

www.serpro.gov.br

Certificate Policy

SERPRO SSL Certification Authority

Server Authentication(SSL/TLS)

(SERPRO SSL CA)

Version 3.1

June, 2021



Índice

Review Control.....	9
1. INTRODUCTION.....	10
1.1. Overview.....	10
1.2. Document Name and Identification.....	10
1.3. PKI Participants - ICP-Brasil.....	11
1.3.1. Certification Authority.....	11
1.3.2. Registration Authorities.....	11
1.3.3. Subscribers.....	11
1.3.4. Relying Parties.....	11
1.3.5. Certificate Managers.....	11
1.3.6. Other Participants.....	12
1.4. Certificate Usage.....	12
1.4.1. Appropriate Certificate Usage.....	12
1.4.2. Prohibited Certificate Uses.....	13
1.5. Policy Administration.....	13
1.5.1. Organization Administering the Document.....	13
1.5.2. Contact Person.....	13
1.5.3. Person Determining CP/CPS Suitability for the Policy.....	13
1.5.4. CPS Approval Procedures.....	14
1.6. Acronyms.....	14
2. Publication AND REPOSITORY RESPONSIBILITIES.....	15
2.1. Repositories.....	16
2.2. Publication of Certificate Information.....	16
2.3. Access Controls on Repositories.....	16
2.4. Time or Frequency of Publication.....	16
3. IDENTIFICATION AND AUTHENTICATION.....	16
3.1. Naming.....	16
3.1.1. Types of names.....	16
3.1.2. Need for Names To Be Meaningful.....	16
3.1.3. Anonymity or Pseudonymity of Subscribers.....	16
3.1.4. Rules For Interpreting Various Names Forms.....	16
3.1.5. Uniqueness of Names.....	16
3.1.6. Recognition, Authentication, and Role of Trademarks.....	16
3.1.7. Trademark Recognition.....	16
3.2. Initial Identity Validation.....	16
3.2.1. Method to Prove Possession of Private Key.....	16
3.2.2. Authentication of Organization Identity.....	16
3.2.3. Authentication of Individual Identity.....	16
3.2.4. Non-Verified Subscriber Information.....	16
3.2.5. Validation of Authority.....	16

3.2.6. Criteria for Interoperation.....	16
3.2.7. Device or Application Authentication.....	16
3.2.8. Complementary procedures.....	16
3.3. Identification and authentication for Re-Key Requests.....	16
3.3.1. Identification and Authentication For Routine Re-Key.....	16
3.3.2. Identification and Authentication for Re-Key After Revocation.....	16
3.4. Identification and Authentication for Revocation Request.....	16
4. CERTIFICATE LIFE-CYCLE OPERACIONAL REQUIREMENTS.....	16
4.1. Certificate Application.....	17
4.1.1. Who Can Submit a Certificate Application.....	17
4.1.2. Enrollment Process and Responsibilities.....	17
4.2. Certificate Application Processing.....	17
4.2.1. Performing Identification and Authentication Functions.....	17
4.2.2. Approval or Rejection of Certificate Applications.....	17
4.2.3. Time to Process the Certificate Applications.....	17
4.2.4. Certificate Authority Authorisation (CAA).....	17
4.3. Certificate Issuance.....	17
4.3.1. CA actions During Certificate Issuance.....	17
4.3.2. Notifications to Subscriber By the CA of Issuance of certificate.....	17
4.4. Certificate Acceptance.....	17
4.4.1. Conduct Constituting Certificate Acceptance.....	17
4.4.2. Publication of the Certificate by the CA.....	17
4.4.3. Notification of Certificate Issuance by the ca to other entities.....	17
4.5. Key pair and Certificate Usage.....	17
4.5.1. Subscriber Private Key and Certificate Usage.....	17
4.5.2. Relying Party Public Key and Certificate Usage.....	17
4.6. Certificate Renewal.....	17
4.6.1. Circumstances for Certificate Renewal.....	17
4.6.2. Who May Request Renewal.....	17
4.6.3. Processing Certificate Renewal Requests.....	17
4.6.4. Notification of New Certificate Issuance to Subscriber.....	17
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate.....	17
4.6.6. Publication of the Renewal Certificate by CA.....	17
4.6.7. Notification of Certificate Issuance by the CA to Other Entities.....	17
4.7. Certificate Re-key.....	17
4.7.1. Circumstances for Certificates Re-Key.....	17
4.7.2. Who May Request Certification of a New Public Key.....	17
4.7.3. Processing Certificate Re-Keying Request.....	18
4.7.4. Notification of New Certificate Issuance to Subscriber.....	18
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate.....	18
4.7.6. Publication of a new CA certified key.....	18
4.7.7. Notification of Certificate Issuance By the CA to Other Entities.....	18
4.8. Certificate Modification.....	18
4.8.1. Circumstances for Certificate Modification.....	18

