CA.	http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/AC_SERPRO_-_site.pdf The AC Serpro intermediate CA signs subordinate CAs: AC Serpro ACF and ACProderJ. The AC Serpro ACF sub-CA signs certificates for end-users. I think the ACProderJ is used to sign certificates for the RAs. From Serpro: The Final Authority Certifier of SERPRO (SERPROACF) is an second level CA, signed by the first level Authority Certifier, ACSERPRO, that is signed by the root Authority Certifier of ICP-Brazil. The SERPROACF possess in its structure six agencies for approval of certificate for final users. The SERPROACF emits certificates for final users, these certificates is in compliance with the format defined for standard ITU X.509 and is defined in version 3, in accordance with the profile established in RFC 3280.
CP/CPS	Serpro Intermediate CA, signed by ICP-Brazil: https://ccd.serpro.gov.br/acserpro/docs/DPC%20ACSERPRO%20v1.0.pdf https://ccd.serpro.gov.br/acserpro/docs/PC%20ACSERPRO%20v1.0.pdf Serpro ACF sub-CA, signed by Serpro CA: https://ccd.serpro.gov.br/serproacf/docs/dpcserproacf_v2.0.pdf

	https://ccd.serpro.gov.br/serproacf/docs/pcserproacfA1_v2.0.pdf https://ccd.serpro.gov.br/serproacf/docs/pcserproacfA3_v2.2.pdf https://ccd.serpro.gov.br/acserprospb/
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates. DV: Organization attribute is not verified. Only the Domain Name referenced in the certificate is verified to be owned/controlled by the subscriber. OV: Both the Organization and the ownership/control of the Domain Name are verified.	OV ◦ As stated on the CPS (DPC SERPROACF) item 3.1.11.1.2 “If the ownership of the Domain Name is a natural person, a confirmation of identity has to be done as stated on Item 3.1.9.1 and the natural person has to sign the Term as stated on item 4.1.1”. ◦ As stated on the CPS (DPC SERPROACF) item 3.1.11.1.3, “if the ownership of the Domain Name is a Juridical Person, a confirmation of the organization identity and the representative natural person by the presentation of the documentation as stated on item 3.1.10.2 and 3.1.9.1 and the physical presence of the representative Natural Person or the Juridical Person and the Term of Ownership and Responsibility signed by the representative natural person or Juridical Person”.
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	Domain ownership/control ◦ As stated on the CPS (DPC SERPROACF) item 3.1.11.2 “For equipments certificates that uses URL in the common name, to verify the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate or has been authorized by the domain registrant to act on the registrant's behalf, in this case should present the documentation signed by the owner of the domain”. Email address ownership/control ◦ When a request of certificate is submitted by the interested entity, a Term of Ownership and Responsibility is printed out and the entity has to sign out on a presence of the Authority Register, saying that all the information including the email address of the entity are truth, as stated on the CPS (DPC SERPROACF) item 4.1.1 c. ◦ The required documentation for the process are stated on the CPS (DPC SERPROACF) item 3.1.9.1 as follow: a) ID card, b)National ID card, for foreign living in Brazil, c)Passport, for foreign not living in Brazil, d) Proof of Residency. ◦ Also, to request a certificate, the entity has to fill up a form with: a) Name, b) Date of Birth, c) Email address. ◦ All the documentation is checked by the Register Authority. Digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate ◦ When a request of certificate is submitted by the interested entity, a Term of Ownership and Responsibility is printed out and the entity has to sign out on a presence of the Authority

	Register, saying that all the information included in the form are truth, as stated on the CPS (DPC SERPROACF) item 4.1.1 c.
Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	None are applicable.
If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	The sub-CAs audit are done independently of the root CA and are done by the root CA or third parties Audit Company appointed by the root CA. Annually.
CRL update frequency for end-entity certificates.	http://ccd.serpro.gov.br/lcr/acserpro.crl Stated on CPS (DPC SERPROACF), item 4.4.9.2, "The maximum update frequency is 6 hours". Stated on CPS (DPC SERPROACF), item 4.4.3.3, "The maximum time for a cert revoke is every 12 hours.

SERASA

Info Needed	Data
Sub-CA Company	**Serasa S.A.**
Sub-CA URL	http://www.serasa.com.br/us/index.htm (English)
Cert URL	http://publicacao.certificadodigital.com.br/suporte/serasacdv1.cer
CA hierarchy under the sub-CA.	Serasa CA direct under ICP-Brasil root (Serasa Autoridade Certificadora Principal) is allowed to issue sub-CAs. Serasa S.A. has 3 sub-CAs. - Serasa Autoridade Certificadora (belongs to Serasa) signing certificates to banks - Serasa Certificadora Digital (belongs to Serasa) website, email, code signing, signing and encryption certificates. - AC Fenacor (external third party) signing certificates

