# INDEPENDENT AUDIT REPORT
By
Auditor: Alexander J. Osorio D.
CISA ID 1299663

Osorio Delgado y Asociados S.C.
Contadores - Administradores - Ingenieros - Abogados

This is an official document to declare the following facts upon request by The PROVEEDOR DE CERTIFICADOS (PROCERT), C.A.

The American National Standards Institute (ANSI), a private, non-profit organization, accredits other organizations to serve as third-party product, system and personnel. ANSI is signatories to the multilateral agreement (MLA) of International Accreditation Forum (IAF) under ISO/IEC 17065 since Oct, 20, 2008; ANSI has accredited the Information System Audit and Control Association (ISACA), CISA certification program, accreditation ID 0694, under ISO/IEC 17024:2012, General Requirements for Bodies Operating Certification of Persons. ISACA has accredited the Auditor like Certified Information System Auditor (CISA), ID 1299663; thereby, Auditor could be recognized like qualified and independent personnel to carrying out its activities conforming auditor ESI guidelines.

## 1) LEGAL ENVIRONMENT OF AUDITED:

The Proveedor de Certificados (PROCERT), C.A., located at Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, Oficina B-132, Municipio Chacao, Caracas, República Bolivariana de Venezuela, is a private company, authorized by laws and identified with National number RIF J-31635373-7.

PROCERT operates Certification Authority (CA) services known as "PSCProcert" under root certification authority of the Venezuelan State. The operations of electronic certification provide the following services certification Authority for end entities:

- Registration Authority (RA)
- Issue of Certificate
- Distribution of certificate
- Renewal of certificate with rekey
- Revocation and Suspension of certificate,
- Processing certificate revocation list (CRL)
- Checking online certificate status (OCSP)

PROCERT is responsible for establishing and maintaining effective controls over its CA operations, including disclosure of CA business practices, service integrity (including controls in managing the life cycle of the key and certificate), CA environmental controls and network and certificate system security. These controls contain monitoring mechanisms and take actions to correct identified deficiencies.

PROCERT is a trusted third-party entity that certifies the identities of end entities and servers affiliated with it.

PROCERT have requested an audit under the scope, limitations and risks are given below:

SCOPE: "Review of procedures, manuals, systems and control standards implemented support the operation as Certification Authority, according to international standards, legal and sub-legal regulations in force in the Bolivarian Republic of Venezuela and Best Practices, focusing on Electronic Signatures and Infrastructures Policy requirements for Certification Authorities (ETSI TS 101 456 v1.4.3) and Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (ETSI TS 102 042 v2.4.1)".

LIMITATIONS: "Facilities that frame the technical and administrative operations of the Certification Authority; Backup storage center, Alternate Data Center, hardware, software and firmware, Systems and Applications, and Information Security Management System (ISMS) that apply to CA".

AUDIT RISK: Because of inherent limitations in controls, errors or fraud may occur and not be detected, furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions. The relative effectiveness and significance of specific controls in PROCERT and their effect on assessments of control risk for CSP and relying parties depend on their interaction with the controls and other factors present in the locations.

DURATION: The execution time of the audit was 35 working days in the period from 15 June 2017 to 31 July 2017, detailed specification of time spent as follow:

| **Start date of the audit: 2017.06.15** | | **End of the audit: 2017.07.31** |
|---|---|---|
| Documentation evaluation (Stage 1) | 2017.06.15 - 06.30 | 12 days |
| Risk analysis evaluation (Stage 1) | 2017.07.03 - 07.07 | 5 days |
| On-site audit (Stage 2) | 2017.07.10 - 07.21 | 12 days |
| Audit report preparation | 2017.07.24 - 07.31 | 6 days |

AUDIT METHODOLOGY: The conformity assessment performed the audit team auditing method was systematic, independent, documented process facts on records, claims or other important information acquisition and their objective evaluation in order to determine to what extent the requirements are met. The objective evidence collected by the audit team with the following techniques: documentation evaluation, visual inspection, interviewing and technical review;

- Documentation evaluation: Policies from the organization, certificate policies and evaluation of regulatory documents.
- Visual inspection: During the on-site audit on the basis of administrative security measures and physical security protection measures in existence and application of visual assessment of audit along the route.
- Interviewing: Observation persons involved in the certificate policies and the Process they have done, evaluation in targeted areas of assessment issues related to information security.

- **Technical review:** The logical security provisions, technical configuration regulations evaluation of the IT system.

