PKI Consulting
Av. Borges de Medeiros, 2500/1402
Praia de Belas - Porto Alegre - RS 90110.150
Fone: (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 in generating and protecting the asymmetric key pairs for its AUTORIDADE CERTIFICADORA DO SERPRO SSL, during the period of 11 March 2020 to 12 March 2020 at Brasilia, Brazil, with the following identifying information (full identifying information enumerated in Attachment A):

CA Name	Subject Key Identifier	Certificate Serial Number
AUTORIDADE CERTIFICADORA DO SERPRO SSL	AD 16 4F 4B F1 0C BE C2 8A A2 85 18 D7 0D 46 25 93 22 E3 CD	00 95 48 78 A8 22 12 63 53

SERPRO-CA has:

- followed the CA key generation and protection requirements in its:
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL Certification Practice Statement, v1.2, February 2020; and
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL A1 Certificate Policy, v1.2, February 2020.
- included appropriate, detailed procedures and controls in its Key Generation Scripts:
  - Key Ceremony Preparation, 11 March 2020
  - Key Ceremony, 12 March 2020
  - Key Ceremony Finalisation, 12 March 2020
- maintained effective controls to provide reasonable assurance that SERPRO-CA were generated and protected in conformity with the procedures described in its CP/CPS and its Key Generation Scripts
- performed, during the key generation process, the procedures required by the Key Generation Scripts
- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

Certification authority's responsibilities

SERPRO-CA's management is responsible for its assertion, including the fairness of its presentation, and for generating and protecting its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

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

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 documented plan of procedures to be performed for the generation of the certification authority key pairs for the AUTORIDADE CERTIFICADORA DO SERPRO SSL CA;
2) reviewing the detailed CA key generation scripts for conformance with industry standard practices;
3) testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
4) physical observation of all procedures performed during the CA key generation process to ensure that the procedures actually performed during the period of 09 December 2019 to 18 December 2019 were in accordance with the Key Generation Scripts for the AUTORIDADE CERTIFICADORA DO SERPRO SSL; and
5) 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.

Opinion

In our opinion, in all material respects, based on SERPRO-CA management's assertion, SERPRO-CA has generated and protected the asymmetric key pairs for its AUTORIDADE CERTIFICADORA DO SERPRO SSL in accordance with CA Key Generation Criterion 4.1 of 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 CA Key Generation Criterion 4.1 of 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 13:03:15 -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-CA Management's Assertion

Serviço Federal de Processamento de Dados (SERPRO) – Certification Authority (SERPRO-CA) has deployed a public key infrastructure. As part of this deployment, it was necessary to create certificate authority known as AUTORIDADE CERTIFICADORA DO SERPRO SSL.

In order to allow the CA to be installed in a final and useable configuration, a Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of CA's private signing key. This helps assure the non-refutability of the integrity of the AUTORIDADE CERTIFICADORA DO SERPRO SSL's key pair, and in particular, the private signing key.

SERPRO-CA management has securely generated key pair, consisting of a public and private key, in support of its CA operations. The key pair were generated in accordance with procedures described in AUTORIDADE CERTIFICADORA DO SERPRO SSL's Certificate Policy/Certification Practice Statement (CP/CPS), and its Key Generation Scripts, which are in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

SERPRO-CA management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the key generation process.

SERPRO-CA management is responsible for establishing and maintaining procedures over its CA key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the AUTORIDADE CERTIFICADORA DO SERPRO SSL, and for the CA environmental controls relevant to the generation and protection of its CA keys.

SERPRO-CA management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the AUTORIDADE CERTIFICADORA DO SERPRO SSL during the period of 09 December 2019 to 18 December 2019 at Brasilia, Brazil, with the following identifying information:

CA Name	Subject Key Identifier	Certificate Serial Number
AUTORIDADE CERTIFICADORA DO SERPRO SSL	AD 16 4F 4B F1 0C BE C2 8A A2 85 18 D7 0D 46 25 93 22 E3 CD	00 95 48 78 A8 22 12 63 53

SERPRO-CA has:

- followed the CA key generation and protection requirements in its:
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL Certification Practice Statement, v1.2, February 2020; and
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL A1 Certificate Policy, v1.2, February 2020
- included appropriate, detailed procedures and controls in its Key Generation Scripts:
  - Key Ceremony Preparation, 11 March 2020
  - Key Ceremony, 12 March 2020
  - Key Ceremony Finalisation, 12 March 2020
- maintained effective controls to provide reasonable assurance that CA were generated and protected in conformity with the procedures described in its CP/CPS and its Key Generation Scripts
- performed, during the key generation process, the procedures required by the Key Generation Scripts
- generated the CA keys in a physically secured environment as described in its CP/CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.

