Valencia, December 20th, 2017

Independent Qualified Audit Report

To the Management of Firmaprofesional SA:

We have been engaged to report on Firmaprofesional SA management's assertion management, (hereinafter, Firmaprofesional) that for its Certification Authority (CA) operations at Sant Cugat, SPAIN, throughout the period 10th of March 2017 to the 20th of June of 2017 for its Root Certification Authority *Autoridad de Certificacion Firmaprofesional CIF A62634068* and the Delegated Certification Authority *AC Firmaprofesional – INFRAESTRUCTURA*, Firmaprofesional has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - CPS. Declaración de Prácticas de Certificación Version 160229
  - PC. CP Servidor Web. Version 6.3
  - PC. CP Sede Electrónica Version 160229

- maintained effective controls to provide reasonable assurance that:
  - Firmaprofesional's Certification Practice Statement is consistent with its Certificate Policies
  - Firmaprofesional provides its services in accordance with its Certificate Policies 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 lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by Firmaprofesional); 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 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

in accordance with WebTrust Principles and Criteria for Certification Authorities v2.0.

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

Certification authority's responsibilities

Firmaprofesional 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 v2.0.

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:

- obtaining an understanding of Firmaprofesional'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;
- selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- testing and evaluating the operating effectiveness of the controls; and
- performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Firmaprofesioanl and their effect on the assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present in the sites of subscribers and the relying parties. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying parties locations.

Inherent limitations

Because of the nature and inherent limitations of controls, Firmaprofesional'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.

Basis for qualified opinion

During our procedures, we noted that some controls were not fully implemented. Specifically:

1. CA BUSINESS PRACTICES DISCLOSURE
   - 1.1 Certification Practice Statement (CPS):
     - The CPS do not include any reference for "Job Rotation Frequency and Sequence"
   - 1.2 Certificate Policy:
     - The CP do not include any reference "Definitions and Acronyms"

4. CA KEY LIFE CYCLE MANAGEMENT CONTROLS
   - 4.5 CA Key Archival and Destruction:
     - The PSC termination plan does not consider that private keys, including backup copies, will be destroyed or removed from use, so that they cannot be recovered.
   - 4.6 CA Key Compromise:
     - Business continuity plan do not include the requirement of the revocation and reissuance of all certificates that were signed with that CA's private key, in the event of the compromise or suspected compromise of a CA's private signing key.

6. CERTIFICATE LIFE CYCLE MANAGEMENT CONTROLS
   - 6.1 Subscriber Registration:
     - The terms and conditions are not clearly included in the Subscriber Agreement for the requesting entity.
     - In few cases of the sample, we could not verify all verifications conducted by the CA according to the type of certificate due the lack of evidences.
   - 6.4 Certificate Issuance:
     - We have identified some valid certificates with errors:
       - BR certificates with organizationName and without localityName
       - BR certificates with directoryName in subjectAltName ("Sede Electrónica" certificates (Electronic Office of Goverment sites) due Spanish laws requirements)
       - BR certificates with organizationName exceeding the upper bounds of x520organizationName
   - 6.8 Certificate Validation:
     - In some cases, the OCSP responds "unknown" when requesting to "revoked" certificates appearing in CRL.

3. CA ENVIRONMENTAL CONTROLS
   - 3.3 Personnel Security
     - The document with job assignments is not fully updated with the recent job changes.

- There is no evidence of the acceptance of some recent roles changed by the people who occupy them.

- 3.4 Physical and Environmental Security
  - Data Center personnel is authorized to access the PKI room without being accompanied by CA personnel although they have no physical access to CA core equipment.
- 3.6 System Access Management
  - The reasons why security patches are not applied are not systematically documented, although the security officer approves or denies the application of security patches.
  - Some systems do not fully comply with the security access control policy.
- 3.8 Business Continuity Management
  - The termination plan does not consider its obligations to make its public key available to interested parties for a reasonable period, being maintained or transferred to a trusted party.
- 3.10 Audit Logging
  - Not all logs are digitally signed as required per internal normative.
  - Some events such as the start and stop events are not being monitored.

Auditor's opinion

In our opinion, except for the matters described in the preceding paragraphs, throughout the period 10th of March 2017 to the 20th of June of 2017, Firmaprofesional 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 v2.0.

