Certification Practice Statement

SERPRO SSL Certification Authority

Server Authentication(SSL/TLS)

(SERPRO SSL CA)

Version 4.0

2022

SERPRO

CONTENTS

REVIEW CONTROL

Review Date	Staff	Status	Changes

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 item 3.2.3.1.3.(Res. 154 – ICP-Brasil); Update link CPS; Resolution 155, 167, 177 of ICP-Brasil;Update with SSL domain validation information, item 3.2.7.2.1; Item 6.2.3 does not apply; 6.7.1.1.b - corrections; item 6.8 - does not apply;
2.0	2020	Alice Vasconcellos	Approved	
3.0	2021	Lucia Castelli	Revision	Reference for ITI documents;
3.0	2021	Alice Vasconcellos	Approved	
4.0	2022	Lucia Castelli	Revision	Updated: Items: 1.3.2; 3.2.2.4; 3.2.2.4.18; 3.2.2.5; 3.2.2.6; 4.9.1.1; 4.9.2; 4.9.12 and 5.7.3; Included items: 1.2.1.; 1.2.2.; 1.6.1.
4.0	2022	Alice Vasconcellos	Approved	

1. INTRODUCTION

1.1. Overview

1.1.1. This Certification Practices Statement (CPS) describes the practices and procedures employed by the SERPRO SSL Certification Authority (SERPRO SSL CA), wtithin the Brazilian Public Key Infrastructure - ICP-Brasil, in the execution of its services.

1.1.3. This CPS follows updates to the documents of the WebTrust Principles and Criteria [14] and CA / Browser Forum publications - https://cabforum.org/baseline-requirements-documents/

In the event of any inconsistency between this document and the requirements of the CA / Browser Forum - https://cabforum.org/baseline-requirements-documents/ , these will have precedence over these document.

1.1.4. The structure of this CPS is based on RFC 3647.

1.1.5. SERPRO SSL CA keeps all information in this CPS routinely up to date.

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

1.2. Document Name and Identification

This CPS is called the “Certification Practices Statement SERPRO SSL Authority”, a member of ICP-Brasil, and commonly referred to as“ CPS of SERPRO SSL CA ”.

This Certificate Practice Statement(CPS) contains the requirements for the issuance and management of publicly-trusted SSL certificates, as adopted by the CA/Browser Forum.

This CA issues certificates for server authentication (SSL/TLS).

The Object Identifier (OID) for SERPRO SSL CPS is **2.16.76.1.1.137**.

1.2.1. Revisions

2019 – Version 1.0 of the Baseline Requirements Adopted – Refer version 1.6.6 of BR SSL;

2020 – Version 2.0 of the Baseline Requirements Adopted – Refer version 1.7.2 of BR SSL;

2021 – Version 3.0 of the Baseline Requirements Adopted – Refer version 1.7.9 of BR SSL;

1.2.2. Relevant Dates

2020-08-01 8.6 Audit Reports for periods on-or-after 2020-08-01 MUST be structured as defined.

2020-09-30: 4.9.10 OCSP responses MUST conform to the validity period requirements specified; 7.1.4.1 Subject and Issuer Names for all possible certification paths MUST be byte-for-byte identical; 7.1.6.4 Subscriber Certificates MUST include a CA/Browser Form Reserved Policy Identifier in the Certificate Policies extension; 7.2 and 7.3 All OCSP and CRL responses for Subordinate CA Certificates MUST include a meaningful reason code.

2021-12-01: 3.2.2.4 CAs MUST NOT use methods 3.2.2.4.6, 3.2.2.4.18, or 3.2.2.4.19 to issue wildcard certificates or with Authorization Domain Names other than the FQDN

1.3. PKI Participants - ICP-Brasil

1.3.1. Certification Authority

This CPS refers only to the Certification Authority of SERPRO SSL, a member of ICP-Brasil.

The SERPRO SSL CA is the secondary level of the CA hierarchy:

- CA RAIZ - Root-signing all ICP-Brasil issuing CAs and kept offline.
- SERPRO SSL CA - This issuing CA is restricted to only issue OV SSL/TLS certificates.

1.3.2. Registration Authorities

1.3.2.1. 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 this document.

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

Subscribers are legal entities who apply for OV SSL/TLS Certificates from SERPRO SSL CA.

As the certificate subscriber is a legal entity, an individual will be designated as responsible for the certificate, and its corresponding:the private key.

See “Certificate Managers” in section 1.3.5 below.

Preferably, the legal representative of the subscriber will be designated as responsible of the certificate.

1.3.4. Relying Parties

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

A relying party´s rights include:

a) Refuse to use the certificate for purposes other than those provided for in the corresponding CP;

b) Check the certificate's validity at any time. A certificate issued by CA is considered valid when:

i. It is not listed in the CRL of the CA;

ii. It is not expired; and

iii. It can be verified using a valid CA certificate.

Failure to exercise these rights does not remove the responsibility of the CA and the certificate subscriber.

1.3.5. Certificate Managers

As part of this CPS, a Certificate Manager is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant and is responsible for the use of the certificate (and associated private key).

1.3.6. Other Participants

1.3.5.1. The SERPRO SSL 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.

1.3.5.2. Other groups that participated in the development of the Cab / Browser Forum[15] include AICPA / CICA, which is the task force of WebTrust for CA 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 Certificate Policy (CP) implemented by the CA is: CP SERPRO SSL CA A1 which after accreditation by ICP-Brasil, acquired the OID of 2.16.76.1.2.1.105.

The CP lists the applications for which the certificates issued in accordance with this CPS may be used.

OV SSL/TLS/TLS Certificates are used to secure online communication and transactions where the risks of data compromise and fraud exist. The OV SSL/TLS Certificate allows the end entity to prove its identity to other participants and maintain the integrity of the transaction.

At all times, Subscribers are required to use Certificates in accordance with the CP and this CPS and all applicable laws and regulations.

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

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), a government entity of Brazil.

1.5.1. Organization Administering the Document

The organization administering the CP and this 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: certificados@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 Deformining CPS Suitability for the Policy

Name: Pedro Moacir Rigo Motta

Phone: +55 61 20217957

Email: certificados@serpro.gov.br

1.5.4. CPS Approval Procedures

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

Any amendments made to this 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 Review Control, revision table.

1.6. Definitions and Acronyms

The Definitions found in the CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

1.6.1. Definitions

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, or any entity operating under the direct control of a Government Entity.
Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant:i. who signs and submits, or approves a certificate request on behalf of the Applicant, and/orii. who signs and submits a Subscriber Agreement on behalf of the Applicant, and/oriii. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.
Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.
Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Authorization Domain Name: The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the

Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.
Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).
Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. “example.co.uk” or “example.com”). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
CAA: From RFC 8659 (http://tools.ietf.org/html/rfc8659): “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue.”
CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
Certificate: An electronic document that uses a digital signature to bind a public key and an identity.
Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA’s possession or control or to which the CA has access.
Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7. e.g. a Section in a CA’s CPS or a certificate template file used by CA software.
Control: “Control” (and its correlative meanings, “controlled by” and “under common control with”) means possession, directly or indirectly, of the power to:(1) direct the management, personnel, finances, or plans of such entity;(2) control the election of a majority of the directors ; or(3) vote that portion of voting shares required for “control” under the law of the entity’s Jurisdiction of Incorporation or Registration but in no case less than 10%.
Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.
Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.
CSPRNG: A random number generator intended for use in cryptographic system.
Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
DNS CAA Email Contact: The email address defined in Appendix A.1.1.
DNS CAA Phone Contact: The phone number defined in Appendix A.1.2.
DNS TXT Record Email Contact: The email address defined in Appendix A.2.1.
DNS TXT Record Phone Contact: The phone number defined in Appendix A.2.2.
Domain Authorization Document: Documentation provided by, or a CA’s documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
Domain Label: From RFC 8499 (http://tools.ietf.org/html/rfc8499): “An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names.”
Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant: Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.
Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with:i. the Internet Corporation for Assigned Names and Numbers (ICANN),ii. a national Domain Name authority/registry, or iii. a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).
Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to

that organization.
Expiry Date: The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.
Fully-Qualified Domain Name: A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.
Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA’s Root Zone Database.
IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.
IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA. **Key Compromise:** A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.
Key Pair: The Private Key and its associated Public Key.
LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): “A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets.”
Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country’s legal system.
Non-Reserved LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): “The set of valid LDH labels that do not have ‘–’ in the third and fourth positions.”
Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization’s applicable standard for a specific object or object class.
OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Onion Domain Name: A Fully Qualified Domain Name ending with the RFC 7686 “.onion” Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.
Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.
Parent Company: A company that Controls a Subsidiary Company.
P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.
Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder’s corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding Private Key.
Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.
Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Request Token: A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. The CA SHOULD define within its CPS (or a document clearly referenced by the CPS) the format and method of Request Tokens it accepts. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
Note: Examples of Request Tokens include, but are not limited to: i. a hash of the public key; or ii. a hash of the Subject Public Key Info [X.509]; or iii. a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.
Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
Requirements: The Baseline Requirements found in this document.
Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtmlhttps://www.iana.org/assignments/iana-ipv6-special-registry/ iana-ipv6-special-registry.xhtml
Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power. **Subject:** The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.
Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber: 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.
Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Subsidiary Company: A company that is controlled by a Parent Company.
Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.
Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
Test Certificate: This term is no longer used in these Baseline Requirements.
Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.
Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists: Someone who performs the information verification duties specified by these Requirements.
Validity Period: Prior to 2020-09-01, the period of time measured from the date when the Certificate is issued until the Expiry Date. For Certificates issued on or after 2020-09-01, the validity period is as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.
WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.
Wildcard Domain Name: A string starting with “*.” (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.
XN-Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): “The class of labels that begin with the prefix "xn--" (case independent), but otherwise conform to the rules for LDH labels.”

1.6.2. 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 CA SERPRO SSL develop, implement, enforce, and annually update a Certificate Policy and Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

2.1. Repositories

2.1.1. Repositories:

a) The SERPRO SSL CA makes available, right after its issuance, the certificates issued by it and its CRL and OCSP responses;

b) The SERPRO SSL CA implements the necessary resources to guarantee the security of the data in it stored.

2.1.2. The requirements for CA repositories:

a) Physical Location: Address: SGAN 601, Module V, Asa Norte, Brasília, Distrito Federal, Brazil - CEP 70.836-900.

b) Availability;

c) Access protocols - HTTP and HTTPS;

d) Security requirements - complies with the requirements defined in item 5.

2.1.3. The SERPRO SSL CA makes the repository available on a 24 x 7 basis.

2.1.4. The responsible CA provides 02 (two) repositories in segregated network infrastructure, for CRL distribution:

http://certificados2.serpro.gov.br/lcr/ https://repositorio.serpro.gov.br/lcr/

2.2. Publication of Information

The SERPRO SSL CA conforms with the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, they take precedence over this document;

The SERPRO SSL CA publishes and keeps available on its website the information described in item 2.2.2. on its publicly accessible website

https://certificados.serpro.gov.br/serprossl, that is available on a 24x7 basis and at least 99,5% of the month;

Prior to issuing SSL certificates, SERPRO SSL CA checks for CAA records for each extension dNSName in subjectAltName in the certificate to be issued, as specified in RFC 8659;

Section 4.2 of this Certification Practice Statement state the CA's policy on processing CAA Records for Fully-Qualified Domain Names; that policy is consistent with these Requirements. It is clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue. The CA log all actions taken, if any, consistent with its processing practice;

The CA SERPRO SSL publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA SERPRO SSL fulfill this requirement by incorporating these Requirements directly into its Certificate Policy and/or Certification Practice Statements

The following information is published on the website:

a) certificates;
b) CRL;
c) CPS;
d) the CP that this CA implement;
e) A list, regularly updated, containing the linked RA and their respective adresses;
g) The SERPRO SSL CA host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. The SERPRO SSL CA separate Web pages using Subscriber Certificates that are i. valid, ii. revoked, and iii. Expired, as bellow:

- Valid Certificates: https://active-repositorio.serpro.gov.br/
- Revoked Certificates: https://revoked-repositorio.serpro.gov.br/
- Expired Certificates: https://expired-repositorio.serpro.gov.br/

2.3. Time or Frequency of Publication

The frequency of publication of CRL and the frequency of updating OCSP records are specified in Sections 4.9.7 and 4.9.9. of this document.

The SERPRO SSL CA reviews this CPS at least once a year and makes the necessary changes so that the CA operation remains accurate, transparent and complies with the requirements listed in Section 8 of this document.

The SERPRO SSL CA closely monitors the ballots taking place at the CA / Browser Forum (https://cabforum.org/ballots/) and updates to the Baseline Requirements, keeping CA operations up to date with these Requirements in a timely manner.

The Review Control revisions table, indicates revisions and updates made to this CPS by adding a date for recording changes and increasing the version number of the CPS, even if none another change is made to the document.