4.8.2. Who May Request Certificate Modification.....	18
4.8.3. Processing Certificate Modification Requests.....	18
4.8.4. Notification New Certificate Issuance to Subscriber.....	18
4.8.5. Conduct Constituting Acceptance of Modified Certificate.....	18
4.8.6. Publication of the Modified Certificate by the CA.....	18
4.8.7. Notification of Certificate Issuance by the CA to Other Entities.....	18
4.9. Certificate Revocation and Suspension.....	18
4.9.1. Circumstances for revocation.....	18
4.9.2. Who Can Request Revocation.....	18
4.9.3. Procedure for Revocation Request.....	18
4.9.4. Revocation Request Grace Period.....	18
4.9.5. Time Within Which CA Must Process the Revocation Request.....	18
4.9.6. Revocation Checking Requirements for Relying Parties.....	18
4.9.7. CRL Issuance Frequency.....	18
4.9.8. Maximum Latency for CRLs.....	18
4.9.9. Online Revocation / Status Check Availability.....	18
4.9.10. Online Revocation Checking Requirements.....	18
4.9.11. Other Forms of Revocation Advertisements Available.....	18
4.9.12. Special Requirements Related of Key Compromise.....	18
4.9.13. Circumstances For Suspension.....	18
4.9.14. Who can request suspension.....	18
4.9.15. Procedure for Suspension Request.....	18
4.9.16. Limits on Suspension Period.....	19
4.10. Certificate Status Services.....	19
4.10.1. Operational Characteristics.....	19
4.10.2. Services Availability.....	19
4.10.3. Operational features.....	19
4.11. End of Subscription.....	19
4.12. Key Escrow and Recovery.....	19
4.12.1. Key recovery and custody policy and practices.....	19
4.12.2. Session Key Encapsulation and Recovery Policy and Practices.....	19
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	19
5.1. Physical Control.....	19
5.1.1. Site Location and Construction.....	19
5.1.2. Physical Access.....	19
5.1.3. Power and Air Conditioning.....	19
5.1.5. Fire Prevention and Protection.....	20
5.1.6. Media Storage.....	20
5.1.7. Waste Disposal.....	20
5.1.8. Off-Site Backup.....	20
5.2. Procedural Controls.....	20
5.2.1. Trusted Roles.....	20
5.2.2. Number of Persons Required per Task.....	20
5.2.3. Identification and Authentication for Each Role.....	20

5.2.4. Roles Requiring Separation of Duties.....	20
5.3. Personnel Controls.....	20
5.3.1. Qualifications, Experience, and Clearance Requirements.....	20
5.3.2. Background Check Procedures.....	20
5.3.3. Training Requirements and Procedures.....	20
5.3.4. Retraining Frequency and Requirements.....	20
5.3.5. Job Rotation Frequency and Sequence.....	20
5.3.6. Sanction for Unauthorized Actions.....	20
5.3.7. Independent Contractor Requirements.....	20
5.3.8. Documentation Supplied to Personnel.....	20
5.4. Audit Logging Procedures.....	20
5.4.1. Types of Event Recorded.....	20
5.4.2. Frequency of Processing and Archiving Audit Logs.....	20
5.4.3. Retention Period for Audit Logs.....	20
5.4.4. Protection of Audit Log.....	20
5.4.5. Audit Log Backup Procedures.....	20
5.4.6. Audit Collection System (Internal Vs. External).....	20
5.4.7. Notification of Event-Causing Subject.....	20
5.4.8. Vulnerability Assessments.....	20
5.5. Records Archival.....	20
5.5.1. Types of Records Archived.....	21
5.5.2. Retention Period for Archive.....	21
5.5.3. Protection of Archive.....	21
5.5.4. Archive Backup Procedures.....	21
5.5.5. Requirements for Time-Stamping of Records.....	21
5.5.6. Archive Collection System (Internal or External).....	21
5.5.7. Procedures to Obtain and Verify Archive Information.....	21
5.6. Key Changeover.....	21
5.7. Compromise and Disaster Recovery.....	21
5.7.1. Incident and Compromise Handling Procedures.....	21
5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted.....	21
5.7.3. Recovery Procedures After Key Compromise.....	21
5.7.4. Business Continuity Capability after Disaster.....	21
5.8. CA or RA Termination.....	21
6. Technical Security Controls.....	21
6.1. Key Pair Generation and Installation.....	21
6.1.1. Key Pair Generation.....	21
6.1.2. Private Key Delivered to Subscriber.....	22
6.1.3. Public Key Delivery to Certificate Issuer.....	22
6.1.4. Public Key Available to Certificate Issuer.....	23
6.1.5. Key sizes.....	23
6.1.6. Public Key Parameters Generation and Quality Checking.....	23
6.1.7. Key Usage Purposes(AS PER X.509 V3 KEY USAGE FIELD).....	23
6.2. Private Key Protection and Cryptographic Module Engineering Controls.....	23
6.2.1. Cryptographic Module Standards and Controls.....	24

