Certificate Policy

SERPRO SSL Certification Authority

Server Authentication(SSL/TLS)

(SERPRO SSL CA)

Version 2.0

2020

SERPRO

Contents

Review Control

Ver.	Review Date	Staff	Status	Changes
1.0	2019	Lucia Castelli	Draft	Inicial
1.0	2019	Osni Bunn	Approved	
2.0	2020	Lucia Castelli	Revision	Update *url – Frauds; Updated de* distribution point of CRL: – Section 7.1.2 “d”*;Updated URL OCSP* and OID OV SSL; Update with itens from Resolution 156, 169 and 179 ICP-Brasil.
2.0	2020	Alice Vasconcellos	Approved	

1. INTRODUCTION

1.1. Overview

This document establishes the requirements that must be observed by SERPRO SSL CA, part of the Brazilian Public Key Infrastructure - ICP-Brasil in the elaboration of its Certificate Policy – CP.

CP SERPRO SSL, developed within the scope of ICP-Brasil, must adopt the structure of the MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRASIL (DOC-ICP-04), as well as following the updates of the documents of the WebTrust Principles and Criteria [6] and CA / Browser Forum publications [7].

In the event of any inconsistency between that document and the requirements of the CA / Browser Forum [7], these will take precedence over the document.

The structure of this CP is based on RFC 3647.

This document is part of the ICP-Brasil set and other regulations referenced in the other rules of ICP-Brasil are referenced in it, as specified in item 10.

The type of certificate issued under this CP is Type A1;

1.2. Document Name and Identification

1.2.1. This CP complies with the recommendations of ICP-Brasil for issuing type A1 signature certificates.

1.2.2. After the SERPRO SSL CA, the following OID was assigned to this Certification Policies, within the scope of ICP-Brasil;

Certificate Type	OID
A1	**2.16.76.1.2.1.105.**

1.3. PKI Participants - ICP-Brasil

1.3.1. Certification Authority

SERPRO SSL Certification Authority (SERPRO SSL CA) is part of the Brazilian Public Key Infrastructure, ICP-Brasil, under the hierarchy of the Brazilian Root Certification Authority.

This CP is implemented by the SERPRO SSL Certification Authority whose CPS is published on its website at the following address: https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf.

1.3.2. Registration Authorities

The SERPRO SSL CA operates an internal Registration Authority, located on the same infrastructure as its CA and referred to in this document as SERPRO RA, where all registration procedures are performed directly by RA staff, as described in Section 3.2.
Also, SERPRO SSL CA authorizes a Delegated Third Party to perform a delegated function and contractually require the Delegated Third Party perform that any person in the Certificate Management Process, whether as an employee or agent verify the identity and trustworthiness of such person(item 5.3.1) as well background checks procedures(item 5.3.2.) and Training Requirements and Procedures(item 5.3.3).

The Registration Authority, involved in issuing SSL/TLS certificates, meets and follows the requirements established in sections 4.2 and 5.3 of CPS.

The web page address (URL) of the CA is https://certificados.serpro.gov.br/serprossl, where is possible to refer to the Registration Authority, which is responsible for processes for receiving, validating and forwarding a request for issuance or revocation digital certificates, and identification of their applicants.

Only SERPRO SSL CA performs the domain validation required by section 3.2.2.4 of the Baseline Requirements (BR) and that the task is delegated to third party.

1.3.3. Subscribers

A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

1.3.4. Relying Parties

A Relying party is any natural person or legal entity that relies on a Valid OV SSL Certificate issued by SERPRO SSL CA. Relying Parties are responsible for verifying the validity of the Certificates.

1.3.5. Other Participants

CA uses the Federal Data Processing Service (SERPRO – Serviço Federal de Processamento de Dados) as a Service Provider Support Service - PSS, Biometric Service Provider - PSBio and Service Provider Trust - PSC, as available at: https://certificados.serpro.gov.br/serprossl.

Other groups that participated in the development of the Cab / Browser requirements Forum[15] include AICPA / CICA, which is the task force of WebTrust for AC and ETSI ESI. The participation of such groups does not imply endorsement, recommendation or approval of the final product.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Usage

The certificates issued under this CP are suitable for use only in the applications presented in the table described below:

Certified Policies	Purpose
CP SERPRO SSL CP A1	Certificates issued under this policy are considered suitable for electronic signature, non-retractability, integrity and authentication.