2.4. Access Controls on Repositories

Read only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

The SERPRO SSL CA verifies the authenticity of the identity and / or attributes of individuals and legalentities of ICP-Brasil before including these attributes in a digital certificate. Individuals and legal entities are prohibited from using names on their certificates that violate the intellectual property rights of the parties.

SERPRO SSL CA reserves the right, without liability to any applicant, to reject applications.

3.1. Naming

3.1.1. Types of names

3.1.1.1. The types of names allowed for CA certificate subscribers are the “distinguished name” ITU X.500 standard, web page address (Fully Qualified Domain Name – FQDN and other information allowed by the Baseline Requirements that allows unequivocal identification of the subscriber.

This CA does not issue a certificate to subsequent CA.

3.1.2. Need for Names To Be Meaningful

To identify the subscribers of the issued certificates, the CA makes use of significant names that make it possible to deformine the identity of the person or organization to which they refer.

Any fully qualified domain name (FQDN), which is embedded into a certificate, either as a component DN or as a subjectAltName dnsName, must conform to the standard semantics for DNS names described in RFC1034 and requirements of the CA/Browser Forum.

Organizational names are syntactically validated on the website https://registro.br/tecnologia/ferramentas/whois/;

3.1.3. Anonymity or Pseudonymity of Subscribers

SERPRO SSL CA does not issue anonymous or pseudonymous Certificates.

3.1.4. Rules For Interpreting Various Names Forms

Fields contained in OV SSL/TLS Certificates are in compliance with the CP.

The use of names in certificates that violate intellectual property rights is prohibited from third parties.

3.1.5. Uniqueness of Names

Identifiers of the “Distinguished name” (DN) type are unique for each certificate holder issued by the CA. Additional numbers or letters may be added to each entity's name to ensure the uniqueness of the field.

3.1.6. Recognition, Authentication, and Role of Trademarks

The SERPRO SSL CA reserves the right to make all decisions regarding disputes arising from equality of names. During the identity verification process, it will be up to the certificate applicant prove its right to use a specific name.

3.1.7. Trademark Recognition

According to the brazilian legislation.

3.2. Initial Identity Validation

In this item and in the following, the CPS describes the general requirements and procedures used by the RA linked to the CA, responsible for carrying out the following processes:

a) identification of the subcriber - identification of the natural or legal person, subscriber of the certificate, based on the identification documents mentioned in items 3.2.2, 3.2.3 and 3.2.7, observed as follows:

i. for individual certificates: Not applicable.

ii. for legal entity certificates: proof that the documents presented refer effectively to the legal entity holding the certificate, and that the natural person who presents himself as the legal representative of the legal entity actually has such an assignment, a power of attorney allowed by public instrument, with specific powers to act before ICP-Brasil, whose original or second certificate copy has been issued within 90 (ninety) days prior to the date of the request.

b) Certificate issuance: after checking the certificate request data with those contained in the documents and biometrics operation, in the identification stage, the issuance of the certificate in the CA system is released. The Subject Alternative Name extension is considered to be strongly related to the public key contained in the certificate, so all parts of that extension must be verified, and the certificate subscriber must prove that it has the rights to this information under the Brazilian law or that it is authorized information subscriber to use them.

3.2.1. Method to Prove Possession of Private Key

The confirmation that the requesting entity controls the private key corresponding to the public key for which the digital certificate is being requested is carried out following the RFC 4210 standard, relating to POP (Proof of Possession).

3.2.2. Authentication of Organization Identity

SERPRO SSL CA verifies the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of Section 3.2.2.1. SERPRO SSL CA inspects any document relied upon for alteration or falsification.

3.2.2.1. General Provisions - Identity

3.2.2.1.1. The procedures used by the RA to confirm the identity of a legal representative are carried out through the physical presence of the legal representative, based on legally accepted identification documents.

3.2.2.1.2. The legal representative of the legal entity requesting the certificate, or the attorney-in-fact established under item 3.2, item 'a', item (ii) above, who will be the subscriber of the private key, will be designated as responsible for the certificate.

3.2.2.1.3. Confirmation of the identity of the organization and the individual responsible for the certificate must be made, in the following forms:

a) presentation of the list of documents listed in item 3.2.2.2;

b) presentation of the list of documents of the person responsible for the certificate, listed in item 3.2.3.1;

c) collection and biometric verification of the individual responsible for the certificate, according to regulations issued, through regulatory instructions, by CA Raiz, which define the procedures for identifying the applicant and communicating irregularities in the process of issuing an ICP-Brasil digital certificate, as well as the procedures for biometric identification at ICP-Brasil; and

d) digital signature of the form of ownership mentioned in item 4.1 by the person responsible for the certificate.

Note 1: The RA may request a handwritten signature from the person responsible for the certificate in a specific form for comparison with the identity document or social contract.

In this case, the digitized manuscript form and digitally signed by the staff of RA will be attached to the certificate's electronic dossier, and the paper original may be discarded.

3.2.2.1.4. Not applicable

3.2.2.1.5. The provisions of item 3.2.2.1.3 may be carried out:

a) upon presence of the person responsible for the certificate; or

b) by videoconference, according to procedures and technical requirements defined in Normative Instruction of CA Raiz, which shall ensure a level of security equivalent to the face-to-face form, guaranteeing the validation of the same identification and biometric information, through the use of secure electronic communication technologies, interaction, documentation and biometric treatment.

3.2.2.2. Documents for the purpose of identifying an organization

a) Regarding its legal qualification:

i. if a legal entity created or authorized to be created by law, a copy of the CNPJ;

ii. if private entity:

1. Simplified certificate issued by the Board of Trade or constitutive act, duly registered with the authoritative body, which allows proof of who are its current legal representatives; and

2. Documents on the election of their legal representatives, when applicable;

Note 1: These confirmations that deal with item 3.2.2.2. may be made electronically documents with barcodes or using official applications of a Brazilian jurisdiction. These validations must be included in the electronic file of the certificate subscriber.

3.2.2.3. Information contained in the certificate issued to an organization:

3.2.2.3.1. The applicant must fill in the following fields of the certificate of a legal entity, with the information contained in the documents presented:

a) Business name and address included in the CNPJ (National Register of Legal Entities) without abbreviations;

b) National Register of Legal Entities (CNPJ);

3.2.2.4. Validation of Domain Authorization or Control

SERPRO SSL CA confirms that prior to issuance, SERPRO SSL CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Subject Alternative Name field of the Certificate using at least one of the methods listed below:

3.2.2.4.1. Validating the Applicant as a Domain Contact

SERPRO SSL CA does not use this method.

3.2.2.4.2. Email, Fax, SMS, or Postal Mail to Domain Contact

SERPRO SSL CA will use 3.2.2.4.2 - for Email, Fax, SMS, or Postal Mail to Domain Contact. For this method the system will send email to the contact available in the "whois"

of the domain. The content of this email must bring a random value (hash) and the person responsible when clicking on the verification link where this value will be informed;

The system may allow the process of approval of the two selection methods above to be successfully carried out by the person in charge in case of presentation to the Agent of negative registration:

"It was not possible to validate the authorization or control of the domain [dominio.abc.br]".

3.2.2.4.3. PHONE CONTCAT WITH DOMAIN CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.4. CONSTRUCTED EMAIL TO DOMAIN CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.5. DOMAIN AUTHORIZATION DOCUMENT

SERPRO SSL CA does not use this method.

3.2.2.4.6. AGREED-UPON CHANGE TO WEBSITE

SERPRO SSL CA does not use this method.

3.2.2.4.7. DNS CHANGE

SERPRO SSL CA does not use this method.

3.2.2.4.8. IP ADDRESS

SERPRO SSL CA does not use this method.

3.2.2.4.9. TEST CERTIFICATE

SERPRO SSL CA does not use this method.

3.2.2.4.10. TLS USING A RANDOM NUMBER

SERPRO SSL CA does not use this method.

3.2.2.4.11. ANY OTHER METHOD

SERPRO SSL CA does not use this method.

3.2.2.4.12. VALIDATING APPLICANT AS A DOMAIN CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.13. EMAIL TO DNS CAA CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.14. EMAIL TO DNS TXT CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.15. PHONE CONTCAT WITH DOMAIN CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.16. PHONE CONTCAT WITH DNS TXT RECORD PHONE CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.17. PHONE CONTCAT WITH DNS TXT RECORD PHONE CONTCAT

SERPRO SSL CA does not use this method.

3.2.2.4.18. AGREED-UPON CHANGE TO WEBSITE V2

This requirement shows that the issuer has management of the request address (Domain URL).

This evidence can be obtained automatically or interactively.

Automatically, the issuer, right after the request in the application, receives instructions in his e-mail on how to proceed to carry out this control test.
To perform this procedure, please follow the steps below:

- Create the file “numerodopedido.txt” and include the content aabbbspe5hspdiypgg99tuvpwzq1mgrke/ylvktlsdi= ; (random value)

- Make this file available at the URL informed in your certificate request, in the

directory "/.well-known/pki-validation", for example:

https://meudominio.gov.br/.well-known/pki-validation/161234.txt;

Thus, considering that the issuer has performed the above procedure, when the validate specialist starts the approval process, the system will perform the validation (of Domain control/management) automatically, without the need for intervention by the validate specialist.

The interactive form must be performed as an alternative to the automatic form.

In this case, when the automatic form is not performed, the Validate Specialist receives the following message:

The system was unable to validate the domain control informed by the holder.

We will use the method 3.2.2.4.2

3.2.2.4.19. AGREED-UPON CHANGE TO WEBSITE - CAME

SERPRO SSL CA does not use this method.

3.2.2.4.20. TLS USING ALPN

SERPRO SSL CA does not use this method.

3.2.2.5. AUTHENTICATION FOR AN IP ADDRESS

3.2.2.5.1 Agreed-Upon Change to Website

This requirement shows that the issuer has management of the request address (IP)

This evidence can be obtained automatically or interactively.

Automatically, the issuer, right after the request in the application, receives instructions in his e-mail on how to proceed to carry out this control test.

To perform this procedure, please follow the steps below:

- Create the file “numerodopedido.txt” and include the content aabbbspe5hspdiypgg99tuvpwzq1mgrke/ylvktlsdi= ; (random value)

- Make this file available at the IP informed in your certificate request, in the

directory "/.well-known/pki-validation", for example:

https://meudominio.gov.br/.well-known/pki-validation/161234.txt;

Thus, considering that the issuer has performed the above procedure, when the validate specialist starts the approval process, the system will perform the validation (of IP address control/management) automatically, without the need for intervention by the validate specialist.

The interactive form must be performed as an alternative to the automatic form.

In this case, when the automatic form is not performed, the Validate Specialist receives the following message:

The system was unable to validate the domain control informed by the holder.

3.2.2.6 WILDCRAD DOMAIN VALIDATION

This authentication will be done in accordance with method 3.2.2.4.2

3.2.2.7. DATA SOURCE ACCURACY

SERPRO SSL CA uses data sources from ICP-Brasil (SAF System) considers it a reliable data source.

Before relying on any data provided, SERPRO SSL CA will verify the following attributes:

- The age of the information provided,
- The frequency of updates to the information source,
- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

3.2.2.8. CAA RECORDS

Prior to issuing SSL certificates, SERPRO SSL CA checks for CAA records for each extension dNSName in subjectAltName in the certificate to be issued, as specified in RFC 8659.

3.2.3. Authentication of Individual Identity

The confirmation of an individual's identity is carried out through the physical presence of the interested party, or by means of videoconference, as procedures and technical requirements of the CA Raiz Normative Instruction, which are necessary security level equivalent to the face-to-face form, an equivalent validation of the same identification and biometric information, through the use of secure electronic technologies of communication, interaction, and biometric treatment. based on legally accepted documents and through the ICP-Brasil biometric identification process.

3.2.3.1. Documents to Identifying

The following documentation, in its original version, must be presented for the purpose of identifying a certificate applicant:

a) Registration of identity or passport if Brazilian; or

b) Voter title with photo; or

c) National Foreigner Card - CNE, if a foreigner domiciled in Brazil; or

d) Passport, if a foreigner not domiciled in Brazil;

e) Photograph of the face of the applicant for an ICP-Brasil digital certificate, as provided in DOC-ICP-05.03 [11];

f) Fingerprints of the applicant for an ICP-Brasil digital certificate, as provided in DOC-ICP-05.03 [11].

NOTE 1: Identity registration(ID) is understood as the documents issued by the Public Security Departments as well as those that, by force of law, are equivalent to an identity document throughout the national territory, provided that they contain photographs.

3.2.3.1.1. In the event of positive identification through the biometric process of ICP-Brasil, it is not necessary to present any of the documents listed in the item and the verification step. Evidence of this process will form part of the applicant electronic dossier.

3.2.3.1.2. The digital documents must be verified by barcode or official applications of the federal entities. Such verification will form part of the certificate subscriber electronic dossier. In the event of positive identification, the verification step according to item 3.2.3.1.3.