2) DOCUMENTS EVALUATED:

1. Certification Practice Statement and Certificate Policy (CPS and CP)
2. Certificate Policy for Electronic Signature for Employee of Private Enterprise. (PC-1)
3. Electronic Signature Certificate Policy for Representatives of Public Companies (PC-2)
4. Certificate Policy for Private Business Representatives (PC-3)
5. Electronic Signature Certificate Policy for Natural Person (PC-4)
6. Certificate Policy for Electronic Signatures for Certified Professionals (PC-5)
7. Secure Server Certificate (SSL) Policy (PC-6)
8. Electronic Certificate Policy for Logic Access Control (PC-7)
9. Electronic Signature Certificate Policy for Public Officials (PC-8)
10. Electronic Transaction Certificate Policy (PC-9)
11. Electronic Certificate of Electronic Invoice Policy (PC-10)
12. Electronic Banking Electronic Certificate Policy (PC-11)
13. Software Signature Electronic Certificate Policy (PC-12)
14. Electronic Certificate Policy for Virtual Private Networks (VPN) (PC-13)
15. Electronic Certificate Policy for Electronic Mail (PC-14)
16. Electronic AC certificate PSCProcert (SHA256)
17. CA CRL (SHA384)
18. Information Security Policies, Risk Assessments, Business Continuity Plan, Incident management, Terms and conditions, Contractual with third parties, Insurances , Internal audit plan, Network Diagrams, Organization Manuals, Personnel Policies, Service Level Agreements, Evidences for secure and conformant operations.

3) AUDIT CRITERIA AND CONDITIONS:

Our audit was conducted in accordance with standards established by the European Telecommunications Standards Institute (ETSI) for the assessment of conformity (ETSI TS 119 403 v2.1.1) and auditors ESI guidelines and CSPs on ETSI TS 102 042 (TR 103 123 v1.1.1), and these standards require that we plan and perform the audit to obtain reasonable assurance that the statement of management is not materially mistake and is based on standards whose requirements and specifications are publicly available. Our audit included (1) obtaining an understanding about PROCERT's keys and certificates lifecycle management business and information privacy practices of and their controls over the integrity of the key and the certificate, over of authenticity and privacy of information of applicant CSP certificate, SC and relying party, over the continuity of key and certificate lifecycle management operations, over development, maintenance and operation of systems integrity, and over the network and Certificate system security requirements; (2) selective testing transactions executed in accordance with disclosed key and certificate lifecycle practices of service (business) and information privacy practices; (3) testing and evaluating the operating effectiveness of controls; and (4) perform other procedures as we considered necessary in the circumstances.

PROCERT has been audited by us according to the standards and technical specifications based on the requirements of "Electronic Signatures and Infrastructures Policy requirements for Certification Authorities (ETSI TS 101 456 v1.4.3)" and "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (ETSI TS 102 042 v2.4.1)", the set of requirements has been expanded based on "Network and Certificate System Security Requirements, v1.0", according the recommendations and requirements of the CA/Browser Forum's specifications, in particular "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates v1.4.5" adopted on April 14, 2017.

The applicable ETSI certification policies requirements are defined in the technical specification **ETSI TS 102 042 V2.4.1 (2013-02)**:

| | |
|---|---|
| LCP | Lightweight Certificates Policy |
| NCP | Normalized Certificates Policy |
| NCP+ | Extended Normalized Certificates Policy |
| DVCP | Domain Validation Certificates Policy |
| IVCP | Individual Validation Certificates Policy |
| OVCP | Organizational Validation Certificates Policy |
| EVCP | Extended Validation Certificates Policy |
| CSCP | CodeSign Certificates Policy |

Additional applicable ETSI certification policies requirements are defined in the technical specification ETSI TS 101 456 v1.4.3 **(2007-05)**:

| | |
|---|---|
| QCP public | Qualified Certificates Policy – for public purpose |
| QCP public+SSCD | Qualified Certificates Policy – QCP for use only with secure-signature-creation devices |

AUDITED CERTIFICATE:

Audited for policy LCP, NCP, NCP+, DVCP, IVCP, OVCP, EVCP, CSCP, QCP public and QCP public+SSCD,
CN: PSCProcert
OU: Proveedor de Certificados PROCERT
Certificate Serial Number: 0B
CA Fingerprint (SHA-256): 3C:FC:3C:14:D1:F6:84:FF:17:E3:8C:43:CA:44:0C:00:B9:67:EC:
93:3E:8B:FE:06:4C:A1:D7:2C:90:F2:AD:B0

The results of the tests and procedures allowed us to evaluate and verify that:

1. The CA has a Certification Practice Statement disclosed and procedures.
2. The CA guarantees that the CA keys are generated in controlled circumstances.
3. The CA ensures that CA private keys remain confidential and maintain their integrity.
4. The CA guarantees that the CA keys are generated in controlled circumstances
5. The CA ensures the integrity and authenticity of the signature verification key (public) of the CA and associated parameters are maintained during its distribution to relying parties.
6. The CA ensures that private signing keys of CA are not used inappropriately.
7. The CA ensures that private signature key of the CA are not used beyond the end of their life cycle.

