Moreira Auditores
By your side

INDEPENDENT ASSURANCE REPORT

To the Management of Instituto Nacional de Tecnologia da Informação ("AC Raiz da ICP- Brasil – Root CA"):

We have been engaged, in a reasonable assurance engagement, to report on AC Raiz da ICP-Brasil – Root CA management's assertion that for its Certification Authority (CA) operations at Brasília, Brazil and Rio de Janeiro, Brazil, throughout the period September 9, 2024 to September 8, 2025, for its CAs as enumerated in the Attachment A, AC Raiz da ICP-Brasil – Root CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Certification Practice Statement Root Certification Authority of Brazil - Version 6.1
- maintained effective controls to provide reasonable assurance that:
  - AC Raiz da ICP-Brasil – Root CA provides its services in accordance with its Certification Practice Statements.
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subordinate CA certificate requests are accurate, authenticated, and approved.
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

in accordance with the Webtrust Principles and Criteria for Certification Authorities, Version 2.2.2.

AC Raiz da ICP-Brasil – Root CA does not escrow its CA keys, does not provide subscriber key generation services, does not provide rekey services and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

AC Raiz da ICP-Brasil – Root CA management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the Webtrust Principles and Criteria for Certification Authorities, Version 2.2.2.

Moreira Auditores
By your side

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of AC Raiz da ICP-Brasil – Root CA key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at AC Raiz da ICP-Brasil – Root CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period September 9, 2024 to September 8, 2025, AC Raiz da ICP- Brasil – Root CA Management's Assertion, as referred to above, is fairly stated, in all material respects, in accordance with the Webtrust Principles and Criteria for Certification Authorities, Version 2.2.2.

This report does not include any representation as to the quality of AC Raiz da ICP-Brasil – Root CA services beyond those covered by the Webtrust Principles and Criteria for Certification Authorities, Version 2.2.2, nor the suitability of any of AC Raiz da ICP-Brasil – Root CA services for any customer's intended purpose.

Use of the WebTrust seal

AC Raiz da ICP-Brasil – Root CA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Moreira Associados Auditores Independentes S/S
Brasília, DF / Brazil
December 04, 2025.

DIEGO ROTERMUND MOREIRA:90693922087

Assinado digitalmente por DIEGO ROTERMUND MOREIRA:90693922087
ND: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=(EM BRANCO), OU=01579286000174, OU =presencial, CN=DIEGO ROTERMUND MOREIRA:90693922087
Razão: Eu sou o autor deste documento
Localização:
Data: 2025.12.04 15:07:56-03'00'
Foxit PDF Editor Versão: 13.1.1

Diego Rotermund Moreira
Partner

Instituto Nacional de Tecnologia da Informação

AC RAIZ DA ICP-BRASIL – ROOT CA MANAGEMENT'S ASSERTION

Instituto Nacional de Tecnologia da Informação ("AC Raiz da ICP-Brasil – Root CA") operates the Certification Authority (CA) services for AC Raiz da ICP-Brasil – Root CA and the subordinated CAs presented in the Attachment A, and provides the following CA services:

- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of AC Raiz da ICP-Brasil – Root CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its repositories presented in the Attachment B, CA business practices management, CA environmental controls, CA key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to AC Raiz da ICP-Brasil – Root CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

AC Raiz da ICP-Brasil – Root CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in AC Raiz da ICP-Brasil – Root CA management opinion, in providing its Certification Authority (CA) services in Brasília, Brazil and Rio de Janeiro, Brazil, throughout the period September 9, 2024 to September 8, 2025, AC Raiz da ICP- Brasil – Root CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:

  —Certification Practice Statement Root Certification Authority of Brazil - Version 6.1

- maintained effective controls to provide reasonable assurance that:
  - AC Raiz da ICP-Brasil – Root CA provides its services in accordance with its Certification Practice Statement.
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subordinate CA certificate requests are accurate, authenticated, and approved.