3.2.3.1.3. Paper documents, which do not exist for verification by barcode or official applications of federative entities, must be verified:

a) by a registration agent other than the one who performed the identification step;

b) by the RA or RA of the CA or the RA of the PSS of the CA; and

c) before the certificate validity begins, which must be automatically revoked if the verification has not occurred until the validity begins.

The biometric verification of the applicant can be performed by typing the data on an official national basis, as regulated in a Normative Instruction issued by Raiz CA(ICP-Brasil), which shall provide for the procedures and official bases admitted for such goal.

3.2.3.2. Information contained in the certificate issued to an individual

3.2.3.2.1. Issuance of digital certificate for an individual person are not avaiable.

3.2.4. **Non-V**erified **Subscriber Information**

Not applicable.

3.2.5. Validation of Authority

Not applicable as no CA certificates are issued by CA SERPRO SSL.

For CA SERPRO SSL certificates, the items assigned in item 3.2.3.1 are used.

3.2.6. Criteria for Interoperation

SERPRO SSL CA does not have any cross-certificates with other CAs.

3.2.7. Device or Application Authentication

3.2.7.1. General Provisions - Identity

3.2.7.1.1. In the case of a certificate issued for equipment, the subscriber will be the individual or legal entity requesting the certificate, who must indicate the person responsible for the private key.

3.2.7.1.2. If the subscriber is a legal entity, the identity of the organization and the individual responsible for the certificate must be confirmed, in the form of item 3.2.2.

3.2.7.1.3. If the holder is a legal entity, the identity of the organization and the individual responsible for the certificate must be confirmed, in the form of item 3.2.2.

3.2.7.1.4. Not applicable

3.2.7.1.5. Not applicable

3.2.7.2. Equipment Identity

3.2.7.2.1. For equipment certificates that use URLs in the identification of the subscriber, it must be verified whether the certificate applicant holds the domain name registration with the authoritative body, or if it has authorization from the domain subscriber to use that

address. In this case, supporting documentation (form of authorization to use the domain or similar), duly signed by the domain owner, must be submitted.

For certificates of type Wildcard, Multidomain, IP or URL, proof of application control over the desired URL is required by including a file or a random value in the application.

The proof of control will be made by the method - Change Agreed on the Site - which follows item 3.2.2.4.18 (Agreed-Upon Change to Website V2) for URL, Wildcard, Multidomain and IP type certificates.

Another method that we will use 3.2.2.4.2 - for Email, Fax, SMS, or Postal Mail to Domain Contact. For this method the system will send email to the contact available in the "whois" of the domain. The content of this email must bring a random value (hash) and the person responsible when clicking on the verification link where this value will be informed;

The system may allow the process of approval of the two selection methods above to be successfully carried out by the person in charge in case of presentation to the Agent of negative registration:

"It was not possible to validate the authorization or control of the domain [dominio.abc.br]".

3.2.7.3. Device or Application Information

3.2.7.3.1. It is mandatory to ICP-Brasil, fill in the following fields of the certificate with the information contained in the documents presented:

a) URL or name of the application;

b) CNPJ;

3.2.7.3.2. Each CP may define as mandatory the filling in of other fields, or the person responsible for the certificate, at its discretion and upon express declaration in the title of ownership and responsibility, may request the filling of fields of the certificate their personal information, according to item 3.2.3.2.

3.2.8. Complementary procedures

3.2.8.1. The SERPRO SSL CA maintains internal policies and procedures that are regularly reviewed in order to comply with the requirements of the various root programs of which the CA is a member, as well as the Requirements defined in the Baseline Requirements of the CA / Browser Forum - https://cabforum.org/baseline-requirements-documents.

3.2.8.2. The entire identification process of the certificate subscriber must be registered with biometric verification and digitally signed by the performers, in the certification solution provided by the CA, using the ICP-Brasil digital certificate at least type A3.

The biometric system of ICP-Brasil must randomly request which finger the staff of RA must present for authentication, which requires the inclusion of all fingers of the staff of RA in the registration of the biometric system.

Such records must be made in such a way as to allow the complete reconstitution of the processes performed, for audit purposes.

3.2.8.3. A file should be kept with copies of all documents used to confirm the identity of an organization and / or an individual. Such copies may be kept on paper or in digital form, subject to the conditions defined in the document MINIMUM SECURITY CHRACATERISTICS FOR RA OF ICP-BRASIL [1].

3.2.8.3.1. Not applicable

3.2.8.3.2. Not applicable

3.2.8.4. The SERPRO SSL CA provide, for RA to their respective chain, an interface for biometric verification of the applicant with the Biometric System of ICP-Brasil, in each process of issuing an ICP-Brasil digital certificate, as established in DOC-ICP -03 [6] and DOC-ICP-05.02 [10].

3.2.8.4.1. In the event of positive identification in the biometric process of ICP-brasil, the presentation of any documentation of the applicant's identity or verification step as per item 3.2.3.1 is not required.

3.3. Identification and authentication for Re-Key Requests

3.3.1. In this item, the CPS establishes the identification and confirmation processes of the applicant registration, used by the CA responsible for generating a new key pair and its corresponding new certificate.

3.3.2. This process can be conducted according to one of the following possibilities:

a) adoption of the same requirements and procedures required in items 3.2.2, 3.2.3 or 3.2.7;

b) by videoconference, according to procedures and technical requirements defined in Normative Instruction of CA Raiz, which shall ensure a level of security equivalent to the face-to-face form, guaranteeing the validation of the same identification and biometric information, through the use of secure electronic technologies communication, interaction, documentation and biometric treatment;

3.4. Identification and Authentication for Revocation Request

Revocation requests is made through a specific form on the page of the RA issuing the certificate, allowing unequivocal identification of the applicant.

Confirmation of the applicant identity is based on the comparison of data provided in the revocation request and the data previously registered with the RA. Certificate revocation requests are logged.

Revocation requests are authenticated to ensure they emanate from authorized persons. The process how the revocation request can be submitted is described in Section 4.9.2.

The reasons for revoking the certificate will always be informed to its subscriber.

Certificate revocation requests will be recorded.

The suspension of certificates is not permitted under ICP-Brasil.

4. CERTIFICATE LIFE-CYCLE OPERACIONAL REQUIREMENTS

4.1. Certificate Application

The minimum requirements and procedures necessary for requesting the issuance of a certificate are:

a) Proof of identification attributes contained in the certificate, as per item 3.2;

b) Through the use of a digital certificate that has security requirements at least equivalent to that of an A3 type certificate, the biometric authentication of the registrar responsible for issuing and revoking certificates; and

c) An ownership form digitally signed by the certificate holder or by the person responsible for the certificate, in the case of a legal entity certificate, according to the addendum referring to the specific FORM [4];

d) The proof of identification attributes may be done by videoconference for the cases referred to in this DCP in items 3.3.1.2, 3.3.2.3 and 3.3.2.4. The videoconference procedures are carried out as provided for in DOC-ICP-05.05[16].

Note 1: If it is technically impossible to digitally sign the form of ownership, such as SSL, equipment, application certificates, the form's handwritten signature or digital signature of the form with the ICP-Brasil certificate, of the certificate holder or person responsible for the form will be accepted. certificate, in the case of a legal entity certificate.

In the case of handwritten signature of the form, it will be necessary to verify the signature against the identification document.

The SERPRO SSL CA will use the SAF system of the ITI itself, where it has access to a database with information about fraud, as well as the list of exceptions in the PsBIO(Biometric System).

4.1.1. Who Can Submit a Certificate Application

The submission of the request must always be made through the RA.

The SERPRO SSL CA accesses an internal database (from ITI itself – SAF ITI) which contains all the certificates previously revoked, due to suspicion of phishing or other fraudulent use or just suspicions.

The SERPRO SSL CA uses this information to identify suspicious certificate requests and make the correct decision whether or not to issue a certificate.

4.1.2. Enrollment Process and Responsibilities

Before issuing a Certificate, the CA obtains the following documentation from the Applicant:

1. A certificate request; and

2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The SERPRO SSL CA obtains any additional documentation that the CA deformines is necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CA obtains from the Applicant an application for a certificate in a form provided by the CA and which complies with the Requirements.

A certificate order must be a valid and current order signed by the Applicant's Representative or on behalf of the legal Applicant.

The certificate request may be submitted and/or signed electronically.

The certificate request contains a request from, or on behalf of, the Legal Applicant for the issuance of a certificate and all information contained therein is correct.

The following items describe the general obligations of the entities involved. If there are specific obligations for the implemented CP, they are described in the CP, in the corresponding item.

4.1.2.1. CA responsibilities

4.1.2.1.1. The SERPRO SSL CA is responsible for the damage it causes.

4.1.2.1.2. The SERPRO SSL CA is jointly responsible for the actions of the entities in its certification chain: RA and PSS.

4.1.2.1.3. When issuing a digital certificate to active civil servants and military personnel of the Union, States and Federal District, authorized by the responsible of the respective competent bodies, the responsibility for any irregularity in the identification of the certificate applicant will fall on the body responsible for identification.

4.1.2.2. CA Obligations

The following items describe the general obligations of the entities involved. The specific obligations for the implemented CP are described in the CP, in the corresponding item.

a) operate in accordance with the CPS of the CA and the CP that implements it;

b) generate and manage your cryptographic key pairs;

c) ensure the protection of your private keys;

d) notify the higher level CA, issuing your certificate, when your private key is compromised and request the immediate revocation of the corresponding certificate;

e) notify its users when it occurs: suspicion of compromise of its private key, issuance of a new key pair and corresponding certificate or the formation of its activities;

f) distribute your own certificate;

g) issue, issue and distribute the RA certificates linked to it and from end users;

h) inform the issuance of the certificate to the respective applicant;

i) revoke the certificates issued by it;

j) issue, manage and publish your CRL and, make available online consultation of certificate status (OCSP - On-line Certificate Status Protocol);

k) publish the CPS and the approved CP on the website, which implements it;

l) publish, on the website, the information defined in item 2.2.2. of this document;

m) publish, on the web page, information on the disqualification of RA;

n) use secure communication protocol when making services available to applicants or users of digital certificates via the web;

o) identify and record all actions performed, in accordance with the norms, practices and rules established by the CG of ICP-Brasil;

p) adopt the security and control measures provided for in the CPS, CP and Security Policy (PS) that it implements, involving its processes, procedures and activities, observing the standards, criteria, practices and procedures of ICP-Brasil;

q) maintain the conformity of its processes, procedures and activities with the norms, practices and rules of ICP-Brasil and with the current legislation;

r) to maintain and guarantee the integrity, confidentiality and security of the information treated by it;

s) to maintain and test annually its Business Continuity Plan - CPN;

t) maintain a civil liability coverage insurance contract resulting from digital certification and registration activities, with sufficient coverage and compatible with the risk of these activities, in accordance with the rules of the CG of ICP-Brasil;

u) inform a relying party and certificate subscribers about the guarantees, coverage, conditions and limitations stipulated by the civil liability insurance policy contracted under the forms above;

v) informing CA Raiz(Root of SERPRO SSL CA), on a monthly basis, the number of digital certificates issued in accordance with the regulations of CA Raiz;

w) not to issue a certificate with an expiration date that extends beyond the expiration date of its own certificate;

x) perform, or delegate to your PSS, the pre-operational audits and annually the operational audits of your RA, directly with their professionals, or through internal audits or independent audit companies, both accredited by CA Raiz. The PSS must present a single audit report for each RA to the CA that use its services; and

y) ensure that all certificate request approvals are carried out by an authorized registrar and workstation.

4.1.2.3. RA Responsibilities

The RA will be responsible for the damages that it causes.

4.1.2.4. RA Obligations

The obligations of the RA are listed below:

a) receive requests to issue or revoke certificates;

b) confirm the identity of the applicant and the validity of the request;

c) forward the certificate issuance or revocation request to the CA using a secure communication protocol, as defined in the document MINIMUM SECURITY CHRACATERISTICS FOR RA of ICP-Brasil[1];

d) inform the respective subscribers of the issuance or revocation of their certificates;

e) maintain the conformity of its processes, procedures and activities with the norms, criteria, practices and rules established by the linked CA and ICP-Brasil, in particular with that contained in the document MINIMUM SECURITY FEATURES FOR ICP-BRASIL RAS [1], as well as in the document WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES [14];

f) maintain and annually test its Business Continuity Plan - CPN;

g) proceed with the recognition of the signatures and the validity of the documents presented in the form of items 3.2.2., 3.2.3. and 3.2.7; and

h) disclose its practices, related to each chain of CA to which it is linked, in accordance with the document WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES [14].

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The SERPRO SSL CA and RA perform the identification and authentication functions as per item 3 of this DCP.

The SERPRO SSL CA does not reuse previous validations.

Each certificate request must pass all validation functions described in section 3.2.

Certificates issued by the SERPRO SSL CA are valid for 12 months.

