

Independent Assurance Report

To the Management of 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 Root Certification Authority (CA) operations at *Brasília, Brazil* and *Florianópolis, Brazil*, throughout the period September 9, 2018 to September 8, 2019, for its CAs as enumerated in the Appendix 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 Statements
 - Security Policy

as listed on the appendix B

- maintained effective controls to provide reasonable assurance that:
 - AC Raiz da ICP-Brasil – Root CA Certification Practice Statements are consistent with its Security Policy
 - AC Raiz da ICP-Brasil – Root CA provides its services in accordance with its Security Policy and 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 were properly authorized and performed to maintain CA systems integrity

in accordance with the [Webtrust Principles and Criteria for Certification Authorities, Version 2.2](#). AC Raiz da ICP-Brasil – Root CA does not escrow its CA keys, 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](#).

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, 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.

Auditor'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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, AC Raiz da ICP-Brasil – Root CA ability to meet the criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period September 9, 2018 to September 8, 2019, 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](#).

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](#) criteria nor the suitability of any of Root – CA's services for any customer's intended purpose.

Use of the WebTrust seal

AC Raiz da ICP-Brasil – Root CA 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.

November 26, 2019

Ernst & Young Auditores Independentes S.S.

Assinado digitalmente por FRANCESCO
GIGLIO BOTTINO.83217258720
FRANCESCO GIGLIO
BOTTINO:83217258720
DN: cn=FRANCESCO GIGLIO
BOTTINO.83217258720, c=BR, o=ICP-
Brasil, ou=2656320005001,
email=francesco.bottino@br.ey.com
Data: 2019.11.27 13:01:34 -03'00'

Francesco Bottino
Partner

AC Raiz da ICP-Brasil – Root CA Management’s Assertion

AC Raiz da ICP-Brasil – Root CA operates the Certification Authority (CA) services for Root CA and the subordinated CAs presented in the appendix A, and provides the following CA services:

- Certificate renewal
- 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 Appendix 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 9, 2018 to September 8, 2019, 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 Statements
 - Security Policy

as listed on the appendix B

- maintained effective controls to provide reasonable assurance that:
 - AC Raiz da ICP-Brasil – Root CA Certification Practice Statements are consistent with its Security Policy
 - AC Raiz da ICP-Brasil – Root CA provides its services in accordance with its Certificate Policies and 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 authorised individuals;
- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the [Webtrust Principles and Criteria for Certification Authorities, Version 2.2](#), including the following:

CA Business Practices Disclosure

Certification Practice Statement (CPS)
Security Policy (SP)

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
Systems 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 Renewal (CA's Controls)
Certificate Issuance
Certificate Distribution
Certificate Revocation

**ITI**Instituto Nacional de
Tecnologia da Informação

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 rekey services, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

EDUARDO
MAGALHAES DE
LACERDA FILHO

Assinado de forma digital
por EDUARDO MAGALHAES
DE LACERDA FILHO
Dados: 2019.11.22 18:17:59
-03'00'

November 22, 2019



APPENDIX A

List of CAs in Scope – Classification by Type

Root CAs
1 – Autoridade Certificadora Raiz Brasileira v1
2 – Autoridade Certificadora Raiz Brasileira v2
3 – Autoridade Certificadora Raiz Brasileira v4
4 – Autoridade Certificadora Raiz Brasileira v5
5 – Autoridade Certificadora Raiz Brasileira v6
6 – Autoridade Certificadora Raiz Brasileira v7

List of CAs in Scope – Detailed Information

CA #	Root CA Name	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Hash Fingerprint (sha256)
1	CN = Autoridade Certificadora Raiz Brasileira v1 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	2048	sha1WithRSA	terça-feira, 29 de julho de 2008 16:17:10	quinta-feira, 29 de julho de 2021 16:17:10	42b22c5c740107be9bff55333bee29bb5d91bf06	cbd8ed38d4a2d677d453d70dd8890af4f6374cba6299943f1ab3a6936c6fd795
2	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	4096	sha512WithRSA	segunda-feira, 21 de junho de 2010 16:04:57	quarta-feira, 21 de junho de 2023 16:04:57	0c39203ab7011fcbd7287d41a0c7fa4aad3224be	fb47d92a9909fd4fa9bec02737543e1f3514ced747407a8d9cfa397b0915067c
3	CN = Autoridade Certificadora Raiz Brasileira v4 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	ECDSA	512	sha512WithECDSA	quinta-feira, 23 de abril de 2015 15:38:58	segunda-feira, 23 de abril de 2035 20:59:58	43692619abddc78df3ac3532115472e8c9990a4d	f0c15afd258fb674e7a96e1a50ff873149364b9ec70d4d93c7a9f1eb6060d020
4	CN = Autoridade Certificadora Raiz Brasileira v5 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	4096	sha512WithRSA	quarta-feira, 2 de março de 2016 10:01:38	sexta-feira, 2 de março de 2029 20:59:38	69a8be75d9c4ef6ce71345e4616ee568f8b6405e	caa53fc6091c6951887c976e378f6ef89aa6377c55d97b6475422b71ed7e9b17
5	CN = Autoridade Certificadora Raiz Brasileira v6 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00cb036869bc2f77e1	EdDSA Ed448	448	EDDSA448	sexta-feira, 28 de dezembro de 2018 10:32:03	terça-feira, 28 de dezembro de 2038 09:00:03	597867e3ec8a31cdf04ef51ea68f4e9d0e7e123e	3b9db9b509352f1d3d71c2bf64d9a38a4e6cebda27809d77f7ac476cbde6e314a
6	CN = Autoridade Certificadora Raiz Brasileira v7 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00e4ac9a3346c92509	EdDSA Ed521	521	EDDSA521	sexta-feira, 28 de dezembro de 2018 10:47:35	terça-feira, 28 de dezembro de 2038 09:00:35	75513119e1c71321873e415fa31be67bfbdb0d9c8	5657e70580eb678983f3ed7dfce091d84cae6549389a47fccda8d0e4dc2cf576

APPENDIX B

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

CA#	Root CA Name (CN)	CPS - Latest Version Available	SP - Latest Version Available	URL
1	AC Raiz de ICP-Brasil v1	DOC-ICP 01 – Versão 5.1 – 13/08/2019	DOC-ICP- 02 – Versão 3.1 – 30/05/2019	Repository Link
2	AC Raiz de ICP-Brasil v2	DOC-ICP 01 – Versão 5.1 – 13/08/2019	DOC-ICP- 02 – Versão 3.1 – 30/05/2019	Repository Link
3	AC Raiz de ICP-Brasil v4	DOC-ICP 01 – Versão 5.1 – 13/08/2019	DOC-ICP- 02 – Versão 3.1 – 30/05/2019	Repository Link
4	AC Raiz de ICP-Brasil v5	DOC-ICP 01 – Versão 5.1 – 13/08/2019	DOC-ICP- 02 – Versão 3.1 – 30/05/2019	Repository Link
5	AC Raiz de ICP-Brasil v6	DOC-ICP 01 – Versão 5.1 – 13/08/2019	DOC-ICP- 02 – Versão 3.1 – 30/05/2019	Repository Link
6	AC Raiz de ICP-Brasil v7	DOC-ICP 01 – Versão 5.1 – 13/08/2019	DOC-ICP- 02 – Versão 3.1 – 30/05/2019	Repository Link