Brazilian Public Key Infrastructure

CERTIFICATION PRACTICE STATEMENT

ROOT CERTIFICATION AUTHORITY OF BRAZIL

(ICP-BRASIL)

DOC-ICP-01

Version 6.1

Text amended by CG ICP-Brasil Resolution No. 208, 2024

Brazilian Public Key Infrastructure

SUMMARY

Brazilian Public Key Infrastructure

CHANGE CONTROL

Act that approved the amendment	Item changed	Description of change
Resolution CG ICP-Brasil No. 208, of 08.11.2024 Version 6.1	1.3.5, 7.1.2.1, 7.1.4.1	Review about PSS and inclusion of chains V12 and V13
Resolution CG ICP-Brasil No. 192, of 11.16.2021 Version 6.0		Review and consolidation in accordance with Decree No. 10,139, of November 28, 2019.
Resolution No. 165, of 04.17.2020 Version 5.2	7.1.2.2	Allow setting of specific bits in EV certificate extensions.
Resolution No. 152, of 08.13.2019 Version 5.1	1.1, 4.2 e 10.4 (included)	Adjustments to WebTrust principles and criteria that reference CABForum requirements.
Resolution No. 151, of 05.30.2019 Version 5.0		Approves version 5.0 of DOC-ICP-01.
Resolution No. 147, of 11.07.2018 Version 4.7	7.1.2, 7.1.4	Authorizes the revocation of the V8 and V9 chains and the issuance of the V10 and V11 chains
Resolution No. 143, of 09.06.2018 Version 4.6	7.1.2 e 7.1.4	Inclusion of chains V6, V7, V8 and V9.
Resolution No. 116, of 12.09.2015 Version 4.5	4.4.3.3, 4.4.9, 7.1.2, subheading c) e 7.1.4, subheading f)	Inclusion of the V5 chain, Revocation of certificates by the Root CA, final CRL and flexibility in the issuance frequency of the Root CA CRL.
Resolution No. 104, of 04.23.2015 Version 4.4	7.1.2, item c) 7.1.4, item e)	Inclusion of the V4 chain

Act that approved the amendment	Item changed	Description of change
Resolution No. 99, of 10.09.2013 Version 4.3	7.1	Item alterado que amplia prazo de validade de certificados das hierarquias da ICP-Brasil que implementam exclusivamente algoritmos de curvas elípticas.
Resolution No. 94, of 9/27/2012 Version 4.2	1.3.3, 1.4, 7.2, 7.2.2, 7.2.2.1, 7.2.2.2, 7.2.6, 7.2.7, 7.2.8, 7.2.8.1, 7.2.8.2, 7.2.9	Changed item that extends the validity period of certificates from ICP-Brasil hierarchies that exclusively implement elliptic curve algorithms.
Act No. 01, of 08.26.2011 maintained version 4.1	7.2	Item changed to correct wording error
Resolution No. 81, of 06.17.2010 Version 4.1	7.1.2, 7.1.4, 7.2.4	Inclusion of V2 and V3 chains
Resolution No. 50, of 11.19.2008 Version 4.0	2.1.1.g, 2.7.1, 2.8.2.2, 2.8.2.3, 6.1.4.2.c	Adding references to Timestamp
Resolution No. 49, of 06.03.08 Version 3.0	1.1.1, 1.1.2, 2.1.1, 2.1.4.2, 2.6.1.1, 2.6.3.1, 2.8.3, 4.4.1.4, 4.4.1.5, 4.4.1.7, 4.4.9, 4.4.10, 5.2.1.6, 6.1.1.1, 6.1.1.3, 6.1.8, 6.1.9, 6.2, 6.2.1, 6.2.2, 6.2.4.1, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.3.2, 6.4.1, 6.4.2, 6.5.1.1, 6.6.2, 6.7, 6.8, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.3, 7.3.1, 7.3.2	Item changed or deleted due to the generation of the second Root CA key
	2.6.1.4, 3.1.1, 5.3.3, 5.3.8, 6.3.1	Item changed or deleted for wording correction
	3.1.7	Item changed for international standard update

Act that approved the amendment	Item changed	Description of change
	7.2.2	Item changed to conform to international standard
Resolution No. 46, of 12.03.2007 Version 2.1	2.6.1.1	Changed the URL of the Root CA webpage to http://acraiz.icpbrasil.gov.br
Resolution No. 38, of 04.18.2006 Version 2.0	Several	Creation of DOC-ICP-01 consolidating previous documents

1 INTRODUCTION

1.1 Overview

1.1.1 ICP-Brasil is a trusted cryptographic platform that guarantees the presumption of legal validity to electronic acts and businesses signed and encrypted with digital certificates and keys issued by this infrastructure.

1.1.2 This document is approved by the Management Committee of ICP-Brasil to identify the practices and procedures of Root CA.

1.1.3 This Certification Practices Statement - CPS describes the practices and procedures employed by the National Institute of Information Technology - ITI in the performance of its services as Root Certifying Authority - Root CA of the Brazilian Public Key Infrastructure - ICP-Brasil

1.1.4 The Root CA has the highest-level certificates in ICP-Brasil. These certificates contain the public keys corresponding to the Root CA's private keys, used to sign their own certificates, their Certificate Revocation Lists - CRL and the certificates of subordinate CAs.

1.1.5 This CPS follows the updates of the Baseline Requirements and Extended Validation SSL and CodeSign Guidelines documents [11], the WebTrust Principles and Criteria [10] and CA/Browser Forum publications, available at https://cabforum.org.

1.1.6 The structure of this CPS is based on RFC 3647 [13].

1.2 Document Name and Identification

This CPS is called "CERTIFICATION PRATICE STATMENT OF THE ROOT CERTIFICATION AUTHORITY OF BRAZIL" and commonly referred to as "CPS of the Root CA". The Object Identifier – OID of this CPS is 2.16.76.1.1.0.

1.3 ICP-Brasil Participants

1.3.1 Certification Authorities

This CPS only refers to the Root Certifying Authority – Root CA of Brazil, ICP-Brasil.

1.3.2 Registration Authorities

The activity of identification and registration of the subordinate CAs will be carried out together with the accreditation process, with no Registration Authorities - RA within the scope of the Root CA.

1.3.3 Subscribers

The certificates issued by the Root CA are held by the Root CA itself or the Subordinate CAs.

1.3.4 Relying Parties

A third party is the party that relies on the content, validity and applicability of the digital certificate.

1.3.5 Other Participants

The list of participants of ICP-Brasil is available at:

http://acraiz.icpbrasil.gov.br/PSSacraiz.pdf. (Text amended by CG ICP-Brasil Resolution No. 208, 2024)

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificates issued by the Root CA have the sole purpose of identifying the Root CA itself or the subordinate CAs and disclosing its public keys in a secure way.

1.4.2 Prohibited Certificate Uses

The certificates issued by the Root CA cannot identify or verify any entity or signature beyond the purposes described in this CPS.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Name: Instituto Nacional de Tecnologia da Informacao - ITI

1.5.2 Contacts

Address: SCN, Quadra 2, Bloco E, CEP 70.712-905, Brasília-DF – Brasil

Telephone: (61) 3424-3853, 3424-3854, 3424-3856

Fax: (61) 3424-3910

Website: http://www.iti.gov.br

E-mail: cgope@iti.gov.br

1.5.3 Person Determining CPS Suitability for the Policy

This document consolidates the Root CA's CPS and Policy.

1.5.4 CPS Approval Procedures

1.5.4.1 This CPS is approved by Management Committee of ICP-Brasil, through analysis and vote of its integral members.

1.5.4.2 The Root CA approval procedures are established at the discretion of the Management Committee ICP-Brasil.

1.6 Definitions and Acronyms

ACRONYM	DESCRIPTION
BCP	Business Continuity Plan
CA	Certification Authority
CPS	Certification Practices Statement
DN	Distinguished Name
DOU	Federal Official Gazette
ICP-Brasil	Brazilian Public Key Infrastructure
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITI	National Institute of Information Technology
ITU	International Telecommunications Union
CRL	Certificate Revocation List
MG ICP-BRASIL	Brazilian Public Key Infrastructure Management Committee
OID	Object Identifier
PC	Certificate Policy
SP	Security Policy
SSP	Support Service Providers
RA	Registration Authority
RFC	Request For Comments
Root CA	Certification Authority of Brazil (ICP-Brasil)
TAE	Time Audit Entity

TP	Timestamp Policy
TSA	Timestamp Authority
TSP	Trusted Service Providers
TSPS	Time Stamping Practices Statement
TSPPS	Trusted Service Provider Practice Statement
UTC	Coordinated Universal Time

2 PUBLICATION OF CERTIFICATION INFORMATION

Soon after its issuance, the certificates issued by it and its CRL are made available in the Root CA repository.

2.1 Repositories

The Root CA repository is accessible 24x7.

2.2 Publication of Certification Information

2.2.1 The Root CA certificate, its CRL and the certificates of the subordinate CAs are published on the Root CA website http://acraiz.icpbrasil.gov.br and https://acraiz.icpbrasil. gov.br, obeying the rules and criteria established in this CPS.

2.2.2 The list of CAs that are part of ICP-Brasil is also found on the Root CA website.

2.2.3 The availability of information published by Root CA on its website, such as certificates, its CRL, its CPS, among others, is 99.99% of the time, 24 hours a day, 7 days a week.

2.2.4 The Root CA includes the identification of its website in the certificates issued.

2.2.5 The Root CA will communicate, in writing, any change in this CPS to the CAs that are members of ICP-Brasil, as well as to all the CAs with which it has cross-certification agreements. This notification will contain the changes made.

2.3 Time or Frequency of Publication

Certificates are published immediately after they are issued. The frequency of issuance of CRL and its publication are described in items 4.9.7, 4.9.8 and 4.10 of this CPS.

2.4 Access Control on Repositories

2.4.1 There is no restriction on access to this CPS, the certificates issued and the CRL of the Root CA.

2.4.2 Appropriate access controls are used to restrict the possibility of writing or modifying this information to authorized personnel. There is read-only permission.

3 IDENTIFICATION AND AUTHENTICATION

The Root CA verifies the authenticity of the identity and/or attributes of ICP-Brasil entities before including these attributes in a digital certificate. Entities are prohibited from using names in their certificates that violate the intellectual property rights of others. The Root CA reserves the right, without liability to any applicant, to reject requests.