The SERPRO SSL CA maintains and implements procedures that are documented, identifying and making additional checks for high-risk certificate requests prior to approval, ensuring that such requests are correctly verified under the requirements contained in the CA/Browser Forum, citing Google's Safe Browsing List: https://transparencyreport.google.com/safe-browsing/search?url=www.bb.com.br&hl=pt_BR

The certificate request includes all factual information about the subject to be included in the certificate and any additional information necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CPS.

In cases where the certificate request does not contain all the necessary information about the Applicant, the CA obtains the remaining information from the Applicant or, having obtained it from a reliable, independent third party data source, confirm with the Applicant. The SERPRO SSL CA establishes and follows a documented procedure for verifying all data requested for inclusion in the certificate by the Applicant.

Applicant information includes, but is not limited to, at least one fully qualified domain name(FQDN) or IP address to be included in the SubjectAltName extension of certificate.

4.2.2. Approval or Rejection of Certificate Applications

The SERPRO SSL CA and RA may, with due formal justification, accept or reject requests for certificates from applicants in accordance with the procedures described in this CPS and “all applicable laws and regulations”.

The SERPRO SSL CA, in its sole discretion, may reject an application and may refuse to issue a Certificate, without incurring any liability for loss or damage arising from such refusal.

The SERPRO SSL CA reserves the right not to disclose the reasons for such refusal.

Applicants who have had their applications rejected can re-apply later.

The SERPRO SSL CA, in its sole discretion, may overturn any decision to approve the applicant's certificate request.

4.2.3. Time to Process the Certificate Applications

The SERPRO SSL CA must comply with the procedures deformined by ICP-Brasil. There will be no maximum time to process requests at ICP-Brasil.

4.2.4. Certificate Authority Authorisation (CAA)

Prior to issuing SSL certificates, SERPRO SSL CA checks for CAA records for each extension dNSName in subjectAltName in the certificate to be issued, as specified in RFC 8659.

4.3. Certificate Issuance

4.3.1. CA actions During Certificate Issuance

4.3.1.1. Upon receipt of an approved Certificate signing request, SERPRO SSL CA proceeds to the Certificate issuance process:

a) The person responsible for RA verifies the complete and correct completion of the certificate request, as well as the applicant's documentation;

b) The person responsible for the RA approves the request, making the certificate available for installation by its applicant;

c) The SERPRO SSL CA software automatically issues an email informing the applicant that the certificate is available for installation.

4.3.1.2. The certificate is considered valid from the moment of its inssuance.

4.3.2. Notifications to Subscriber By the CA of Issuance of certificate

The SERPRO SSL CA software automatically issues an email informing the applicant that the certificate is available for installation.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

4.4.1.1. The receipt of a certificate by the Certificate Holder and the subsequent use of the keys and certificate constitutes acceptance of the certificate by the Certificate Holder. By accepting a certificate, the Certificate Holder:

a) Agrees to be in agreement with the ongoing responsibilities, obligations and duties imposed on him by the Disclaimer and CP implemented by the CA and this CPS;

b) Ensures that, to their knowledge, no unauthorized person has had access to the private key associated with the certificate;

c) Affirms that the certificate information provided during the application process is true and has been accurately published within the certificate.

4.4.1.2. The acceptance of every certificate issued is guaranteed by the signature of the Term of Entitlement by the respective holder. In the case of legal entities, acceptance is made by the individual responsible for the use subsequent to receipt of the certificate.

4.4.2. Publication of the Certificate by the CA

Refer to *§* 2.2 CPS

4.4.3. Notification of Certificate Issuance by the CA to other entities

The SERPRO SSL CA, whenever a digital certificate is issued, will notify the log servers included in the Certificate Transparency initiative.

Likewise, it will notify ICP-Brasil.

4.5. Key pair and Certificate Usage

The subscriber of the certificate for the end user must operate in accordance this CPS of and the Certificate Policies (CP) they implement, established in accordance with this document and the document MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRASIL [7].

4.5.1. Subscriber Private Key and Certificate Usage

4.5.1.1. Subscribers have to protect their Private Key to avoid disclosure to third parties. SERPRO SSL CA provides a Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection.

Subscribers are bound to use the Certificate for its lawful and intended purposes only.

4.5.1.2. Obligations of the Certificate subscriber

The obligations of the certificate subscriber issued in accordance with this CPS and contained in the forms of ownership referred to in item 4.1, are as follows:

a) provide, in a complete and accurate manner, all the information necessary for its identification;

b) guarantee the protection and confidentiality of their private keys, passwords and cryptographic devices;

c) use certificates and private keys in an appropriate manner, as provided for in the corresponding CP;

d) know their rights and obligations, contemplated by the CPS and the corresponding CP and other applicable documents of ICP-Brasil; and

e) inform the issuing CA of any compromise of its private key and request the immediate revocation of the corresponding certificate.

Note: In the case of a certificate issued to a legal entity, equipment or application, these obligations apply to the person responsible for the certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Refer to Section 9.6.4.

4.6. Certificate Renewal

Refer to § 3.3 CPS

4.6.1. Circumstances for Certificate Renewal

Refer to § 3.3 CPS

4.6.2. Who May Request Renewal

Refer to § 3.3 CPS

4.6.3. Processing Certificate Renewal Requests

Refer to § 3.3 CPS

4.6.4. Notification of New Certificate Issuance to Subscriber

Refer to § 3.3 CPS

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Refer to § 3.3 CPS

4.6.6. Publication of the Renewal Certificate by CA

Not applicable.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

Refer to Section 4.3.

4.7. Certificate Re-key

Not applicable.

4.7.1. Circumstances for Certificates Re-Key

Not applicable.

4.7.2. Who May Request Certification of a New Public Key

Not applicable.

4.7.3. Processing Certificate Re-Keying Request

Not applicable.

4.7.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable.

4.7.6. Publication of a new CA certified key

Not applicable.

4.7.7. Notification of Certificate Issuance By the CA to Other Entities

Not applicable.

4.8. Certificate Modification

Not applicable.

4.8.1. Circumstances for Certificate Modification

Not applicable.

4.8.2. Who May Request Certificate Modification

Not applicable.

4.8.3. Processing Certificate Modification Requests

Not applicable.

4.8.4. Notification New Certificate Issuance to Subscriber

Not applicable.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6. Publication of the Modified Certificate by the CA

Not applicable.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for revocation

Certificate revocation is the process by which SERPRO SSL CA prematurely forminates the Validity of a Certificate.

The SERPRO SSL CA will make its certificate revocations public through the use of publicly issued CRLs and publicly available OCSP responder services.

4.9.1.1. Reasons for Revoking a Subscriber Certificate

The SERPRO SSL CA revokes a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that SERPRO SSL CA revoke the Certificate;
2. The Subscriber notifies SERPRO SSL CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. The SERPRO SSL CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The SERPRO SSL CA is made aware proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;
5. The SERPRO SSL CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

The SERPRO SSL CA revoke a certificate within 24 hours and revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
2. The SERPRO SSL CA obtains evidence that the Certificate was misused;
3. The SERPRO SSL CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The SERPRO SSL CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. The SERPRO SSL CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. The SERPRO SSL CA is made aware of a material change in the information contained in the Certificate;
7. The SERPRO SSL CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. The SERPRO SSL CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;

9. The SERPRO SSL CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
11. The SERPRO SSL CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2. The SERPRO SSL CA does not issued certificate to subordinated CAs.

4.9.1.3. In relation to revocation, it should also be noted that:

a) The SERPRO SSL CA will revoke, within the period defined in item 4.9.3.3, the certificate of the entity that fails to comply with the policies, norms and rules established by ICP-Brasil; and

b) The CG of ICP-Brasil or the CA Raiz will deformine the revocation of the certificate of the CA that fails to comply with current legislation or with the policies, norms, practices and rules established by ICP-Brasil.

4.9.1.4. Every certificate must have its validity verified, in the respective CRL, before being used.

4.9.1.4.1. The SERPRO SSL CA supports OCSP requests in accordance with RFC 6960 and and requirements of the document WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES [14].

4.9.1.4.2. The SERPRO SSL CA provides assurances that an CRL can be downloaded in no more than three seconds over an analog phone line, under a normal network condition.

4.9.1.5. The authenticity of the CRL must also be confirmed by verifying the signature of the issuing SERPRO SSL CA and the validity period of the CRL/OCSP.

4.9.2. Who Can Request Revocation

The request to revoke a certificate can only be made and may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate:

a) at the request of the certificate subscriber;

b) at the request of the person responsible for the certificate, in the case of a certificate of equipment, applications and legal entities;

c) at the request of a company or body, when the subscriber of the certificate provided by that company or body is its employee, employee or servant;

d) by the issuing CA;

e) by RA;

f) by deformination of the CG of ICP-Brasil or CA Raiz;

g) by third parties;

h) by active public servants and military personnel from the Union, States and Federal District, authorized by the respective competent bodies for their identification;

4.9.3. Procedure for Revocation Request

4.9.3.1. The procedure for requesting a revocation varies depending on who originates it and the CA will have up to 24 hours after the request to respond to the revocation.

Certificate revocation requests can be made as follows and are available 24 x 7 basis:

a) Through the certificate request page under the option “Revoke”;

b) Sending the specific form available on the certificate request page, filled in as the applicant's data and signed;

c) For Fraud Report, through the service channels in Section 1.5.2, “b”.

4.9.3.2. As general guidelines, it is established that:

a) The applicant for revocation of a certificate will be identified;

b) Revocation requests, as well as the actions resulting from them, will be registered and stored;

c) The justifications for revoking a certificate are documented; and

d) The process of revoking a certificate will end with the generation and publication of an CRL containing the revoked certificate.

4.9.3.3. The maximum time allowed for the completion of the certificate revocation process, after receiving the respective request, for all types of certificates provided for by ICP-Brasil is 24 (twenty four) hours.

4.9.3.4. The SERPRO SSL CA is fully responsible for all damages caused by the use of a certificate in the period between the request for its revocation and the issuance of the corresponding CRL.

4.9.3.5. If specific revocation procedures are required for the implemented CP, they must be described in the CP, in the corresponding item.

4.9.4. Revocation Request Grace Period

4.9.4.1. The revocation request must be immediate when the circumstances defined in item 4.9.1 are confirmed.

4.9.4.2. The SERPRO SSL CA establishes a period of 7 days for the acceptance of the certificate requested by its subscriber, within which the revocation of the certificate may be requested without charging the tariff by SERPRO SSL CA.

4.9.5. Time Within Which CA Must Process the Revocation Request

4.9.5. In the case of a formally constituted request, in accordance with ICP-Brasil rules, SERPRO SSL CA must process the revocation immediately after analyzing the request.

Within 24 hours after receiving a Certificate Problem Report, SERPRO SSL CA will investigate the facts and circumstances related to the Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, SERPRO SSL CA will work with the subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which SERPRO SSL CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation does not exceed the time frame set forth in Section 4.9.1.1.

The date selected by the SERPRO SSL CA will consider the following criteria for evaluation:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of damage);

2. The consequences of the revocation (direct and collateral impacts on the subscribers);

3. The number of Problem Reports with Certificates that have already been received on a given certificate;

4. The entity that made the complaint (for example, a complaint from a bailiff or not, that a website is involved in illegal activities) and

5. Brazilian law.”

4.9.6. Revocation Checking Requirements for Relying Parties

4.9.6. Before relying on a certificate, the relying party must confirm the validity of each certificate in the certification chain according to IETF PKIX standards, including checking the validity of the certificate, chaining the name of the issuer and subscriber, restrictions on the use of keys and certification policies and the revocation status through CRL identified in each certificate in the certification chain.

The authenticity of the CRL must also be confirmed by checking the signature of the CA and the validity period of the CRL.

4.9.7. CRL Issuance Frequency

4.9.7.1. The frequency of issuing CRL referring to end-user certificates is 1 (one) hour.

4.9.7.2. The maximum frequency allowed for the issuance of CRL for end user certificates is 6 (six) hours.

4.9.7.3. Not applicable

4.9.7.4. Not applicable

4.9.8. Maximum Latency for CRLs

The CRL is published in the repository within a maximum of 4 (four) hours after its generation.

4.9.9. Online Revocation / Status Check Availability

The OCSP responses conform to RFC6960 and/or RFC5019 and are signed by the CA SERPRO SSL, issuing the certificates whose revocation status is being checked.

4.9.10. Online Revocation Checking Requirements

The SERPRO SSL CA support the HTTP GET method, as described in RFC 6960 and check the status of the issued certificates, as well as the CRLs.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive.

OCSP responses have a validity interval greater than or equal to eight hours;

4.9.11. Other Forms of Revocation Advertisements Available

Not applicable

4.9.12. Special Requirements Related of Key Compromise

See section 4.9.1.

4.9.13. Circumstances For Suspension

Not applicable.

4.9.14. Who can request suspension

Not applicable

4.9.15. Procedure for Suspension Request

Not applicable

4.9.16. Limits on Suspension Period

Not applicable

4.10. Certificate Status Services

4.10.1. Operational Characteristics

The SERPRO SSL CA provides a certificate status service in the form of an CRL/OCSP.

