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) – Certificate Authority:

Scope

We have been engaged, in a reasonable assurance engagement, to report on Serviço Federal de Processamento de Dados (SERPRO) management's assertion, that for its Certification Authority (CA) services in Brazil for SERPRO-CA and the subordinated CAs presented in the Appendix A, during the period May 30, 2022 through May 29, 2023, SERPRO-CA has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its:
  - Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
  - SERPRO-CA's Certification Practice Statement is consistent with its Certificate Policy
  - SERPRO-CA provides its services in accordance with its Certificate Policy and 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;
  - The integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - The Subscriber information is properly authenticated (for the registration activities performed by SERPRO-CA); and
  - 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.

in accordance with the WebTrust Principles and Criteria for Certification Authorities -Version 2.2.2

SERPRO-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in SERPRO-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

SERPRO-CA does not escrow its CA keys and does not provide the following services: subscriber key generation and management, certificate rekey, certificate suspension, certificate validation. 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 -Version 2.2.2

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 behavior.

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 life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and 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.

SERPRO-CA's makes use of external registration authorities for specific subscriber registration activities as disclosed in SERPRO-CA'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 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.

Opinion

In our opinion, through the period May 30, 2022 through May 29, 2023, 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 -Version 2.2.2

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 - Version 2.2.2 criteria nor the suitability of any of SERPRO-CA's services for any customer's intended purpose.

Use of the WebTrust seal

SERPRO-CA'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.

Porto Alegre, RS, Brazil, October 02, 2023

JOAO IVONIR MOREIRA:18835759072

Assinado de forma digital por JOAO IVONIR MOREIRA:18835759072
Dados: 2023.10.16 14:14:31 -03'00'

João Ivonir Moreira
CRC/RS-025692/O-4
PKI Contabilidade e Auditoria Ltda.
CNPJ 18.885.468/0001-76 – CRC/RS-007849/

Serviço Federal de Processamento de Dados (SERPRO) – Certificate Authority (SERPRO-CA) operates Certification Authority (CA) services for AC SERPRO and the subordinated CAs presented in the Appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing (using CRL repository)
- Subordinate CA certification

SERPRO-CA does not escrow its CA keys and does not provide the following services: subscriber key generation and management, certificate rekey, certificate suspension, certificate validation.

The management of SERPRO-CA 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, 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, even effective controls can only provide reasonable assurance with respect to SERPRO-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

SERPRO-CA management has assessed its disclosures of its certificate practices and controls over its CA services.

Based on the assessment, SERPRO-CA's management opinion, in providing its Certification Authority (CA) services in Brazil, through the period May 30, 2022 through May 29, 2023, SERPRO-CA has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its:
  - Certification Practice Statement
  - Certificate Policy
- maintained effective controls to provide reasonable assurance that:
  - SERPRO-CA's Certification Practice Statement is consistent with its Certificate Policy
  - SERPRO-CA provides its services in accordance with its Certificate Policy and 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;
  - The integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - The Subscriber information is properly authenticated (for the registration activities performed by SERPRO-CA); and
  - 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.

in accordance with WebTrust Principles and Criteria for Certification Authorities -Version 2.2.2 including the following:

CA Business Practices Disclosure

- Certification Practice Statement
- Certificate Policy Management

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
- 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

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing (using CRL repository)

Brasília, DF, Brazil, October 02, 2023

NEOSIGNER Assinatura ICP-Brasil
PEDRO MOACIR RIGO MOTTA
CPF: 266.698.971-20
16/10/2023
SERPRO

Pedro Moacir Rigo Motta
Legal Representative

Serviço Federal de Processamento de Dados (SERPRO) – Certificate Authority

APPENDIX A

LIST OF IN SCOPE CAs

Root CA
AC SERPRO
AC JUS
AC RFB
AC MRE
AC INMETRO
Secure Email (S/MIME) CAs
AC PR
AC SERPRO ACF
AC SERPRO ACF SSL
AC SEFAZ CE
AC SERPRO RFB
AC SERPRO JUS
AC INFOCOMEX
AC INVIA
AC NACIONAL
AC PROCERTI
AC SAFE-ID BRASIL
AC SDI
AC PRIMECERT
AC ALTERNATIVE
AC BRASIL CERTEC
AC PROCERTI
Timestamp CAs
AC SERPRO ACF TS
OV SSL Issuing CAs
AUTORIDADE CERTIFICADORA DO SERPRO SSL