3.1 Naming

3.1.1 Type of Names

The subordinate CAs, therefore certificate holders, will have a name that uniquely identifies them within the scope of ICP-Brasil. This identification will be given by DNs (Distinguished Names) – standard ITU-T X.501.

3.1.2 Need for Names to be Meaningful

All certificates issued by the Root CA must include a unique identifier that represents the subordinate CA for which the certificate was issued, as per item 7.1.4.

3.1.3 Anonymity or Pseudonym of Certificate Holders

Not applicable.

3.1.4 Rules for Interpreting Various Types of Names

Distinguished names in certificates are interpreted using ITU-T X.501 standards and ASN.1 syntax.

3.1.5 Uniqueness of Names

"Distinguished Name" - DN identifiers must be unique for each subsequent CA. For each CA, additional numbers or letters can be added to the name to ensure the uniqueness of the field, as per the ITU-T X.509 standard. The "Unique Identifiers" extension will not be accepted to differentiate CAs with identical names.

3.1.6 Procedure for resolving name disputes.

The Root CA reserves the right to make all decisions regarding name disputes of subsequent CAs. During the authentication process, the CA requesting the certificate must prove its right to use a specific name (DN) in its certificate, in accordance with the legislation in force.

3.1.7 Recognition, Authentication and Role of Trademarks

3.1.7.1 Entities may not request certificates with any content that violates the intellectual property rights of third parties.

3.1.7.2 It is not Root CA's role to verify the applicant's right to use a registered trademark.

3.1.7.3 Root CA reserves the right to revoke any certificate involved in a dispute.

3.2 Initial Identity Validation

The Root CA performs the identification of the applicant using any legal means of communication or investigation necessary to identify the legal or natural person.

3.2.1 Method to Prove Possession of Private Key

The Root CA verifies that an accredited CA has a private key corresponding to the public key for which the digital certificate is being requested. RFC 4210 [14], updated by RFC 6712 [16], is used for this purpose.

3.2.2 Authentication of Organization Identity

3.2.2.1 The identification of a CA by the Root CA is conducted through the procedures described in the document CRITERIA AND PROCEDURES FOR ACCREDITATION OF ICP-BRASIL'S MEMBERS [6].

3.2.2.2 The Root CA maintains internal policies and procedures that are regularly reviewed to comply with the requirements of the various root programs of which Root CA is a member, as well as the Baseline Requirements, EV Guidelines and Guidelines of EV Code Signing.

3.2.3 Authentication of Individual Identity

Not applicable.

3.2.4 Non-Verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

In the issuance of a subsequent CA certificate, it is verified whether the natural person is the legal representative of the CA.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

3.3.1.1 The process of generating, by the Root CA, a new certificate for a subordinate CA can be done in a simplified way, before the expiration of the validity of the current certificate of the CA.

3.3.1.2 For this, a legal representative of the CA must complete and sign, on paper or digitally, the REVALIDATION FORM OF REGISTRATION DATA AND REQUEST FOR A NEW CERTIFICATE [7]. Upon receipt of this form, provided that the documentation is regularly updated, Root CA will begin the process of issuing the new certificate.

3.3.2 Identification and authentication for new keys after revocation

The request for a new CA certificate after the revocation or expiration of the previous certificate must be carried out by completing the REVALIDATION FORM OF REGISTRATION DATA AND REQUEST FOR A NEW CERTIFICATE [7]. This form must be signed by a legally constituted representative of the CA and delivered to the Root CA. Upon receipt of this form, provided that the documentation is regularly updated, Root CA will begin the process of issuing the new certificate.

3.4 Identification and Authentication for Revocation Request

3.4.1 The certificate revocation requester shall be identified. Only the agents described in item 4.9.2 can request the revocation of the certificate of a subordinate CA.

3.4.2 The procedure for requesting certificate revocation by the Root CA is described in item 4.9.3. Certificate revocation requests must be logged.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The Root CA maintains its own lists of individuals and entities from which it will not accept certificate requests. In addition, other external sources, such as government deny lists or internationally recognized blacklists that are applicable to the jurisdictions in which Root CA operates, are used to filter out unwanted applicants.

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 The request for a Root CA certificate is made by the Management Committee of ICP-Brasil, which delegates the execution of these functions to ITI.

4.1.1.2 The request for a subordinate CA certificate must be made by their legal representatives.

4.1.2 Enrollment Process and Responsibilities

The responsibilities of CA are:

a) the issuance and management of your cryptographic key pair;

b) the issuance and distribution of your digital certificate;

c) the issuance, dispatch and distribution of subordinate CA certificates;

d) the publication of certificates issued by it;

e) the revocation of certificates issued by it;

f) the issuance, management, and publication of its List of Revoked Certificates – CRL;

g) inspection and auditing of CAs, Time Stamp Authorities - TSAs, ARs, Support Service Providers - PSS, Biometric Service Providers - PSBio and Trust Service Providers - PSC qualified accordingly with the criteria established by the Management Committee of ICP-Brasil - CG of ICP-Brasil;

h) the implementation of cross-certification agreements, according to the guidelines established by the CG of ICP-Brasil;

i) the adoption of security and control measures, provided for in this CPS and in the SECURITY POLICY OF ICP-BRASIL [1], involving its processes, procedures and activities;

j) maintenance of processes, procedures and activities in accordance with current legislation and with the norms, practices and rules established by the CG of ICP-Brasil;

k) the maintenance and guarantee of the integrity, secrecy and security of the information handled by it; and

l) maintenance and regular testing of its Business Continuity Plan - BCP.

4.2 Certificate Application Processing

4.2.1 Root CA certificate request

4.2.1.1 The request for a certificate for a subordinate CA is only possible after the granting of its accreditation request and the consequent authorization for the operation of the CA in question by the Root CA, as provided in the document CRITERIA AND PROCEDURES FOR ACCREDITATION OF ICP-BRASIL'S MEMBERS [6].

4.2.1.2 The subordinate CA must forward the request for its certificate to the Root CA through its legal representatives, using the standard defined in the regulation edited by normative instruction of the Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

4.2.1.3 Root CA does not receive certificates for end users, in accordance with MP No. 2,220-2, of August 24, 2001. Therefore, for Root CA, there is no scenario of restrictions or authorizations for the processing of records DNS for certificate authority authorization.

4.2.2 Execution of identification and authentication functions

The Root CA performs the identification and authentication functions according to item 3.2 of this CPS.

4.2.3 Approving or rejecting certificate requests

The Root CA can accept or reject requests for certificates from the subordinate CAs in accordance with the procedures observed in item 3.2 of this CPS.

4.2.4 Time to process the certificate request

Root CA guarantees that the ceremony for issuing a certificate for a subordinate CA occurs within a maximum of 30 (thirty) business days after the CA's authorization to operate in question.

4.3 Certificate Issuance

4.3.1 Root CA Actions During Certificate Issuance

4.3.1.1 The issuance of a certificate by Root CA is done in a specific ceremony, with the presence of a representative of Root CA, the accredited CA, auditors and guests, in which all procedures performed are registered.

4.3.1.2 As The public keys of self-signed certificates are published in the DOU.

4.3.1.3 The certificate is considered valid from the moment it is issued.

4.3.1.4 Issuance of Root CA certificates and subordinate CAs is done on Root CA equipment that operates offline.

4.3.1.5 The issuance of certificates by the Root CA for subordinate CAs will be subject to:

a) the submission of an insurance policy covering civil liability resulting from digital certification and registration activities, with sufficient coverage compatible with the risk of these activities; and

b) payment of the fee referred to in item 1.2 of the document GUIDELINES OF THE TARIFF POLICY OF THE ROOT CERTIFICATION AUTHORITY OF ICP-BRASIL [4].

4.3.1.6 The Direct Administration of the Union, the States, the Federal District and the Municipalities is exempt from paying the fee and presenting the policy provided for in the previous item.

4.3.1.7 The Root CA delivers the issued certificate, in a format defined in accordance with the regulation issued by the normative instruction of the Root CA that defines the standards and cryptographic algorithms of ICP-Brasil, to the legal representative of the accredited CA present at the ceremony.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

After issuing the certificate, the Root CA sends a confirmation email.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 When the Root CA issues a certificate to a subordinate CA, it guarantees that the information contained in that certificate has been verified in accordance with this CPS.

4.4.1.2 Upon delivery of the certificate, during the ceremony of its issuance by Root CA, the CA certifies its receipt by means of the signature of Certificate Issuance Ceremony Term, Public Key Delivery Ceremony Term and Term of Agreement by your legal representative.

4.4.1.3 Acceptance of the certificate occurs when the data contained therein are verified by the CA or when the corresponding private key is used for the first time.

4.4.1.4 Verification of the certificate data must be conducted by the subscribers within 2 (two) business days, counted from its receipt, after which the certificate will be considered accepted.

4.4.1.5 Upon accepting the certificate, the titular CA:

a) agrees with the responsibilities, obligations and duties imposed on it by the Term of Agreement and this CPS;

b) guarantees that to its knowledge, no unauthorized person has had access to the private key associated with the certificate; and

c) affirms that all certificate information provided during the accreditation process is true and is correctly and completely reproduced in the certificate.

4.4.1.6 The non-acceptance of a certificate within the established period implies a new ceremony, where the non-accepted certificate is revoked and a new certificate is issued.

4.4.2 Publication of the Certificate by the Root CA

The Root CA certificate and the certificates of the subordinate CAs are published in accordance with item 2.2 of this CPS.

4.4.3 Notification of Certificate Issuance by the Root CA to Other Entities

The Notification will be given in accordance with item 2.2 of this CPS.

4.5 Key Pair and Certificate Usage

The subscriber CA of a certificate issued by the Root CA must operate in accordance with its own Certification Practices Statement - CPS and with the Certificate Policies - PC that it implements, established in accordance with the documents MINIMUM REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENT OF THE CERTIFICATION AUTHORITIES OF ICP-BRASIL [2] and MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES AT ICP-BRASIL [3].

4.5.1 Subscriber Private Key and Certificate Usage

The subscriber CA must use its private key and ensure the protection of this key as provided for in its own CPS.

4.5.2 Relying Party Public Key and Certificate Usage

4.5.2.1 Relying third parties must comply with the terms established in this CPS, as a condition of trust in the certificate.