4.10.2. Services Availability

The SERPRO SSL CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of Three seconds or less under normal operating conditions.
SERPRO SSL CA maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by SERPRO SSL CA.
SERPRO SSL CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3. Operational features

Refer to § 4.9 CPS

4.11. End of Subscription

4.11.1. If it is necessary to forminate the services of the CA or RA, SERPRO SSL CA will carry out the applicable procedures described in the document CRITERIA AND PROCEDURES FOR CACREDITATION OF THE INTEGRATING ENTITIES OF ICP-Brasil [6].

4.11.2. Procedures for notifying users and transferring custody of their data and file records include:

a) Notification to the subscriber certificate by email.

b) Progressive transfer of the service and operational records to a successor that has the same security requirements as the defunct entity;

c) Preservation of any records not transferred to a successor.

d) The public keys of the certificates issued by the dissolved CA will be stored by another CA after approval by the Root CA.

e) When there is more than one interested CA, it will assume responsibility for the storage of public keys, the one indicated by SERPRO SSL CA.

f) Upon forminating its activities, SERPRO SSL CA will transfer, if applicable, the documentation of the digital certificates issued to the CA that has assumed the custody of the respective public keys.

g) If the public keys have not been taken over by another CA, the documents relating to digital certificates and the respective public keys will be passed on to the Root CA.

4.12. Key Escrow and Recovery

4.12.1. Key recovery and custody policy and practices

Not applicable.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

At the following items, the security controls implemented by the CA and the RA linked to securely perform their key generation, identification, certification, auditing and record archiving functions are available. The requirements stipulated in CA / Browser Forum Network – https://cabforum.org/baseline-requirements-documents.

5.1. Physical Control

5.1.1. Site Location and Construction

5.1.1.1. The location and certification system used for SERPRO SSL CA operation are not publicly identified. Internally, shared environments that allow visibility in the issuance and revocation of certificates are not allowed. These operations are segregated in closed and physically protected compartments.

5.1.1.2. All aspects of the construction of SERPRO SSL CA facilities, relevant to physical security controls, were performed by specialized technicians, especially those described below:

a) All support equipment installations, such as: air conditioning machines, generator sets, UPS, batteries, power and telephone distribution boards, rectifiers and stabilizers and the like;

b) Installations for telecommunications systems;

c) Grounding and lightning protection system; and

d) Emergency lighting.

5.1.2. Physical Access

Physical access to SERPRO SSL CA premises is managed and controlled internally in accordance with the ICP-BRASIL SECURITY POLICY [8].

5.1.2.1. Access Levels

Entry to SERPRO SSL CA Data Centers containing the CAs certificate manufacturing facility is achieved only through a limited number of access points controlled by security personnel on duty full time (24 hours per day, 365 days per year).

All critical CA operations take place within a physically secure facility with four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

The secure parts of SERPRO SSL CA hosting facilities are protected using physical access controls with biometric scanners or card access systems making them accessible only to appropriately authorized individuals. CA operational facilities are physically locked and alarmed when unoccupied.

All personnel and visitors entering and leaving CA operational facilities are logged. Entry, exit, and activities within CA facilities are under constant video surveillance. Third party support services personnel is granted restricted access to secure CA operational facilities only when required and such access is authorized and accompanied. Access rights to CA facilities are regularly reviewed and updated.

5.1.2.1.2. The first level - or level 1 - is located after the first barrier to access the premises of the CA. To enter a level 1 area, each individual is identified and registered by armed security. From that level, people who are not part of the CA's operation move duly identified and accompanied. No type of CA operational or administrative process is performed at this level.

5.1.2.1.3. Except for the cases provided for by law, the carrying of weapons is not permitted in the premises of the environment where the equipment used in the operation of the CA is installed, at levels higher than level 1. From that level, recording equipment, photography, video, sound or similar, as well as portable computers, have their entrance controlled and can only be used with formal authorization and supervision.

5.1.2.1.4. The second level - or level 2 - is internal to the first level and requires, just like the first, the individual identification of the people who enter it. This is the minimum level of security required for the execution of any CA operational or administrative process. The transition from the first to the second level requires identification by electronic means, and the use of a badge.

5.1.2.1.5. The third level - or level 3 - is internal to the second level and is the first level to house material and sensitive activities of the CA operation. Any activity related to the life

cycle of digital certificates is located from that level. People who are not involved in these activities are not allowed to access that level. Persons who do not have permission to access cannot remain at this level if they are not properly authorized, identified and accompanied by at least one employee who has this permission.

5.1.2.1.6. At the third level, both the entrances and exits of each authorized person are controlled. Two types of control mechanisms are required to enter this level: individual identification, such as electronic card, and biometric identification.

5.1.2.1.7. Cell phones, as well as other portable communication equipment, except those required for the operation of the CA, are not allowed from level 3 onwards.

5.1.2.1.8. The fourth level - or level 4 - is internal to the third level, it is the one in which there are especially sensitive activities of CA operation, such as: issuing and revoking certificates and issuing CRL. All the systems and equipment necessary for these activities are located from that level. Level 4 has the same access controls as level 3 and, additionally, requires, at each access to its environment, the identification of at least 2 (two) authorized persons. At this level, the permanence of these people is required while the environment is occupied.

5.1.2.1.9. On the fourth level, all the walls, floor and ceiling are covered with steel and concrete. The walls, floor and ceiling are solid, constituting a watertight cell against threats of improper access, water, steam, gases and fire. The cooling and power ducts, as well as the communication ducts, do not allow physical invasion of the fourth level areas. Additionally, these level 4 environments - which constitute the so-called safe room - are protected against external electromagnetic interference.

5.1.2.1.10. The safe room is built according to the applicable Brazilian standards. Any omissions in these standards must be remedied by relevant international standards.

5.1.2.1.11. There are three types of services housed in the fourth level environment:

a) Online production equipment and storage safe;

b) Off-line production equipment and storage vault;

c) Network and infrastructure equipment (firewall, routers, switches and servers).

5.1.2.1.12. The fifth level - or level 5 - is internal to the level 4 environments, and comprises locked safes and reinforced cabinets. Cryptographic materials such as keys, activation data, their copies and cryptographic equipment are stored in a level 5 or higher environment.

5.1.2.1.13. To ensure the safety of the stored material, the safe or cabinet meets the following minimum specifications:

a) Be made of steel or material of equivalent strength; and

b) Have a key lock.

5.1.2.1.14. The sixth level - or level 6 - consists of small deposits located inside the fifth level safe or cabinet. Each of these deposits has an individual lock. The activation data for the CA is stored in one of these deposits.

5.1.2.2. Physical detection system

5.1.2.2.1. All passages between the access levels, as well as the level 4 operating rooms, are monitored by video cameras connected to a 24x7 recording system. The positioning and the capacity of these cameras do not allow the recovery of passwords typed in the access controls.

5.1.2.2.2. The storage media resulting from the 24x7 recording are stored for at least 7 (seven) years. They are tested (checking random stretches at the beginning, middle and end of the media) at least every 3 (three) months, with the choice of at least one medium per week. These media are stored in a third level environment.

5.1.2.2.3. All gateways between access levels 3 and 4 of the environment are monitored by an alarm notification system. Where there are, starting from level 2, glass separating access levels, a glass breaking alarm mechanism must be implemented, which must be switched on continuously.

5.1.2.2.4. In all fourth level environments, a motion detection alarm remains active as long as the room access criterion is not met. As soon as, due to the departure of one or more trusted employees, the minimum occupation criterion is no longer met, automatic reactivation of the presence sensors occurs.

5.1.2.2.5. The alarm notification system uses 2 (two) notification means: audible and visual.

5.1.2.2.6. The video camera monitoring system, as well as the alarm notification system, is permanently monitored by an armed guard and is located in a level 3 environment. The monitoring system facilities, in turn, are monitored by video cameras whose positioning allows the monitoring of the guard's actions.

5.1.2.3. Access Control System

The access control system is based on a level 4 environment.

5.1.2.4. Emergency mechanisms

5.1.2.4.1. Specific mechanisms have been put in place to ensure the safety of CA personnel and equipment in emergency situations. These mechanisms allow the unlocking of doors by means of mechanical activation, for the emergency exit of all environments with access control. The exit made through these mechanisms immediately triggers door opening alarms.

5.1.2.4.2. All procedures regarding emergency mechanisms are documented. The emergency mechanisms and procedures are checked every six months, through simulation of emergency situations.

5.1.3. Power and Air Conditioning

5.1.3.1. The infrastructure of the CA certification environment is designed with systems and devices that guarantee the uninterrupted supply of electricity to the facilities. The conditions of energy supply are maintained in order to meet the availability requirements of the CA systems and their respective services. A grounding system is in place.

5.1.3.2. All power cables are protected by appropriate pipes or ducts.

5.1.3.3. Pipes, ducts, gutters, switchgear, distribution and formination boxes and boxes are used, designed and constructed in order to facilitate inspections and the detection of attempted breaches. Separate ducts are used for power, telephone and data cables.

5.1.3.4. All cables are cataloged, identified and periodically inspected, at least every 6 months, in search of evidence of violation or other abnormalities.

5.1.3.5. Records on the cable network topology are kept up to date, observing the confidentiality requirements established by the ICP-BRASIL SECURITY POLICY [8]. Any changes to this network are previously documented.

5.1.3.6. Temporary installations, exposed wiring or directly connected to outlets are not permitted without the use of suitable connectors.

5.1.3.7. The air conditioning system meets the temperature and humidity requirements of equipment used in the environment and has dust filters. In level 4 environments, the air conditioning system is independent and fault tolerant.

5.1.3.8. The temperature of the environments served by the HVCA system is permanently monitored by the alarm notification system.

5.1.3.9. The air conditioning system of level 4 environments is internal, with air exchange performed only by opening the door.

5.1.3.10. The redundancy capacity of the entire CA power and air conditioning structure is guaranteed through:

a) Generators of compatible size;

b) Reserve generators;

c) Redundant UPS systems;

d) Redundant air conditioning systems.

5.1.4. Water Exposures

The solid structure of the level 4 environment, built in the form of a watertight cell, provides physical protection against exposure to water, infiltrations and floods, from any external source.

5.1.5. Fire Prevention and Protection

5.1.5.1. The fire prevention systems of the level 4 areas allow preventive alarms before visible smoke, triggering alarms with the presence of particles that characterize the overheating of electrical materials and other combustible materials present in the installations.

5.1.5.2. In the premises of the CA it is not allowed to smoke or carry objects that produce fire or spark.

5.1.5.3. The safe room has a system for early smoke detection and a gas fire extinguishing system. The access doors to the safe room are locks, one door only opens when the previous one is closed.

5.1.5.4. In the event of a fire in the CA premises, the safe room's internal temperature does not exceed 50 degrees Celsius, and the room will withstand this condition for at least one hour.

5.1.6. Media Storage

All media containing production software and data, audit, archive, or backup information are stored within SERPRO SSL CA facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage such as water, fire, and electromagnetic.

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance to the manufacturer s' guidance prior to disposal.

5.1.8. Off-Site Backup

SERPRO SSL CA maintains copies of CA private keys, archived audit logs, and other sensitive information at secured off-site locations. All copies of private keys are stored in a system or device validated as meeting FIPS 140 Level 3 to ensure that they are only accessible by trusted personnel.

5.2. Procedural Controls

The following items describe the requirements for the characterization and recognition of qualified profiles in the CA together with the responsibilities defined for each profile. For each task associated with the defined profiles, the number of people required for its execution is established.

5.2.1. Trusted Roles

5.2.1.1. The separation of tasks for critical functions is a practice adopted, in order to prevent an employee from misusing the certification system without being detected. The actions of each employee are limited according to their profile.

5.2.1.2. The SERPRO SSL CA establishes a minimum of 3 (three) distinct profiles for its operation, distinguishing the day-to-day operations of the system, the management and auditing of these operations, as well as the management of substantial changes in the system.

5.2.1.3. All operators of the CA certification system receive specific training before obtaining any type of access. The type and level of access are deformined, in a formal document, based on the needs of each profile.

5.2.1.3.1. The SERPRO SSL CA conducts an examination, for issuing chain certificates of the type SSL, on the operators of the CA certification system, according to the requirements of principles and criteria WebTrust Baseline [14].

5.2.1.4. When an employee leaves the CA, their access permissions are revoked immediately. When there is a change in the position or function that the employee occupies within the CA, their access permissions are reviewed. There is a revocation list, with all the resources, previously made available, which the employee must return to the CA upon the formination.

5.2.2. Number of Persons Required per Task

5.2.2.1. Multiuser control is required for the generation and use of SERPRO SSL CA private key, as described in 6.2.2.

5.2.2.2. All tasks performed in the environment where the CA certification equipment is located require the presence of at least 2 (two) operators (employees) of SERPRO SSL CA. The other tasks can be performed by a single operator.