6.2.2. Private Key (n out of m) Multi-person Control.....	24
6.2.3. Private Key Escrow.....	24
6.2.4. Private key backup.....	24
6.2.5. Private Key Archival.....	24
6.2.6. Private Key Transfer into or from a Cryptographic Module.....	24
6.2.7. Private Key Storage in Cryptographic Module.....	25
6.2.8. Activating Private Keys.....	25
6.2.9. Deactivating Private Keys.....	25
6.2.10. Destroying Private Keys.....	25
6.3. Other Aspects of Key Pair Management.....	25
6.3.1. Public Key Archival.....	25
6.3.2. Certificate Operational Periods and Key Pair Usage Periods.....	25
6.4. Activation Data.....	26
6.4.1. Activation Data Generation and Installation.....	26
6.4.2. Activation Data Protection.....	26
6.4.3. Other Aspects of Activation Data.....	26
6.5. Computer Security Controls.....	26
6.5.1. Specific Computer Security Technical Requirements.....	26
6.5.2. Computational Security Ration.....	27
6.6. Lifecycle Technical Controls.....	27
6.6.1. System Development Controls.....	27
6.6.2. Security Management Control.....	27
6.6.3. Lifecycle Security Control.....	28
6.6.4. CLR Generation Controls.....	28
6.7. Network Security Controls.....	28
6.7.2. Firewall.....	29
6.7.3. Intrusion Detection System (IDS):.....	29
6.7.4. Unauthorized Access Registration.....	30
6.8. Time-Stamping.....	30
7. CERTIFICATE, CRL AND OCSP PROFILES.....	30
7.1. Certificate Profile.....	30
7.1.1. Version number.....	30
7.1.2. Certificate Content and Extensions; Application of RFC 5280.....	30
7.1.3. Algorithm Object Identifiers.....	33
7.1.4. Name formats.....	33
7.1.5. Name restrictions.....	34
7.1.6. Certificate Policy Object Identifier.....	34
7.1.7. Usage of the Policy Constraints Extension.....	35
7.1.8. Policy Qualifier Syntax and Semantics.....	35
7.1.9. Processing Semantics for Critical Certificate Policies Extensions.....	35
7.2. CRL Profile.....	35
7.2.1. Version Number.....	35
7.2.2. CRL and CRL Entry Extensions.....	35
7.3. OCSP profile.....	36

7.3.1. Version number.....	36
7.3.2. OCSP Extensions.....	36
8. CONFORMITY AUDIT AND OTHER ASSESSMENTS.....	36
8.1. Frequency and Circumstances of Assessments.....	36
8.2. Identification / Qualification of Assessor.....	36
8.3. Assessor's Relationship to Assessed Entity.....	36
8.4. Topics Covered by Assessment.....	36
8.5. Actions Taken as a Result of Deficiency.....	36
8.6. Communication of Results.....	36
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS9. OTHER BUSINESS AND LEGAL Matters	36
9.1. Fees.....	37
9.1.1. Certificate Issuance or Renewal Fees.....	37
9.1.2. Certificate Access Fees.....	37
9.1.3. Revocation or Status Information aAccess Fee.....	37
9.1.4. Rates for Other services.....	37
9.1.5. Refund policy.....	37
9.2. Financial Responsibility.....	37
9.2.1. Insurance Coverage.....	37
9.2.2. Other Asset.....	37
9.2.3. Insurance or Warranty Coverage for End-Entities.....	37
9.3. Confidentiality of Business Information.....	37
9.3.1. Scope of Confidential Information.....	37
9.3.2. Information Not Within the Scope of Confidential Information.....	37
9.3.3. Responsibility to Protect Confidential Information.....	37
9.4. Privacy of Personal Information.....	37
9.4.1. Privacy Plan.....	37
9.4.2. Information Treated as Private.....	37
9.4.3. Information not Deemed Private.....	37
9.4.4. Responsibility to Protect Private Information.....	37
9.4.5. Notice and Consent to use Private Information.....	37
9.4.6. Disclosure Pursuant to Judicial or Administrative Process.....	37
9.4.7. Other Information Disclosure Circumstances.....	37
9.4.8. Relying Parties Information.....	37
9.5. Intellectual Property Rights.....	37
9.6. Representations and Warranties.....	37
9.6.1. CA Representations and Warranties.....	38
9.6.2. RA Representations and Warranties.....	38
9.6.3. Subscriber Representations and Warranties.....	38
9.6.4. Relying Parties Representations and Warranties.....	38
9.6.5. Representations and Warranties of Other Participants.....	38
9.7. Disclaimer of Warranties.....	38
9.8. Limitations of liability.....	38
9.9. Indemnities.....	38
9.10. Term and Termination.....	38

9.10.1. Term.....	38
9.10.2. Termination.....	38
9.10.3. Effect of Termination and Survival.....	38
9.11. Individual Notices and Communications with Participants.....	38
9.12. Amendments.....	38
9.12.1. Procedure for Amendments.....	38
9.12.2. Notification Mechanism and Periods.....	38
9.12.3. Circumstances Under Which the OID Must be Changed.....	38
9.13. Dispute Resolution Provisions.....	38
9.14. Governing Law.....	38
9.15. Compliance With Applicable Law.....	38
9.16. Miscellaneous Provisions.....	38
9.16.1. Entire Agreement.....	38
9.16.2. Assignment.....	39
9.16.3. Severability.....	39
9.16.4. Enforcement (attorneys' fees and waiver of rights).....	39
9.16.5. Force Majeure.....	39
9.17. Other Provisions.....	39
10. Referenced documents.....	39
11. REFERÊNCIAS BIBLIOGRÁFICAS.....	40

Review Control

Ver.	Review Date	Staff	Status	Changes
1.0	01/09/2019	Lucia Castelli	Draft	Inicial
1.0	01/09/2019	Osni Bunn	Approved	
1.1	22/11/2019	Lucia Castelli	Revision	Addition statements from CabForum 1.6.6.
1.1	22/11/2019	Osni Bunn	Approved	
1.2	26/02/2020	Lucia Castelli	Revision	Update url - <i>Frauds</i>
1.2	26/02/2020	Osni/Alice	Approved	
1.3	13/03/2020	Lucia Castelli	Revision	Updated de distribution point of CRL: – Section 7.1.2 “d”
1.3	13/03/2020	Alice Vasconcellos	Approved	
2.0	12/05/2020	Lucia Castelli	Revision	Updated URL OCSP and OID OV SSL; Update with itens from Resolution 156 and 169 (ICP-BRASIL).
2.0	12/05/2020	Alice Vasconcellos	Approved	
3.0	Novembro/2020	Lucia Castelli	Revision	Update with section from Resolution 179(ICP_BRASIL)
3.0	Novembro/2020	Alice Vasconcellos	Approved	
3.1	June/2021	Lucia Castelli	Revision	Update Reference for ITI documents;
3.1	June/2021	Alice Vasconcellos	Approved	