Applications and other programs that support the use of a digital certificate of a certain type, contemplated by ICP-Brasil, must accept any certificate of the same type, or higher, issued by any CA accredited by AC Raiz.

Applications for the certificate defined on this CP must take into account the security level provided for the type of certificate. This level of security is characterized by the minimum requirements defined for aspects such as: cryptographic key size, key storage media, key pair generation process, certificate holder identification procedures, frequency of issuing the corresponding Revoked Certificate List (CRL) and extension of the certificate validity period.

Type A1 certificates are used in applications such as identity verification and electronic document signing with verification of the integrity of your information.

1.4.2. Prohibited Certificate Uses

Certificate use is restricted by using Certificate extensions on key usage and extended key usage.

Any usage of the Certificate inconsistent with these extensions is not authorized

There are no restrictions or prohibitions on the use of certificates issued by that CA.

SSL certificates issued under this CPS do not guarantee that the equipment on which the certificate was installed is not free from defects, malware or viruses.

1.5. Policy Administration

This CPS is administered by SERPRO – Serviço Federal de Processamento de Dados(Brazil) is a government entity of Brazil.

1.5.1. Organization Administering the Document

The organization administering the CP/CPS is SERPRO

1.5.2. Contact Person

a) Subscribers, Relying Parties, Application Software Suppliers, and other third parties can submit an e-mail to:

Name: Pedro Moacir Rigo Motta
Address: SGAN 601, Module V, Asa Norte, Brasília, Federal District, CEP 70.836-900.
Email: certificates@serpro.gov.br
Phone: +556120217957

b) Certificate Problem reports of suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates via e-mail or webpage:

Web page: https://atendimento.serpro.gov.br/certificacaodigital
E-mail: css.serpro@serpro.gov.br
Phone: +55 08007282323

1.5.3. Person Determining CP/CPS Suitability for the Policy

Name: Pedro Moacir Rigo Motta
Phone: +55 61 20217957
Email: certificates@serpro.gov.br

1.5.4. CPS Approval Procedures

ITI(National Institute of Information Technology(https://www.gov.br/iti/en) will approve the CP/CPS, along with any amendments.

Any amendments made to the CP/CPS will be reviewed by the Certificate Policy Authority(ITI) for consistency with the practices that are implemented prior to its approval.

Changes made will be tracked within the revision table - Review Control.

1.6. Acronyms

AICPA American Institute of Certified Public Accountants
ADN Authorization Domain Name CA Certification Authority
BCP Business Continuity Plan
CAME Automatic Certificate Management Environment
CA Raiz - Root Certification Authority of ICP-Brasil
CAA Certification Authority Authorization
ccTLD Country Code Top-Level Domain
CEI INSS Specific Register
CICA Canadian Institute of Chartered Accountants
CMM-SEI Capability Maturity Model from Software Engineering Institute
CMVP Cryptographic Module Validation Program
CN Common Name
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List DBA Doing Business As
DNS Domain Name System
DRP Disaster Recovery Plan
DN Distinguished Name
DMZ Demilitarized Zone

DNS Domain Name System ETSI European Telecommunications Standards Institute ESI Electronic Signatures and Infrastructures EV Extended Validation (WebTrust for Certification Authorities) FIPS (US Government) Federal Information Processing Standard FQDN Fully-Qualified Domain Name IM Instant Messaging GR General Registry – Brazilian ID IANA Internet Assigned Numbers Authority ICANN Internet Corporation for Assigned Names and Numbers ICP-Brasil - Brazilian Public Key Infrastructure IDS Intrusion Detection System IEC International Electrotechnical Commission IETF PKIX Internet Engineering Task Force - Public-Key Infrastructured (X.509) IRP Incident Recovery Plan ISO International Organization for Standardization ITU International Telecommunications Union NIST (US Government) National Institute of Standards and Technology NIS – Brazilian Social Identification Number OCSP Online Certificate Status Protocol OID Object Identifier PKI Public Key Infrastructure OU Organization Unit PASEP - Brazilian Program for the Formation of Public Servants' Heritage PIS - Brazilian Social Integration Program POP Proof of Possession PSBio Biometric Service Provider RFC Request For Comments RA Registration Authority S/MIME Secure MIME (Multipurpose Internet Mail Extensions) SSL Secure Sockets Layer SNMP Simple Network Management Protocol SP Security Policy SSP Support Service Providers TLS Transport Layer Security TSP Trust Service Provider UF Federation Unit URL Uniform Resource Locator VoIP Voice Over Internet Protocol