5.2.3. Identification and Authentication for Each Role

5.2.3.1. Persons who occupy the profiles designated by the CA go through a rigorous selection process. Every CA employee has his or her identity and profile verified before:

a) Be included in a list of access to the premises of the CA;

b) Be included in a list for physical access to the CA certification system;

c) Receive a certificate to perform their operational activities in the CA;

d) Receive an account in the CA certification system.

5.2.3.2. The certificates, accounts and passwords used for employee identification and authentication:

a) They are directly assigned to a single operator (duly qualified CA employee);

b) are not shared; and

c) Are restricted to actions associated with the profile for which they were created.

5.2.3.3. The SERPRO SSL CA implements a standard for the use of "strong passwords", defined in its Security Manual and in compliance with ICP-BRAZIL'S SECURITY POLICY [8], together with procedures for the validation of these passwords."

5.2.4. Roles Requiring Separation of Duties

No person can have more than one of the roles listed in section 5.2.1 at a time.

To accomplish this separation of duties, SERPRO SSL CA specifically designates individuals to trusted roles.

SERPRO SSL CA´s systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

The following items describe requirements and procedures, implemented by the CA, the RA and PSS linked to all their staff, regarding aspects such as: background and suitability check, professional training and retraining, job rotation, sanctions for actions unauthorized controls, hiring controls and documentation to be provided. DCP guarantees that all employees of the CA and the linked RA and PSS, in charge of operational tasks, have registered in a contract or form of responsibility:

a) The forms and conditions of the profile they occupy;

b) The commitment to observe the applicable CA rules, policies and rules;

c) The commitment to observe the applicable rules, policies and rules of ICP-Brasil; and

d) The commitment not to divulge confidential information to which they have access.

SERPRO SSL CA and RA staff involved in activities directly related to the processes of issuance, dispatch, distribution, revocation and management of certificates are admitted in

accordance with the established in the Security Policy of the CA and the SECURITY POLICY OF ICP-BRASIL [8].

5.3.2. Background Check Procedures

5.3.2.1. In order to safeguard the security and credibility of the CA, all personnel involved in activities directly related to the processes of issuing, issuing, distributing, revoking and managing certificates, are subjected to the following processes, before the activities of:

a) Criminal records check;

b) Credit records check;

c) Checking the history of previous jobs; and

d) Employment and education history

SERPRO SSL CA personnel do not have access to the trusted functions until all necessary checks are completed and results analyzed. All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are subject to background checks at least every year.

5.3.3. Training Requirements and Procedures

All CA and related RA personnel involved in activities directly related to the certificate issuance, issuance, distribution, revocation and management processes receive documented training, with evidence at the end of the training when assigning a concept that assigns mastery of the following themes:

a) Principles and security mechanisms of the CA and related RA;

b) Certification system in use in the CA;

c) Disaster recovery and business continuity procedures;

d).Recognition of signatures and validity of the documents presented, in the form of item 3.2.2, 3.2.3. and 3.2.7; and

e) Other matters relating to activities under its responsibility.

5.3.4. Retraining Frequency and Requirements

The SERPRO SSL CA and RA personnel involved in activities directly related to the certificate issuance, issuance, distribution, revocation and management processes are kept up to date on any technological changes in the CA or RA certification system.

5.3.5. Job Rotation Frequency and Sequence

SERPRO SSL CA does not implement job rotation.

5.3.6. Sanction for Unauthorized Actions

5.3.6.1. SERPRO SSL CA in the event of an unauthorized action, real or suspected, to be carried out by a person in charge of the CA's operational process or RA, will immediately suspend that person's access to its certification system, institute administrative proceedings for investigate the facts and, if applicable, adopt the appropriate legal measures.

5.3.6.2. The administrative process referred to above will contain, at a minimum, the following items:

a) Report of the occurrence with “modus operandis”;

b) Identification of those involved;

c) Any damages caused;

d) Penalties applied, if applicable; and

e) Conclusions.

5.3.6.3. After the administrative process is completed, the CA will forward its conclusions to the CA Root.

5.3.6.4. The punishments that can be applied, as a result of administrative proceedings, are:

a) Warning;

b) Suspension for a specified period; or

c) Definitive impediment to exercise functions within the scope of ICP-Brasil.”

5.3.7. Independent Contractor Requirements

SERPRO SSL CA does not assign Trusted Roles to external Contractors.

5.3.7. The staff of the CA and related RA, in the exercise of activities directly related to the processes of issuing, issuing, distributing, revoking and managing certificates, are hired as established in the ICP-BRASIL SECURITY POLICY[8].

5.3.8. Documentation Supplied to Personnel

5.3.8.1 SERPRO SSL CA makes available to all staff :

a) This CPS;

b) CP that it implements;

c) ICP-BRASIL'S SECURITY POLICY [8];

d) The SERPRO SSL CA Security Policy;

e) Operational documentation related to its activities; and

f) Contracts, rules and policies relevant to its activities.

5.3.8.2. All documentation is classified and kept up to date, according to the information classification policy, defined by the SERPRO SSL CA.

5.4. Audit Logging Procedures

5.4. In the following items, this CPS describes the aspects of the audit and event registration systems implemented by the CA in order to maintain a safe environment.

5.4.1. Types of Event Recorded

5.4.1.1. All actions performed by CA personnel, in the performance of their duties, are recorded so that each action is associated with the person who performed it. The SERPRO SSL CA records in files for auditing purposes all events related to the security of its certification system, which are:

a) Initiation and formination of the certification system;

b) Attempts to create, remove, set passwords or change system privileges for CA operators;

c) Changes in the configuration of the CA or its keys;

d) Changes in certificate creation policies;

e) Attempts to access (login) and exit the system (logoff);

f) Unauthorized attempts to access system files;

g) Generation of CA's own keys or keys of end users;

h) Issuance and revocation of certificates;

i) Generation of CRL, certificate revocation lists and OCSP directory entry;

j) Attempts to initiate, remove, enable and disable users of systems and to update and recover their keys;

k) Failed operations of writing or reading in the certificate and CRL repository, when applicable; and

l) Write operations in this repository, when applicable.

5.4.1.1.1. This CA has the possibility to audit up to 3% of the SSL certificates issued.

5.4.1.2. The SERPRO SSL CA records, electronically or manually, security information not directly generated by its certification system, which are:

a) Records of physical accesses;

b) Maintenance and changes in the configuration of your systems;

c) Changes in qualified personnel and profiles;

d) Discrepancy and commitment reports; and

e) Records of destruction of storage media containing cryptographic keys, certificate activation data or personal information of users.

5.4.1.3. The minimum audit records to be maintained by the CA include in addition to the above:

a) Application records, including records relating to rejected applications;

b) Certificate generation requests, even if the generation is not successful;

c) CRL issuance request records.

5.4.1.4. All audit records, electronic or manual, contain the date and time of the recorded event and the identity of the agent that caused it.

5.4.1.5. To facilitate the audit processes, all documentation related to the CA services is stored, either electronically or manually, in a single location, in accordance with ICP-BRASIL'S SECURITY POLICY [8].

5.4.1.6. The RA linked to SERPRO SSL CA, by CPS, electronically records in audit files, all events related to the validation and approval of the request, as well as to the revocation of certificates. The following events included in audit files:

a) The registry agents who performed the operations;

b) Date and time of operations;

c) The association between the agents that carried out the validation and approval and the certificate generated;

d) The digital signature of the performer.

5.4.1.7. The SERPRO SSL CA stores, electronically, copies of documents for identification, presented at the time of requesting and revoking certificates and forms of ownership.

5.4.2. Frequency of Processing and Archiving Audit Logs

The audit periodicity of records will not exceed one week, and the audit records are analyzed by the CA's operational personnel. All significant events are explained in a records audit report. Such an analysis involves a brief inspection of all records, verifying that they have not been altered. Then, a more detailed investigation of any alerts or irregularities in these records is carried out. All actions taken as a result of this analysis are documented.

5.4.3. Retention Period for Audit Logs

The CA maintains its audit records locally for at least 2 (two) months at SERPRO facilities and subsequently stores them in the manner described in item 5.5.3.

5.4.4. Protection of Audit Log

5.4.4.1. Audit records generated electronically must be protected against unauthorized reading, modification and removal. These records are classified and maintained according to their classification.

5.4.4.2. Audit information generated manually must be protected against unauthorized reading, modification and removal. These records are classified and maintained according to their classification.

5.4.4.3. The protection mechanisms described in this item comply with the ICP-BRASIL SECURITY POLICY [8].

5.4.5. Audit Log Backup Procedures

The SERPRO SSL CA performs backup procedures for the entire certification system (operating systems, application and database) in two ways:

a) Daily: backup copy; and

b) Weekly: copy stored for audit processes.

5.4.6. Audit Collection System (Internal Vs. External)

The SERPRO SSL CA audit data collection system is a combination of automated and manual processes performed by the operating system, the CA certification systems, the access control system and the operational personnel. The location of the resources is shown in the table below:

Process	Collection System	Registered by
Success and failure of attempts to change operating system security parameters	Automatic	Operational system
Application start and stop	Automatic	Operational system
Success and failure of log-in and log-out attempts	Automatic	Operational system
Success and failure of attempts to create, modify, or delete system accounts	Automatic	Operational system
Success and failure of attempts to create, modify or delete users of authorized systems	Automatic	Operational system
Success and failure of attempts to request, generate, sign, issue or revoke keys and certificates	Automatic	CA or RA software
Success and failure of attempts to create, modify or delete Certificate subscriber information	Automatic	RA Software
Backup and restore logs	Automatic and manual	Operational system and Operations staff
System configuration changes	Manual	Operations staff
Software and hardware updates	Manual	Operations staff
System maintenance	Manual	Operations staff
Staff changes	Manual	Operations staff
Records of physical accesses	Automatic and manual	Access control software and Operations staff

5.4.7. Notification of Event-Causing Subject

Events recorded by SERPRO SSL CA set of audit systems are not notified to the person, organization, device or application that caused the event.

5.4.8. Vulnerability Assessments

Events that indicate possible vulnerability, detected in the periodic analysis of the CA audit records, are analyzed in detail and, depending on their severity, recorded separately. Resulting corrective actions are implemented and recorded for audit purposes.

In addition, the CA's security program includes an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that may result in unauthorized access, disclosure, misuse, alteration or destruction of any certificate data or in the certificate's own life cycle;

2. Evaluates the probability and possible damage of these threats, taking into account the sensitivity of the certificate data and the management process of the same; and

3. Evaluates the policies, procedures, information systems, technology and other agreements that the CA has to combat these threats.

5.5. Records Archival

The following items describe the general policy for archiving records, for future use, implemented by the CA and the related RA.

5.5.1. Types of Records Archived

The following information is recorded and filed by the CA:

a) Certificate requests;

b) Certificate revocation requests;

c) Notifications of compromise of private keys;

d) Issuance and revocation of certificates;

e) CRL emissions;

f) Exchange of cryptographic keys of the CA; and

g) Audit information provided for in item 5.4.1.

5.5.2. Retention Period for Archive

The retention periods for each archived record are as follows:

a) CRL referring to digital signature certificates are permanently retained for historical consultation purposes.

b) The dossiers of the subscribers must be retained, at least, for 7 (seven) years, counting from the date of expiration or revocation of the certificate; and

c) Other information, including audit files, must be retained for at least 7 (seven) years.

5.5.3. Protection of Archive

All archived records are classified and stored with security requirements compatible with their classification, according to the ICP-BRASIL SECURITY POLICY [8].

5.5.4. Archive Backup Procedures

5.5.4.1. A second copy of all archived material is stored outside the CA and is given the same type of protection used by it in the main archive.

5.5.4.2. Backup copies follow the retention periods defined for the records of which they are copies.

5.5.4.3. The integrity of these backup copies is checked at least every 6 (six) months.

5.5.5. Requirements for Time-Stamping of Records

The SERPRO SSL CA servers are synchronized with the time provided by CA RAIZ through its Trusted Time Source - FCT according to DOC-ICP 07 [16]. All information generated that has any time stamp is given the time in GMT, including the certificates issued by that equipment.

In the case of manually made records, these contain the Brazilian Standard Time.

5.5.6. Archive Collection System (Internal or External)

SERPRO SSL CA file data collection system is a combination of automated and manual processes performed by the operating system, CA certification systems and operating personnel.

Process	Collection System	Registered by
Certificate requests	Automatic and manual	Access control software and Operations staff
Certificate revocation requests	Automatic and manual	Access control software and Operations staff
Private key compromise notifications	Manual	Operations staff
Certificate issues and revocations	Automatic	CA or RA software
CRL emissions	Automatic	CA or RA software
Formal correspondence	Manual	Operations staff

5.5.7. Procedures to Obtaing and verife Archive Information

The integrity of the files of the CA and RA is checked either when the file is prepared, or daily with automatic script execution.

5.6. Key Changeover

5.6.1. The SERPRO SSL CA communicates to the Certificate subscribers, by e-mail, the need to renew the certificate, 30 days in advance, with instructions for its renewal.