	Federação Nacional dos Corretores de Seguros Privados e de Resseguros, de Capitalização, de Previdência Privada e das Empresas Corretoras de Seguros e de Resseguros (AC Fenacor)
CP/CPS	http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a1.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a2.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a3.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a4.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s1.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s2.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s3.pdf http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s4.pdf
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates.	IV/OV http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf Section 3.1.1 (Google Translate) Validation of the request for certificate - comprises the steps, performed by the presence the physical person, based on the identification documents mentioned in items 3.1.9, 3.1.10 and 3.1.11: i. confirmation of the identity of an individual: evidence that the person who presents himself as or certificate holder for or as legal representative of a juridical person is that the data are really in the documentation submitted; ii. confirmation of the identity of an organization: evidence that the documents submitted actually refer to the legal holder of the certificate and that the person who presents as legal representative of the legal person truly has such a provision; iii. issuing the certificate: Conference of the data request with the certificate in the documents and release of issue in the system of AC 3.1.9.1. Documents for identification of an individual Must be submitted the following documentation in its original version, for identification of a individual requesting the certificate: a) Identity or Passport ballot, if Brazil; b) National Foreign Portfolio - CNE, if foreign domiciled in Brazil; c) Passport, alien is not domiciled in Brazil; d) if the above documents have been shipped more than 5 (five) years or have no photo, a recent color photograph or an identity document with photo color, is given a maximum five (5) years from the date of validation presence;

	e) proof of residence or domicile, issued for at most 3 (three) months from the date of validation presence and f) another official document with photo, in case of license types A4 and S4. 3.1.10.2. Documents for identification of an organization Confirmation of the identity of a corporation should be made upon presentation of at least the following documents: a) Related to their legal qualification: i. if legal person established or authorized its creation by law, a copy of the constitutive act and CNPJ; ii. private entity if: 1. act of incorporation, duly registered with the competent body and 2. documents of the election of its directors, where applicable; b) on its tax qualification: i. proof of registration in the National Register of Legal Persons - CNPJ or ii. proof of registration in the Register of Specific Social Security - CIS.
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf (Google Translate) domain ownership/control We check the ownership of the domain name at FAPESP, domain name Brazilian responsable (http://www.fapesp.org/). 3.1.11.2. Procedures for identification of equipment or application For licenses to use equipment or application URL in the Common Name field should be whether the applicant holds the certificate of registration of the domain name from the national authority, or if you have permission of the holder of the domain to use that name. In this case must be presented presented related documentation (term of authorization to use domain or similar) duly signed by holder of the domain. email address ownership/control SERASA] We don´t have this description on our CP/CPS There is no reference in CP/CPS digitally signing code objects There is no reference in CP/CPS
Review the CP/CPS for potentially	We detected that only “Delegation of Domain / Email validation to third parties” is a potentially

problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	problematic practice. InBrazil, Registration Authorities (RA) perform such functions. Acording to ICP-Brasil regulation, RA contract and conduct their own audit process, but the audit reports are presented to the related CA. Audit process is regulated by ICP-Brasil as below: a) audit companies request a registration to operate in ICP-Brasil infra-structure b) RA and CA contract the audit company and presents to ITI the audit schedule c) ITI approves the audit schedule d) RA or CA send the audit report to ITI e) ITI analizes the audit report
If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	Serasa contract and conduct their own audit process . Audit process is regulated by ICP-Brasil as below: f) audit companies request a registration to operate in ICP-Brasil infra-structure g) RA and CA contract the audit company and presents to ITI the audit schedule h) ITI approves the audit schedule i) RA or CA send the audit report to ITI j) ITI analizes the audit report We don´t have any of this audit reports right now. We are analizing have one of them in 1 year.
CRL update frequency for end-entity certificates.	http://publicacao.certificadodigital.com.br/repositorio/lcr/serasacdv1.crl 4.4.9.2. The maximum frequency allowed for the issuance of CRL for the certificates of end users is 6 hours.

Certisign

Info Needed	Data
Sub-CA Company	**Certisign Certificadora Digital S.A**.
Sub-CA URL	http://www.certisign.com.br
Cert URL	http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Multipla_G3.cer
CA hierarchy under the sub-CA.	This sub-CA only issues end-entity certificates.
CP/CPS	http://icp-brasil.certisign.com.br/repositorio/dpc http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_Certisign_Multipla_v3.0.pdf http://icp-brasil.certisign.com.br/repositorio/pc/AC_Certisign_Multipla/PC_A1_AC_Certisign_Multipla_v2.3.pdf

Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates.	OV DPC_AC_Certisign_Multipla_v3.0.pdf 3.1.11. Authentication of Equipment Identify or Equipment Application 3.1.11.1. General Resolutions 3.1.11.1.1. Regarding certificates issued for equipment or application, the titular is the natural person or the legal entity that claims the certificate, who indicates the responsible for the private key. 3.1.11.1.2. If the titular be natural person, your identity is confirmed as written in the item 3.1.9.1 and it signs the titular term regarding the item 4.1.1.
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	DPC_AC_Certisign_Multipla_v3.0.pdf domain ownership/control 3.1.11.2. Procedures for identification purposes of an equipment or application For equipment certificates or application certificates that use URL in Common Name, is verified if the certificate applicant detain the domain name register with the relevant agency, or if it has titular domain authorization for using that name. In this case it's showed evidential documentation (term of authorization term of domain or similar) properly signed by the titular of domain.
Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	Long-lived DV certificates Not applicable. Certisign does not issue DV certificates. All production certificates are OV. Wildcard DV SSL certificates Not applicable. Certisign does not issue Wildcard certificates. Delegation of Domain / Email validation to third parties Authentication procedures are defined in DPC_AC_Certisign_Multipla_v3.0.pdf Issuing end entity certificates directly from roots Not applicable. Certisign's hierarchy are composed by an Intermediate CA. Allowing external entities to operate unconstrained subordinate CAs Certisign only issues end-entity certs from this sub-CA. Distributing generated private keys in PKCS#12 files Not applicable. Each subscriber must generate its own private key as per PC_A1_AC_Certisign_Multipla_v2.3.pdf Certificates referencing hostnames or private IP addresses PC_A1_AC_Certisign_Multipla_v2.3.pdf 7.1.2.8 Certisign Múltipla CA Implements the extension Authority Information Access, not critical, including the access address to the On-line Certificate

	Status Protocol service (http://ocsp.certisign.com.br). OCSP Responses signed by a certificate under a different root Not applicable. Certisign does not permit Indirect OCSP Responses. CRL with critical CIDP Extension Not applicable. Certisign doesn't issue certificates with CIDP extension. Generic names for CAs It's not a CPS requirements, but by internal procedure, Certisign always includes the term "Certisign" in their CAs.
If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	The root CA audit includes this sub-CA and it is done annually.
CRL update frequency for end-entity certificates.	http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl DPC_AC_Certisign_Multipla_v3.0.pdf, 4.4.9.2. The CRL update frequency is 1 (one) hour.

Secretaria da Receita Federal

Info Needed	Data
Sub-CA Company	**Secretaria da Receita Federal**
Sub-CA URL	http://www.receita.fazenda.gov.br/
Cert URL	http://www.receita.fazenda.gov.br/acsrf/acsrfv1.crt
CA hierarchy under the sub-CA.	
CP/CPS	http://www.receita.fazenda.gov.br/acsrf/index.htm (all documents) http://www.receita.fazenda.gov.br/acsrf/DPCACSRFv2.1.pdf
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates.	
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of	

http://www.mozilla.org/projects/security/certs/policy/.	
Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	
If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	
CRL update frequency for end-entity certificates.	http://www.receita.fazenda.gov.br/acsrf/acsrfv1.crl

Presidência da República

Info Needed	Data
Sub-CA Company	**Presidência da República**
Sub-CA URL	http://www.presidencia.gov.br/ingles/
Cert URL	http://acraiz.icpbrasil.gov.br/credenciadas/AC_PR_20092006.crt
CA hierarchy under the sub-CA.	
CP/CPS	AC-PR: http://www.planalto.gov.br/ACPR/ (all documents) CPS: http://www.planalto.gov.br/ACPR/pdf/DPCACPR.pdf CP (A3): http://www.planalto.gov.br/ACPR/pdf/PCACPR_A3.pdf
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates.	
The section numbers and text (in	

English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	
Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	
If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	
CRL update frequency for end-entity certificates.	http://ccd.serpro.gov.br/lcr/ACPRv1.crl

Imprensa Oficial do Estado de São Paulo

Info Needed	Data
Sub-CA Company	**Imprensa Oficial do Estado de São Paulo**
Sub-CA URL	http://www.imprensaoficial.com.br/PortalIO/Certificacao/Sobre/Apresentacao_7_0.aspx
Cert URL	http://icp-brasil.certisign.com.br/repositorio/certificados/AC_IMESP.cer
CA hierarchy under the sub-CA.	
CP/CPS	http://www.imprensaoficial.com.br/PortalIO/Certificacao/Sobre/Repositorio_7_6.aspx CPS: http://icp-brasil.certisign.com.br/repositorio/dpc/AC_IMESP/DPC_AC_IMESP_v3.0.pdf
Identify if the SSL certificates chaining	

up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates.	
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	
Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	
If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	
CRL update frequency for end-entity certificates.	http://icp-brasil.certisign.com.br/repositorio/lcr/ACImprensaOficialSP/LatestCRL.crl

Poder Judiciário Brasileiro

Info Needed	Data
Sub-CA Company	**Poder Judiciário Brasileiro**
Sub-CA URL	http://www.acjus.gov.br/
Cert URL	http://www.acjus.gov.br/repositorio/certificados_lcr/cert_acjus.cer

CA hierarchy under the sub-CA.	
CP/CPS	http://www.acjus.gov.br/repositorio (all documents) CPS: http://www.acjus.gov.br/acjus/dpcacjus.pdf
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates.	
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.	
Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	
If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	
CRL update frequency for end-entity certificates.	http://www.acjus.gov.br/acjus/acjusv1.crl