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The follow items bellow, refer to section 2 of CPS:

2.1. Repositories

2.2. Publication of Certificate Information

2.3. Access Controls on Repositories

2.4. Time or Frequency of Publication

3. IDENTIFICATION AND AUTHENTICATION

The follow items bellow, refer to section 3 of CPS

The follow items bellow refer to section 4 to CPS

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The follow items bellow refer to section 5 of CPS

5.5.1. Types of Records Archived

5.5.2. Retention Period for Archive

5.5.3. Protection of Archive

5.5.4. Archive Backup Procedures

5.5.5. Requirements for Time-Stamping of Records

5.5.6. Archive Collection System (Internal or External)

5.5.7. Procedures to Obtaing and verife Archive Information

5.6. Key Changeover

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

5.7.3. Recovery Procedures After Key Compromise

5.7.3.1. Entity certificate is revoked

5.7.3.2. Entity key is compromised

5.7.4. Business Continuity Capability after Disaster

5.8. CA or RA Termination

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The CA key pair is generated by the CA itself, in a cryptographic hardware module with FIPS 140-1 level 3 security standard, using RSA algorithm for generating the key pair and 3-DES algorithm for its protection, after the approval of the request for accreditation and the subsequent authorization to operate within the scope of ICP-Brasil. The generation is through a ceremony with the participation of CA personnel with a reliable function to execute the key generation script and the participation of qualified auditors.

The Certificate Holder generates the key using applications for this purpose. When the certificate holder is a legal entity, it will indicate by its legal representative (s), the person responsible for the generation of the cryptographic key pairs and for the use of the certificate.

The private key is stored using:

• For individual or legal certificates, the applicant must store the private key with a high level of security, this is protected by a password.

The CA recommends that the private key be backed up, thereby preventing loss of the certificate.

The algorithm to be used for the cryptographic keys of certificate holders adopts the RSA standard as defined in the document ICP-BRASIL STANDARDS AND CRYPTOGRAPHIC ALGORITHMS [1].

The CA rejects a certificate request if the requested public key does not meet the requirements set out in sections 6.1.5 and 6.1.6. If you have a private key, we require the signature suite sha2WithRSA, according to ICP-Brasil guidelines.

When generated, the private key of the titleholder is recorded encrypted, by a symmetric algorithm approved in the document ICP-Brasil STANDARDS AND CRYPTOGRAPHIC ALGORITHMS [1], in the storage medium defined for each type of certificate A1 provided by ICP-Brasil.

The private key travels encrypted, using the same algorithms mentioned in the previous paragraph, between the generating device and the media used for its storage.

The private key storage media ensures, by appropriate technical and procedural means, at a minimum that:

a) the private key is unique and its secrecy is sufficiently assured;

b) the private key cannot, with reasonable security, be deducted and must be protected against forgeries carried out using currently available technologies; and

c) the private key can be effectively protected by the legitimate holder against use by third parties.

This storage medium does not modify the data to be signed, nor does it prevent such data from being presented to the signatory prior to the signature process.

6.1.2. Private Key Delivered to Subscriber

Parties other than the Subscriber not archive the Subscriber Private Key without authorization by the Subscriber.

6.1.3. Public Key Delivery to Certificate Issuer

The certificate request message follows the PKCS # 10 format, which includes, in the message itself, its digital signature, made with the private key corresponding to the public key contained in the request.

Public keys are delivered to the certificate issuer through an online exchange using automatic functions from the CA certification software.

6.1.4. Public Key Available to Certificate Issuer

The ways to make the CA certificate available, and all certificates in the certification chain, to CA certificate issuer include:

a) When a certificate is made available to its subscriber, the PKCS # 7 standard, defined in the STANDARDS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL [9] will be used;

b) CA website https://certificados.serpro.gov.br/serprossl.

c) Other safe means approved by the CG of ICP-Brasil.

6.1.5. Key sizes

The size of the cryptographic keys associated with the certificates issued by the CA is, at least, L = 2048 bits;

The algorithms and the size of the keys used in the different types of ICP-Brasil certificates are defined in the document ICP-BRASIL STANDARDS AND CRYPTOGRAPHIC ALGORITHMS [1].

