EY - RJ
Praia de Botafogo, 370
Botafogo, Rio de
Janeiro.
CEP: 22250-909

Tel: +55 21 3263 7000
Fax: +55 21 3263 7002
ey.com.br

Independent Assurance Report

To the Management of Instituto Nacional de Tecnologia da Informação:

Scope

We have been engaged, in a reasonable assurance engagement, to report on Instituto Nacional de Tecnologia da Informação (ITI) management's assertion, that for its Certification Authority (CA) services in Brazil for the Root CAs presented in the appendix A, during the period September 9th, 2017 through September 8th, 2018, ITI has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement and provided services in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that:
    - ITI 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 life cycles;
    - 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 was restricted to authorized individuals;
    - The continuity of key and certificate management operations was maintained; and
    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

For the root level Certification Authority, based on the AICPA in accordance with the Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1.

Certification authority's responsibilities

ITI's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1.

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 behavior.

Building a better working world

EY - RJ
Praia de Botafogo, 370
Botafogo, Rio de Janeiro.
CEP: 22250-909

Tel: +55 21 3263 7000
Fax: +55 21 3263 7002
ey.com.br

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 ITI's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy of relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate life cycle 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 our examination provides a reasonable basis for our opinion.

ITI's makes use of external registration authorities for specific subscriber registration activities as disclosed in ITI's business practices. Our examination did not extend to the controls exercised by the external registration authorities.

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 ITI 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, subordinate CAs and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, ITI's ability to meet the aforementioned 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.

EY - RJ
Praia de Botafogo, 370
Botafogo, Rio de
Janeiro.
CEP: 22250-909

Tel: +55 21 3263 7000
Fax: +55 21 3263 7002
ey.com.br

Opinion

In our opinion, through the period September 9th 2017 to September 8th 2018, ITI management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1.

This report does not include any representation as to the quality of ITI's services beyond those covered by the Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1 criteria nor the suitability of any of ITI's services for any customer's intended purpose.

Use of the WebTrust seal

ITI'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.

FRANCESCO GIGLIO BOTTINO:83217258720

Digitally signed by FRANCESCO GIGLIO BOTTINO:83217258720
DN: cn=FRANCESCO GIGLIO BOTTINO:83217258720, c=BR, o=ICP-Brasil, ou=Autenticado por AR Vanguarda, email=francesco.bottino@br.ey.com
Date: 2018.11.23 12:00:35 -02'00'

November, 2018
Ernst & Young Auditores Independentes S.S.
Francesco Bottino
Partner

PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN, Quadra 02 Bloco E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3875 - https://www.iti.gov.br

Assertion by Management of Instituto Nacional de Tecnologia da Informação. Regarding Its Disclosure of Its Business Practices and Its Controls Over Its Certification Authorith Operations During the Period
September 09th, 2017 Through September 08th, 2018

We as management of Instituto Nacional de Tecnologia da Informação (ITI) are responsible for operating a Certification Authority (CA) at Brazil for Root Cas listed in the appendix A:

- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate status information processing (using an online repository)

ITI makes use of external registration authorities for specific subscriber registration activities as disclosed in its business practice disclosures.

The management of ITI is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure, 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 ITI's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ITI management has assessed its disclosures of its certificate practices and controls over its CA services. Based on the assessment, ITI's management opinion, in providing its Certification Authority (CA) services for the Root Cas in Brazil, through the period September 9th, 2017 to September 08th, 2018, ITI has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement and provided services in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that:
    - ITI 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 life cycles;

- Subordinate CA certificate requests are accurate, authenticated, and approved

PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN, Quadra 02 Bloco E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3875 - https://www.iti.gov.br

- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

In accordance with the Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1, including the following:

CA Business Practices Disclosure

Certification Practice Statement
Certificate Practice Statement Management

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 Life Cycle Management Controls
CA Key Archival and Destruction
CA Key Compromise
CA Cryptographic Hardware Life Cycle Management
CA-Key Escrow

Certificate Life Cycle Management Controls

Certificate Renewal
Certificate Rekey

Certificate Issuance

PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN, Quadra 02 Bloco E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3875 - https://www.iti.gov.br

Certificate Distribution
Certificate Revocation
Certificate Validation

November, 2018

Instituto Nacional de Tecnologia da Informação – Certificate Authority

GASTAO JOSE DE OLIVEIRA RAMOS:15016609187

Assinado de forma digital por GASTAO JOSE DE OLIVEIRA RAMOS:15016609187
Dados: 2018.11.22 19:22:47 -02'00'

GASTÃO JOSÉ DE OLIVEIRA RAMOS
Diretor-Presidente

PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN, Quadra 02 Bloco E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3875 - https://www.iti.gov.br

APPENDIX A

Root CA Name	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Hash SHA-256 Fingerprint
CN = Autoridade Certificadora Raiz Brasileira v1 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	(2048 bits)	sha1WithRSA	Jul 29 19:17:10 2008 GMT	Jul 29 19:17:10 2021 GMT	42b22c5c740107be9bff55333bee29bb5d91bf06	cbd8ed38d4a2d677d453d70dd8890af4f6374cba6299943f1ab3a6936c6fd795
CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	(4096 bits)	sha512WithRSA	Jun 21 19:04:57 2010 GMT	Jun 21 19:04:57 2023 GMT	0c39203ab7011fcbd7287d41a0c7fa4aad3224be	fb47d92a9909fd4fa9bec02737543e1f3514ced747407a8d9cfa397b0915067c
CN = Autoridade Certificadora Raiz Brasileira v4 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	ECDSA	(512 bits)	sha512WithECDSA	Apr 23 18:38:58 2015 GMT	Apr 23 23:59:58 2035 GMT	43692619abddc78df3ac3532115472e8c9990a4d	f0c15afd258fb674e7a96e1a50ff873149364b9ec70d4d93c7a9f1eb6060d020
CN = Autoridade Certificadora Raiz Brasileira v5 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	01	RSA	(4096 bits)	sha512WithRSA	Mar 2 13:01:38 2016 GMT	Mar 2 23:59:38 2029 GMT	69a8be75d9c4ef6ce71345e4616ee568f8b6405e	caa53fc6091c6951887c976e378f6ef89aa6377c55d97b6475422b71ed7e9b17