4.5.2.2 Procedures for reliability by the relying party are described in item 9.6.4 of this CPS.

4.6 Renewal of Certificates

Not applicable.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the Root CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate 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 Requests

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 the Re-Keyed Certificate by the Root CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the Root 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 of 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 Root CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 A subordinate CA certificate of the Root CA may be revoked at any moment, at the request of the CA holder of the certificate itself or by reasoned decision of the Root CA, safeguarding the principles of the contradictory and ample defense

4.9.1.2 A certificate must be revoked

a) when improper or defective issuance of the same is verified;

b) when it is necessary to change any information contained in the certificate;

c) in the event of dissolution of the subscriber CA of the certificate; or

d) in the event of compromise of the CA's private key or its storage media

4.9.1.3 The Root CA may revoke or determine the revocation of the certificate or cross-certification of the CA that fails to comply with current legislation, or the policies, norms, practices and rules established for ICP-Brasil.

4.9.1.4 The public keys of certificates issued by a dissolved CA will be stored by another CA, after approval by the Root CA.

4.9.1.5 When there is more than one CA interested, the one indicated by the CA that ends its activities will assume responsibility for storing the public keys.

4.9.1.6 The CA that ends its activities will transfer, if applicable, the documentation of the digital certificates issued to the CA that has taken over the custody of the respective public keys.

4.9.1.7 If the public keys have not been assumed by another CA, the documents referring to the digital certificates and the respective public keys will be passed on to the Root CA.

4.9.2 Who Can Request Revocation

4.9.2.1 The revocation of the certificate of a subordinate CA can only be done:

a) by determination of Root CA;

b) at the request of the CA holder of the certificate; or

c) by court order.

4.9.3 Procedure for Revocation Request

4.9.3.1 The request for revocation of the certificate to the Root CA must be made by completing the CA CERTIFICATE REVOCATION REQUEST FORM [8]. This form must be signed by your legal representative. When using the electronic version of the form, it must be digitally signed and sent to Root CA. The form can also be completed on paper, delivered personally by the representative to Root CA and signed upon delivery.

4.9.3.2 The CA certificate revocation process is preceded, when applicable, by the receipt by the Root CA of the revocation request and ends when a new CRL, containing the revoked certificate, is issued, and published by the Root CA. Once this process is complete, the Root CA informs the affected CA of the certificate revocation.

4.9.3.3 The period for revocation of the subordinate CA of the Root CA is a maximum of 24 (twenty-four) hours. The period will start from the receipt by the Root CA of the revocation request from the certificate subscriber CA or the revocation order issued by the Root CA itself.

4.9.3.4 A revoked CA certificate can only be used for verification of signatures generated during the period in which said certificate was valid.

4.9.4 Revocation Request Grace Period

The revocation request must be immediate when the circumstances defined in item 4.9.1 of this CPS are verified.

4.9.5 Time Within Which Root CA Must Process the Revocation Request

As established in item 4.9.3.3.

4.9.6 Revocation Checking Requirements for Relying Parties

The status of the certificates (for revoked certificates) will be available according to item 2.1.

4.9.7 CRL Issuance Frequency

4.9.7.1 The Root CA CRL is updated, at most, every 90 (ninety) days. In case of revocation of the subordinate CA certificate, the Root CA issues a new CRL within the period provided for in item 4.9.3 and notifies all subordinate CAs.

4.9.7.2 In the case of revocation of the Root CA's own certificate, a CRL must be issued with a validity period equal to that of the certificate, ending the CRL issuance by this Certifying Authority.

4.9.8 Maximum Latency for CRLs

The CRL is published to the repository within one business day after it is generated.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation requests to the Root CA certification system will not be accepted. The only way to query the certificate status online is through the CRL.

4.9.10 On-Line Revocation Checking Requirements

Not applicable.

4.9.11 Other Forms of Revocation Advertisements Available

Information on the revocation of a subordinate CA and the self-signed Root CA may also be disclosed through its publication in the Official Gazette of the Union or on the Root CA website.

4.9.12 Special requirements in case of key compromise

4.9.12.1 In case the private key of a subordinate CA is compromised, it must notify the Root CA.

4.9.12.2 The CA shall ensure that its CPS contains provisions that define the means that will be used to notify a compromise or suspected compromise.

4.9.13 Circumstances for Suspension

Suspension of subordinate CA certificates is not allowed, except in specific cases and determined by the Management Committee

4.9.14 Who Can Request Suspension

Root CA or subsequent CA, approved by the Management Committee.

4.9.15 Procedure for Suspension Request

Suspension request procedures will be defined by specific supplementary rule.

4.9.16 Limits on Suspension Period

Suspension periods will be established by specific rule of the CPS and associated PCs.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Root CA provides a certificate status service in the form of an CRL distribution point.

4.10.2 Service Availability

See item 2.2 of this CPS.

4.10.3 Operational Features

See item 2.2 of this CPS.

4.11 End of Subscription

Observing the provisions of the item "Withdrawal of accreditation" of the document CRITERIA AND PROCEDURES FOR ACCREDITATION OF ICP-BRASIL'S MEMBERS [6], the CPS of the subsequent CA must describe the requirements and procedures that must be adopted in cases of termination of the CA's services responsible.

4.12 Key Escrow and Recovery

The custody (escrow) of the private keys of the Root CA is not allowed.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The ICP-Brasil Root CA certificate management process includes the following controls:

a) physical security and environmental controls;

b) systems integrity controls, including configuration management, maintaining reliable code integrity, and incident detection and prevention;

c) network security and firewall management, including port restrictions and IP address filtering;

d) user management, segregation of functions, qualification, awareness and training;

e) logical access controls, with registration of activities and inactivity, to provide individual responsibilities; and

f) ICP-Brasil Root CA security program.

5.1 Physical Controls

The ICP-Brasil's Root CA maintains security policies for the assets and systems used in the certificate management processes. These policies cover physical access controls, natural disaster protection, fire safety, support failures (such as power, telecommunications, data links, and others), structure collapse, flooding, theft protection, unauthorized access, and disaster recovery. These controls must be implemented to prevent loss, damage or compromise of assets, interruption of business activities related to certificate management processes, theft of information and compromise of information processing facilities.

5.1.1 Site Location and Construction

The ICP-Brasil Root CA, for the execution of activities related to the certified management processes, uses facilities approved by the Management Committee of ICP-Brasil. These facilities must comply with classification standards and fire resistance test methods and practices for physical security relating to data storage.

5.1.2 Physical Access

5.1.2.1 The Physical access to the operational premises of Root CA is managed and controlled internally in accordance with the requirements defined in the Security Policy of ICP-Brasil.

5.1.2.2 The Access control is conducted by keys, passwords, cryptographic cards, biometric identifications and other devices so that only authorized people participate in the relevant activities. In addition, physical access and all environments are monitored through Closed Circuit TV (CCTV), with 24x7 digital recording.

5.1.2.3 The Root CA certification system is in secure redundant environments, like a safe room, located in geographically segregated facilities. Physical security and access controls through biometric identification restrict access to equipment and systems related to certificate management processes.

5.1.2.4 At least 4 (four) levels of physical access to the various environments of the Root CA are defined, and 2 (two) more levels related to the protection of private keys:

5.1.2.4.1 The first level – or level 1 – the first access barrier to the Root CA facilities. At level 1, everyone must be identified and registered inside an area guarded by armed security or another qualified professional, when Root CA facilities are in a security area. From this level onwards, people outside the CA's operation transit duly identified and accompanied. No type of operational or administrative process related to CA certificate management shall be performed at this level.

5.1.2.4.2 Except for the cases defined by law, the carrying weapons will not be admitted on the premises of Root CA, from level 1 onwards. From that level onwards, recording, photography, video, sound or similar equipment, as well as portable computers, will have their entry controlled and can only be used with formal authorization and supervision.

5.1.2.4.3 The second level – or level 2 – is internal to the first and requires individual identification of the persons entering it. This is the minimum level of security required for the execution of any operational or administrative process of the Root CA. Passing from the first to the second level requires electronic identification and the use of a badge.

5.1.2.4.4 The third level – or level 3 – is located within the second and will be the first level to house sensitive material and activities related to the Root CA certificate management processes.

5.1.2.4.5 Persons not involved in these activities should not be allowed access to this level. Persons who do not have access permission will not be able to remain on that level if they are not accompanied by someone who has this permission.

5.1.2.4.6 At the third level, both the entries and exits of each authorized person are controlled. Two types of control mechanisms are required for entry at this level: some form of individual identification, such as an electronic card, and biometric identification.

5.1.2.4.7 Cell phones, as well as other portable communication and data storage equipment, except those required for the operation of the Root CA, are not admitted from level 3.

5.1.2.4.8 **Fourth level** – or level 4 – inside the third, is where activities that are particularly sensitive to the Root CA operation take place, such as issuing and revoking certificates and issuing CRLs. All systems and equipment necessary for these activities are located on this level. Level 4 has the same access controls as level 3 and, additionally, requires, in each access to its environment, the identification of at least 2 (two) authorized persons. At this level, the permanence of these people must be required while the environment is occupied.

5.1.2.4.9 At the fourth level, all walls, floor and ceiling are clad in steel and concrete or other material of equivalent strength. The walls, floor and ceiling are one piece, constituting a watertight cell against threats of improper access, water, steam, gases and fire. Cooling and power ducts, as well as communication ducts, do not allow physical invasion of fourth-level areas. Additionally, these level 4 environments – which constitute the so-called safe rooms – have protection against external electromagnetic interference or have rack-type equipment that has this characteristic.

5.1.2.4.10 The safe rooms are built according to applicable Brazilian standards and any omissions from these standards are remedied by relevant international standards.

5.1.2.4.11 There may be, in the CA, several fourth-level environments to shelter and segregate, when applicable:

a) online production equipment and storage vault;

b) offline production equipment and storage vault; and

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

5.1.2.4.12 The access doors to the vault room are locks, where a door should only open when the previous one is closed.

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

5.1.2.4.14 Fifth level – or level 5 – inside level 4 environments, comprises a vault or reinforced locked cabinet. Cryptographic materials such as keys, activation data, their copies and cryptographic equipment are stored in an environment of level 5 or higher.