We require the signature suite sha2WithRSA,according to ICP-Brasil guidelines and modulus size, when encoded, is at least 2048 bits, and the modulus size, in bits, is evenly divisible by 8.

6.1.6. Public Key Parameters Generation and Quality Checking

The parameters for generating asymmetric CA keys follow the pattern defined in the document STANDARDS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL[9].

The CA SERPRO SSL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent is in the range between 2^16 + 1 and 2^256 - 1. The modulus have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

6.1.7. Key Usage Purposes(AS PER X.509 V3 KEY USAGE FIELD)

The certificates issued on this CP have activated the bits digitalSignature e keyEncipherment.

Certificates issued under this policy are considered suitable for electronic signature, non-retractability, integrity and authentication.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The CA's private key is generated, stored and used only on specific cryptographic hardware, therefore there is no traffic at any time.

6.2.1. Cryptographic Module Standards and Controls

The CA's asymmetric key generation cryptographic module adopts the standard defined in the document STANDARDS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL[9].

The certificate subscribers' cryptographic key generation modules are those defined in the document STANDARDS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL[9] - Each implemented CP specifies the additional applicable requirements.

6.2.2. Private Key (n out of m) Multi-person Control

6.2.2.1. The CA implements multiple control for the activation and deactivation of its private key through physical access controls and the certification software.

6.2.2.2. A minimum of 2 (two) subscribers of the activation key (“n”) from a group of 15 (fifteen) (“m”) is required to activate the CA key.

6.2.3. Private Key Escrow

SERPRO SSL CA does not escrow Private Keys for any reason.

6.2.4. Private key backup

Any certificate holder may, at its discretion, keep a backup copy of its own private key.

The CA does not keep a backup copy of the private key of the holder of a digital signature certificate issued by it.

6.2.5. Private Key Archival

The private keys of the certificate subscribers issued by the CA are not archived.

Archiving is defined as storing the private key for future use, after the period of validity of the corresponding certificate.

6.2.6. Private Key Transfer into or from a Cryptographic Module

The CA's private key is inserted into the cryptographic module in accordance with RFC 4210 and 6712.

6.2.7. Private Key Storage in Cryptographic Module

Refer to section 6.1.1.(CP)

6.2.8. Activating Private Keys

The private key is activated upon password requested by the private key protection software. The password must be created and maintained only by the Certificate Holder, and for their exclusive use and knowledge.

The Certificate Holder must adopt a password to protect the private key, and it is recommended that passwords be changed at least every 3 months.

6.2.9. Deactivating Private Keys

The deactivation of the private key occurs when the “browser” used to establish a secure connection is closed.

6.2.10. Destroying Private Keys

The removal of the key from the certificate's storage media must be done through options provided by the browser used to generate the key pair. The option allows you to delete the private key.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The CA stores the public keys of the CA itself and of the certificate holders, as well as the CRLs issued, after the expiration of the corresponding certificates, permanently, for verification of signatures generated during their validity period.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The private key of the CA and the certificate holders issued by it are used only during the validity period of the corresponding certificates. The CA's public key can be used during the entire period of time determined by the applicable legislation, for verification of signatures generated during the validity period of the corresponding certificate.

Type A1 certificates, provided for in this CP, are valid for up to 1 year.

6.4. Activation Data

In the following items, the general security requirements regarding the activation data are described. Activation data, distinct from cryptographic keys, are those required for the operation of some cryptographic modules. Each implemented CP must describe the specific applicable requirements.

6.4.1. Activation Data Generation and Installation

CA private key activation data is unique and random.

6.4.2. Activation Data Protection

CA activation data is protected against unauthorized use by individual cryptographic cards with password and is stored in a level 6 security environment.

6.4.3. Other Aspects of Activation Data

Not applicable

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

SERPRO SSL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance;

The SERPRO SSL CA ensures that the generation of its key pair is performed in an offline environment, to prevent unauthorized remote access.

The general requirements for computational security of the equipment where the cryptographic key pairs of the certificate subscribers issued by the CA are generated are described in the implemented CP.