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

Attachment A

CA Certificate for AUTORIDADE CERTIFICADORA DO SERPRO SSL

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 10756980373495898963 (0x954878a822126353)
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da
Informacao - ITI, CN=Autoridade Certificadora Raiz Brasileira v10
        Validity
            Not Before: Mar 12 19:31:42 2020 GMT
            Not After : Jul  1 12:00:59 2032 GMT
        Subject: C=BR, O=ICP-Brasil, OU=Autoridade Certificadora Raiz
Brasileira v10, CN=Autoridade Certificadora do SERPRO SSLv1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:eb:58:d0:54:15:f6:ec:65:73:c9:99:09:bb:2a:
                    c4:7b:3a:a3:04:67:4b:48:90:c5:47:21:9d:c3:16:
                    e6:f0:db:6b:d0:00:3c:6e:58:43:68:de:40:48:33:
                    a3:a8:31:12:30:0e:f1:17:7f:33:9d:f9:19:58:13:
                    0b:c4:9d:ce:6f:4d:bb:d5:6e:86:f5:ba:a0:4f:0a:
                    7f:b2:f8:59:b3:dd:54:71:b6:56:ea:c0:7b:83:2c:
                    73:31:31:96:2f:17:05:31:e0:6b:ba:b3:34:42:93:
                    15:b2:9f:21:0c:7e:52:ba:fe:6b:7c:fd:18:07:d6:
                    eb:cf:ad:24:d7:4e:2e:1c:6e:b6:e6:b0:1c:6d:12:
                    87:9f:b5:ec:58:9d:59:51:07:30:47:3c:75:83:42:
                    f5:36:55:0a:a6:c9:34:f9:e3:80:c5:37:15:49:54:
                    53:3b:7d:e4:fa:7e:86:bd:ef:37:e0:c5:cc:88:6e:
                    8e:ae:f7:9d:e2:2b:27:12:f4:27:97:80:1e:70:25:
                    ce:b9:4b:8c:de:f5:d9:fa:47:49:19:3a:4d:cb:51:
                    ce:cb:47:28:15:d2:82:25:24:82:c5:4f:f2:4d:b4:
                    e2:02:24:49:4d:cf:2b:6e:fa:2b:dc:8e:e4:ef:04:
                    78:64:34:7c:6a:50:db:5b:f4:9b:c3:52:44:32:d6:
                    d0:a8:c3:97:10:e5:7b:88:45:08:b9:bd:3f:b8:d4:
                    f6:83:4a:0c:e2:9b:bc:0c:0c:61:23:0c:b6:61:00:
                    a9:8d:f0:9b:cd:8b:b6:6d:fd:67:69:bb:8e:11:0d:
                    81:e2:61:6d:ff:38:28:c5:ae:45:2e:c3:3e:d0:88:
                    e9:0a:2f:2e:cf:d4:6a:2e:f6:05:a3:da:48:cb:90:
                    53:8b:b2:4c:91:57:db:82:a7:0e:bf:bb:e4:41:fd:
                    f1:17:bb:0e:0d:d2:27:09:54:48:6c:1d:11:eb:1a:
                    47:9b:e6:e9:8a:dc:7d:b7:98:a9:f9:27:f6:e1:01:
                    65:29:b8:f2:d2:0c:15:02:76:84:c9:ff:e2:40:5f:
                    ad:f2:a8:1c:14:13:ba:e6:4c:9f:1f:fd:af:b3:a8:
                    98:83:94:cd:84:52:ad:8e:9a:90:89:3c:88:ed:89:
                    11:91:f4:db:2c:57:5c:81:96:e2:45:45:2c:e5:31:
                    62:d0:19:12:e0:f0:16:ba:93:b5:1a:05:7d:b0:97:
                    64:f6:09:b7:67:e2:8d:64:38:28:02:7b:bb:0a:f8:
                    6a:d4:95:ed:ea:de:ea:3b:de:96:cc:1c:7d:ab:d8:
                    62:ed:3e:9e:95:dd:55:16:b5:79:61:ae:64:c4:cf:
                    4b:82:1f:97:70:10:f0:7e:70:cb:23:56:28:a3:36:
                    dd:31:b9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Certificate Policies:
                Policy: 2.16.76.1.1.137
                  CPS: https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf
                Policy: 2.16.76.1.2.1.105
                  CPS: https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf

            X509v3 CRL Distribution Points:

                Full Name:
```

```
                URI:http://acraiz.icpbrasil.gov.br/LCRacraizv10.crl

            X509v3 Authority Key Identifier:

keyid:74:F3:7E:FF:FC:9F:53:7A:F1:7C:EB:AB:3E:A4:A6:DA:18:BA:45:63

            X509v3 Subject Key Identifier:
                AD:16:4F:4B:F1:0C:BE:C2:8A:A2:85:18:D7:0D:46:25:93:22:E3:CD
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha512WithRSAEncryption
         83:bd:69:0e:61:a9:1a:94:01:c1:dd:97:22:7c:8f:72:2f:2b:
         93:b6:34:7c:79:85:e5:7c:37:ac:62:be:f3:30:55:65:99:db:
         95:82:10:a0:b9:e0:4c:67:19:a1:b7:d0:69:2e:af:7f:71:e0:
         56:bb:5a:bc:b0:a8:1e:e6:83:4d:cb:24:8f:98:12:45:7b:e0:
         8b:8e:d0:7b:67:52:e3:93:44:3f:ec:0e:7d:94:c0:83:65:a8:
         e8:8c:99:52:12:71:fa:a5:d8:71:03:52:43:e7:c1:34:74:6b:
         28:9b:74:ae:7e:e0:56:c5:d3:5f:82:cb:e9:40:d5:c3:a0:aa:
         78:f1:59:64:c8:be:03:28:50:9d:24:4c:6d:ce:e4:79:22:57:
         10:6c:1d:45:ae:60:79:9b:6c:e8:18:6e:a3:ed:47:68:7a:f9:
         a2:90:8b:f4:d6:56:be:f2:4c:a7:ec:21:79:68:db:9b:44:4d:
         1c:7f:0c:6e:96:29:39:2c:d3:35:b8:b2:30:7d:45:70:61:b6:
         d0:88:1f:33:6d:a2:d4:39:2d:a5:53:fa:58:af:eb:1e:2d:0e:
         d5:04:f1:e9:b3:f8:2e:18:1f:61:29:e8:bf:0d:fe:3d:29:68:
         c3:56:99:6e:df:e0:2e:66:10:47:aa:22:b9:df:75:49:7f:d5:
         30:bf:74:6f:c7:c1:42:a1:b4:f9:e0:e0:ab:01:57:e7:16:cf:
         05:ea:c3:37:74:f8:75:bb:b0:1b:5b:70:dd:a5:ea:38:a0:11:
         f9:90:10:34:7d:e2:ef:2e:4e:ef:98:e9:ce:ab:ae:28:3c:c3:
         28:8f:e8:3a:c7:40:74:bf:bb:46:a8:ea:cd:05:92:b8:f3:a3:
         1a:53:fb:9a:26:2f:a8:9b:1f:8b:7b:d1:1f:c8:8c:f7:f4:16:
         d1:60:67:55:26:f3:bf:f4:ff:2f:9f:95:e7:35:7b:26:ab:38:
         b0:d3:c1:0d:2e:31:dc:ae:ba:38:f2:d4:66:dd:85:f4:fc:15:
         20:a2:2b:63:31:4a:b2:ce:52:93:81:0f:14:3a:97:e2:5d:e2:
         73:aa:fc:6f:50:c3:bf:1e:06:4a:f5:a9:27:37:75:90:5d:65:
         f1:20:51:b4:d4:e1:ec:10:e4:dd:d8:d7:5d:a9:ba:ed:87:9a:
         a6:64:4f:b5:23:1c:04:1f:ec:ac:41:0c:e5:57:4a:67:3c:be:
         4a:d1:b4:6e:3c:2a:af:1f:82:6b:d0:29:b0:57:63:ea:0f:a7:
         64:8c:8f:d2:cb:be:d7:0e:44:cf:f1:a7:40:b9:88:c8:13:29:
         c1:a1:0d:1b:b6:a6:3f:d2:b2:4f:4f:77:73:b5:ea:56:03:04:
         47:84:a6:ef:3b:5c:98:90
```