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the Webtrust Principles and Criteria for Certification Authorities, Version 2.2.2, including the following:

CA Business Practices Disclosure
- Certification Practice Statement (CPS)

CA Business Practices Management
- Certification Practice Statement Management
- CPS Consistency

CA Environmental Controls
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls
- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Certificate Lifecycle Management Controls
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Lifecycle Management

AC Raiz da ICP-Brasil – Root CA does not escrow its CA keys, does not provide subscriber key generation services, does not provide rekey services and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

December 04, 2025
Brasília, DF/ Brazil

Alysson Marques
AC Raiz da ICP-Brasil – Root CA
Instituto Nacional de Tecnologia da Informação - ITI

Documento assinado digitalmente
gov.br
ALYSSON MARQUES
Data: 04/12/2025 14:52:39-0300
Verifique em https://validar.iti.gov.br

ATTACHMENT A

List of CAs in Scope

Root CAs
Autoridade Certificadora Raiz Brasileira v4
Autoridade Certificadora Raiz Brasileira v5
Autoridade Certificadora Raiz Brasileira v6
Autoridade Certificadora Raiz Brasileira v7
Autoridade Certificadora Raiz Brasileira v10
Autoridade Certificadora Raiz Brasileira v11
Autoridade Certificadora Raiz Brasileira v12
Autoridade Certificadora Raiz Brasileira v13

List of CAs in Scope – Detailed Information

CA#	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	SKI	Fingerprint
1	CN = Autoridade Certificadora Raiz Brasileira v4 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v4 OU = Instituto Nacional de Tecnologia da Informacao – ITI O = ICP-Brasil C = BR	01	ECDSA	512	sha512 ECDSA	43692619abddc78df3ac3532115472e8c9990a4d	f0c15afd258fb674e7a96e1a50ff873149364b9ec70d4d93c7a9f1eb6060d020
2	CN = Autoridade Certificadora Raiz Brasileira v5 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v5 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	4096	sha512 RSA	69a8be75d9c4ef6ce7345e4616ee568f8b6405e	caa53fc6091c6951887c976e378f6ef89aa6377c55d97b6475422b71ed7e9b17
3	CN = Autoridade Certificadora Raiz Brasileira v6 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v6 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00cb036869bc2f77e1	EDDSAED 448	448	EDDSA448	597867e3ec8a31cdf04ef51ea68f4e9d0e7 e123e	3bdb9b509352f1d3d71c2bf64d9a38a4e6cebda27809d77f7ac476cbde6e314a

CA#	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	SKI	Fingerprint
4	CN = Autoridade Certificadora Raiz Brasileira v7 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v7 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00e4ac9a3346c92509	EDDSAED521	521	EDDSA521	75513119e1c71321873e415fa31be67bfdb0d9c8	5657e70580eb678983f3ed7dfce091d84cae6549389a47fccda8d0e4dc2cf576
5	CN = Autoridade Certificadora Raiz Brasileira v10 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v10 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00d2d58b44bf819342	RSA	4096	sha512 RSA	74f37efffc9f537af17cebab3ea4a6da18ba 4563	6e0bff069a26994c15de2c4888cc54af84882e5495b7fbf66be9ccffec7489f6
6	CN = Autoridade Certificadora Raiz Brasileira v11 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v11 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	242b60d4cd 43697f	RSA	4096	sha512 RSA	9cad62e197ed809e73391edc51bec704cb d81ea9	1406710058180fa4081aab3f246f1702429c552a11fa3143b84c88cb3ab8e5e7
7	CN= Autoridade Certificadora Raiz Brasileira v12 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira V12 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00e18ff4b61d07bd0f	RSA	4096	sha512 RSA	6ac17ad792c1ba694ed6e2f3c2998489be55740e	d8478e37ce19c690cf657381e68fe600e4e1a042536830f06847e03e554c4b01
8	CN= Autoridade Certificadora Raiz Brasileira v13 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira V13 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00f99f32155da328b8	ECDSA	512	Sha512ECDSA	33a0796a79825cb3f9f1ef3485244e8aeaeadc6a	2b07d0bc02c4a6e0478ed22d0d99e8f97e1827b269097696a7feb6aad30c3ac8

ATTACHMENT B

List of CAs in Scope – Certification Practice Statement and Security Policy

CA#	CA	CPS - Latest Version Available	SP - Latest Version Available	URL
1	Autoridade Certificadora Raiz Brasileira v4	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link
2	Autoridade Certificadora Raiz Brasileira v5	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link
3	Autoridade Certificadora Raiz Brasileira v6	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link
4	Autoridade Certificadora Raiz Brasileira v7	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link
5	Autoridade Certificadora Raiz Brasileira v10	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link
6	Autoridade Certificadora Raiz Brasileira v11	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link
7	Autoridade Certificadora Raiz Brasileira v12	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link
8	Autoridade Certificadora Raiz Brasileira v13	DOC-ICP 01 – Version 6.1 – 08/07/2024	DOC-ICP 02 – Version 4.0 – 11/16/2021	Repository Link