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 ACSERPRO.

The Authority Certifier of SERPRO (ACSERPRO), is signed by the root Authority Certifier of ICP-Brazil.

The ACSERPRO emits certificates for sub-CA, 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 ACSERPRO implements version 2 of standard ITU X.509 for the Certificate Revocation Lists (CRL), and the frequency of emission of these lists is of 35 days.

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

ACSERPRO		
CPS	DPC ACSERPRO	https://ccd.serpro.gov.br/acserpro/docs/DPC%20ACSERPRO%20v1.0.pdf
CP	PC ACSERPRO	https://ccd.serpro.gov.br/acserpro/docs/PC%20ACSERPRO%20v1.0.pdf

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 ACSERPRO item 1.3.3, " The ACSERPRO only issue certificates for sub-CA's 1 level under the ACSERPRO as well can create their own subordinates, following the rules stated on the CPS ACSERPRO.

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**
        - Not applicable

    - **Email address ownership/control**
        - Not applicable

    - **Digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate**
        - Not applicable

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 only by the root CA.

- **Who can perform the audits for sub-CAs.**
    - 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

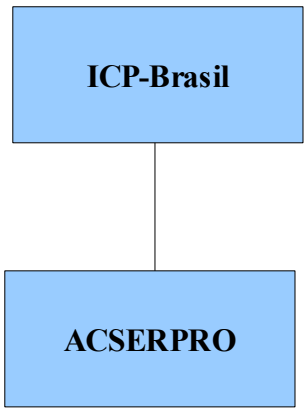
2. **Sub-CA Corporate URL**

   www.serpro.gov.br

3. **Sub-CA cert download URL**

   https://ccd.serpro.gov.br/acserpro/docs/serprov2.crt

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



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

ACSERPRO		
CPS	DPC ACSERPRO	https://ccd.serpro.gov.br/acserpro/docs/DPC%20ACSERPRO%20v1.0.pdf
CP	PC ACSERPRO	https://ccd.serpro.gov.br/acserpro/docs/PC%20ACSERPRO%20v1.0.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**
     - Not applicable
   - **Email address ownership/control**
     - Not applicable
   - **Digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate**
     - Not applicable

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.**
     - Not applicable

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 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 ACSERPRO), item 4.4.9.1, "The maximum update frequency is 45 days".

Stated on CPS (DPC ACSERPRO), item 4.4.3 "The maximum time for a cert revoke is every 24 hours.