1. INTRODUCTION

1.1. Overview

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

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

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

1.1.3. The structure of this CP is based on RFC 3647.

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

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

1.1.6. Not applicable

1.1.7. Not applicable

1.1.8. Not applicable

1.1.9. Not applicable

1.1.10. Not applicable

1.1.11. Not applicable

1.1.12. Not applicable

1.2. Document Name and Identification

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

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

Certificate Type	OID
A1	2.16.76.1.2.1.105.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 1.2”).

1.3. PKI Participants - ICP-Brasil

1.3.1. Certification Authority

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

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

1.3.2. Registration Authorities

1.3.2.1. The Registration Authority, involved in issuing SSL certificates, meets and follows the requirements established in sections 4.2 and 5.3 of this document.

The web page (URL) is <https://certificados.serpro.gov.br/serprossl> where the data below referring to the Registration Authorities, responsible for the processes of receiving, validating and forwarding the request for issuance or revocation of digital certificates, and identification of their applicants:

- a) list of all accredited RA, with information on the CP they implement;
- b) list of RA that have been disqualified from the CA chain, with the respective date of disqualification;

1.3.3. Subscribers

The Certificates issued by the CA are for equipment or applications, with individuals and companies holding the certificates.

As the certificate holder is a legal entity, an individual will be designated as responsible for the certificate, who will be the holder of the private key.

Preferably, the legal representative of the legal entity or one of its legal representatives will be designated as responsible for the certificate.

1.3.4. Relying Parties

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

1.3.5. Certificate Managers

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

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 1.3”).

1.4. Certificate Usage

1.4.1. Appropriate Certificate Usage

(*) (“1.4.1.1. The certificates issued under this CP are suitable for use only in the applications presented in the table described below:

Certified Policies	Aplicações Apropriadas
CP SERPRO SSL CP A1	<p>Certificates issued under this policy are considered suitable for electronic signature, non-retractability, integrity and authentication.</p> <p>They can be used in the following applications:</p> <ul style="list-style-type: none">• Confirmation of Identity on the web;• E-mail;• On-Line Transactions;• Virtual Private Network (VPN);• Electronic Transactions;• Creating a session key and signing electronic documents with verification of the integrity of your information.

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

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

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

1.4.2. Prohibited Certificate Uses

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

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

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

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

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 1.4”).*

1.5. Policy Administration

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

1.5.1. Organization Administering the Document

The organization administering the CP/CPS is SERPRO

1.5.2. Contact Person

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

Name: Pedro Moacir Rigo Motta

Address: SGAN 601, Module V, Asa Norte, Brasília, Federal District, CEP 70.836-900.

Email: certificates@serpro.gov.br

Phone: +556120217957

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

Web page: <https://atendimento.serpro.gov.br/certificacaodigital>

E-mail: css.serpro@serpro.gov.br

Phone: +55 08007282323

1.5.3. Person Determining CP/CPS Suitability for the Policy

Name: Pedro Moacir Rigo Motta

Phone: +55 61 20217957

Email: certificates@serpro.gov.br

1.5.4. CPS Approval Procedures

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

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

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 1.5”).

1.6. Acronyms

SIGLA	DESCRIÇÃO
CA	Certification Authorities
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AICPA	American Institute of Certified Public Accountants
AR	Autoridades de Registro
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CICA	Canadian Institute of Chartered Accountants
CMM-SEI	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DNS	Domain Name System
DPC	Declaração de Práticas de Certificação
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

IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	<i>Intrusion Detection System</i>
IEC	<i>International Electrotechnical Commission</i>
IETF PKIX	<i>Internet Engineering Task Force - Public-Key Infrastructured (X.509)</i>
INMETRO	<i>Instituto Nacional de Metrologia, Qualidade e Tecnologia</i>
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	<i>National Institute of Standards and Technology</i>
OCSP	<i>Online Certificate Status Protocol</i>
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession PS Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 1.6”).

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The follow items bellow, refer to § 2 CPS:

2.1. Repositories

2.2. Publication of Certificate Information

2.3. Access Controls on Repositories

2.4. Time or Frequency of Publication

3. IDENTIFICATION AND AUTHENTICATION

The follow items bellow, refer to § 3 CPS

3.1. Naming

3.1.1. Types of names

3.1.2. Need for Names To Be Meaningful

3.1.3. Anonymity or Pseudonymity of Subscribers

3.1.4. Rules For Interpreting Various Names Forms

3.1.5. Uniqueness of Names

3.1.6. Recognition, Authentication, and Role of Trademarks

3.1.7. Trademark Recognition

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

3.2.2. Authentication of Organization Identity

3.2.3. Authentication of Individual Identity

3.2.4. Non-Verified Subscriber Information

3.2.5. Validation of Authority

3.2.6. Criteria for Interoperation

3.2.7. Device or Application Authentication

3.2.8. Complementary procedures

3.3. Identification and authentication for Re-Key Requests

3.3.1. Identification and Authentication For Routine Re-Key

3.3.2. Identification and Authentication for Re-Key After Revocation

3.4. Identification and Authentication for Revocation Request

4. CERTIFICATE LIFE-CYCLE OPERACIONAL REQUIREMENTS

The follow items bellow refer to § 4 CPS

- 4.1. Certificate Application**
 - 4.1.1. Who Can Submit a Certificate Application**
 - 4.1.2. Enrollment Process and Responsibilities**
- 4.2. Certificate Application Processing**
 - 4.2.1. Performing Identification and Authentication Functions**
 - 4.2.2. Approval or Rejection of Certificate Applications**
 - 4.2.3. Time to Process the Certificate Applications**
 - 4.2.4. Certificate Authority Authorisation (CAA)**
- 4.3. Certificate Issuance**
 - 4.3.1. CA actions During Certificate Issuance**
 - 4.3.2. Notifications to Subscriber By the CA of Issuance of certificate**
- 4.4. Certificate Acceptance**
 - 4.4.1. Conduct Constituting Certificate Acceptance**
 - 4.4.2. Publication of the Certificate by the CA**
 - 4.4.3. Notification of Certificate Issuance by the ca to other entities**
- 4.5. Key pair and Certificate Usage**
 - 4.5.1. Subscriber Private Key and Certificate Usage**
 - 4.5.2. Relying Party Public Key and Certificate Usage**
- 4.6. Certificate Renewal**
 - 4.6.1. Circumstances for Certificate Renewal**
 - 4.6.2. Who May Request Renewal**
 - 4.6.3. Processing Certificate Renewal Requests**
 - 4.6.4. Notification of New Certificate Issuance to Subscriber**
 - 4.6.5. Conduct Constituting Acceptance of a Renewal Certificate**
 - 4.6.6. Publication of the Renewal Certificate by CA**
 - 4.6.7. Notification of Certificate Issuance by the CA to Other Entities**
- 4.7. Certificate Re-key**
 - 4.7.1. Circumstances for Certificates Re-Key**
 - 4.7.2. Who May Request Certification of a New Public Key**

- 4.7.3. Processing Certificate Re-Keying Request**
- 4.7.4. Notification of New Certificate Issuance to Subscriber**
- 4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate**
- 4.7.6. Publication of a new CA certified key**
- 4.7.7. Notification of Certificate Issuance By the CA to Other Entities**
- 4.8. Certificate Modification**
 - 4.8.1. Circumstances for Certificate Modification**
 - 4.8.2. Who May Request Certificate Modification**
 - 4.8.3. Processing Certificate Modification Requests**
 - 4.8.4. Notification New Certificate Issuance to Subscriber**
 - 4.8.5. Conduct Constituting Acceptance of Modified Certificate**
 - 4.8.6. Publication of the Modified Certificate by the CA**
 - 4.8.7. Notification of Certificate Issuance by the CA to Other Entities**
- 4.9. Certificate Revocation and Suspension**
 - 4.9.1. Circumstances for revocation**
 - 4.9.2. Who Can Request Revocation**
 - 4.9.3. Procedure for Revocation Request**
 - 4.9.4. Revocation Request Grace Period**
 - 4.9.5. Time Within Which CA Must Process the Revocation Request**
 - 4.9.6. Revocation Checking Requirements for Relying Parties**
 - 4.9.7. CRL Issuance Frequency**
 - 4.9.8. Maximum Latency for CRLs**
 - 4.9.9. Online Revocation / Status Check Availability**
 - 4.9.10. Online Revocation Checking Requirements**
 - 4.9.11. Other Forms of Revocation Advertisements Available**
 - 4.9.12. Special Requirements Related of Key Compromise**
 - 4.9.13. Circumstances For Suspension**
 - 4.9.14. Who can request suspension**
 - 4.9.15. Procedure for Suspension Request**

4.9.16. Limits on Suspension Period

4.10. Certificate Status Services

4.10.1. Operational Characteristics

4.10.2. Services Availability

4.10.3. Operational features

4.11. End of Subscription

4.12. Key Escrow and Recovery

4.12.1. Key recovery and custody policy and practices

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The follow items bellow refer to § 5 CPS

5.1. Physical Control

5.1.1. Site Location and Construction

5.1.2. Physical Access

5.1.2.1. Access Levels

5.1.2.2. Physical detection system

5.1.2.3. Access Control System

5.1.2.4. Emergency mechanisms

5.1.3. Power and Air Conditioning

5.1.4. Water Exposures

- 5.1.5. Fire Prevention and Protection**
- 5.1.6. Media Storage**
- 5.1.7. Waste Disposal**
- 5.1.8. Off-Site Backup**
- 5.2. Procedural Controls**
 - 5.2.1. Trusted Roles**
 - 5.2.2. Number of Persons Required per Task**
 - 5.2.3. Identification and Authentication for Each Role**
 - 5.2.4. Roles Requiring Separation of Duties**
- 5.3. Personnel Controls**
 - 5.3.1. Qualifications, Experience, and Clearance Requirements**
 - 5.3.2. Background Check Procedures**
 - 5.3.3. Training Requirements and Procedures**
 - 5.3.4. Retraining Frequency and Requirements**
 - 5.3.5. Job Rotation Frequency and Sequence**
 - 5.3.6. Sanction for Unauthorized Actions**
 - 5.3.7. Independent Contractor Requirements**
 - 5.3.8. Documentation Supplied to Personnel**
- 5.4. Audit Logging Procedures**
 - 5.4.1. Types of Event Recorded**
 - 5.4.2. Frequency of Processing and Archiving Audit Logs**
 - 5.4.3. Retention Period for Audit Logs**
 - 5.4.4. Protection of Audit Log**
 - 5.4.5. Audit Log Backup Procedures**
 - 5.4.6. Audit Collection System (Internal Vs. External)**
 - 5.4.7. Notification of Event-Causing Subject**
 - 5.4.8. Vulnerability Assessments**
- 5.5. Records Archival**

