Valencia, May 30th 2016

Independent Qualified Audit Report

To the Management of Autoritat de Certificació Consorci d'Administració Oberta de Catalunya (Consorci AOC):

We have audited the Assertion by the Autoritat de Certificació Consorci d'Administració Oberta de Catalunya, (hereinafter, Consorci AOC) according its services as Certification Authority for issuing SSL certificates (through the *"EC-SectorPublic", "EC-AL", "EC-GENCAT", "EC-SAFP", "EC-UR", "EC-URV" and "EC-PARLAMENT"* subordinates issued by *"EC-ACC"* Entitat de certificació Agència Catalana de Certificació as detailed in appendix 1) during the period from the 21st of December 2014 to the 20th of December of 2015.

In this period, Consorci AOC has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines and provided such services in accordance with its disclosed practices Certification Practices Statement with the relevant exceptions detailed in the Auditor's Opinion section.
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and certificates it manages was established and protected throughout their life cycles.
- 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 – SSL Baseline with Network Security – Version 2.

Consorci AOC's management is responsible for its assertion. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the AICPA/CPA Canada and, accordingly, included (1) obtaining an understanding of Consorci AOC' SSL certificate life cycle

management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates; (2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management 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 audit provides a reasonable basis for our opinion.

Auditor's Opinion

In our opinion, Consorci AOC management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria with Network Security with the following relevant exceptions:

- Specific errors in Certificate Content and Extensions such as the inclusion of the SubjectAltName extension for Electronic Office Certificates as required by Spanish law, the absence of the localityName or stateOrProvinceName when organization names its included, fields and in the formal profile definition, etc.
- The OCSP responder respond with a "good" status when receives a request for status of a certificate that has not been issued by *"EC-SectorPublic".*

Inherent Limitations

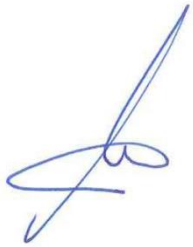
Because of the nature and inherent limitations of controls, there may be undetected errors or instances of fraud. Furthermore, the projection of any conclusions based in our findings, to future periods subsequent to the date of our report, is subject to the risk that there may be:

(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.

Exclusions

The relative effectiveness and significance of specific controls at Consorci AOC 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.

This report does not include any representation as to the quality of Consorci AOC's certification services beyond those covered by the WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, or the suitability of any of Consorci AOC' services for any customer's intended purpose.

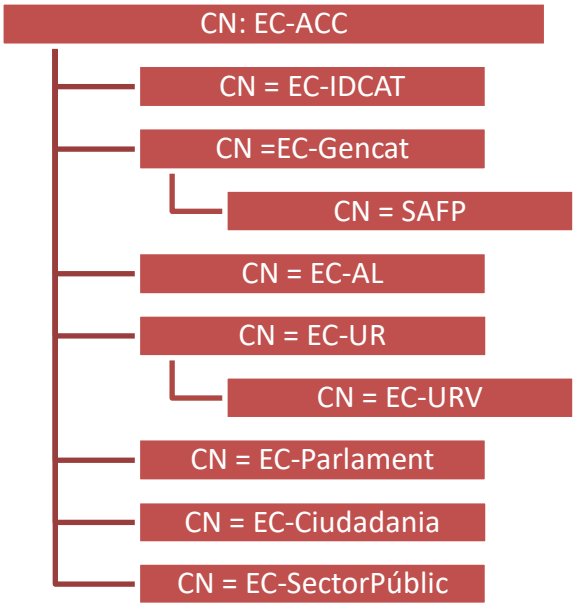


F. Mondragon, Auditor

auren

Appendix 1 Hierarchy

Consorci AOC hierarchy



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

May, 20th, 2016

The *Consorci d'Administració Oberta de Catalunya* (hereinafter AOC Consortium) acts as 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 "EC-ACC" and its intermediate Certification Authorities (CA) "EC-AL", Catalan Local Government; "EC-GENCAT" Generalitat of Catalonia, which includes "EC-SAFP," Secretary of Administration and Public Function; "EC-UR", Universities and Research, which includes "EC-URV," Rovira i Virgili University; "EC-idCAT" Citizens; and "EC-Parlament" Parliament of Catalonia; "EC-Ciutadania" and "EC-SectorPublic", 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 AOC Consortium is responsible for establishing and maintaining effective controls over the operations and procedures of the EC-ACC, 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 AOC Consortium as CSP. Additionally, because of changes in conditions, the effectiveness of the controls may vary from time to time.

Therefore, AOC Consortium, 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 AOC Consortium)
- 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 by AOC Consortium
- 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:

- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2