8. The CA guarantees the security of cryptographic device throughout its lifecycle.
9. The CA does not generate or store the keys of the signatories (CSP and SC).
10. The CA guarantees that if stored certificates are issued in secure user devices this is carried out safely.
11. The device safe storage of users meets at least the requirements of FIPS 140-2 standard in their security and implementation of cryptographic algorithms standards.
12. The CA ensures that the identification evidence and accuracy of names and associated data signatories (CSP and SC) are duly examined as part of the registration service (RA) based on reliable official sources.
13. The CA ensures that administrative and management methods applied are appropriate and correspond to recognized standards. The CA provides security of objects and information are given adequate protection. The CA provides security for employees and increase recruitment procedures and supports the reliability of the CA.
14. The CA gives assurance that his organization is reliable and that its signatories (CP and SC) legally and physically exist.

## 4) SUMMARY OF REQUIREMENTS FOR AUDIT

ETSI TS 101 456 v1.4.3 and ETSI TS 102 042 v2.4.1 specifications contains the following requirements:

### 1 Certification Practice Statement (CPS)

The CA has a presentation and disclose of its practices and policies.

### 2 Public Key Infrastructure – key management life cycle

The CA ensures that CA keys are created under controlled conditions. The CA ensures that private CA keys are treated confidentially and that their integrity is maintained. The CA ensures that the integrity and authenticity of the (published) CA public keys together with all associated parameters are preserved. The CA does not generate nor store private signature keys of the certification owner (subject).

### 3 Public key infrastructure – certificate management life cycle

The CA ensures that the identification confirmation of a participant (CSP) and of a certificate owner (subject) as well as the correctness of their names and their related data are either checked as part of the defined service or proved by attestations from appropriate and licensed sources. It also ensures that applications for a certificate take place in a correct and authorized way, completely according to the collected proofs respectively attestations. The CA ensures that the certificates are handed out in a secure way so that their authenticity is maintained. The CA ensures that the legal terms and conditions are made available to the participants (subscriber) and to the relying parties. The CA ensures that certificates are made available to the participants (subscriber), certificate owners (subject) and relying parties to the extent necessary. The CA ensures that certificates are blocked at short notice using authorized and verified blocking queries.

## 4 CA Management and Operation

The CA ensures that the applied administrative and management methods are appropriate and correspond to acknowledged standards. The CA ensures that the objects and information worthy of protection receive an appropriate protection. The CA ensures that the employees and the hiring procedures amplify and support the CA company's trustability. The CA ensures that physical access to critical services is controlled and that the physical risks for the objects worthy of protection are minimized. The CA ensures that the CA systems are operated safely, according to specification. The CA ensures that the access to the CA systems is restricted to appropriate, authorized persons. The CA is to use trustworthy systems and products that are protected against modifications. The CA ensures that in case of a catastrophe the operation is restored as soon as possible. The CA ensures that in case of a cessation of the CA operation the potential interference of users (subscriber) and relying parties is minimized and that the continued maintenance of records that are required as proof of certification in legal proceedings is given. The CA ensures that statutory requirements are met. The CA ensures that all relevant information of a certificate is recorded for a reasonable period of time, especially for the purpose of proof of certification in legal proceedings.

## 5 Organization

The CA ensures that its organization is reliable.

## 6 Additional requirements

The CA allows third parties to check and test their certificates. The CA does not make use of Cross Certificates that identify the CA as the Subject.

The CA/Browser Forum Network and Certificate System Security Requirements, v. 1.0 contains the following requirements:

1 the CA ensure general protections for the network and supporting systems.

2 the CA shall implements trusted roles, delegated third parties, and system accounts.

3 the CA shall implement a security support system under the control of CA or delegated third party trusted roles to logging, monitoring, & alerting

4. The CA shall implement detection and prevention controls under the control of CA or delegated third party trusted roles to protect certificate systems against viruses and malicious software, document and follow a vulnerability correction process, perform a vulnerability scan and penetration test on the CA's and each delegated third party's certificate systems.