This report does not include any professional opinion regarding the quality of Firmaprofesional' s services, beyond those covered by the Webtrust for Certification Authorities Criteria, nor the suitability of any of Firmaprofesional's services for any customer's intended purposes

F. Mondragon, Auditor

auren

Attestation of the Directors on its business practices and controls as Certification Services Provide

December, 19th, 2016

Firmaprofesional, SA (hereinafter Firmaprofesional) operates as a Certification Services Provider (CSP), as defined by the Spanish law 59/2003 of December 19, on electronic signature (Law 59/2003) through its certification hierarchy, consisting of a Root Certification Authority (CA) and three Delegated or Subordinated Certification Authorities (AC Firmaprofesional - CA1, AC Firmaprofesional - AAPP, AC Firmaprofesional - INFRASTRUCTURA and AC Firmaprofesional - CUALIFICADOS), providing the following services:

- Subscriber registration.
- Electronic Certificates lifecycle management (issuance, renewal, suspension, rehabilitation and distribution - using on-line repository -).
- Certificates Status Information publication through certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP).
- Secure Signature-Creation Devices (SSCD) Lifecycle Management as smartcards or cryptographic USB tokens.

To carry out the provision of certification services, Firmaprofesional outsources some tasks to Registration Authorities (RA), as identifying Certificate Applicants, as permitted by law 59/2003. These tasks are performed as set out in the Firmaprofesional Certification Policies and Practices and agreements between Firmaprofesional and RA's

The Management of Firmaprofesional is responsible for establishing and maintaining effective controls over the operations and procedures of the AC Firmaprofesional, including demonstrations of its Business Practices as CA, service integrity (including controls to manage the lifecycle of the keys, certificates and SSCD, in the latter case, if applicable) and controls applied to the CA environment. These controls contain monitoring mechanisms, and actions are taken to correct the deficiencies.

There are inherent limitations in some controls, including the possibility of human error and the circumvention or override of controls. On the occasions that a risk analysis recommends the inclusion of compensating controls to meet the inherent limitations mentioned, these are included. Still, even effective controls can only provide reasonable assurance regarding the operations, procedures and environment Firmaprofesional as CSP. Additionally, because of changes in conditions, the effectiveness of the controls may vary from time to time.

Therefore, Firmaprofesional, with the full support of management:

- Discloses its Business Practices on lifecycle management of keys and certificates, as well as their privacy of information, and provides its services under such statements.
- Maintains effective controls to provide reasonable assurance that:
    - Subscriber information is properly authenticated (for the registration activities performed by Firmaprofesional).
    - The integrity of keys and certificates is maintained throughout their lifecycle.
    - The privacy of private keys is maintained throughout their lifecycle.

- Access to information of subscribers and users is restricted to authorized personnel and information is protected from uses not specified in the business practices published Firmaprofesional.
- Continuity of operations relating to the management of the lifecycle of the keys and certificates is maintained.
- The tasks of exploration, development and maintenance of CA systems are properly authorized and performed to maintain data integrity.

All aligned with internationally accepted standards:

- ISO 9001 Quality management systems - Requirements.
- ISO 27001 Information technology - Security techniques - Information security management systems – Requirements.
- WEBTRUST (SM/TM) FOR CERTIFICATION AUTHORITIES, Trust Service Principles and Criteria for Certification Authorities Version 2.0.

Principle 1: CA Business Practices Disclosure

Certification Practices Statement and Certificate Policies for AC Raíz, AC Firmaprofesional - CA1, AC Firmaprofesional - AAPP, AC Firmaprofesional - INFRAESTRUCTURA and AC Firmaprofesional - CUALIFICADOS (https://www.firmaprofesional.com/esp/cps-eng-2), including:

- CPS - Certification Practices Statement
- Corporate Certificate for Professional Membership Organisations policy (with or without SSCD)
- Corporate Certificate for Legal Representatives policy (with SSCD)
- Corporate Certificates for Natural Persons policy (with or without SSCD)
- Corporate Certificates for Legal Persons policy (with or without SSCD)
- Corporate Company Seal Certificates policy (software or hardware based)
- Corporate certificate for Electronic Invoicing policy (with or without SSCD)
- Electronic Office Certificate policy
- Digital stamps for the Civil Service, public bodies or corporations policy
- Certificate of Public Employees policy
- Web SSL Server Certificate policy
- Web SSL Server Extended Validation Certificate policy
- Code Signing Certificate policy
- Secure Service Certificate (TSA/VA) policy
- Time stamping service policy
- Validation service policy

Principle 2: Service Integrity

- Keys lifecycle management controls
    - CA key pair generation
    - CA Key Storage, Backup and Recovery
    - CA Public Key Distribution
    - CA keys and End Entity certificates usage
    - CA Key Archival and Destruction
    - CA Cryptographic Hardware Life Cycle Management
    - CA-Provided Subscriber Key Generation Services (if supported)
- Certificates lifecycle management controls
    - Subscriber Registration
    - Certificate Issuance and Renewal
    - Certificate Revocation
    - Certificate Suspension
    - Certificate Distribution
    - Certificate Validation
    - Integrated Circuit Card (ICC) Life Cycle Management (if supported)

Principle 3: CA Environmental Controls

- Logical and physical access to CA systems and data is restricted to authorized individuals.
- The continuity of key and certificate management operations is maintained.
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.