The server computers used by the CA, directly related to the processes of issuing, issuing, distributing, revoking or managing certificates, implement, among others, the following characteristics:

a) Control of access to CA services and profiles;

b) Clear separation of tasks and attributions related to each qualified profile of the CA;

c) Restricted access to the CA databases;

d) Use of encryption for database security, when required by the classification of your information;

e) Generation and storage of CA audit records;

f) Internal security mechanisms to guarantee the integrity of data and critical processes; and

g) Mechanisms for backup copies (backup).

These characteristics are implemented by the operating system or by combining it with the certification system and with physical security mechanisms.

Any equipment, or part of it, when sent for maintenance has the sensitive information contained therein erased and input and output control is carried out, recording the serial number and the dates of sending and receiving. Upon returning to the facilities where the equipment used to operate the CA resides, the equipment that has undergone maintenance is inspected. In all equipment that is no longer used permanently, all stored sensitive information relating to the activity of the CA is permanently destroyed. All of these events are recorded for audit purposes.

Any equipment incorporated into the CA is prepared and configured as provided for in the implemented security policy or in another applicable document, in order to present the level of security necessary for its purpose.

6.5.2. Computational Security Ration

Not applicable

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

The CA has a SERPRO Digital Certification System, developed in open code.

All customizations are carried out initially in a development environment and after completion of the tests it is placed in an approval environment. Finishing the approval process for customizations, the Data Center Manager assesses and decides when the implementation will be in the production environment.

The design and development processes conducted by the CA provide sufficient documentation to support external safety assessments of the CA components.

6.6.2. Security Management Control

System security administration is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2.1 of CPS.

Configuration management, for the installation and continuous maintenance of the certification system used by the CA, involves testing planned changes in the Development and Homologation Environment, isolated, before their implementation in the Production environment, including the following activities:

a) Installation of new versions or updates in the products that constitute the platform of the certification system;

b) Implementation or modification of Certification Authorities with customizations of certificates, web pages, scripts etc;

c) Implementation of new operational procedures related to the processing platform including cryptographic modules; and

d) Installation of new services on the processing platform.

6.6.3. Lifecycle Security Control

Not applicable

6.6.4. CLR Generation Controls

Before being published, all CRL generated by the CA must be checked for consistency of their content, comparing it with the expected content in relation to the CRL number, date / time of issue and other relevant information.

6.7. Network Security Controls

The controls implemented to guarantee the confidentiality, integrity and availability of the CA's services are as follows:

a) Connectivity infrastructure:

i. Secure accommodation of communication equipment;
ii. Secure firewall and router services;
iii. Secure LAN service;
iv. Secure back office service;
v. Secure and redundant internet service; and
vi. Segmented Networks.

b) Incident prevention and assessment:

i. Intrusion detection;
ii. Vulnerability analysis;
iii. Secure server configuration; and
iv. Technical audits.

c) Infrastructure Administration:

i. Server monitoring;
ii. Network monitoring;
iii. URL monitoring; and
iv. Bandwidth reporting.

In the servers and elements of Infrastructure and network protection used by the CA, only the strictly necessary services are enabled.

The servers and elements of Infrastructure and network protection, such as routers, hubs, switches, firewalls located in the network segment that hosts the CA certification system, are located and operate in a level 4 environment.

The most recent versions of the operating systems and server applications, as well as any corrections (patches) made available by the respective manufacturers are implemented immediately after tests in a development and approval environment.

Logical access to the elements of Infrastructure and network protection is restricted, through an authentication and access authorization system. Routers connected to external networks implement packet data filters, which allow only connections to services and servers previously defined as open to external access.

6.7.2. Firewall

Firewall mechanisms are implemented in equipment for specific use, configured exclusively for this function. The firewall promotes the isolation, in specific subnets, of the server equipment with external access - the known “demilitarized zone” (ZDM) - in relation to the equipment with access exclusively internal to the CA.
The firewall software, among other features, implements audit logs.

6.7.3. Intrusion Detection System (IDS):

The intrusion detection system is capable of recognizing attacks in real time and responding automatically, with measures such as: sending SNMP traps, running programs defined by the network administration, sending e-mail to administrators, sending alert messages to the firewall or to the management terminal, promote the automatic disconnection of suspicious connections, or even reconfigure the firewall.

The intrusion detection system is capable of recognizing different attack patterns, including against the system itself, presenting the possibility of updating its recognition base.

The intrusion detection system provides the recording of events in logs, recoverable in text files, in addition to implementing configuration management.