5.6.2. Details of the procedures are described in the implemented CP.

5.7. Compromise and Disaster Recovery

The CA declares that the requirements related to the notification and disaster recovery procedures are described in the BCP - CA Business Continuity Plan - as established in the SECURITY POLICY OF ICP-BRASIL [8], guaranteeing the continuity of its critical services.

5.7.1. Incident and Compromise Handling Procedures

5.7.1.1. The Business Continuity Plan (BCP), is of restricted access, tested at least once a year, ensuring the continuity of critical services. It also has the Incident Response Plan (IRP) and Disaster Recovery Plan (DRP). The BCP, DRP and IRP are available for verification by the Qualified Auditors, when requested.

5.7.1.2. The procedures in the BCP of the RA linked to recover, in whole or in part, the activities of the RA, are as follows:

a) Identification of events that may cause interruptions in business processes, for example equipment failure, floods and fires, if applicable;

b) Identification and agreement of all responsibilities and emergency procedures;

c) Implementation of emergency procedures that allow recovery and restoration within the necessary timeframes.

d) Documentation of agreed processes and procedures;

e) Adequate training of personnel in the defined emergency procedures and processes, including crisis management; and

f) Test and update plans.

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

The SERPRO SSL CA has a Business Continuity Plan, which contains actions to be taken in the event that computational resources, software and / or data are corrupted and which can be summarized in the following:

a) All the corrupted elements are identified;

b) The moment of the commitment is deformined and it is critical to invalidate the transactions executed after that moment;

c) An analysis of the level of commitment is made to deformine the actions to be performed, which can vary from a simple restoration of a security backup to the revocation of the CA certificate.

5.7.3. Recovery Procedures After Key Compromise

5.7.3.1. Entity certificate is revoked

The SERPRO SSL CA has a BCP that specifies the actions to be taken in the event that the CA's certificate is revoked, and which can be summarized as follows:

a) CA SERPRO SSL, CA Raiz, Certificate subscribers and CCADB will be notified by secure communication;

b) The SERPRO SSL CA revokes the certificates issued by it;

c) The SERPRO SSL CA requests a new certificate;

d) The procedures for issuing new certificates to users are initiated.

5.7.3.2. Entity key is compromised

The SERPRO SSL CA has a BCP that specifies the actions to be taken in case of compromise of its private key. After the identification of the crisis, the managers of the digital certification process are notified who activate the teams involved, to activate the contingency site.

5.7.4. Business Continuity Capability after Disaster

The SERPRO SSL CA has a DRP(Disaster Recovery Plan) that specifies the actions to be taken in the event of a natural or other disaster. The purpose of this plan is to reestablish the main operations of the CA when the operation of systems is significantly and adversely affected by fire, strikes, etc.

The plan ensures that any impact on system operations will not have a direct and immediate operational impact within ICP-Brasil of which the CA is a part. This means that the plan must have as its primary goal, reestablish CA to make accessible the logical records kept within the software. The recovery actions approved within the plan will be taken, in order of priority.

5.8. CA or RA Termination

According to CRITERIA AND PROCEDURES FOR CA ACREDITATION OF ICP-BRAZIL'S INTEGRATING ENTITIES [6].

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. The SERPRO SSL 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.

6.1.1.2. Key pairs are generated only by the corresponding Certificate subscriber. The specific procedures are described in each implemented CP.

6.1.1.3. The CP implemented by the CA defines the means used to store the respective private keys, based on the applicable requirements established by the document MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRASIL [7].

6.1.1.4. The SERPRO SSL CA key pair generation process uses a cryptographic module that implements the security characteristics defined in the STANDRADS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL [9].

6.1.1.5. Each CP implemented by the CA defines the process used for the generation of cryptographic keys of the certificate subscribers, based on the applicable requirements established by the document MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES AT ICP-BRASIL [7].

6.1.1.6. The SERPRO SSL CA private key is generated, stored and used only on specific cryptographic hardware. The SERPRO SSL CA cryptographic module follows the standard “Homologation of ICP-Brasil NSH-3.

6.1.2. Private Key Delivered to Subscriber

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

6.1.3. Public Key Delivery to Certificate Issuer

6.1.3.1. SERPRO SSL CA will deliver a copy of its public key to CA Raiz, in PKCS # 10 format. This delivery will be made by a legal representative of the CA, in a specific ceremony, on a date and time previously established by the CA.

6.1.3.2. 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 STANDRADS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL [9] will be used;

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

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

6.1.5. Key sizes

6.1.5.1. The CP implemented by the CA will define the sizes of the cryptographic keys associated with the issued certificates, based on the applicable requirements established by the document “MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES AT ICP-BRASIL (7).

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 STANDRADS 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)

6.1.7.1. Certificates issued by the SERPRO SSL CA has the bits digitalSignature and keyEncipherment are actived. The purposes for which the cryptographic keys of the certificate subscribers issued by the CA can be used, as well as the possible restrictions applicable in accordance with the applications defined for the corresponding certificates, are specified on each CP that it implements.

6.1.7.2. The SERPRO SSL CA's private key is used only for the signature of the certificates issued by it and its CRL.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The SERPRO SSL 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

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

6.2.1.2. The certificate subscribers' cryptographic key generation modules are those defined in the document STANDRADS 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 SERPRO SSL 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

Not applicable

6.2.4. Private key backup

6.2.4.1. As a general guideline, any entity holding a certificate may, at its discretion, maintain a backup copy of its own private key.

6.2.4.2. The SERPRO SSL CA maintains a backup copy of its own private key. This copy is stored encrypted and protected with a security level not lower than that defined for the original version of the key and approved by the CG of ICP-Brasil, and maintained for the validity period of the corresponding certificate.

6.2.4.3. The SERPRO SSL CA does not maintain a backup copy of the digital signature Certificate subscriber private key.

6.2.4.4. The backup copy must be stored, encrypted, by a symmetric algorithm defined in the STANDRADS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL [9] document, and protected with a security level not lower than that defined for the original key.

6.2.5. Private Key Archival

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

6.2.5.2. 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 SERPRO SSL 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

6.2.8. Activating Private Keys

The activation of the CA's private key is implemented by means of cryptographic cards, password protected, after the identification of 2 of the custodians of the activation key of the cryptographic key. The activation key subscribers are the CA Certification System Administrators.

The passwords used comply with the password policy established by the CA.

6.2.9. Deactivating Private Keys

The SERPRO SSL CA's private key, stored in a cryptographic module, is deactivated when it is no longer needed through a mechanism made available by the certification software that allows the deletion of all information contained in the cryptographic module.

This procedure is implemented by means of cryptographic cards, password protected, after the identification of 2 of the custodians of the activation key of the cryptographic key.

The activation key subscribers are the CA Certification System Administrators. The passwords used obey the password policy established by the CA.

6.2.10. Destroying Private Keys

When the CA's private key is deactivated, due to expiration or revocation, it must be eliminated from the cryptographic module's memory. Any disk space, where the key is eventually stored, must be overwritten. All backup copies of the CA's private key and the custodians' cryptographic cards will be destroyed. The agents authorized to carry out these operations are the administrators and custodians of the CA activation keys.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The SERPRO SSL CA stores the public keys of the CA itself and of the certificate subscribers, as well as the CRL 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

Certificates issued by the CA are valid for 12 months.

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

6.3.2.2. Not applicable.

6.3.2.3. Each CP implemented by the CA defines the maximum validity period of the certificate it defines, based on the applicable requirements established by the MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRAZIL [7].

6.3.2.4. The validity allowed for CA certificates is limited to the validity of the CA certificate, as long as the same standard algorithm for the generation of asymmetric keys implemented by the hierarchically superior CA is maintained.

6.4. Activation Data

The following items describe the general security requirements for activation data. The activation data, distinct from cryptographic keys, are those required for the operation of some cryptographic modules.

6.4.1. Activation Data Generation and Installation

6.4.1.1. The activation data for the CA's private key is unique and random.

6.4.1.2. Each implemented CP ensures that the activation data of the certificate subscriber's private key, if used, are unique and random.

6.4.2. Activation Data Protection

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

6.4.2.2. Each implemented CP ensures that the private key activation data of the certificate subscriber, if used, is protected against unauthorized use.

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.

6.5.3. Registration Authority Security Control

6.5.3.1. These are set out in the document “MINIMUM SECURITY CHRACATERISTICS FOR RA of ICP-Brasil[1]”.

6.5.3.2. These are set out in the document “MINIMUM SECURITY CHRACATERISTICS FOR RA of ICP-Brasil[1]”, section 6.5.32 “Workstations.

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

6.6.1.1. The SERPRO SSL 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.

6.6.1.2. 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

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

6.6.2.2. 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

6.7.1. General Guidelines.

6.7.1.1. 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; and

v. Secure and redundant internet service.

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.

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

6.7.1.3. 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.

6.7.1.4. 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.

6.7.1.5. 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

6.7.2.1. 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” (DMZ) - in relation to the equipment with access exclusively internal to the CA.

6.7.2.2. The firewall software, among other features, implements audit logs.

6.7.3. Intrusion Detection System (IDS):

6.7.3.1. 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 forminal, promote the automatic disconnection of suspicious connections, or even reconfigure the firewall.

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

6.7.3.3. 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

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

Refer to § 7.1.2. CP.

7.1.3. Algorithm Object Identifiers

Refer to § 7.1.3 CP

7.1.4. Name formats

Refer to § 7.1.4. CP

7.1.5. Name restrictions

Refer to § 7.1.5 CP

7.1.6. Certificate Policy Object Identifier

The Object Identifier (OID) of this CPS, assigned by ICP-Brasil is **2.16.76.1.1.137.**

The CA/Browse Forum CP OID for OV certificates is **2.23.140.1.2.2**.

7.1.7. Usage of the Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifier Syntax and Semantics

Not applicable.

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 to item 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-calssuer 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

The SERPRO SSL CA undergoes prior auditing, for accreditation purposes, and annual audits, for accreditation maintenance purposes.

The annual audits implemented is for ITI Operacional, WebTrust, ISO 27001:2013 and ISO27701:2019.

An annual audit is performed by an independent external auditor to assess SERPRO SSL CA´s compliance with requirements set forth above.

An audit period must not exceed one year in duration. In addition to that, more than one compliance audit per year is possible if this is requested by SERPRO SSL CA or is a result of unsatisfactory results of a previous audit.

8.2. Identification / Qualification of Assessor

The CA's audit is performed by an independent external and a Qualified Auditor, it means:

Independence from the subject of the audit; The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4); Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function; For audits conducted in accordance with the WebTrust standard) licensed by WebTrust; Bound by law, government regulation, or professional code of ethics;

Also inspections are also carried out in this CA SERPRO SSL using criterias from ICP-Brasil.

8.3. Assessor's Relationship to Assessed Entity

The SERPRO SSL CA audits are performed by ICP-Brasil, through its own staff, or by relying party authorized by it, subject to the provisions of the document CRITERIA AND PROCEDURES FOR CRARYING OUT AUDITS AT ICP-BRASIL MEMBERS [3].

8.4. Topics Covered by Assessment

8.4.1. Inspections and audits carried out within the scope of ICP-Brasil aim to verify that the processes, procedures and activities of the entities that are part of ICP-Brasil are in compliance with their respective CPS, CP, SP and other rules and procedures established by ICP-Brasil and with the principles and criteria defined by WebTrust [14], as well as the basic requirements of the CA / Browse Forum[15].

8.4.2. The SERPRO SSL CA received a previous audit from CA Raiz for the purpose of accreditation at ICP-Brasil and which is audited annually, for the purpose of maintaining accreditation, based on the provisions of the document CRITERIA AND PROCEDURES FOR CRARYING OUT AUDITS AT ICP-BRAZIL'S ENTITIES[3]. This document addresses the objective, frequency and scope of the audits, the identity and qualification of the auditor and other related topics.

8.4.3. The related ICP-Brasil entities (CA, RA and PSS), also received prior audit, for accreditation purposes, and that the CA is responsible for carrying out annual audits on these entities, for the purposes of maintaining accreditation, as provided in the document mentioned in the previous paragraph.

8.5. Actions Taken as a Result of Deficiency

8.5. In accordance with the CRITERIA AND PROCEDURES FOR SUPERVISION OF THE INTEGRATING ENTITIES OF ICP-BRASIL [2] and with the CRITERIA AND

PROCEDURES FOR PERFORMING AUDITS AT THE INTEGRATING ENTITIES OF ICP-BRASIL [3].

8.6. Communication of Results

8.6 In accordance with the CRITERIA AND PROCEDURES FOR SUPERVISION OF THE INTEGRATING ENTITIES OF ICP-BRASIL[2] and with the CRITERIA AND PROCEDURES FOR PERFORMING AUDITS AT THE INTEGRATING ENTITIES OF ICP-BRASIL [3].

