Subordinate CAs Operated by Third Parties For Internal Use

1. **General description of the sub-CAs operated by third parties.**

The Federal Service of Data processing - SERPRO is a public company, tied with the Treasury department. Created on 1º of December of 1964, for the Law nº 4,516, with the objective to modernize and to give to agility the strategical sectors of the Brazilian Public Administration. The Company, whose business is the rendering of services in Technology of the Information and Communications for the public sector, is considered one of the biggest Organizations of the sector, in Latin America.

The Serpro was the first authority certifier credential for ICP-Brazil. The company searches since the creation of its Center of Digital Certification - CCD, in 1999, to divulge the use of this technology for the some segments with that it works.

The Serpro is the first Brazilian public company to conquer the certification British Standard 7799, known as BS7799, the certification was granted to the Serpro for the operation services, maintenance of the Authorities Certifiers produced in the Serpro, between them and the SERPROACF.

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. The SERPROACF implements version 2 of standard ITU X.509 for the Certificate Revocation Lists (CRL), and the frequency of emission of these lists is of 60 minutes.

2. **The CP/CP Statement that the sub-CAs are required to follow.**

SERPROACF		
CPS	DPC SERPROACF	https://ccd.serpro.gov.br/serproacf/docs/dpcserproacf_v2.0.pdf
CP	PC SERPROACF A1	https://ccd.serpro.gov.br/serproacf/docs/pcserproacfA1_v2.0.pdf
CP	PC SERPROACF A3	https://ccd.serpro.gov.br/serproacf/docs/pcserproacfA3_v2.2.pdf
CP	PC SERPROACF-SPB	https://ccd.serpro.gov.br/acserprospb/

3. **Requirements (technical and contractual) for sub-CAs in regards to whether or not sub-CAs are constrained to issue certificates only within certain domains, and whether or not sub-CAs can create their own subordinates.**

- As stated on the CPS (DPC SERPROACF) item 3.1.2.2., "The SERPROACF does not issue certificates for subordinates".

4. **Requirements (typically in the CP or CPS) 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 our Mozilla CA certificate 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.

5. **Description of audit requirements for sub-CAs (typically in the CP or CPS)**

- **Whether or not the root CA audit includes the sub-CAs**.
  - 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.

- **Who can perform the audits for sub-CAs.**
  - The root CA or third parties Audit Company appointed by the root CA.

- **Frequency of the audits for sub-CAs.**
  - Annually

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).

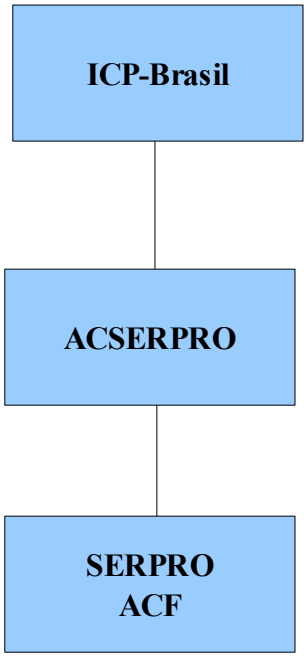
In addition to the information listed above, you will also need to provide the following information for each CSP.

1. **Sub-CA Company Name**
   SERPRO – Serviço Federal de Processamento de Dados

2. **Sub-CA Corporate URL**
   www.serpro.gov.br

3. **Sub-CA cert download URL**
   https://ccd.serpro.gov.br/acserpro/docs/serprofinalv2.crt

4. **General CA hierarchy under the sub-CA.**



5. **Sub-CA CP/CPS Links**

SERPROACF		
CPS	DPC SERPROACF	https://ccd.serpro.gov.br/serproacf/docs/dpcserproacf_v2.0.pdf
CP	PC SERPROACF A1	https://ccd.serpro.gov.br/serproacf/docs/pcserproacfA1_v2.0.pdf
CP	PC SERPROACF A3	https://ccd.serpro.gov.br/serproacf/docs/pcserproacfA3_v2.2.pdf
CP	PC SERPROACF-SPB	https://ccd.serpro.gov.br/acserprospb/

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**
  - 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.

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.**

Not applicable.

- **OV: Both the Organization and the ownership/control of the Domain Name are verified.**

    - 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”.

8. **Review the CP/CPS for Potentially Problematic Practices. Provide further info when a potentially problematic practice is found.**

    None

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 or third parties Audit Company appointed by the root CA are responsible to perform Audit on the sub-CA SERPROACF, and follow the rules stated on the document DOC-ICP-08 at:

    http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-08_-_v._3.0.pdf.

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.**

    Stated on CPS (DPC SERPROACF), item 4.4.9.2, “The maximum update frequency is 6 hours”. Actually the process occurs in 1 hour.

    Stated on CPS (DPC SERPROACF), item 4.4.3.3, “The maximum time for a cert revoke is every 12 hours.