6.7.4. Unauthorized Access Registration

Attempts for unauthorized access - on routers, firewall or IDS - are recorded in files for analysis, are automated. The frequency of examination of the log files is daily or when an event occurs, and all actions taken as a result of this examination are documented.

6.8. Time-Stamping

Not Applicable

7. CERTIFICATE, CRL AND OCSP PROFILES

The following items specify the formats of certificates and CRL/OCSP generated according to this CP. Information about adopted standards, their profiles, versions and extensions is included.

The minimum requirements established in the following items are obligatorily met in all types of certificates accepted under ICP-Brasil.

The CA meets all the requirements established in items 2.2(CPS), 6.1.5. and 6.1.6. of this CP.

7.1. Certificate Profile

The SERPRO SSL CA generate non-sequential Certificate serial numbers greater than zero (0), containing at least 64 bits of output from a CSPRNG.

All certificates issued by SERPRO SSL CA are in accordance with the format defined by the ITU X.509 or ISO / IEC 9594-8 standard, according to the profile established in RFC 5280

7.1.1. Version number

SERPRO SSL CA issue X.509 version 3 Certificates.

7.1.2. Certificate Content and Extensions; Application of RFC 5280

In this item, CP describes all used certificate extensions and their criticality.
ICP-Brasil defines the following extensions as mandatory:

a) **“Authority Key Identifier”, non-critical**: contains the SHA-1 hash of the CA public key;

b) **"Key Usage", critical**: configured as provided in item 7.1.2.7 of this document;

c) **“Certificate Policies”, non-critical**: contains the CP **OID 2.16.76.1.2.1.105** and the URL address of the website https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf with the CPS.
Server authentication certificates (SSL / TLS) contain the OID of the CA / B Forum Guidelines requirements certificate policy (**OV SSL = 2.23.140.1.2.2)**.

d) **“CRL Distribution Points”, non-critical**: contains the URL address of the web page where the AC CRL is obtained:

http://repositorio.serpro.gov.br/lcr/acserprosslv1.crl
http://certificados2.serpro.gov.br/lcr/acserprosslv1.crl

e) **“Authority Information Access”, does not criticize**, containing the id-ad-calssuer access method, using the HTTP access protocol for the recovery of the certification chain at the following address:

http://repositorio.serpro.gov.br/cadeias/serprossl.p7b

The second entry contains the access method id-ad-ocsp, with the respective address http://ocsp.serpro.gov.br/acserprosslv1 of the OCSP responder, using the access protocol, HTTP.

ICP-Brasil also defines the **non-critical "Subject Alternative Name"** extension as mandatory, with the following formats:

- **For equipment or application certificate:**

  4 (four) otherName fields, mandatory, containing, in this order:

  i. OID = **2.16.76.1.3.8** and content = business name in the CNPJ (National Register of Legal Entities), without abbreviations, if the certificate is a legal entity;

  ii. OID = **2.16.76.1.3.4** and content = in the first 8 (eight) positions, the date of birth of the person responsible for the certificate, in the format ddmmaaaa; in the 11 (eleven) subsequent positions, the person's Individual Taxpayer Registration (CPF); in the 11 (eleven) subsequent positions, the Social Identification number - NIS (PIS, PASEP or CI); in the 15 (fifteen) subsequent positions, the RG number of the person responsible; in the 10 (ten) subsequent positions, the abbreviations of the RG issuing agency and the respective UF.

  iii. OID = **2.16.76.1.3.2** and content = name of the person responsible for the certificate;

  iv. OID = **2.16.76.1.3.3** and content = in the 14 (fourteen) positions the number of National Register of Legal Entities (CNPJ), if the certificate is for individuals legal;

- **For certificates of type SSL / TLS:** Field dNSName, mandatory, containing one or more domains owned or controlled by the holder, following the rules defined in RFC 5280 and RFC 2818, and in accordance with the WebTrust principles and criteria [6] and the CA / Browse Forum requirements [7].

