CAIXA	**Title:** **Subordinate CAs Operated by Third Parties For External Use – Mozilla**	**Date:** **04/22/2009**

Subordinate CAs Operated by Third Parties For External Use

This section applies when your root signs subordinate CAs for companies who use the sub-CA to sign other sub-CAs or certificates for other companies or individuals not affiliated with their company. For instance, this section applies to you if your root issues sub-CAs that are used by Certificate Service Providers (CSP).

In addition to the information listed above, you will also need to provide the following information for each CSP.

1. Sub-CA Company Name

CAIXA ECONOMICA FEDERAL (CAIXA)

2. Sub-CA Corporate URL

http://www.caixa.gov.br

3. Sub-CA cert download URL

https://icp.caixa.gov.br/repositorio/ACCAIXA.cer

4. General CA hierarchy under the sub-CA.

The General CA hierarchy is already provided by the ITI.

5. Sub-CA CP/CPS Links

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

6. The section numbers and text (in English) in the CP/CPS that demonstrate that reasonable measures are taken 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 our Mozilla CA certificate policy.

- **domain ownership/control**

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.
(Extract from https://icp.caixa.gov.br/repositorio/DPCACCAIXAPF.pdf)

- **email address ownership/control**

There is no reference in CP/CPS.

- **digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate**

There is no reference in CP/CPS.

7. Identify if the SSL certificates chaining up to the sub-CA 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.**

SSL certificates that chains up to the sub-CA are OV.

8. Review the CP/CPS for Potentially Problematic Practices. 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 FIPS 140-1 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.

9. 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 our Mozilla CA certificate policy.

The root CA audit includes this sub-CA and it is done annually.

10. Provide information about the CRL update frequency for end-entity certificates. There should be a statement in the CP/CPS that the sub-CA must follow to the effect that the CRL for end-entity certs is updated whenever a cert is revoked, and at least every 24 or 36 hours.

4.4.9. Frequency of issuing CRL
4.4.9.1 The CA CAIXA PF's CRL is updated at most every 6 (six) hours.
4.4.9.2 The serial numbers of certificates of any entity that is final deleted will appear in the CRL issued by the CA CAIXA PF. These figures remain CRL issued until the expiration date of certificates be achieved, being removed from the first CRL issued after the date of their expirations.
4.4.9.3 CRL is issued every 6 (six) hours, even when there is no change or update, to ensure the periodicity of the information.

(Extract from https://icp.caixa.gov.br/repositorio/DPCACCAIXAPF.pdf)