- 5.5.1. Types of Records Archived**
- 5.5.2. Retention Period for Archive**
- 5.5.3. Protection of Archive**
- 5.5.4. Archive Backup Procedures**
- 5.5.5. Requirements for Time-Stamping of Records**
- 5.5.6. Archive Collection System (Internal or External)**
- 5.5.7. Procedures to Obtaining and Verifying Archive Information**
- 5.6. Key Changeover**
- 5.7. Compromise and Disaster Recovery**
 - 5.7.1. Incident and Compromise Handling Procedures**
 - 5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted**
 - 5.7.3. Recovery Procedures After Key Compromise**
 - 5.7.3.1. Entity certificate is revoked**
 - 5.7.3.2. Entity key is compromised**
 - 5.7.4. Business Continuity Capability after Disaster**
- 5.8. CA or RA Termination**
- 6. Technical Security Controls**
 - 6.1. Key Pair Generation and Installation**
 - 6.1.1. Key Pair Generation**

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

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

The private key is stored using:

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

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

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

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

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

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

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

- a) the private key is unique and its secrecy is sufficiently assured;*
- b) the private key cannot, with reasonable security, be deducted and must be protected against forgeries carried out using currently available technologies; and*
- c) the private key can be effectively protected by the legitimate holder against use by third parties.*

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

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.1.1.”).*

6.1.2. Private Key Delivered to Subscriber

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

() ““6.1.2. It is the sole responsibility of the certificate holder to generate and keep his private key. If the CA is notified that a certificate's private key has been passed on to an unauthorized person or organization, the CA will arrange for the immediate revocation of the referring public key.*

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.1.2”).*

6.1.3. Public Key Delivery to Certificate Issuer

() (“Public keys are delivered to the CA through an online exchange using automatic functions from the CA's certification software.*

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.1.3.”)

6.1.4. Public Key Available to Certificate Issuer

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

- a) When a certificate is made available to its subscriber, the PKCS # 7 standard, defined in the STANDARDS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL [9] will be used;
- b) CA website <https://certificados.serpro.gov.br/serprossl>.
- c) Other safe means approved by the CG of ICP-Brasil.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.1.4”).

6.1.5. Key sizes

(*) (“6.1.5.1. The size of the cryptographic keys associated with the certificates issued by the CA is, at least, L = 2048 bits;

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.1.5.1”).

6.1.6. Public Key Parameters Generation and Quality Checking

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.1.6”).

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

(*) (“The certificates issued on this CP have activated the bits *digitalSignature e keyAgreement*.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.1.7”).

6.2. Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1. Cryptographic Module Standards and Controls

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

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

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.1”).*

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

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

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

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.2.”).*

6.2.3. Private Key Escrow

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

6.2.4. Private key backup

() (“6.2.4.1. Any certificate holder may, at its discretion, keep a backup copy of its own private key.*

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

6.2.4.3. *Not applicable.*

6.2.4.4. *Not applicable.*

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.4.”).*

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.*

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.5)”.*

6.2.6. Private Key Transfer into or from a Cryptographic Module

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

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.6)”*

6.2.7. Private Key Storage in Cryptographic Module

Refer to § 6.1.1.1. (CP)

6.2.8. Activating Private Keys

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

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

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.8)*”

6.2.9. Deactivating Private Keys

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

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.9)*”

6.2.10. Destroying Private Keys

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

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.2.10)*”

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

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

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.3.1)*”.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

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

6.3.2.2. *Not applicable.*

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

6.3.2.4. *Not applicable.*

6.3.2.5. *Not applicable.*

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.3.2”)

6.4. Activation Data

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.4”).

6.4.1. Activation Data Generation and Installation

(*) (“CA private key activation data is unique and random.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.4.1”).

6.4.2. Activation Data Protection

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.4.2”).

6.4.3. Other Aspects of Activation Data

Not applicable

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

(*) (“6.5.1.1. *The CA ensures that the generation of its key pair is performed in an offline environment, to prevent unauthorized remote access.*

6.5.1.2. *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.*

6.5.1.3. *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).

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

6.5.1.5. 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 AC 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.

6.5.1.6. 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.

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.5.1”).*

6.5.2. Computational Security Ration

Not applicable

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

() (“6.6.1.1. The CA has a SERPRO Digital Certification System, developed in open code.*

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

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.

** Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.6.1”).*

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.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.6.2”).

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.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 6.6.4”).

6.7. Network Security Controls

The follow items bellow refer to § 7 CPS

6.8. Time-Stamping

Not Applicable

7. CERTIFICATE, CRL AND OCSP PROFILES

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

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

The AC meets all the requirements established in items 2.2, 6.1.5. and 6.1.6. of this PC.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7”).