7.1.2.4. All fields and extensions in the SERPRO SSL CA certificates are defined according to RFC 5280.

The “otherName” fields defined as mandatory by ICP-Brasil must comply with the following specifications:

a) Information set defined in each otherName field must be stored as a string of type ASN.1 OCTET STRING or PRINTABLE STRING;

b) When the CPF, NIS (PIS, PASEP or CI), ID, CNPJ, CEI, or Voter Registration numbers are not available, the corresponding fields must be completely filled in with "zero" characters;

c) If the ID number is not available, the issuing agency and UF field should not be filled out. The same occurs for the municipality and UF field, if there is no registration number for the voter registration;

d) All information of variable size referring to numbers, such as ID must be filled with "zero" characters to its left so that the maximum possible size is completed;

e) The 10 (ten) positions of the information about the issuing body of the ID and UF refer to the maximum size, and only the positions necessary for its storage, from left to right, should be used. The same applies to the 22 (twenty-two) positions of the information on municipality and UF of the Title of Voter;

f) Only the characters A to Z and 0 to 9 can be used, and special characters, symbols, spaces or any other are not allowed.

7.1.2.5. Additional otherName fields, containing specific information and form of filling and storage defined by the CA, may be used with OID assigned or approved by the Root CA.

7.1.2.6. The other fields that make up the "Subject Alternative Name" extension may be used, in the form and for the purposes defined in RFC 5280.

7.1.2.7. The CA implements the following extensions, defined as mandatory by ICP-Brasil.

a) for Server Authentication certificates (SSL / TLS):

"**Key Usage", critical:** Only bits digitalSignature e keyAgreement actived;
"**Extended Key Usage"**, **no critical**: contains the purpose server authentication OID = 1.3.6.1.5.5.7.3.1. and also the purpose: client authentication OID = 1.3.6.1.5.5.7.3.2;

7.1.3. Algorithm Object Identifiers

7.1.3.1. The cryptographic algorithms used for signing the certificates by the AC are those admitted within the scope of ICP-Brasil, according to ICP-BRASIL STANDARDS AND CRYPTOGRAPHIC ALGORITHMS [1];

7.1.3.1.1. Certificates issued by the CA are signed using the SHA-256 cryptographic algorithm with a hash function (OID = 1.2.840.113549.1.1.1).

7.1.4. Name formats

7.1.4.1. The digital certificate issued for server authentication (SSL/TLS) adopts the "Distinguished Name" (DN) of the ITU X.500/ISO 9594 standard, as follows:

C = BR

O = name of the certificate holder in an individual certificate; in a legal entity certificate, it must contain the business name contained in the National Register of Legal Entities (CNPJ)

CN = if present, this field must contain a single domain name owned or controlled by the owner

ST = Federation Unit of the certificate holder's physical address

L = city of the holder's physical address

Business Category (OID 2.5.4.15) = type of commercial category, which must contain: "Private Organization" or "Government Entity" or "Business Entity" or "NonCommercial Entity" SERIALNUMBER (OID 2.5.4.5) = CPF or CNPJ, as per type of person Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR

NOTE: The name will be written up to the limit of the available field size, the abbreviation being prohibited.

7.1.5. Name restrictions

7.1.5.1. In this CP item, the restrictions applicable to the names of certificate holders are described;

7.1.5.2. ICP-Brasil establishes the following restrictions on names, applicable to all certificates:

a) accent marks, umlauts or cedillas should not be used; and

b) in addition to the alphanumeric characters, only the following special characters may be used:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

Table 3

7.1.6. Certificate Policy Object Identifier

The OID assigned to this Certificate Policy is: **2.16.76.1.2.1.105.**
Every certificate issued under this CP must contain, in the “Certificate Policies” extension, the corresponding OID.

7.1.7. Usage of the Policy Constraints Extension

Not Applicable

7.1.8. Policy Qualifier Syntax and Semantics

In certificates issued under this CP, the policyQualifiers field of the “Certificate Policies” extension contains the address of the web page (URL): http://repositorio.serpro.gov.br/docs/dpcserprossl.pdf

7.1.9. Processing Semantics for Critical Certificate Policies Extensions

Critical extensions must be interpreted in accordance with RFC 5280.

7.2. CRL Profile

7.2.1. Version Number

The CRL generated by SERPRO SSL CA implement version 2 in accordance with IETF PKIX RFC 5280.

7.2.2. CRL and CRL Entry Extensions

7.2.2.1. This CA implements the CRL extensions defined as mandatory, according Section 7.2.2.2.

7.2.2.2. ICP-Brasil defines the following RLC extensions as mandatory:

a) **“Authority Key Identifier”:** must contain the SHA-1 hash of the CA public key that signs the CRL; and
b) **“CRL Number”: non-critical**: it must contain a sequential number for each CRL issued by CA.

