PKI Consulting
Av. Borges de Medeiros, 2500/1402
Praia de Belas - Porto Alegre - RS 90110.150
Fone: +55 51 3398 5740
www.pkiconsulting.com

Independent Assurance Report

To the Management of Serviço Federal de Processamento de Dados (SERPRO) Certification Authority (SERPRO-CA):

Scope

We have been engaged, in a reasonable assurance engagement, to report on SERPRO-CA management's assertion that for its Certification Authority (CA) operations in Brasilia, Brazil, as of 16 March 2020 for its CAs as enumerated in Attachment A, SERPRO-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL Certification Practice Statement, v1.2, February 2020
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL Certificate Policy, v1.2, February 2020
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL's Certification Practice Statement is consistent with its Certificate Policy
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL provides its services in accordance with its Certificate Policy and Certification Practice Statement
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated (for the registration activities performed by SERPRO-CA)
- suitably designed, and placed into operation, 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 v2.2.

SERPRO-CA does not escrow its CA keys, does not provide subscriber key generation, storage and recovery services, does not provide integrated circuit card management services, does not provide certificate suspension services, does not provide certificate rekey services and does not provide third-party subordinate CA or cross certificate issuance or management. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

SERPRO-CA'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 Principles and Criteria for Certification Authorities v2.2.

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 SERPRO-CA's 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) evaluating the suitability of the design of the controls; and

(3) performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of SERPRO-CA's controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Suitability of controls

The suitability of the design of the controls at SERPRO-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 suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, SERPRO-CA'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.

Opinion

In our opinion, as of 16 March 2020 SERPRO-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 v2.2.

This report does not include any representation as to the quality of SERPRO-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2, nor the suitability of any of SERPRO-CA’s services for any customer's intended purpose.

JOAO IVONIR
MOREIRA:18835759072

Assinado de forma digital por JOAO IVONIR MOREIRA:18835759072
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=(EM BRANCO), ou=89138168000171, cn=JOAO IVONIR MOREIRA:18835759072
Dados: 2020.03.20 13:06:22 -03'00'

João Ivonir Moreira - CRC/RS-025692/O-4
PKI Contabilidade e Auditoria Ltda - CNPJ 18.885.468/0001-76 – CRC/RS-007849/O
Porto Alegre, Rio Grande do Sul, Brazil
20 March 2020

SERPRO
Serviço Federal de Processamento de Dados

SERPRO-CA Management's Assertion

Serviço Federal de Processamento de Dados (SERPRO) operates the Certification Authority (CA) services as enumerated in Attachment A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of SERPRO-CA is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber 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, controls placed into operation can only provide reasonable assurance with respect to SERPRO-CA's Certification Authority operations.

SERPRO-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in SERPRO-CA management's opinion, in providing its Certification Authority (CA) services at Brasilia, Brazil, as of 16 March 2020, SERPRO-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL Certification Practice Statement, v1.2, February 2020
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL Certificate Policy, v1.2, February 2020
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL's Certification Practice Statement is consistent with its Certificate Policy
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL provides its services in accordance with its Certificate Policy and Certification Practice Statement
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by SERPRO-CA); and
- suitably designed, and placed into operation, 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 v2.2.

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

SERPRO-CA does not escrow its CA keys, does not provide subscriber key generation, storage and recovery services, does not provide subordinate CA certification, does not provide certificate suspension services, does not provide integrated circuit card management services, does not provide certificate suspension services, does not provide certificate rekey services and does not provide third-party subordinate CA or cross certificate issuance or management.

SERPRO
Assinado digitalmente por:
PEDRO MOACIR RIGO MOTTA
CPF:/CNPJ 26669897120
Assinado em: 20/03/2020
Sua autenticidade poderser confirmada no endereco :
<http://www.serpro.gov.br/assinador-digital>

Pedro Moacir Rigo Motta
Legal Representative of SERPRO Certification Authority
20 March 2020

ATTACHMENT A

LIST OF IN SCOPE CAs

OV SSL Issuing CA
AUTORIDADE CERTIFICADORA DO SERPRO SSL

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
AUTORIDADE CERTIFICADORA DO SERPRO SSL	1	CN = Autoridade Certificadora do SERPRO SSLv1 OU = Autoridade Certificadora Raiz Brasileira v10 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v10 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	00 95 48 78 A8 22 12 63 53	rsaEncryption	4096	sha512WithRSAEncrypt	March 12, 2020 19:31:42 GMT	July 1, 2032 13:00:59 GMT+1	AD 16 4F 4B F1 0C BE C2 8A A2 85 18 D7 0D 46 25 93 22 E3 CD	08 FC 94 2D 51 76 E5 68 AC BE F9 C5 95 F3 6A 20 DE 6A CF 9E A3 0C 6F 5F CE DD 48 21 6E D5 B0 70