

Report of Independent Accountant

To the Management of Instituto Nacional de Tecnologia da Informação (ITI):

We have examined the [assertion](#) by the management of Instituto Nacional de Tecnologia da Informação (ITI) that in providing its Certification Authority (CA) services at Brazil for the Root CAs listed in **Appendix A**, during the period from September 09th 2016 through September 08th 2017, 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
 - 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 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

for the Root CAs listed in **Appendix A**, based on the AICPA [Trust Service Principles and Criteria for Certification Authorities, Version 2.0](#).

ITI management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

AC Raiz makes use of external registration authorities for specific subscriber registration activities as disclosed in AC Raiz' business practice disclosures. Our examination did not extend to the controls exercised by the external registration authorities.

Our examination was conducted in accordance with attestation standards established by the AICPA, and accordingly, included (1) obtaining an understanding of AC Raiz' key and certificate life cycle management business practices and its controls over key and certificate integrity, over the continuity of key and certificate life cycle management operations, and over the 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.

The relative effectiveness and significance of specific controls at AC Raiz 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.

Because of the nature and inherent limitations of controls, AC Raiz' 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.

In our opinion, for the period from September 09th 2016 through September 08th 2017, ITI management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA [Trust Service Principles and Criteria for Certification Authorities, Version 2.0](#).

The WebTrust seal of assurance for certification authorities on ITI's website 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.

This report does not include any representation as to the quality of ITI's CA services beyond those covered by the [Trust Service Principles and Criteria for Certification Authorities, Version 2.0](#), nor the suitability of any of ITI's services for any customer's intended purpose.



PRESIDÊNCIA DA REPÚBLICA – CASA CIVIL
SCN – Quadra 2 Bloco E - 70712-905 – Brasília/DF
Telefone: (61) 3424-3853 / 3926/ 3875 – iti.gabinete@iti.gov.br

December 2017.

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

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

AC Raiz makes use of external registration authorities for specific subscriber registration activities as disclosed in AC Raiz' business practice disclosures.

Management of ITI is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to AC Raiz' operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ITI Management has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in ITI Management's opinion, in providing its CA services for the Root CAs listed in **Appendix A** at Brazil during the period from September 09th, 2016 through September 08th, 2017, 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
 - 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 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.

For the Root CAs listed in **Appendix A**, based on the AICPA [Trust Service Principles and Criteria for Certification Authorities, Version 2.0](#), including the following:

CA Business Practices Disclosure

CA Business Practices Management
Certification Practice Statement Management

Service Integrity

CA Key Life Cycle 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 Life Cycle Management

Certificate Life Cycle Management Controls

Certificate Renewal
Certificate Rekey
Certificate Issuance

Certificate Distribution
Certificate Revocation
Certificate Validation

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

GASTAO JOSE DE OLIVEIRA RAMOS:15016609187
Assinado de forma digital por GASTAO
JOSE DE OLIVEIRA RAMOS:15016609187
Dados: 2017.12.20 18:02:01 -02'00'

GASTÃO JOSÉ DE OLIVEIRA RAMOS
Diretor-Presidente

Appendix A

| Root | Subject Key Identifier | Certificate Serial Number |
|---|---|---------------------------|
| Autoridade Certificadora Raiz Brasileira v1 | 42:B2:2C:5C:74:01:07:BE:9B:FF:55:33:3B:EE:29:BB:5D:91:BF:06 | 1 (0x1) |
| Autoridade Certificadora Raiz Brasileira v2 | 0C:39:20:3A:B7:01:1F:CB:D7:28:7D:41:A0:C7:FA:4A:AD:32:24:BE | 1 (0x1) |
| Autoridade Certificadora Raiz Brasileira v4 | 43:69:26:19:AB:DD:C7:8D:F3:AC:35:32:11:54:72:E8:C9:99:0A:4D | 1 (0x1) |
| Autoridade Certificadora Raiz Brasileira v5 | 69:A8:BE:75:D9:C4:EF:6C:E7:13:45:E4:61:6E:E5:68:F8:B6:40:5E | 1 (0x1) |