SERPRO SSL CA makes the Audit Report publicly available at https://serpro.gov.br/links-fixos-superiores/pss-serpro/acserprossl

8.7. Self-Audits

SERPRO SSL CA performs regular internal audits of its operations, personnel, and compliance with this CP/CPS.

During the period in which SERPRO SSL CA issues Certificates, CA monitors adherence to this CP/CPS and the CA/B Forum requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

9.1.1. The fees for issuing and renewing certificates by CA Raiz are defined in the document PRICING POLICY GUIDELINES OF THE RAIZ CERTIFICATON AUTHORITY OF ICP-BRASIL [13].

9.1.2. Certificate Access Fees

Not applicable.

9.1.3. Revocation or Status Information aAcess Fee

There is no revocation fee or access fee to status information.

9.1.4. Rates for Other services

Charge Fees for other services of CA Raiz are defined in the document PRICING POLICY GUIDELINES OF THE RAIZ CERTIFICATOR AUTHORITY OF ICP-BRASIL [13].

9.1.5. Refund policy

Not applicable.

9.2. Financial Responsibility

SERPRO SSL CA liability will be verified as provided by Brazilian law.

9.2.1. Insurance Coverage

Refer to § 4 CPS

9.2.2. Other Asset

As per this CPS regulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

Refer to § 4 CPS

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

9.3.1.1. All information collected, generated, transmitted and maintained by the CA and the linked RA are considered confidential, except for the information mentioned in item 9.3.2.

9.3.1.2. As a general principle, no documents, information or records provided to the linked RA should be disclosed.

9.3.2. Information Not Within the Scope of Confidential Information

The following documents from the CA and linked RA are considered non-confidential documents:

a) certificates and CRL / OCSP issued by the CA;

b) corporate or personal information that is part of certificates or public directories;

c) the CP implemented by the CA;

d) the CPS of the CA;

e) public version of the PS; and

f) the completion of the audit reports.

9.3.2.1. Certificates, CRL and corporate or personal information that are necessarily part of them or from public directories are considered non-confidential information.

9.3.2.2. The following CA documents are also considered non-confidential documents:

a) any applicable CP;

b) any CPS;

c) public versions of the Security Policy - PS; and

d) the completion of the audit reports.

9.3.2.3. The SERPRO SSL CA may also disclose, on a consolidated or segmented basis by type of certificate, the number of certificates or time stamps issued within the scope of ICP-Brasil.

9.3.3. Responsibility to Protect Confidential Information

9.3.3.1. Participants who receive or have access to confidential information have mechanisms that ensure protection and confidentiality, avoiding its use or disclosure to a relying party, under penalty of liability, in accordance with the law.

9.3.3.2. The digital signature key of SERPRO SSL CA was generated and is maintained by the CA itself, which is responsible for its secrecy. Disclosure or improper use of the private signature key by the CA will be your sole responsibility.

9.3.3.3. subscribers of certificates issued to individuals or those responsible for the use of certificates issued to legal entities, equipment or applications, will be responsible for the generation, maintenance and confidentiality of their respective private keys. In addition, they are responsible for the disclosure or improper use of these same keys.

9.3.3.4. Not applicable.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

CA ensures the protection of personal data in accordance with its Privacy Policy.

9.4.2. Information Treated as Private

As a general principle, any document, information or record that contains personal data provided to the CA will be considered confidential, unless otherwise provided for by law, or when expressly authorized by the respective subscriber, in accordance with applicable law.

9.4.3. Information not Deemed Private

Information on revocation of end-user certificates is provided in the CA CRL / OCSP.

9.4.4. Responsibility to Protect Private Information

CA and RA are responsible for the improper disclosure of confidential information, under the forms of the applicable legislation.

9.4.5. Notice and Consent to use Private Information

The private information obtained by the CA may be used or disclosed to a relying party with the express authorization of the respective subscriber, according to the applicable legislation.

The certificate subscriber and his legal representative will have wide access to any of his own data and identifications, and will be able to authorize the disclosure of his records to other people.

Formal permits can be presented in two ways:

a) by electronic means, containing a valid signature guaranteed by a certificate recognized by ICP-Brasil; or

b) by means of a written request with a recognized signature.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

As a general guideline, no document, information or record under the custody of the CA will be provided to anyone, except the subscriber or his legal representative, duly constituted by a public or private instrument, with specific powers, prohibited substitution.

Private or confidential information under the custody of the CA may be used for the instruction of administrative or judicial proceedings, or by court order or the competent administrative authority, subject to the applicable legislation regarding the secrecy and protection of data before relying party.

9.4.7. Other Information Disclosure Circumstances

Not applicable.

9.4.8. Relying Parties Information

No document, information or record under the custody of RA or SERPRO SSL CA, shall be provided to any person, except when the person requesting it, by means of a duly constituted instrument, is authorized to do so and correctly identified.

9.5. Intellectual Property Rights

According to Brazilian legislation.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

The SERPRO SSL CA declares and warrants the following, as well as the requirements of the CA / Browser Forum [15]:

9.6.1.1. Certificate authorization

The SERPRO SSL CA implements procedures to verify the authorization to issue an ICP-Brasil certificate, contained at Sections 3 and 4.

9.6.1.2. Accuracy of information

The SERPRO SSL CA implements procedures to verify the accuracy of the information in the certificates, contained at Sections 3 and 4.

The Root CA, in the scope of the accuracy of the information contained in the certificates that it issues, analyzes, audits and inspects the processes of the subsequent CAs and RA in the form of its CPS, CP and complementary standards.

9.6.1.3. Applicant identification

The SERPRO SSL CA implements procedures to verify the identification of certificate applicants, contained at Sections 3 and 4.

The SERPRO SSL CA, within the scope of the identification of the applicant contained in the certificates it issues, analyzes, audits and inspects the processes of the subsequent CA and RA in the form of its CPS, CP and complementary standards.

9.6.1.4. Consent of the subscribers

The SERPRO SSL CA implements forms of consent or ownership, contained at Sections 3 and 4.

9.6.1.5. Service

The SERPRO SSL CA maintains 24x7 access to its repository with the information of its own certificate and the CRL / OCSP.

9.6.1.6. Revocation

The SERPRO SSL CA will revoke ICP-Brasil certificates for any reason specified in the ICP-Brasil rules and in the CA / Browser Forum documents [15].

9.6.1.7. Legal Existence

This CPS is in legal compliance with MP 2,200-2, of August 24, 2001, and applicable legislation.

9.6.2. RA Representations and Warranties.

Refer to § 4.

9.6.3. Subscriber Representations and Warranties

9.6.3.1. All information necessary for the identification of the certificate subscriber must be provided in a complete and accurate manner. By accepting the certificate issued by the CA, the subscriber is responsible for all information provided by it and contained in that certificate.

9.6.3.2. The SERPRO SSL CA informs to the Root CA of any compromise of its private key and requests the immediate revocation of its certificate.

9.6.4. Relying Parties Representations and Warranties

9.6.4.1. A relying party must:

a) refuse to use the certificate for purposes other than those provided for in this CPS;

b) verify, at any time, the validity of the certificate.

9.6.4.2. The SERPRO SSL CA certificate is considered valid when:

i. has been issued by the CA;

ii. not appear as revoked by the CA;

iii. is not expired; and

iv. can be verified using the valid CA certificate.

9.6.4.3. The use or acceptance of certificates without observing the measures described is at the risk and expense of the relying party who uses or accepts the use of the respective certificate.

9.6.5. Representations and Warranties of Other Participants

Not applicable.

9.7. Disclaimer of Warranties

Not applicable.

9.8. Limitations of liability

The CA is not liable for damages that are not attributable to it or that it has not caused, in accordance with current legislation.

9.9. Indemnities

The CA is liable for any damage that it causes, and is imputable to it, in accordance with the legislation in force, ensuring the right of recourse against the responsible agent or entity.

9.10. Term and Termination

9.10.1. Term

This CPS takes effect as of the publication that approves it, and will remain valid and effective until it is revoked or replaced, expressly or tacitly.

9.10.2. Termination

This CPS will remain in force for an indefinite period, remaining valid and effective until it is revoked or replaced, expressly or tacitly.

9.10.3. Effect of Termination and Survival

The acts performed under this CPS are valid and effective for all legal purposes, taking effect even after their revocation or replacement.

9.11. Individual Notices and Communications with Participants

Notifications, subpoenas, requests or any other necessary communication subject to the practices described in this CPS will be made, preferably, by digitally signed e-mail, or, if

this is not possible, by letter from the competent authority or publication in the Federal Official Gazette.

9.12. Amendments

9.12.1. Procedure for Amendments

Any changes to this CPS must be submitted to CA Raiz(Root CA).

9.12.2. Notification Mechanism and Periods

Change in this CPS will be published on the SERPRO SSL CA website.

9.12.3. Circumstances Under Which the OID Must be Changed.

Not applicable.

9.13. Dispute Resolution Provisions

9.13.1. Disputes arising from this CPS will be resolved in accordance with current legislation.

9.13.2. The SERPRO SSL CA CPS will not prevail over the standards, criteria, practices and procedures of ICP-Brasil.

9.14. Governing Law

This DCP is governed by the legislation of the Federative Republic of Brazil, notably Provisional Measure No. 2,200-2, dated 08.24.2001, and the legislation that replaces or changes it, as well as the other laws and regulations in force in Brazil.

9.15. Compliance With Applicable Law

The SERPRO SSL CA is subject to the applicable legislation, committing itself to fulfill and observe the obligations and rights provided for by law.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

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

9.16.2. Assignment

The rights and obligations provided for in this DCP are of a public order and unavailable, and cannot be assigned or transferred to relying party.

9.16.3. Severability

The invalidity, nullity or ineffectiveness of any of the provisions of this CPS will not prejudice the other provisions, which will remain fully valid and effective. In this case, the

invalid, null or ineffective provision will be considered as unwritten, so that this CPS will be interpreted as if it did not contain such provision, and as far as possible, maintaining the original intention of the remaining provisions.

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

According to current legislation.

9.16.5. Force Majeure

SERPRO SSL CA is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond SERPRO SSL CA´s reasonable control. The operation of the Internet is beyond SERPRO SSL CA´s reasonable control.

9.17. Other Provisions

This CPS was submitted for approval, during the accreditation process of SERPRO SSL CA, as established in the document CRITERIA AND PROCEDURES FOR CACREDITATION 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. REFER TOENCED 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 Name	Code
[2]	CRITERIA AND PROCEDURES FOR SUPERVISION OF THE MEMBERS OF ICP-BRASIL	**DOC-ICP-09**
[3]	CRITERIA AND PROCEDURES FOR PERFORMING AUDITS AT THE INTEGRATING ENTITIES OF ICP-BRASIL	**DOC-ICP-08**
[6]	CRITERIA AND PROCEDURES FOR CACREDITATION OF ICP-BRAZIL'S INTEGRATING ENTITIES	**DOC-ICP-03**
[7]	MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRASIL	**DOC-ICP-04**
[8]	SECURITY POLICY OF ICP-BRASIL	**DOC-ICP-02**

[12]	MINIMUM REQUIREMENTS FOR PRCATICE STATEMENTS BY ICP-BRASIL TIME STAMP AUTHORITIES	**DOC-ICP-12**
[13]	ICP-BRASIL ROOT CERTIFICATION AUTHORITY FEE POLICY	**DOC-ICP-06**
[16]	GUIDELINES FOR FREQUENCY AND TIME SYNCHRONIZATION IN THE BRAZILIAN PUBLIC KEY INFRASTRUCTURE ICP-BRASIL	**DOC-ICP 07**

10.2. The documents below approved by Normative Instruction of CA Raiz, 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 Name	Code
[1]	MINIMUM SECURITY CHRACATERISTICS FOR RA OF ICP-BRASIL	**DOC-ICP-03.01**
[9]	STANDRADS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL	**DOC-ICP-01.01**
[10]	PROCEDURES FOR IDENTIFYING APPLICANTS AND COMMUNICATING IRREGULRAITIES IN THE PROCESS OF ISSUING A ICP-BRASIL DIGITAL CERTIFICATE	**DOC-ICP-05.02**
[11]	PROCEDURES FOR BIOMETRIC IDENTIFICATION AT ICP-BRASIL PROCEDURES FOR CONFIRMING REGISTRATION OF DIGITAL CERTIFICATE APPLICANTS USING VIDEOCONFERENCE	**DOC-ICP-05.03**
[16]	PROCEDURES FOR CONFIRMING REGISTRATION OF DIGITAL CERTIFICATE APPLICANTS USING VIDEOCONFERENCE	**DOC-ICP-05.05**

10.3. The documents below are approved by CA Raiz and can be changed, when necessary, by publishing a new version on the website http://www.iti.gov.br

Ref	Document Name	Code
[4]	TEMPLATE OF HOLDING TERMS(FORM)	**ADE-ICP-05.B**

11. BIBLIOGRAPHIC REFERENCES

BRAZILIAN ASSOCIATION OF TECHNICAL STANDRADS. 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.