The auditor evaluated the risk assessments performed by PROCERT, and found to be appropriate. During the on-site audit, the auditor reviewed the internal and external factors, interested parties, then started from the information received and on-site experienced evaluated the results of the organisation's risk assessment. The risk improvement plan approved by the leadership, resources allocated to the measures. During the audit it was found that PROCERT, adequately handle the risks identified in relation to the potential. The document used in risk management rating is the Risk Assessment Guide owns by PROCERT. PROCERT shall identify and evaluate the risks as follows in annual:

- Identify the foreseen internal and external threats, which may allow the certificate data or certificate management processes unauthorized access, disclosure, alteration, destruction or other abuse.
- It discovers these threats and the expected probability of occurrence in the event of damage.
- Evaluate the processes used to eliminate the identified threats, security measures and systems are appropriate.

5) THE OUTCOMES OF THE AUDITING:

In our opinion, the PSCProcert" operated by “Proveedor de Certificados PROCERT” has been found PASSED in all material respects, for the period from June 15, 2017 to July 31, 2017 the CA and has been deemed FULLY COMPLIANT with the requirements established in "Electronic Signatures and Infrastructures Policy requirements for Certification Authorities (ETSI TS 101 456 v1.4.3)" and "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (ETSI TS 102 042 v2.4.1.

6) NEXT AUDIT:

The next assessment has to be successfully finalized before July 2018 under ETSI 319 411 in order to obtain/maintain the root program certificate validity.

This report does not include any representation as to the quality of PROCERT 's services beyond those covered by the "Electronic Signatures and Infrastructures Policy requirements for Certification Authorities (ETSI TS 101 456 v1.4.3)" and "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (ETSI TS 102 042 v2.4.1)", nor the suitability of any of the PROCERT 's services for any purpose intended by the customer.

Firmado digitalmente por Alexander
Osorio Delgado
Nombre de reconocimiento (DN): c=VE,
st=Caracas, l=AVENIDA URDANETA ESQ.
JESUITAS TORRE BANDAGRO PISO 7
OFNA 71 MUNICIPIO LIBERTADOR,
o=Administracion, ou=006, ou=8872421,
ou=Auditor, cn=Alexander Osorio
Delgado, email=aosoriod@gmail.com
Fecha: 2017.08.29 02:38:22 -04'30'

Alexander J. Osorio, CISA (1299663)
CI V-8872421 Telephone: 58412 3328072 – 58212 5374258 - 58212 8613604
email: alexander.osorio@inacomp.com.ve / aosoriod@gmail.com / aosorio@oda.com.ve
Auditor – Chartered Public Accountant (CPA) - Computer Engineer - Business Administration
MSc Financial Systems and Data Security Audit Specialist
Comptroller National Audit Bureau (CGRBV), Registered Auditor
Caracas, Venezuela July 31, 2017
Website: www.oda.com.ve

# Certificate of Accreditation

## Personnel Certification

The **American National Standards Institute** hereby affirms that

## Information Systems Audit and Control Association

3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, United States

**ACCREDITATION ID# 0694**

meets the ANSI accreditation program requirements and those set forth in

ISO/IEC 17024:2012: Conformity assessment- General requirements for bodies operating certification of persons

for programs within the following

**SCOPE OF ACCREDITATION**

GRANTED 2013-12-04: Certified In Risk and Information Systems Control (CRISC)
GRANTED 2011-06-23: Certified in the Governance of Enterprise IT (CGEIT)
GRANTED 2005-09-08: Certified Information Security Manager (CISM)
GRANTED 2005-09-08: Certified Information Systems Auditor (CISA)

Lane Hallenbeck

ANSI VICE PRESIDENT, ACCREDITATION SERVICES

2020-09-08
VALID THROUGH

ANSI
ACCREDITED

Certificate ID: TEEAJECD

CISA® Certified Information Systems Auditor®
An ISACA® Certification

ISACA SINCE 1969

# CERTIFIED INFORMATION SYSTEMS AUDITOR®

ISACA hereby certifies that

## Alexander J. Osorio

has successfully met all requirements and is qualified as a Certified Information Systems Auditor; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

02 May 2012
Date of Certification

31 January 2019
Expiration Date

1299663
Certificate Number

International President of ISACA and ITGI

Chief Executive Officer of ISACA and ITGI

ANSI
ANSI Accredited Program
PERSONNEL CERTIFICATION
#0694

ISACA®
*Trust in, and value from, information systems*