5.1.2.4.15 To ensure the safety of the stored material, the safe or cabinet must comply with the following minimum specifications:

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

b) have a lock with a key.

5.1.2.4.16 **Sixth level** – or level 6 – consists of small stores located inside the fifth level vault or cabinet. Each of these deposits has individual access to its content. The Root CA private key activation data is stored in these buckets.

5.1.3 Physical Detection Systems

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

5.1.3.2 The video images resulting from the 24x7 recording are stored for at least 7 (seven) years. They are evaluated (verification of random sections at the beginning, middle and end of the file) at least every 3 (three) months, with the choice of at least 1 (one) image for each week. These tapes are stored in a third-level environment.

5.1.3.3 All passage doors between access levels 3 and 4 of the environment are monitored by an alarm notification system. Wherever there is, from level 2 onwards, glass separating access levels, a breakage alarm mechanism is installed, which is on continuously.

5.1.3.4 In all fourth-level rooms, a motion detection alarm remains active if the room access criterion is not met. As soon as, due to the departure of one or more employees, the minimum occupancy criterion is no longer satisfied, the presence sensors are automatically reactivated.

5.1.3.5 The alarm notification system uses at least 2 (two) means of notification: audible and visual.

5.1.3.6 The video camera monitoring system, as well as the alarm notification system, are permanently monitored by a qualified professional and are in a level 3 environment. The monitoring system installations, in turn, are monitored by video cameras whose positioning allows monitoring the actions of monitoring professionals.

5.1.4 Emergency Mechanisms

5.1.4.1 Specific mechanisms are implemented by Root CA to guarantee the safety of its 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 the door opening alarms.

5.1.4.2 The Root CA may specify and implement other emergency mechanisms, specific and necessary for each type of installation. All procedures regarding emergency mechanisms are documented. Emergency mechanisms and procedures are checked every six months, through simulation of emergency situations

5.1.5 Power and Air Conditioning

5.1.5.1 The infrastructure of the Root CA certification environment is dimensioned with systems and devices that guarantee the uninterrupted supply of electricity to the facilities. The energy supply conditions are maintained to meet the availability requirements of Root CA systems and their respective services.

5.1.5.2 The facilities of Root CA, in addition to being connected to the electrical network provided by the energy concessionaire, have resources that guarantee the redundancy capacity of the entire energy and air conditioning structure for its uninterrupted operation, even in the event of failure in the power supply by the concessionaire. Are they:

a) power generator of compatible size;

b) standby power generator, operating redundantly;

c) redundant power supply system (no-breaks);

d) grounding system and protection against atmospheric discharges; and

e) emergency lighting.

5.1.5.3 All electrical cables are protected by appropriate pipes or ducts. Pipes, ducts, gutters, frames and boxes are used - for passage, distribution and termination - designed and built-in order to facilitate inspections and the detection of attempted violations. Separate ducts are used for power, telephone and data cables. All cables are catalogued, identified and periodically inspected, at least every 6 (six) months, in search of evidence of violation or other abnormalities.

5.1.5.4 The air conditioning system meets the temperature and humidity requirements required by the equipment used in the environment, has dust filters and is independent of the air conditioning system of the building where it is located.

5.1.5.5 In level 4 environments, the air conditioning system is independent, fault tolerant, redundant and composed of precision air conditioning systems and comfort refrigeration for the administrative area and other environments. The air conditioning system for level 4 environments is internal, with air exchange performed only by opening the door and the temperature of the environments served by the air conditioning system is permanently monitored by the alarm notification system.

5.1.6 Water Exposures

The entire structure of the Root CA Level 4 environment is built in the form of a watertight cell, to provide physical protection against infiltration and flooding from any external source. In addition, there is a moisture detection alarm system and a monitoring team ready to respond to any unlikely exposure to water.

5.1.7 Fire Prevention and Protection

5.1.7.1 It is not allowed to smoke or carry objects that produce fire or sparks in the CA facilities.

5.1.7.2 The facilities have a smoke detection system, an early fire detection system, through the analysis of ionic particles, and a fire extinguishing system using inert gas, non-corrosive, non-combustible and non-reactive with most substances.

5.1.7.3 The fire prevention systems, internal to the environments, allow preventive alarms before visible smoke, triggered only in the presence of particles that characterize the overheating of electrical materials and other combustible materials present in the installations.

5.1.7.4 In the event of a fire at the Root CA facilities, the increase in the internal temperature inside the vault room must not exceed 50 (fifty) degrees Celsius and the room must withstand this condition for at least 1 (one) hour.

5.1.8 Media Storage

The Root CA complies with the Brazilian standard NBR 11.515/NB 1334 - Physical Security Criteria Relative to Data Storage [12] to guarantee the security of stored media, having specific environments that guarantee that the media stored in them do not suffer any type of damage generated by external factors and protected against fire and water damage.

5.1.9 Waste Disposal

All paper documents with sensitive information are shredded before disposal. All no longer usable electronic devices that were previously used to store sensitive information are permanently erased or physically destroyed.

5.1.10 External (off-site) security (backup) installations for CA

The Root CA has a contingency facility (off-site) that meets the same safety requirements as the main facility. Its location is geographically separated from the main facility so that, in the event of an accident that renders the main facility inoperable, the contingency facility will not be affected and can become fully operational, under identical conditions, in a maximum of 48 (forty-eight) hours.

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 The Root CA guarantees the segregation of tasks for critical functions, to avoid conflicts of interest and provide adequate security for operations. The actions of everyone are limited according to the profile to which they are associated.

5.2.1.2 The Root CA establishes the following different trusted profiles: infrastructure coordination, security coordination, Root CA operation, operation of the time audit entity – TAE, audit and holders of the activation key of the certification chains. The division of responsibilities is distributed as follows:

a) Infrastructure coordination: Plan, coordinate and monitor the processes related to the management of infrastructure technology resources, especially those related to software, information systems, databases and communication networks; maintain the availability of the infrastructure for the publication of information; coordinate and monitor the implementation and maintenance activities of information and cryptographic systems of Root CA and TAE; carry out the installation, customization and integration of the information systems acquired or developed within the scope of Root CA; responsible for change management and configuration control;

b) Security coordination: Plan, coordinate and monitor the continuity management of the Root CA, the repository of Signature Policies, certificates and CRLs, as well as the TAE; coordinate and monitor the activities related to the access policy and management of the IT environment, in order to guarantee security; maintain and guarantee the integrity, secrecy and security of the information handled by Root CA; monitor investigations and assessments of damage resulting from security breaches; to be responsible for the implementation of the practices and policies of security and management of the operators of Root CA; identify, map and analyze risks; develop appropriate action plans for the identified risks; and prepare the technology contingency plan for the infrastructure of Root CA;

c) Operation of the Root CA: Manage the implementation, maintenance and operation of the cryptographic systems of the Root CA of ICP-Brasil; manage the lifecycle of certificates; coordinate the issuance, publication and revocation of certificates within the scope of the Root CA of ICP-Brasil; managing contents of Root CA repositories and coordinating the management processes of people involved in Root CA activities;

d) Operation of the Time Audit Entity: Coordinate and monitor the activities of Root CA and TAE regarding the definition, execution, development and acquisition of time stamping systems; coordinate the auditing and synchronization of TSAs Time Stamp Systems; operate the Time Audit Entity – TAE of ICP-Brasil; coordinate the issuance, distribution and revocation of TAE certificates; and coordinate the registration, alteration and deregistration of Time Stamp Authorities – TSA;

e) Audit: Responsible for monitoring and supervising compliance with certification activities in line with the rules and guidelines of Root CA, responsible for verifying compliance with this CPS and the Security Policy within the scope of Root CA;

f) Holders of the certification chain activation key: Designated persons, to represent the following bodies, who hold the keys for activation of the certification chains, necessary for the operation of the cryptographic security module (hardware) of the Root CA :

g) Presidency of ITI;

h) Directorate of Public Key Infrastructure at ITI;

i) ITI Audit, Inspection and Standardization Board;

j) Institutional Security Office of the Presidency of the Republic; and

k) Directorate of Technology of the Presidency of the Republic.

5.2.2 Number of Persons Required per Task

5.2.2.1 Access to the certificate management system, used for generating and revoking certificates and generating CRLs, is performed through multi-user control, using shared secrecy, by people with trusted profiles.

5.2.2.2 The private keys of the Root CA certification chains are stored in cryptographic hardware, located inside a secure environment – vault room. The requirement of multiple control for the use of the Root CA private keys is established, so that at least 3 (three) secret partition holders of the 05 (five) possible, are required for the use of the private keys of the chains of certification.

5.2.2.3 All tasks performed in the environment where Root CA certification equipment is located require the presence of at least 2 (two) of its employees with qualified profiles as defined in the Access Profile Matrix. Other CA tasks may be performed by a single employee with a qualified profile.

5.2.3 Identification and Authentication for Each Role

5.2.3.1 For the assignment of persons to a trusted role, Root CA performs a background check. Each role described in item 5.2.1 of this CPS is identified and authenticated to ensure that the person is assigned the right role, which can support the activities of the Root CA.

5.2.3.2 All Root CA employees have their identity and profiles verified before:

a) be included in an access list to Root CA facilities;

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

c) receive credentials to conduct their operational activities at Root CA; and

d) receive an account in the Root CA certification system.

5.2.3.3 The certificates, accounts and passwords used to identify and authenticate employees must:

a) be directly attributed to a single person;

b) not allow sharing; and

c) be restricted to actions associated with the profile for which they were assigned.

5.2.4 Roles Requiring Separation of Duties

Root CA imposes the segregation of activities for personnel specifically assigned to the functions defined in item 5.2.1. It is not allowed, under any circumstances, to act in the following functions concurrently:

a) Coordination of the Infrastructure and Operation of the Root CA or Time Audit Entity;

b) Coordination of Security and Operation of the Root CA or Weather Audit Entity;

c) Infrastructure or Security Audit and Coordination;

d) Audit and Operation of the Root CA or Time Audit Entity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

5.3.1.1 All Root CA personnel involved in activities related to the lifecycle of certificates, such as the processes for issuing, issuing, distributing, revoking and managing certificates, are admitted in accordance with the provisions of the ICP-Brasil Security Policy.

