Praia de Botafogo, 370
8º ao 10º andar – Botafogo – 22250-040
Rio de Janeiro – RJ – Brasil
Tel.: +55 21 3263 1000
www.ey.com.br

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 *Florianópolis, Brazil*, throughout the period September 9, 2021 to September 8, 2022, 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
- 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.

Praia de Botafogo, 370
8º ao 10º andar – Botafogo – 22250-040
Rio de Janeiro – RJ – Brasil
Tel.: +55 21 3263 1000
www.ey.com.br

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 Control 1 - *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and 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.

Praia de Botafogo, 370
8º ao 10º andar – Botafogo – 22250-040
Rio de Janeiro – RJ – Brasil
Tel.: +55 21 3263 1000
www.ey.com.br

Opinion

In our opinion, throughout the period September 9, 2021 to September 8, 2022, *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.

January, 30 2023

Rio de Janeiro, RJ/ Brazil

FRANCESCO GIGLIO BOTTINO:83217258720

Digitally signed by FRANCESCO GIGLIO BOTTINO:83217258720
DN: cn=FRANCESCO GIGLIO BOTTINO:83217258720, c=BR, o=ICP-Brasil, ou=(em branco), email=francesco.bottino@br.ey.com
Date: 2023.01.31 09:28:43 -03'00'

Francesco Bottino

Ernst & Young Auditores Independentes S.S.
Partner

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
- 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 *Florianópolis, Brazil*, throughout the period September 09, 2021 to September 08, 2022, *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
- 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 Life Cycle 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.

January, 30 2023

Brasília, DF/ Brazil

MAURICIO AUGUSTO COELHO

Assinado de forma digital por MAURICIO AUGUSTO COELHO
Dados: 2023.01.30 14:35:31 -03'00'

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

ATTACHMENT A

List of CAs in Scope

Root CAs
Autoridade Certificadora Raiz Brasileira v2
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

List of CAs in Scope – Detailed Information

CA#	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
1	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	4096	sha512With RSA	0c39203ab7011fcbd7287d41a0c7fa4aad3224be	FB47D92A9909FD4FA9BEC02737543E1F3514CED747407A8D9CFA397B0915067C
2	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	sha512With ECDSA	43692619abddc78df3ac3532115472e8c9990a4d	F0C15AFD258FB674E7A96E1A50FF873149364B9EC70D4D93C7A9F1EB6060D020

CA#	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
3	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	sha512With RSA	69a8be75d9c4ef6ce71345e4616ee568f8b6405e	CAA53FC6091C6951887C976E378F6EF89AA6377C55D97B6475422B71ED7E9B17
4	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	EDDSAED448	448	EDDSA448	597867e3ec8a31cdf04ef51ea68f4e9d0e7e123e	3BDB9B509352F1D3D71C2BF64D9A38A4E6CEBDA27809D77F7AC476CBDE6E314A
5	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
6	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	D2D58B4BF819342	RSA	4096	sha512With RSA	74f37efffc9f537af17cebab3ea4a6da18ba4563	6E0BFF069A26994C15DE2C4888CC54AF84882E5495B7FBF66BE9CCFFEC7489F6
7	CN = Autoridade Certificadora Raiz Brasileira v11	CN = Autoridade Certificadora Raiz Brasileira v11	242B60DCD43697F	RSA	4096	sha512With RSA	9cad62e197ed809e73391edc51bec704cbd81ea9	1406710058180FA4081AAB3F246F1702429C552A11FA3143B84C88CB3AB8E5E7

CA#	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
	OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR						

ATTACHMENT B

List of CAs in Scope – Certification Practice Statement and Certificate Policies

CA#	CA	CPS - Latest Version Available	SP - Latest Version Available	URL
1	Autoridade Certificadora Raiz Brasileira v2	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link
2	Autoridade Certificadora Raiz Brasileira v4	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link
3	Autoridade Certificadora Raiz Brasileira v5	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link
4	Autoridade Certificadora Raiz Brasileira v6	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link
5	Autoridade Certificadora Raiz Brasileira v7	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link
6	Autoridade Certificadora Raiz Brasileira v10	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link
7	Autoridade Certificadora Raiz Brasileira v11	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link