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 extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - Certification Practice Statement;

    including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the *AC Raiz da ICP-Brasil – Root CA* website and provided such services in accordance with its disclosed practices.

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by *AC Raiz da ICP-Brasil – Root CA)*.

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.7.8.

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 – Extended Validation SSL – Version 1.7.8.

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* - 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.

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

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* EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates,
2. selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management 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 the 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, 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 WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.7.8.

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 – Extended Validation SSL – Version 1.7.8, nor the suitability of any of *AC Raiz da ICP-Brasil – Root CA* services for any customer's intended purpose.

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

Use of the WebTrust seal

AC Raiz da ICP-Brasil – Root CA use of the WebTrust for Certification Authorities – Extended Validation SSL 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 09:29:59 -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 CAs presented in Attachment A and provides Extended Validation SSL ("EV SSL") CA services.

The management of *AC Raiz da ICP-Brasil – Root CA* is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, and EV SSL 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* Certification Authority 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 EV SSL CA services. Based on that assessment, in *AC Raiz da ICP-Brasil – Root CA* management's opinion, in providing its EV SSL Certification Authority (CA) services at *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 extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - Certification practice statement

  including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the *AC Raiz da ICP-Brasil – Root CA* website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by *AC Raiz da ICP-Brasil – Root CA*)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.7.8.

January, 30 2023

Brasília, DF/ Brazil

MAURICIO AUGUSTO COELHO

Assinado de forma digital por MAURICIO AUGUSTO COELHO
Dados: 2023.01.30 14:30:51 -03'00'

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

ATTACHMENT A

List of CAs in Scope

Root CAs
Autoridade Certificadora Raiz Brasileira v10

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 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	D2D58 B4BF81 9342	RSA	4096	sha512WithRSA	74f37efffc9f537af17cebab3ea4a6da18ba4563	6E0BFF069A26994C15DE2C4888CC54AF84882E5495B7FBF66BE9CCFFEC7489F6

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 v10	DOC-ICP 01 – Version 6.0 – 16/11/2021	DOC-ICP 02 – Version 4.0 – 16/11/2021	Repository Link