5.3.1.2 All Root CA employees who exercise reliable profiles or perform critical functions have registered in a contract or term of responsibility:

a) the terms and conditions of the profile they occupy; and

b) the commitment not to divulge confidential information to which they have access.

5.3.1.3 Prior to involving any person in the certificate management process, either as a required server or contracted employee, the Root CA verifies the identity and trustworthiness of such person.

5.3.1.4 The Root CA employs enough employees who have specialized knowledge, experience and the necessary qualifications for the activities it performs.

5.3.1.5 Root CA personnel meet requirements through specialist knowledge, experience and qualifications with formal training and education and actual experience.

5.3.1.6 Root CA personnel, servants and/or contracted employees, have attributions defined according to the level of responsibilities, considering the sensitivity of the position and based on the duties and levels of access, background screening, training and qualification. Root CA personnel who work directly with the certificate management system are formally appointed to trust roles.

5.3.2 Background check Procedures

5.3.2.1 All Root CA personnel in positions of trust must be free from conflicts of interest that could impair the impartiality of the CA's operations. Any person who has a background that may be inappropriate for the position **shall not** be appointed to a role of trust.

5.3.2.2 All persons holding positions of trust shall be selected based on loyalty, trustworthiness and integrity, and shall be subject to background checks.

5.3.2.3 All Root CA personnel in activities directly related to the issuance, dispatch, distribution, revocation and management of certificates are submitted annually to:

a) criminal background check;

b) verification of credit situation;

c) verification of past employment history;

d) proof of education and residence; and

e) signing of specific terms of confidentiality and responsibility.

5.3.2.4 Staff do not have access to the trust functions until the necessary checks are completed and the results analyzed.

5.3.3 Training Requirements

5.3.3.1 All Root CA personnel in activities related to the issuance, dispatch, distribution, revocation and management of certificates receive sufficient training to master the following topics:

a) Root CA security policy and procedures;

b) certification software in use at Root CA;

c) disaster recovery and business continuity procedures; and

d) activities under their responsibility.

5.3.3.2 The Root CA keeps records of the training performed and ensures that the staff maintain the level of skills that allow them to perform their tasks satisfactorily.

5.3.4 Frequency and requirements for technical recycling

5.3.4.1 All Root CA personnel in activities directly related to the processes of issuance, dispatch, distribution, revocation and management of certificates will keep up to date on any technological changes in the certification system of Root CA

5.3.4.2 The Root CA provides training in information security and secure environment management at least once a year to all employees directly related to the certification processes. Refresher training is carried out by Root CA whenever necessary.

5.3.5 Job Rotation Frequency and Sequence

The frequency for the rotation of positions has not been defined, but Root CA guarantees that any change in the team will not affect operational effectiveness or safety.

5.3.6 Sanctions for Unauthorized Actions

In the event of a violation of policies or unauthorized action, actual or suspected, carried out by a person related to the processes of issuance, dispatch, distribution, revocation or management of certificates, Root CA immediately suspends its access and privileges, until the investigation is finalized, and takes appropriate administrative and legal measures, applying the appropriate sanctions.

5.3.7 Independent Contractor Requirements

The employee hired by Root CA must follow what is established in the SECURITY POLICY OF ICP-BRASIL [1] for the exercise of their activities, being subject to the same processes, procedures, evaluation, security control and training as the servers of the Root CA.

5.3.8 Documentation Supplied to Personnel

The Root CA provides for all its staff:

a) CPS of Root CA;

b) ICP-Brazil Security Policy;

c) operational documentation relating to its activities; and

d) contracts, standards, policies and other information that are relevant to its activities.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

5.4.1.1 Audit records are generated for all events related to operation and security and to other services of Root CA. Whenever possible, security audit records are automatically generated, when not possible, a logbook, paper form, or other physical mechanism should be used. All security audit records, electronic or not, are maintained and made available for compliance audits.

5.4.1.2 The Root CA ensures that all events related to certificate management processes are logged in a way that allows for traceability. All actions performed by Root CA personnel, in the performance of their duties, are recorded so that each action is associated with the person who performed it.

5.4.1.3 The Root records all security-related events of the certification system in audit files. Among others, the following events must be included in the audit files:

a) initiation and shutdown of the certification system;

b) attempts to create, remove, set passwords or change system privileges of Root CA operators;

c) changes in the configuration of the Root CA and/or its keys;

d) changes in certificate creation policies;

e) attempts to access (login) and exit the system (logout);

f) unauthorized attempts to access system files;

g) generation of Root CA's own keys;

h) issuance and revocation of certificates;

i) CRL generation;

j) attempts to initiate, remove, enable and disable users, and to update and retrieve their credentials; and

k) failed write and read operations in the directory of certificates and CRLs.

5.4.1.4 All audit records, electronic or manual, must contain the date and time of the event and the identification of the user who performed it. Root CA also collects and consolidates, electronically or manually, security information not generated directly by the certification system, such as:

a) records of physical accesses;

b) maintenance and changes in systems configuration;

c) personnel changes;

d) discrepancy and compromise reports; and

e) records of unusable media containing cryptographic keys, certificate activation data or personal information of users.

5.4.1.5 To facilitate the audit process, all records related to the operation and other services of Root CA are collected and consolidated, electronically or manually, in a single place, in accordance with the Security Policy of ICP-Brasil.

5.4.2 Frequency of Processing Log

5.4.2.1 The Root CA guarantees that its audit records are analyzed, depending on their criticality, weekly, monthly or whenever its certification system is used (offline), or even, in case of suspected security compromise.

5.4.2.2 All significant events are described in an audit report. This review involves a brief inspection of all records to verify that they have not been altered, followed by a more detailed investigation of any alerts or irregularities noted. All actions taken because of this analysis are documented.

5.4.3 Retention Period for Audit Log

The Root CA keeps its audit records in its own facilities, main and backup, for at least 7 (seven) years, or more if required by law. The Root CA makes these audit records available to the qualified auditor upon request.

5.4.4 Protection of Audit Records

5.4.4.1 The audit event logging system includes mechanisms to protect audit files from unauthorized reading, modification and deletion. Manual audit information is also protected from unauthorized reading, modification and deletion.

5.4.4.2 Events are recorded in such a way that they are protected from deletion or destruction (except for transfer to long-term media).

5.4.4.3 Event logs are protected to prevent alteration and detect tampering and to ensure that only individuals with authorized access can perform operations, without modifying the integrity, authenticity and confidentiality of the data, if necessary.

5.4.5 Audit Log Backup Procedures

5.4.5.1 Event logs and audit summaries of the certificate management system, cryptographic platforms and other infrastructure components, used by Root CA, have weekly, monthly and annual backups, or whenever there is any use of such equipment when in an offline environment.

5.4.5.2 Audit records are stored in a safe fireproof location (vault room or security safe), under the control of authorized persons in a position of trust, and in a location different from the components that originated them. Backup copies of audit records are protected to the same degree as the originals.

5.4.6 Audit data collection system (internal or external)

5.4.6.1 The Root CA internal audit data collection system is a combination of automated and manual processes, performed by its operational personnel or its systems.

5.4.6.2 The Audit processes begin at system startup and end only at system shutdown. The audit collection system ensures the integrity and availability of the collected data and, if necessary, protects its confidentiality.

5.4.7 Notification of Event-Causing Subject

When an event is logged by the audit system suite, no notification is sent to the person, organization, device, or application that caused it, however, events that are considered potential security breach issues involving the certificate lifecycle or infrastructure, these will be escalated to the security team to take appropriate measures for correction or mitigation.

5.4.8 Vulnerability Assessments

5.4.8.1 The events that represent a possible vulnerability, detected in the analysis of the audit records, are analyzed in detail and, depending on their severity, are recorded separately. As a result, corrective actions are implemented and recorded for auditing purposes.

5.4.8.2 The Root CA also performs regular vulnerability assessment covering key assets related to issuing, disclosing and managing certificates.

5.5 Records Archival

5.5.1 Types of Records Archived

5.5.1.1 The Root CA stores records with sufficient detail to establish the validity of a signature and the proper operation of the CA system.

5.5.1.2 Audit information (see details in item 5.4.1) and subordinate CA accreditation processes are stored.

5.5.2 Retention Period for Archive

The documentation related to the events listed in the previous item are retained for the following period:

a) digital signature certificates and respective CRLs must be retained permanently, for historical consultation purposes;

b) The copies of CA accreditation processes for at least 30 (thirty) years 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

5.5.3.1 All files are protected and stored physically with the same security requirements as your installation. Backup copies of information are kept in a different location and separate from those where they originated, with security and availability requirements.

5.5.3.2 The archives are created in such a way that they cannot be deleted or destroyed (except after transfer to long-term media) for the period they are to be retained. Archiving protections ensure that only authorized trusted access can perform operations, without modifying the integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism must be defined for periodically transferring the archived data to new media.

5.5.4 Archive Backup Procedures

5.5.4.1 A second copy of all the material described in item 5.4.1 is stored outside Root CA, receiving the same type of protection used by it. These copies follow the retention periods defined for the records they are backed up to. The Root CA must verify the integrity of the backups at least every 6 (six) months.

5.5.4.2 Backup copies are made for archiving the Root CA systems online or offline. Backups are stored in a fire rated media vault. The backup of offline environment information is performed at the end of any ceremony and kept in a location outside the environment, following the same security criteria.

5.5.5 Requirements for Time-Stamping of Records

Data and time information for records is based on official international time, Coordinated Universal Time – UTC and follows the format YYYYMMDDHHMMSSZ, including seconds even if the number of seconds is zero.

5.5.6 Archive Collection System (Internal or External)

All file data collection systems used by Root CA in its operational procedures are internal. The data collection system meets the security requirements of this item 5.

5.5.7 Procedures to Obtain and Verify Archive Information

5.5.7.1 Information storage media are verified upon creation. Periodically, statistical samples of archived information are evaluated to verify the continued integrity and readability of the information through restoration procedures.

5.5.7.2 Only Root CA authorized equipment, people in trusted roles and other authorized people can access the files. Requests to obtain information are coordinated by administrators of the secure environment in functions of trust (Audit, Infrastructure Coordination and Security Coordination).

5.5.7.3 The verification of file information must be formally requested from the Root CA, precisely identifying the type and period of information to be verified. The requester of information verification must be identified.

