

## 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 10<sup>th</sup> of March 2017 to the 20<sup>th</sup> 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 SSL certificate lifecycle management business practices in its:
  - CPS. Declaración de Prácticas de Certificación Version 160229
  - PC. CP Servidor Web. Version 6.3
  - PC. CP Sede Electrónica Version 160229including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Firmaprofesional 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 Firmaprofesional)
  
- 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



### **Certification authority's responsibilities**

Firmaprofesional'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.

### **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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Firmaprofesional's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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 Firmaprofesional 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:

#### **PRINCIPLE 1: Baseline Requirements Business Practices Disclosure**

- Firmaprofesional has disclosed its commitment to conform to the 1.1.6 version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum. However, this is not the latest version of the requirements.

#### **PRINCIPLE 2: Service Integrity**

- **2 CERTIFICATE CONTENT AND PROFILE:**
  - 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 Government sites) due Spanish laws requirements)
    - BR certificates with organizationName exceeding the upper bounds of x520organizationName
  - We could not verify that the CA hosts test Web pages using Subscriber Certificates that are valid, revoked, and expired.
- **3 CERTIFICATE REQUEST REQUIREMENTS**
  - The terms and conditions are not clearly included in the Subscriber Agreement for the requesting entity.
- **4 VERIFICATION PRACTICES**
  - In few cases of the sample, we could not verify all verifications conducted by the CA due the lack of evidences.
  - In few cases of the sample, some data used to verify a certificate request could had been obtained exceeding the age stated in normative prior to issuing the certificate.
- **5 CERTIFICATE REVOCATION AND STATUS CHECKING**
  - The CA does not have published clearly instructions for subscribers or third parties to report possible problems.
  - The OCSP service respond with a "good" status for Certificates that have not been issued.
  - In some cases, the OCSP responds "unknown" when requesting to "revoked" certificates appearing in CRL.

- 6 EMPLOYEE AND THIRD PARTIES
  - The document with job assignments is not fully updated with the recent job changes.
  - Although personnel performing information verification duties is adequately training, in few cases, we could not evidence records of the training to all personnel performing information verification duties (Validation Specialists) with skills-training that covers all requirements.

PRINCIPLE 3: CA Environmental Security

- Some systems do not fully comply with the security access control policy.
- Not all logs are digitally signed as required per internal normative.

PRINCIPLE 4: Network and Certificate Systems Security Requirements


- Some systems in Secure Zones do not fully comply with security access control requirements.
- We could not verify the performing of a Vulnerability Scan on private IP addresses at least once per quarter.

**Auditor's Opinion**

In our opinion, except for the matters described in the preceding paragraphs, throughout the period 10<sup>th</sup> of March 2017 to the 20<sup>th</sup> 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 – SSL Baseline with Network Security v2.

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

This report does not include any representation as to the quality of Firmaprofesional's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2, nor the suitability of any of Firmaprofesional's services for any customer's intended purpose.



F. Mondragon, Auditor

**auren**

## **Attestation of the Directors on its business practices and controls on SSL Baseline with Network Security**

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 - INFRASTRUCTURA and AC Firmaprofesional - AAPP, 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)

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 27001 Information technology - Security techniques - Information security management systems – Requirements
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2



A handwritten signature in black ink, appearing to read 'Wally', is centered on a light yellow rectangular background.