7.1. Certificate Profile

(*) (“All certificates issued by the CA under this CP conform to the format defined by the ITU X.509 version 3 or ISO/IEC 9594-8 standard.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1”).

7.1.1. Version number

(*) ("All certificates issued by the CA, according to this CP, implement the version 3 certificate defined in the ITU X.509 standard, according to the profile established in RFC 5280.

* *Our translation from* – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.1").

7.1.2. Certificate Content and Extensions; Application of RFC 5280

(*) (*7.1.2.1. In this item, PC describes all used certificate extensions and their criticality.

7.1.2.2. ICP-Brasil defines the following extensions as mandatory:

- a) "**Authority Key Identifier**", **non-critical**: contains the SHA-1 hash of the CA public key;
- b) "**Key Usage**", **critical**: configured as provided in item 7.1.2.7 of this document;
- c) "**Certificate Policies**", **non-critical**: contains the CP **OID 2.16.76.1.2.1.105** and the URL address of the website <https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf> with the CPS.

Server authentication certificates (SSL / TLS) contain the OID of the CA / B Forum Guidelines requirements certificate policy (**OV SSL = 2.23.140.1.2.2**).

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

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

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

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

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

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

➤ **For equipment or application certificate:**

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

- i. OID = 2.16.76.1.3.8 and content = business name in the CNPJ (National Register of Legal Entities), without abbreviations, if the certificate is a legal entity;
 - ii. OID = 2.16.76.1.3.4 and content = in the first 8 (eight) positions, the date of birth of the person responsible for the certificate, in the format ddmmaaaa; in the 11 (eleven) subsequent positions, the person's Individual Taxpayer Registration (CPF); in the 11 (eleven) subsequent positions, the Social Identification number - NIS (PIS, PASEP or CI); in the 15 (fifteen) subsequent positions, the RG number of the person responsible; in the 10 (ten) subsequent positions, the abbreviations of the RG issuing agency and the respective UF.
 - iii. OID = 2.16.76.1.3.2 and content = name of the person responsible for the certificate;
 - iv. OID = 2.16.76.1.3.3 and content = in the 14 (fourteen) positions the number of National Register of Legal Entities (CNPJ), if the certificate is for individuals legal;
- **For certificates of type SSL / TLS:** Field `dNSName`, mandatory, containing one or more domains owned or controlled by the holder, following the rules defined in RFC 5280 and RFC 2818, and in accordance with the WebTrust principles and criteria [6] and the CA / Browse Forum requirements [7].

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

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

- a) Information set defined in each otherName field must be stored as a string of type ASN.1 OCTET STRING or PRINTABLE STRING;
- b) When the CPF, NIS (PIS, PASEP or CI), ID, CNPJ, CEI, or Voter Registration numbers are not available, the corresponding fields must be completely filled in with "zero" characters;
- c) If the ID number is not available, the issuing agency and UF field should not be filled out. The same occurs for the municipality and UF field, if there is no registration number for the voter registration;
- d) All information of variable size referring to numbers, such as ID must be filled with "zero" characters to its left so that the maximum possible size is completed;
- e) The 10 (ten) positions of the information about the issuing body of the ID and UF refer to the maximum size, and only the positions necessary for its storage, from left to right, should be used. The same applies to the 22 (twenty-two) positions of the information on municipality and UF of the Title of Voter;
- f) Only the characters A to Z and 0 to 9 can be used, and special characters, symbols, spaces or any other are not allowed.

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

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

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

a) Not applicable

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

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

for Open Banking Transport certificates:

"Key Usage", critical: only *digitalSignature* and *keyEncipherment* bits are enabled;

"Extended Key Usage", not critical: contains the purpose: client authentication, OID = 1.3.6.1.5.5.7.3.2;

c, d, e, f and g → Not applicable.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.2").

7.1.3. Algorithm Object Identifiers

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

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.3").

7.1.4. Name formats

(*) ("7.1.4.1. Not applicable

7.1.4.2. Not applicable

7.1.4.3. Not applicable

7.1.4.4.

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

C = BR;

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

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

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

L = city of the holder's physical address;

Business Category (OID 2.5.4.15) = type of commercial category, which must contain: "Private Organization" or "Government Entity" or "Business Entity" or "NonCommercial Entity" ;

SERIALNUMBER (OID 2.5.4.5) = CPF or CNPJ, as per type of person;

Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR.

b) SSL Open Banking Certificate (Transportation):

The SSL Open Banking (Transportation) digital certificate adopts the "Distinguished Name" (DN) of the ITU X.500/ISO 9594 standard, with the following contents:

C = BR;

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

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

ST = unit of the federation of the certificate holder's physical address;

L = city of the holder's physical address;

OU = Participant Code associated with CNPJ listed in OpenBanking Brasil Directory Service;

UID = Software Statement ID registered in the Directory Service of OpenBanking Brasil and belonging to the CNPJ and Participant Code.

Business Category(OID 2.5.4.15), = type of commercial category, which must contain: "Private Organization" or "Government Entity" or "Business Entity" or "NonCommercial Entity";

Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR;

Serial Number(OID 2.5.4.5) = National Register of Legal Personnel (CNPJ) of the legal entity holding the certificate and associated with the organizational UnitName attribute and Software Statement ID, during validation with the OpenBanking Brasil Directory Service;

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

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.4”).*

7.1.5. Name restrictions

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

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

- a) accent marks, umlauts or cedillas should not be used; and
- b) in addition to the alphanumeric characters, only the following special characters may be used:

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

\	5C
---	----

Tabela 3 - Caracteres especiais admitidos em nomes

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.5”).