5.6 Key Changeover

5.6.1 The subordinate CA must initiate, up to 3 (three) months before the expiration date of its certificate, the process of generating a new pair of keys and issuing a new certificate.

5.6.2 If the certificate of a subordinate CA expires or is revoked, the Root CA immediately removes that certificate from the directory and from its website, keeping it permanently stored for the purpose of historical consultation.

5.6.3 Private keys used to sign subsequent CA certificates shall be retained until such time as all CA certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

5.7.1.1 Root CA has a Business Continuity Plan – PCN, with restricted access, evaluated at least once a year, to guarantee the continuity of its critical services. It also has an Incident Response Plan and a Disaster Recovery Plan.

5.7.1.2 The Root CA annually evaluates, reviews and updates these procedures. The Business Continuity Plan must include, at a minimum:

a) the conditions for activating the plan;

b) emergency procedures;

c) fallback procedures;

d) restoration procedures;

e) schedule for maintenance of the plan;

f) awareness and education requirements;

g) individual responsibilities;

h) Recovery Time Objective (RTO);

i) regular testing of contingency plans;

j) the plan to maintain or restore Root CA's business operations in a timely manner following interruption or failure of critical business processes;

k) defining requirements for storing critical cryptographic materials in an alternate location;

l) definition of acceptable system interruptions and a recovery time;

m) frequency for making backup copies;

n) distance between the recovery facilities and the main site of Root CA; and

o) procedures to protect your facilities after a disaster and before restoring the safe environment at the original or remote location.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

5.7.2.1 The Root CA maintains a contingency site at a geographically separate location that mirrors its primary facility so that if any software or data becomes corrupted, it can be restored from the backup site via a secure connection. Backups of all relevant software and data are taken regularly on both sites.

5.7.2.2 If any equipment is damaged or rendered inoperable, but the private keys are not destroyed, operation must be re-established as soon as possible, giving priority to the ability to generate certificate status information - CRLs, in accordance with the Plan of Root CA Disaster Recovery. Other procedures are described in the PCN of Root CA.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 If a private key of the Root CA or subsequent CAs is compromised, lost or destroyed:

a) all users who have received a certificate must be notified as soon as possible; and

b) a new CA key pair must be generated or an alternative existing CA hierarchy must be used to generate new certificates.

5.7.3.2 Other procedures are described in the PCN of the Root CA.

5.7.4 Business Continuity Capabilities After a Disaster

5.7.4.1 The infrastructure and security team will use all reasonable means to monitor the Root CA facility after a natural disaster or other type of disaster, to protect against loss, further damage and theft of materials and confidential information.

5.7.4.2 The Disaster Recovery Plan together with the Business Continuity Plan, as described in item 5.7.1, establishes procedures so that information on the status of certificates is available 24 hours a day, 365 days a year.

5.8 Root CA Termination

In the event of the need to terminate the operation of the Root CA, the impact of termination should be minimized as much as possible, considering the prevailing circumstances. In this case, at least the following measures must be taken:

a) carry out the notification of all member entities of ICP-Brasil;

b) ensure that any disruption caused by termination of the Root CA is minimized as much as possible;

c) ensure that Root CA's archived records are maintained;

d) ensure that certificate status information services are provided and maintained for the applicable period;

e) maintain the operation of Root CA for a minimum period of 1 (one) year after notification of its extinction, except in cases of succession;

f) assist with the orderly transfer of services and operational records to a successor to the Root CA, if any;

g) ensure that a revocation process is maintained for all digital certificates issued by Root CA; and

h) store Root CA data for the period provided for by law.

5.9 Root CA Security Program

5.9.1 ICP-Brasil's Root CA security program includes an annual Risk Assessment that:

a) identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration or destruction of any certificate data or certificate management processes;

a) assesses the likelihood and harm caused by these threats, taking into account the sensitivity of the certificate data and certificate management processes; and

b) evaluates the sufficiency of the policies, procedures, information systems, technology and other measures that ICP-Brasil has in place to combat such threats.

5.9.2 Based on the Risk Assessment, Root CA of ICP-Brasil develops, implements and maintains a Security Plan that consists of procedures, measures and security products designed to achieve the objectives set out above and to manage and control the risks identified during the Risk Assessment process.

5.9.3 The Security Plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of certificate data and the certificate management process. The Security Plan also considers the available technology and the cost of implementing the control measures and implements an acceptable level of security appropriate to the damage that may result from a security breach and the criticality of the data to be protected.

6 TECHNICAL SECURITY CONTROLS

The Root CA shall have to monitor technological developments and, when necessary, update the cryptographic standards and algorithms used in ICP-Brazil, a regulation edited by normative instruction of Root CA

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 The Root CA cryptographic key pair is generated by the Root CA itself, in specific hardware, in accordance with the regulation issued by the normative instruction of the Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

6.1.1.2 The pair of cryptographic keys of a subordinate CA is generated by the CA itself, after its accreditation request has been granted and the consequent authorization to operate within the scope of ICP-Brasil.

6.1.1.3 The algorithms and cryptographic devices to be used for the Root CA's cryptographic keys are defined in a regulation issued by the Root CA's normative instruction.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 The subordinate CA delivers to the Root CA a copy of its public key, in a format defined in a regulation edited by normative instruction of the Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

6.1.3.2 This delivery is made by a legally constituted representative of the CA, in a specific ceremony, on a date and time previously established by the Root CA. All events occurring at this ceremony are recorded for auditing purposes.

6.1.4 Delivery of Root CA public key to third parties

6.1.4.1 The delivery of the Root CA certificate to subordinate CAs is made at the time of availability of the CA certificate, in the format defined in a regulation issued by normative instruction of the Root CA that defines the cryptographic standards and algorithms of ICP-Brazil.

6.1.4.2 The availability of the Root CA certificate for other users and parts of PKI-Brasil is carried out in one of the following ways:

a) when the certificate is made available to its holder;

b) in directory;

c) on the website of Root CA or of the CAs and TSAs that are members of ICP-Brasil; or

d) by other secure means defined by the GC of ICP-Brasil.

6.1.5 Key Sizes

The size of the asymmetric cryptographic keys of the Root CA and of the subordinate CAs is defined in a regulation edited by normative instruction of the Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 The asymmetric key generation parameters of the Root CA adopt the standard defined in the regulation edited by normative instruction of the Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

6.1.6.2 The parameters are verified in accordance with the rules referenced in the regulation issued by the normative instruction of Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The Root CA's private key is used only for signing its own certificate, the certificates of the subordinate CAs and its CRL.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The Root CA private key is stored in encrypted form in the same secure hardware component used for its generation. Access to this component is controlled through an activation cryptographic key.

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module of Root CA adopts the standard defined in a regulation edited by normative instruction of Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

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

The cryptographic activation key of the secure hardware component that stores the Root CA's private key is divided into 5 (five) parts and distributed among 5 (five) persons designated by the Root CA. The presence of only 3 (three) of these 5 (five) people is required to activate the component and the consequent use of the Root CA private key.

6.2.3 Private Key Escrow

The custody (escrow) of the private keys of the Root CA is not allowed.

6.2.4 Private Key Backup

6.2.4.1 The Root CA maintains a backup copy of its own private key. This copy is stored encrypted and protected with a security level no lower than that defined for the original version of the key, and kept for the period of validity of the corresponding certificate.

6.2.4.2 The Root CA does not keep a backup copy of the private keys of the CAs of the level immediately after its own.

6.2.5 Private Key Archiving

Not applicable.

6.2.6 Private Key Transfer into a Cryptographic Module

The Root CA's private key is inserted in the cryptographic module in accordance with what is established in the Technical Conduct Manuals of ICP-Brasil.

6.2.7 Private Key Storage on Cryptographic Module

See item 6.1.1.

6.2.8 Method of Activating Private Key

The activation of the Root CA's private key is implemented through the cryptographic module, after identification of the responsible operators. This identification is conducted by means of a password and a hardware access control device (token).

6.2.9 Method of Deactivating Private Key

When the Root CA's private key is deactivated, due to expiration or revocation, it must be deleted from the cryptographic module's memory. Any disk space where the key was eventually stored must be overwritten.

6.2.10 Method of Destroying Private Key

In addition to what is established in item 6.2.9, all backup copies of the Root CA's private key must be destroyed, as well as all hard disks, tokens, cryptographic modules and any storage media that have hosted them for some period.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public keys of the Root CA and of the subordinate CAs are permanently stored, after the expiration of the corresponding certificates, for verification of the signatures generated during their validity period.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Root CA's private key is only used during the validity period of the corresponding certificate. The Root CA's public key can be used for the entire period determined by the applicable legislation to verify the signatures generated during the validity period of the corresponding certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The Root CA private key activation data is unique and random, physically installed in hardware access control devices (token).

6.4.2 Activation Data Protection

The Root CA private key activation data is protected from unauthorized use through encryption mechanism and physical access control.

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 issuance of the Root CA key pair and the certificates of the subordinate CAs must be performed in an offline environment, to prevent unauthorized remote access. The information used in these procedures must be kept in the offline environment, with restricted access.

6.5.1.2 Each Root CA server computer related to the issuance, dispatch, distribution, revocation and certificate management processes has the following characteristics:

a) access control to Root CA services and profiles;

b) clear separation of tasks and attributions related to each Root CA profile;

c) use of encryption for database security;

d) generation and storage of Root CA audit records;

e) internal security mechanisms to guarantee the integrity of critical data and processes; and

f) mechanisms for backup copies.

6.5.2 Computer Security Rating

Not applicable.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Root CA uses software designed and developed through a rigorous formal methodology, specific for critical security environments.

6.6.2 Security Management Controls

A formal configuration management methodology is used for installation and ongoing maintenance of the Root CA certification system. New versions of this software are only installed after communication from the manufacturer and tests in an approval environment by Root CA.

6.6.3 Life Cycle Security Controls

Not Applicable.

6.7 Network Security Controls

The Root CA server computer hosting the certification system operates offline, physically disconnected from any network.

6.8 Time-Stamping

Not Applicable.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

The format of all certificates issued by the Root CA complies with the ITU-T X.509 or ISO/IEC 9594 standard, noting:

a) the Root CA certificate is the only self-signed ICP-Brasil certificate, with a maximum validity of 20 (twenty) years when using elliptic curve cryptography, or 13 (thirteen) years for other cases, this period may be revised according to the definitions established by the GC of ICP-Brasil.

b) the CA certificate of subordinate CA is signed by the Root CA and has a validity limited to the validity of the certificate of the Root CA, and this period may be revised according to the definitions established by the CG of ICP-Brasil.