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial	SHA256 Fingerprint
AC SERPRO	1	CN = Autoridade Certificadora SERPRO v3 OU = Autoridade Certificadora Raiz Brasileira v2 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	07	35E191B6DCB8A855462B5556A8D4A9ADEF0321595DB77D6B54FF568EB42AD41A
	2	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v5 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	05	35330581E9224B72CB340FA44B8F57DA79AC0A3C95160CBD4519ECC11BAB5C12
AC SERPRO ACF	1	CN = Autoridade Certificadora SERPRO Final v4 OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v3 OU = Autoridade Certificadora Raiz Brasileira v2 O = ICP-Brasil C = BR	04	A890C4EE24B12559794B1C29FABF5B3094A6EAFEA58A965D446BAFF5CC242FF4
	2	CN = Autoridade Certificadora SERPRO Final v5 OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	03	D4E68BDB73C00FF9160A8DBEC971F640A7A0F71145100A6C6C94B187577AE575F
AC SERPRO RFB	1	CN = Autoridade Certificadora SERPRORFB v4	CN = AC Secretaria da Receita Federal do Brasil v3	11	83B664811462D27C1A4EEDB7155A8277805C80E34FDCD999D3D8D61CAFF84203

CA #	Cert #	Subject	Issuer	Serial	SHA256 Fingerprint
		OU = Secretaria da Receita Federal - RFB O = ICP-Brasil C = BR	OU = Autoridade Certificadora Raiz Brasileira v2 O = ICP-Brasil C = BR		
	2	CN = Autoridade Certificadora SERPRORFB v5 OU = Secretaria da Receita Federal - RFB O = ICP-Brasil C = BR	CN = AC Secretaria da Receita Federal do Brasil v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	0B	B1E93A025411FED62316E99953D61446F1BC3C205F7D8A746C4D8149C24959AB
AC SERPRO JUS	1	CN = AC SERPRO-JUS v5 OU = Autoridade Certificadora da Justica v5 O = ICP-Brasil C = BR	CN = Autoridade Certificadora da Justica v5 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	06	A9C0A24D692735DFDD4C1C6D8E1CACCAB301933889A9888AF283F9F0C651D0AD
AC SERPRO FINAL SSL	1	CN = Autoridade Certificadora do SERPRO Final SSL OU = CSPB-1 O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	02	A662265119E95E01B257A5AEFAC4B8E1C09725D8E59081B7785522F33B1A150F
AC SERPRO ACF TS	1	CN = Autoridade Certificadora do SERPROACF TIMESTAMPING OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	04	F14BBAAC4D43B18DA09205DE151AF69F9D86088F85CE54F50C65C2546C5D5E70
AC SEFAZ CE	1	CN = Autoridade Certificadora SEFAZCE	CN = Autoridade Certificadora SERPRO v4	06	2BC067A88EAE745D722E4329D6E3FBA6BED3D14DD07EEC22F9A057A334B48F71

CA #	Cert #	Subject	Issuer	Serial	SHA256 Fingerprint
		OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR		
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
AC JUS	1	CN = Autoridade Certificadora da Justica v4 OU = Autoridade Certificadora Raiz Brasileira v2 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	09	6748E76D430BE8499FB00F414F2C6CE9D93276C5D47D9CC334DEE884100AD21E
	2	CN = Autoridade Certificadora da Justica v5 OU = Autoridade Certificadora Raiz Brasileira v O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v5 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	07	A517E77E9F362C6AF120CF64F130D026D8064A595EDE6C0CAA3DC08559B85F56
AC RFB	1	CN = AC Secretaria da Receita Federal do Brasil v3 OU = Autoridade Certificadora Raiz Brasileira v2 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	08	B123A861174F40C01E50D039652E64F9E34DF9F762F36891987E2AB371627EF9
	2	CN = AC Secretaria da Receita Federal do Brasil v4	CN = Autoridade Certificadora Raiz Brasileira v5	04	2C7A8AD75458F7E2FE8D7F7884A585127E4F242BD5C3EBEA499DACB630315E21