7.1.6. Certificate Policy Object Identifier

(*) (“The OID assigned to this Certificate Policy is: **2.16.76.1.2.1.105**.”)

Every certificate issued under this PC must contain, in the “Certificate Policies” extension, the corresponding OID.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.6”).

7.1.7. Usage of the Policy Constraints Extension

Not Applicable

7.1.8. Policy Qualifier Syntax and Semantics

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.8”).

7.1.9. Processing Semantics for Critical Certificate Policies Extensions

(*) (“Critical extensions must be interpreted in accordance with RFC 5280.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.1.9”).

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.

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.2.1”).

7.2.2. CRL and CRL Entry Extensions

(*) (“7.2.2.1. This CA implements the CRL extensions defined as mandatory, according Section 7.2.2.2.

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

a) **“Authority Key Identifier”**: must contain the SHA-1 hash of the CA public key that signs the CRL; and

b) **“CRL Number”**: **non-critical**: it must contain a sequential number for each CRL issued by CA.

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.2.2”*).

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.

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.3.1”*).

7.3.2. OCSP Extensions

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

The second entry contains the access method id-ad-ocsp, with the respective address <http://ocsp.serpro.gov.br/acserprossl.v1> of the OCSP responder, using the access protocol, HTTP.

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 7.3.2”*).

8. CONFORMITY AUDIT AND OTHER ASSESSMENTS

8.1. Frequency and Circumstances of Assessments

8.2. Identification / Qualification of Assessor

8.3. Assessor's Relationship to Assessed Entity

8.4. Topics Covered by Assessment

8.5. Actions Taken as a Result of Deficiency

8.6. Communication of Results

8.7. SELF-AUDITS

Refer § 8.7 CPS

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS9. OTHER BUSINESS AND LEGAL MATTERS

Each Sections bellow are refered § 9 CPS

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

9.1.2. Certificate Access Fees

9.1.3. Revocation or Status Information aAccess Fee

9.1.4. Rates for Other services

9.1.5. Refund policy

9.2. Financial Responsibility

9.2.1. Insurance Coverage

9.2.2. Other Asset

9.2.3. Insurance or Warranty Coverage for End-Entities

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

9.3.2. Information Not Within the Scope of Confidential Information

9.3.3. Responsibility to Protect Confidential Information

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

9.4.2. Information Treated as Private

9.4.3. Information not Deemed Private

9.4.4. Responsibility to Protect Private Information

9.4.5. Notice and Consent to use Private Information

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

9.4.7. Other Information Disclosure Circumstances

9.4.8. Relying Parties Information

9.5. Intellectual Property Rights

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

9.6.2. RA Representations and Warranties.

9.6.3. Subscriber Representations and Warranties

9.6.4. Relying Parties Representations and Warranties

9.6.5. Representations and Warranties of Other Participants

9.7. Disclaimer of Warranties**9.8. Limitations of liability****9.9. Indemnities****9.10. Term and Termination****9.10.1. Term****9.10.2. Termination****9.10.3. Effect of Termination and Survival****9.11. Individual Notices and Communications with Participants****9.12. Amendments****9.12.1. Procedure for Amendments****9.12.2. Notification Mechanism and Periods****9.12.3. Circumstances Under Which the OID Must be Changed****9.13. Dispute Resolution Provisions****9.14. Governing Law****9.15. Compliance With Applicable Law****9.16. Miscellaneous Provisions****9.16.1. Entire Agreement**

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

* *Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 9.16.1”).*

9.16.2. Assignment**9.16.3. Severability****9.16.4. Enforcement (attorneys' fees and waiver of rights)****9.16.5. Force Majeure****9.17. Other Provisions**

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

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 9.17”).

10. Referenced documents

(*) (“10.1. The documents below are approved by Resolutions of the Management Committee of ICP-Brazil, 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.	Nome do documento	Código
[3]	CRITERIA AND PROCEDURES FOR ACCREDITATION OF ICP-BRAZIL'S INTEGRATING ENTITIES	DOC-ICP-03
[4]	MINIMUM REQUIREMENTS FOR THE PRACTICES STATEMENTS OF THE CONFIDENT SERVICE PROVIDERS ICP-BRASIL	DOC-ICP-17
[8]	MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRASIL	DOC-ICP-04
[5]	MINIMUM REQUIREMENTS FOR PRACTICE STATEMENTS BY ICP-BRASIL TIME STAMP AUTHORITIES	DOC-ICP-12

10.2. The documents below approved by Normative Instruction of AC 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.	Nome do documento	Código
[1]	STANDARDS AND CRYPTOGRAPHIC ALGORITHMS OF ICP-BRASIL	DOC-ICP-01.01
[2]	OID ASSIGNMENT AT ICP-BRAZIL	DOC-ICP-04.01
[6]	<i>WebTrust Principles and Criteria for Registration Authorities e Certification Authorities</i>	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/

		overview-of-webtrust-services
[7]	Baseline Requirements – CA/Browser Forum – versão 1.6.6.	https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.6.pdf

* Our translation from – https://repositorio.serpro.gov.br/docs/CP_SERPRO_SSL_CA.pdf, § 10”).

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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