7.1.1 Version number(s)

7.1.1.1 The Root CA certificate implements certificate version 3 of the ITU-T X.509 standard.

7.1.1.2 The certificate of the subordinate CA implements the certificate version 3 of the ITU-T X.509 standard.

7.1.2 Certificate Extensions

7.1.2.1 The certificate of the subordinate CA implements the certificate version 3 of the ITU-T X.509 standard.

a) ***basicConstraints***: contains the field cA=True. The *pathLenConstraint* field is not used.

b) ***keyUsage***: contains only the *keyCertSign*(5) and *cRLSign*(6) bits torned on. The other bits are off.

c) ***cRLDistributionPoints***: contains the web address where the CRL corresponding to the certificate is obtained:

i. for initial chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraiz.crl;

ii. for V1 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl;

iii. for V2 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl;

iv. for V3 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv3.crl;

v. for V4 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv4.crl.

vi. for V5 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv5.crl.

vii. for V6 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv6.crl.

viii. for V7 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv7.crl.

ix. for V8 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv8.crl.

x. for V9 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv9.crl.

xi. for V10 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv10.crl.

xii. for V11 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv11.crl.

xiii. for V12 chain certificates:http://acraiz.icpbrasil.gov.br/LCRacraizv12.crl;
(Text amended by CG ICP-Brasil Resolution No. 208, 2024)

xiv. for V13 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv13.crl;
(Text amended by CG ICP-Brasil Resolution No. 208, 2024)

d) ***Certificate Policies***: specifies the Object Identifier (OID) of the CPS of the Root CA and the id-qt-cps attrib with the web addr of this CPS (http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf).

e) ***SubjectKeyIdentifier***: contains the hash of the Root CA public key.

7.1.2.2 The certificate of the subordinate CA may implement any of the extensions foreseen in version 3 of the ITU-T X.509 standard.

7.1.2.2.1 The following extensions are mandatory:

a) **"Authority Key Identifier", not critical**: the keyIdentifier field must contain the hash, obtained with an algorithm from the SHA family, of the public key of the CA issuing the certificate.

b) **"Subject Key Identifier", non-critical**: must contain the hash, obtained with an algorithm from the SHA family, of the public key of the CA holder of the certificate;

c) **"Key Usage", critical**: the keyCertSign and cRLSign bits must be activated, and other bits can be activated for specific cases;

d) **"Certificate Policies", not critical**. The policyIdentifier field must contain:

i. if the CA issues certificates to other CAs, the CPS OID of the certificate holder CA; or

ii. if the CA issues certificates to end users, the OID of the deployed PCs, containing the policyQualifiers field with the id-qt-cps attribute and the web address of the CA's CPS.

e) **"Basic Constraints", critical**: must contain the field cA=True; and

f) **"CRL Distribution Points"**, non-critical: must contain a web address where the CRL corresponding to the certificate is obtained, according to item 7.1.2.1.c.

7.1.2.2.2 For CAs that issue SSL certificates, the following extensions are also mandatory:

a) **"Extended Key Usage", not critical**: must contain the purpose server authentication OID = 1.3.6.1.5.5.7.3.1. Can contain purpose client authentication OID = 1.3.6.1.5.5.7.3.2; and

b) **"Authority Information Access", non-critical**: the first entry must contain the access method id-ad-caIssuer, using one of the following access protocols, HTTP, HTTPS or LDAP, for retrieving the certificate chain.

7.1.3 Algorithm Object Identifiers

7.1.3.1 . The Root CA certificate is signed using the algorithm defined in the regulation issued by the Root CA normative instruction that defines the standards and cryptographic algorithms of ICP-Brasil.

7.1.3.2 The subordinate CA certificate is signed using an algorithm defined in a regulation edited by normative instruction of the Root CA that defines the standards and cryptographic algorithms of ICP-Brasil.

7.1.4 Name Forms

7.1.4.1 The names of the holder and issuer of the Root CA certificate, contained in the "Distinguished Name" (DN) field, are the same and follow the ITU-T X.501/ISO/IEC 9594-2 standard, as below described:

a) for initial chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao - ITI

CN = Autoridade Certificadora Raiz Brasileira

b) for V1 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao - ITI

CN = Autoridade Certificadora Raiz Brasileira v1

c) :for V2 chain certificate

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v2

d) for V3 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v3

e) for V4 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v4

f) for V5 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v5

g) for V6 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v6

h) for V7 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v7

i) for V8 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v8

j) for V9 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v9

k) for V10 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v10

l) for V11 chain certificate:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v11

m) for V12 chain certificate: (Text amended by CG ICP-Brasil Resolution No. 208, 2024)

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao – ITI

CN = Autoridade Certificadora Raiz Brasileira v12

n) for V13 chain certificate: (Text amended by CG ICP-Brasil Resolution No. 208, 2024)

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v13

7.1.4.2 The names of the holder and issuer of the subordinate CA, contained in the field “Distinguished Name” (DN), follow the ITU-T X.501/ISO/IEC 9594-2 standard , this way:

a) Holder's DN:

C = BR

O = ICP-Brasil

OU = <CN of chain>

CN = <subordinate CA name>

b) DN of the issuer:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informacao - ITI

CN = <CN of chain>

7.1.5 Name Constraints

7.1.5.1 Special characters or accents are not allowed in the DN fields.

7.1.5.2 The name of the CA holding the certificate must be submitted for approval in the accreditation process.

7.1.6 CPS Object Identifier)

The OID of this CPS is 2.16.76.1.1.0

7.1.7 Usage of Policy Constraints Extension

Does not apply to the Root CA. If the CA issues certificates to end users, the “Policy Constraints” extension may be used as defined by RFC 5280 [15].

7.1.8 Policy Qualifiers Syntax and Semantics

The certificates issued by the Root CA implement policy qualifiers in the “Certificate Policies” extension, as described in item 7.1.2 of this CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

All certificates of subordinate CAs must be checked for validity in the CRL of the Root CA before being used. The authenticity of the Root CA CRL must also be verified by verifying the Root CA signature and the validity period of the CRL.

7.2.1 Version Number(s)

Root CA implements its CRL according to version 2 of the ITU X.509 standard.

7.2.2 CRL and CRL Entry Extensions

The CRL issued by the Root CA implements the following extensions provided for in RFC 5280 [15]:

a) **AuthorityKeyIdentifier**: contains the same value as the "Subject Key Identifier" field of the Root CA certificate;

b) **cRLNumber**: contains a sequential number for each CRL issued.

7.3 OCSP Profile

Not Applicable.

7.3.1 Version Number(s)

Not Applicable.

7.3.2 OCSP Extentions

Not Applicable

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The inspections and audits conducted within the scope of ICP-Brasil are intended to verify that the processes, procedures and activities of the entities that are part of ICP-Brasil are in compliance with their respective CPS, PCs, TSPS, TPs, TSPPS, PS and other standards and procedures established by ICP-Brasil.

8.1 Frequency and Circumstances of Assessment

The member entities of ICP-Brasil undergo a prior audit, for accreditation purposes, and annual audits, for accreditation maintenance purposes.

8.2 Identity/Qualifications of Assessor

The inspection of entities that are part of ICP-Brasil is conducted by the Root CA, through its own team, at any time, without prior notice, observing the provisions of the document CRITERIA AND PROCEDURES FOR SUPERVISION OF ICP-BRASIL ENTITIES [5] .

8.3 Assessor's Relationship to Assessed Entity

Except for the audit of Root CA itself, which is the responsibility of the CG of ICP-Brasil, the audits of the entities that are part of ICP-Brasil are carried out by Root CA, through its own team or third parties authorized by it, subject to the provisions in the document CRITERIA AND PROCEDURES FOR PERFORMING AUDITS IN ICP-BRASIL ENTITIES [9].

8.4 Topics Covered by the Assessment

Main Documents of ICP-Brasil (DOC-ICP-NN) and its complementary documents (DOC-ICP-NN.nn), as well as the rules applicable to WebTrust Audit.

8.5 Actions Taken as a Result of Deficiency

CRITERIA AND PROCEDURES FOR PERFORMING AUDITS IN ICP-BRASIL ENTITIES [9] and CRITERIA AND PROCEDURES FOR SUPERVISING ICP-BRASIL'S ENTITIES [5].

8.6 Communication of Results

CRITERIA AND PROCEDURES FOR PERFORMING AUDITS IN ICP-BRASIL ENTITIES [9] and CRITERIA AND PROCEDURES FOR SUPERVISING ICP-BRASIL'S ENTITIES [5].

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fees for issuing and renewing a certificate by the Root CA are defined in the document GUIDELINES OF THE TARIFF POLICY OF THE ROOT CERTIFICATION AUTHORITY OF ICP-BRASIL [4].

9.1.2 Certificate Access Fees

Not Applicable.

9.1.3 Revocation or Status Information Access Fee

There is no fee for revocation or access to certificate status information managed by the Root CA.

9.1.4 Fees for other services

Rates for other Root CA services are defined in the document GUIDELINES OF THE TARIFF POLICY OF THE ROOT CERTIFICATION AUTHORITY OF ICP-BRASIL [4].

9.1.5 Refund Policy

Not Applicable.

9.2 Financial Responsibility

The Root CA’s responsibility will be verified as provided for in Brazilian law.

9.2.1 Insurance Coverage

Not Applicable.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

As a general principle, every document, information or record containing personal data provided to Root CA will be confidential, unless otherwise provided for by law, or when expressly authorized by the respective holder, pursuant to the applicable legislation.

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.2.2 The following documents from the Root CA, the next level CAs, the TSAs and PSCs are also considered non-confidential documents:

a) any applicable PC;

b) any CPS;

c) any applicable TP (Timestamp Policy);

d) any TSPS (Time Stamping Practices Statement);

e) any TSPPS (Trusted Service Provider Practice Statement);

f) public versions of the Security Policy – PS; and

g) the completion of audit reports.

9.3.2.3 Root CA may also disclose, in a consolidated or segmented manner 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

The Participants who receive or have access to confidential information must have mechanisms to ensure protection and confidentiality, preventing its use or disclosure to third parties, under penalty of liability, as provided by law.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The Root CA will ensure the protection of personal data in accordance with its Privacy Policy.