7.3. OCSP profile

7.3.1. Version number

OCSP supports the v1 protocol version under the “IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP” document.

7.3.2. OCSP Extensions

The “Authority Information Access” field, without criticism, contains the id-ad-caIssuer access method, using the HTTP access protocol for retrieving the certification chain at the following address: http://repositorio.serpro.gov.br/cadeias/serprossl.p7b

The second entry contains the access method id-ad-ocsp, with the respective address http://ocsp.serpro.gov.br/acserprosslv1 of the OCSP responder, using the access protocol, HTTP.

8. CONFORMITY AUDIT AND OTHER ASSESSMENTS

8.1. Frequency and Circumstances of Assessments

8.2. Identification / Qualification of Assessor

8.3. Assessor's Relationship to Assessed Entity

8.4. Topics Covered by Assessment

8.5. Actions Taken as a Result of Deficiency

8.6. Communication of Results

8.7. SELF-AUDITS

Refer to section 8.7 of CPS

9. OTHER BUSINESS AND LEGAL MATTERS

Each Sections bellow are refered to section 9 of CPS.

9.7. Disclaimer of Warranties

9.8. Limitations of liability

9.9. Indemnities

9.10. Term and Termination

9.10.1. Term

9.10.2. Termination

9.10.3. Effect of Termination and Survival

9.11. Individual Notices and Communications with Participants

9.12. Amendments

9.12.1. Procedure for Amendments

9.12.2. Notification Mechanism and Periods

9.12.3. Circumstances Under Which the OID Must be Changed

9.13. Dispute Resolution Provisions

9.14. Governing Law

9.15. Compliance With Applicable Law

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

This CP represents the obligations and duties applicable to the CA and RA. If there is a conflict between this CPS and other resolutions of the CG of ICP-Brasil, the last edited will always prevail.

9.16.2. Assignment

9.16.3. Severability

9.16.4. Enforcement (attorneys' fees and waiver of rights)

9.16.5. Force Majeure

9.17. Other Provisions

This CP was submitted for approval, during the accreditation process of SERPRO SSL CA, as established in the document CRITERIA AND PROCEDURES FOR ACCREDITATION OF THE INTEGRATING ENTITIES OF ICP-BRASIL [3]. As part of this process, in addition to compliance with this document, the compatibility between the CP and CPS of SERPRO SSL CA was verified.

10. REFERENCED DOCUMENTS

10.1. The documents below are approved by Resolutions of the Management Committee of ICP-Brasil, and may be changed, when necessary, by the same type of legal provision. The website http://www.iti.gov.br publishes the most updated version of these documents and the Resolutions that approved them.

Ref.	Document	Code
[3]	CRITERIA AND PROCEDURES FOR ACCREDITATION OF ICP-BRAZIL'S INTEGRATING ENTITIES	**DOC-ICP-03**
[4]	MINIMUM REQUIREMENTS FOR THE PRACTICES STATEMENTS OF THE CONFIDENT SERVICE PROVIDERS ICP-BRASIL	**DOC-ICP-17**
[8]	MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRASIL	**DOC-ICP-04**
[5]	MINIMUM REQUIREMENTS FOR PRACTICE STATEMENTS BY ICP-BRASIL TIME STAMP AUTHORITIES	**DOC-ICP-12**

10.2. The documents below approved by Normative Instruction of Raiz CA, which can be changed, when necessary, by the same type of legal provision. The website http://www.iti.gov.br publishes the most updated version of these documents and the Normative instructions that approve them.

Ref.	Document	Code
[1]	STANDARDS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL	**DOC-ICP-01.01**
[2]	OID ASSIGNMENT AT ICP-BRAZIL	**DOC-ICP-04.01**
[6]	WebTrust Principles and Criteria for Registration Authorities e Certification Authorities	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services
[7]	Baseline Requirements – CA/Browser Forum – versão 1.6.6.	https://cabforum.org/

11. BIBLIOGRAPHIC REFERENCES

BRAZILIAN ASSOCIATION OF TECHNICAL STANDARDS. 11.515 / NB 1334: Physical security criteria related to data storage. 2007.

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003.

RFC 4210, IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), september 2005.

RFC 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for HighVolume Environments, september 2007

RFC 5280, IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

RFC 6712, IETF - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 2003.