CA #	Cert #	Subject	Issuer	Serial	SHA256 Fingerprint
		OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR		
AC PR	1	CN = Autoridade Certificadora da Presidencia da Republica v3 OU = Autoridade Certificadora Raiz Brasileira v2 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	0A	70DBEBC77A5295C7E34009025F1B740211DDCC9E1A0C0FFA3489557CDE412463
	2	CN = Autoridade Certificadora da Presidencia da Republica v4 OU = Autoridade Certificadora Raiz Brasileira v2 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v2 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	11	FC4F9981DA6873E9BE67FA344FE00D03DEC8BF9C4E83D9DD2712A0F874D6B9B4
	3	CN = Autoridade Certificadora da Presidencia da Republica v5 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v5 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	0A	98C4101A3208B59712655B250B520BC2B5ECFB5C964F42A473D4C3821F92C5A9
AC MRE	1	CN = Autoridade Certificadora Ministerio das Relacoes Exteriores OU = Autoridade Certificadora Raiz Brasileira v4 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v4 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	02	C5C2C9B61303B521EAFB936CE67C78077BB8B686543E96B344901850CAB6F8B5

CA #	Cert #	Subject	Issuer	Serial	SHA256 Fingerprint
AC SDI	1	CN = Autoridade Certificadora SDI OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	10	8923C77BA2866BB17480FB2A035B683217ABFF27B7F455141535DBAE54073301
AC SAFEID	1	CN = Autoridade Certificadora SAFE-ID BRASIL OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	9	F7641DF15120AD6895F93430D5D7A2272DCB500239D5E623FEC4C2692215F34F
AC PROCERTI	1	CN = Autoridade Certificadora PROCERTI OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	7	E78BA5C40FDF78415E08E8BA759B5CACB0D0FAEEB18E7B09F9B8DF528A4C73E5
AC NACIONAL	1	CN = Autoridade Certificadora NNACIONAL OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	14	34AFD324C54C54A2E94FDACB22B52BF4430FE00411BF1871ED81A692ADA4B773
AC INVIA	1	CN = Autoridade Certificadora NACIONAL OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	13	7143F26C9BC783DF57F41E066D0A6B80511666CC8399E4ED76DC2D2A9522F2A8

CA #	Cert #	Subject	Issuer	Serial	SHA256 Fingerprint
AC INFOCOMEX	1	CN = Autoridade Certificadora INFOCOMEX OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	8	9699D2C03365C8A1CDC0C3B420B16755F2A7CFD581CA7767F751C9F3774D3BEA
AC PRIMECERT	1	CN = Autoridade Certificadora PRIMECERT OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	11	FE7AE1EEF13E8ECF01F2838AFD1925D1C8470A10594AE7F2D352A24F548AD7A6
AC INMETRO	1	CN = Instituto Nacional de Metrologia Qualidade e Tecnologia INMETRO OU = Autoridade Certificadora Raiz Brasileira v6 O = ICP-Brasil C = BR	CN = Autoridade Certificadora Raiz Brasileira v6 OU = Instituto Nacional de Tecnologia da Informacao - ITI O = ICP-Brasil C = BR	0xb7af2f22a71d1254	7541edb55a5c76b0fe83aa6a94ee3b2b4b8a9cef (OID 1.3.101.113: id-Ed448: Curve448)
AC ALTERNATIVE	1	CN = Autoridade Certificadora ALTERNATIVE OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	12	88219FCBC3939AA0A9B3F98E67EB32936ECA0F0C0D0D91FBCE8A048C3FB76E16
AC BRASIL CERTEC	1	CN = Autoridade Certificadora BRASIL CERTEC OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	008070E29932877EF2	8340083C2E39E6DC1DB7AEC1729C3568D2126A1786F0C1C553A893AF704B3F4F

CA #	Cert #	Subject	Issuer	Serial	SHA256 Fingerprint
AC PROCERTI	1	CN = Autoridade Certificadora PROCERTI OU = Servico Federal de Processamento de Dados - SERPRO O = ICP-Brasil C = BR	CN = Autoridade Certificadora SERPRO v4 OU = Autoridade Certificadora Raiz Brasileira v5 O = ICP-Brasil C = BR	7	E78BA5C40FDF78415E08E8BA759B5CACB0D0FAEEB18E7B09F9B8DF528A4C73E5