9.4.2 Information Treated as Private

As a general principle, every document, information or record containing personal data provided to Root CA will be considered confidential, unless otherwise provided for by law, or when expressly authorized by the respective holder, pursuant to the applicable legislation.

9.4.3 Information Not Deemed Private

Information on revocation of subordinate CA is provided in the Root CA CRL.

9.4.4 Responsibility to Protect Private Information

The Root CA is responsible for the improper disclosure of confidential information, under the terms of the applicable legislation.

9.4.5 Notice and Consent to Use Private Information

9.4.5.1 The private information obtained by Root CA may be used or disclosed to third parties with the express authorization of the respective owner, in accordance with the applicable legislation.

9.4.5.2 The certificate holder and his legal representative will have full access to any of his own data and identifications, and may authorize the disclosure of his records to other people.

9.4.5.3 Formal authorizations 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 notarized signature.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.6.2 The private or confidential information under the custody of Root CA may be used for the instruction of an administrative or judicial process, or by court order or the competent administrative authority, observing the applicable legislation regarding the secrecy and protection of data before third parties.

9.4.7 Other Information Disclosure Circumstances

Not applicable.

9.5 Intellectual Property Rights

In accordance with current legislation.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The Root represents and warrants the following:

9.6.1.1 Authorization for certificate

The Root CA and subsequent CA implement procedures to verify the authorization to issue an ICP-Brasil certificate, contents, for Root CA, in items 3 and 4 of this CPS and subsequent CAs in the documents MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES AT ICP-BRASIL [3] and MINIMUM REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENT OF THE CERTIFICATION AUTHORITIES OF ICP-BRASIL [2]. Root CA, within the scope of authorizing the issuance of a certificate, analyzes, audits and supervises the processes of subsequent CAs in the form of its CPSs, PCs and complementary standards.

9.6.1.2 Accuracy of information

The Root CA and subsequent CA implement terms of consent or ownership, contained, for Root CA, in items 3 and 4 of this CPS and subsequent CAs in the documents MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES IN ICP-BRASIL [3] and MINIMUM REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENT OF THE CERTIFICATION AUTHORITIES OF ICP-BRASIL [2].

9.6.1.3 Identification of the applicant

The Root CA and subsequent CA implement procedures to verify the identification of applicants contained in the certificates, contents, for Root CA, in items 3 and 4 of this CPS and subsequent CAs in the documents MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES AT ICP-BRASIL [3] and MINIMUM REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENT OF THE CERTIFICATION AUTHORITIES OF ICP-BRASIL [2]. Root CA, within the scope of identifying the applicant in the certificates it issues, analyzes, audits and supervises the processes of subsequent CAs in the form of its CPSs, PCs and complementary standards.

9.6.1.4 Consent of Holders

The Root CA and subsequent CA implement terms of consent or ownership, contents, for Root CA, in items 3 and 4 of this CPS and subsequent CAs in the documents MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES AT ICP-BRASIL [3] and MINIMUM REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENT OF THE CERTIFICATION AUTHORITIES OF ICP-BRASIL [2].

9.6.1.5 Service

The Root CA maintains 24x7 access to its repository with information on its own certificates, subsequent CAs and CRLs.

9.6.1.6 Revocation

The Root CA will revoke ICP-Brasil certificates for any reason specified in the ICP-Brasil rules and in the documents Baseline Requirements, EV Guidelines and/or EV Code Signing Guidelines.

9.6.1.7 Legal Existence

This CPS is in legal compliance with MP No. 2200-2, of August 24, 2001, and applicable legislation.

9.6.2 RA Representations and Warranties

Not applicable.

9.6.3 Subscriber Representations and Warranties

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

9.6.3.2 The CA holder must inform the Root CA of any compromise of its private key and request the immediate revocation of its certificate.

9.6.4 Relying Party Representations and Warranties

9.6.4.1 Third parties must:

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

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

9.6.4.2 The Root CA certificate or a CA certificate of the level immediately subsequent to that of the Root CA is considered valid when:

a) has already been issued by Root CA;

b) not included in the last CRL of the Root CA;

c) is not expired; and

d) can be verified using the valid Root CA certificate.

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

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

Not applicable.

9.8 Limitations of Liability

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

9.9 Indemnification

The Root CA is responsible for the damages that it causes, and are attributable to it, in accordance with current legislation, ensuring the right of recourse against the responsible agent or entity.

9.10 Term and Termination

This CPS comes into force from the publication of the Resolution of the Management Committee that approves it and will remain valid and effective until it is revoked or replaced, expressly or tacitly.

9.10.1 Term

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

9.10.2 Effect of Termination and Survival

9.10.2.1 The acts performed during the term of this CPS are valid and effective for all legal purposes, producing effects even after their revocation, extinction or replacement.

9.10.2.2 In case of disqualification of a CA subsequent to the Root CA, the following procedures must be adopted:

a) the Root CA will disclose the fact in the Official Gazette and on its website (repository);

b) the subsequent CAs, RAs and TPSs operationally linked shall cease, in relation to the CPs subject to disqualification, their activities of issuing certificates within the scope of ICP-Brasil immediately after the communication referred to in the previous paragraph;

c) in case of total disqualification of a CA:

i. the public keys of the certificates issued by it must be stored by another CA, after approval by the Root CA;

ii. when there is more than one CA interested, the one indicated by the CA that ends its activities will assume responsibility for storing the public keys;

iii. the CA that ends its activities will transfer, if applicable, the documentation of the digital certificates issued to the CA that has taken over the custody of the respective public keys; and

iv. if the public keys have not been assumed by another CA, the documents referring to the digital certificates and the respective public keys will be passed on to the Root CA.

9.10.2.3 In the case of Root CA, the Management Committee of ICP-Brasil will define the extinction procedures.

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 email, or, failing that, by official letter from the competent authority or publication in the Federal Official Gazette.

9.12 Amendments

9.12.1 Procedure for Amendment

Any change in this CPS must be submitted by Root CA to the approval of the CG of ICP-Brasil.

9.12.2 Notification mechanism and periods

Changes to this CPS will be published in the DOU and on the ITI website.

9.12.3 Circumstances Under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

This CPS is governed by the legislation of the Federative Republic of Brazil, notably Provisional Measure No. 2,200-2, of 24.08.2001, and the legislation that replaces or amends it, as well as other laws and regulations in force in Brazil.

9.15 Compliance with Applicable Law

The Root CA is subject to the legislation applicable to it, 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 Root CA. If there is a conflict between this CPS and other resolutions of the GC ICP-Brasil, the last edited one will always prevail.

9.16.2 Assignment

The rights and obligations provided for in this CPS are of public order and unavailable, and cannot be assigned or transferred to third parties.

9.16.3 Independence of provisions

The invalidity, nullity or ineffectiveness of any of the provisions of this CPS will not affect the other provisions, which will remain fully valid and effective. In this case, the invalid, null or ineffective provision will be considered unwritten, so that this CPS will be interpreted as if it did not contain such provision, and as far as possible, maintaining the original intent of the remaining provisions.

9.16.4 Enforcement (lawyers' fees and waiver of rights)

In accordance with current legislation.

9.17 Other Provisions

Not applicable.

10 REFERENCED DOCUMENTS

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

REF.	DOCUMENT NAME	COD
[1]	SECURITY POLICY OF ICP-BRASIL Approved by Resolução nº 02, de 25 de setembro de 2001	DOC-ICP-02
[2]	MINIMUM REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENT OF THE CERTIFICATION AUTHORITIES OF ICP-BRASIL Approved by Resolução nº 08, de 12 de dezembro de 2001	DOC-ICP-05
[3]	MINIMUM REQUIREMENTS FOR CERTIFICATE POLICIES AT ICP-BRASIL Approved by Resolução nº 07, de 12 de dezembro de 2001	DOC-ICP-04
[4]	GUIDELINES OF THE TARIFF POLICY OF THE ROOT CERTIFICATION AUTHORITY OF ICP-BRASIL Approved by Resolução nº 10, de 14 de fevereiro de 2002	DOC-ICP-06
[5]	CRITERIA AND PROCEDURES FOR SUPERVISING ICP-BRASIL'S ENTITIES Approved by Resolução nº 25, de 24 de outubro de 2003	DOC-ICP-09
[6]	CRITERIA AND PROCEDURES FOR ACCREDITATION OF ICP-BRASIL'S MEMBERS Approved by Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03
[9]	CRITERIA AND PROCEDURES FOR CONDUCTING AUDITS IN ICP-BRASIL'S ENTITIES Approved by Resolução nº 24, de 29 de agosto de 2003	DOC-ICP-08

10.2 The documents below are approved by Root CA, and may be amended, when necessary, by publishing a latest version on the website http://www.iti.gov.br.

REF.	DOCUMENT NAME	COD
[7]	REVALIDATION FORM OF REGISTRATION DATA AND REQUEST FOR A NEW CERTIFICATE	ADE-ICP.01.A
[8]	CA CERTIFICATE REVOCATION REQUEST FORM	ADE-ICP.01.B

10.3 The documents referenced in the WebTrust Principles and Criteria [10], as well as the Baseline Requirements and Extended Validation SSL and CodeSign Guidelines [11], are published respectively by CPA - Chartered Professional Accountants Canada and CA/Browser Forum.

REF.	DOCUMENT NAME	ADDRESS
[10]	WEBTRUST PRINCIPLES AND CRITERIA	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria
[11]	BASELINE REQUIREMENTS, EXTENDED VALIDATION SSL e CODESIGN GUIDELINES	https://cabforum.org

11 BIBLIOGRAPHICAL REFERENCES

[12] 2007. BRAZILIAN ASSOCIATION OF TECHNICAL STANDARDS. 11.515/NB 1334: Physical security criteria related to data storage. 2007.

[13] RFC 3647, IETF - *Internet* X.509 P*ublic Key Infrastructure Certificate Policy and Certification Practices Framework*, *november* 2003.

[14] RFC 4210, IETF - *Internet* X.509 *Public Key Infrastructure Certificate Management Protocol (CMP), September* 2005.

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

[16] RFC 6712, IETF - *Internet* X.509 *Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), September* 2012.