



## PKI Consulting

Av. Borges de Medeiros, 2500/1402

Praia de Belas - Porto Alegre - RS 90110.150

Fone: +55 51 3398 5740

[www.pkiconsulting.com](http://www.pkiconsulting.com)

## INDEPENDENT ASSURANCE REPORT

To the Management of Serviço Federal de Processamento de Dados (SERPRO) – Certification Authority (“AUTORIDADE CERTIFICADORA SERPRO” or “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, throughout the period of May, 30 2020 to May, 29 2021 for its CAs as enumerated in [Attachment A](#), SERPRO-CA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - [AUTORIDADE CERTIFICADORA DO SERPRO SSL Certification Practice Statement, v 4.0 November 2020](#); and
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL A1 Certificate Policy, v3.0, November 2020

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the SERPRO-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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by SERPRO-CA)
- 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
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities SSL Baseline with Network Security v2.5](#).

### Certification authority’s responsibilities

SERPRO’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 SSL Baseline with Network Security v2.5](#).

### 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



## **PKI Consulting**

Av. Borges de Medeiros, 2500/1402

Praia de Belas - Porto Alegre - RS 90110.150

Fone: +55 51 3398 5740

[www.pkiconsulting.com](http://www.pkiconsulting.com)

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 SSL certificate lifecycle management business practices including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of SERPRO-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (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 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 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 effectiveness of 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.



## PKI Consulting

Av. Borges de Medeiros, 2500/1402

Praia de Belas - Porto Alegre - RS 90110.150

Fone: +55 51 3398 5740

[www.pkiconsulting.com](http://www.pkiconsulting.com)

### Emphasis of Matter

During the audit, it was detected that all 526 certificates issued since the beginning of the CA SERPRO SSL operation contained an error in the Subject Alternative Name field, which included different information than expected for this type of certificate.

AC SERPRO confirmed this finding and reported that on June 1, 2021, it was alerted by the CAB/Forum, after running a "lint" test, about the following errors in its certificates: 18 Organization Name Too Long (MUST be less than 65 characters); 526 Invalid SAN entries (MUST be FQDN or IP address); 1 IP address in DNS name; 10 DNSName was not an FQDN.

AC SERPRO determined that the root cause for this error was a certificate profile misconfiguration and immediately changed the system configuration and started the certificate revocation process, with subsequent re-issuance, a process that is in progress. Additionally, it implemented a verification using the "lint" test (CA CHECKER) to keep issuances in compliance with BR SSL requirements.

### Opinion

In our opinion, throughout the period May, 30 2020 to May, 29 2021 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 SSL Baseline with Network Security v2.5](#).

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 SSL Baseline with Network Security v2.5](#) nor the suitability of any of SERPRO-CA's services for any customer's intended purpose.

A handwritten signature in black ink, appearing to read 'João Ivonir Moreira'.

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

August, 25 2021

## SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO) – MANAGEMENT’S ASSERTION

Serviço Federal de Processamento de Dados (SERPRO) – Certification Authority (“AUTORIDADE CERTIFICADORA DO SERPRO SSL” or “SERPRO-CA”) operates the Certification Authority (CA) services as enumerated in [Attachment A](#) and provides SSL CA services.

SERPRO-CA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, In SERPRO CA management’s opinion, except for the matters described in the emphasis-of-matter paragraph below, in providing its SSL Certification Authority (CA) services at Brasilia, Brazil, throughout the period of May, 30 2020 to May, 29 2021, SERPRO-CA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - [AUTORIDADE CERTIFICADORA DO SERPRO SSL Certification Practice Statement, v 4.0 November 2020](#); and
  - AUTORIDADE CERTIFICADORA DO SERPRO SSL A1 Certificate Policy, v3.0, November 2020

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the SERPRO-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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by SERPRO-CA)
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

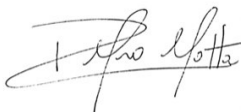
in accordance with the [WebTrust Principles and Criteria for Certification Authorities SSL Baseline with Network Security v2.5](#).

### Emphasis of Matter

During the audit, it was detected that all 526 certificates issued since the beginning of the CA SERPRO SSL operation contained an error in the Subject Alternative Name field, which included different information than expected for this type of certificate.

AC SERPRO confirmed this finding and reported that on June 1, 2021, it was alerted by the CAB/Forum, after running a "lint" test, about the following errors in its certificates: 18 Organization Name Too Long (MUST be less than 65 characters); 526 Invalid SAN entries (MUST be FQDN or IP address); 1 IP address in DNS name; 10 DNSName was not an FQDN.

AC SERPRO determined that the root cause for this error was a certificate profile misconfiguration and immediately changed the system configuration and started the certificate revocation process, with subsequent re-issuance, a process that is in progress. Additionally, it implemented a verification using the "lint" test (CA CHECKER) to keep issuances in compliance with BR SSL requirements.



Pedro Moacir Rigo Motta  
Legal Representative of SERPRO Certification Authority  
August, 25 2021

## ATTACHMENT A - LIST OF IN SCOPE CAs

<b>OV SSL Issuing CA</b>
AUTORIDADE CERTIFICADORA DO SERPRO SSL

## CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial	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	08FC942D5176E568ACBEF9C595F36A20DE6ACF9EA30C6F5FCEDD48216ED5B070