

Independent Qualified Audit Report

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

We have audited the Statements performed by the Autoritat de Certificació Consorci d'Administració Oberta de Catalunya Management, (hereinafter, Consorti AOC) according its services as issuer of Extended Validation ("EV") digital 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, Consorti AOC has:

- Disclosed its Extended Validation certificate and key life cycles management practices and procedures, including its commitment to provide EV certificates in conformity with the CA/Browser Forum Guidelines for Extended Validation (EV) 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:
 - Extended Validation Subscriber information was properly collected, reviewed and verified ; and
 - The integrity of the keys and Extended Validation certificates was established and protected through their life cycles.

in accordance with WebTrust requirements for the Certification Authorities Extended Validation, imposed by the WebTrust Criteria for Certification Authorities of AICPA/CPA Canada (WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5).

Consorti AOC Management is responsible for its Statements. Our responsibility is to express an opinion on Consorti AOC's Statements, based on our audit.

Consorti AOC uses external registration authorities for specific subscriber registration activities as outlined in the Certification Policy and Certification Practice Statement of

Consorti AOC. Our work does not include the control verification on external registration authorities.

The audit was conducted in accordance with standards for assurance engagements of WebTrust Criteria for Certification Authorities, established by the organizations competent in this matter, namely the AICPA/CPA Canada. Our audit included:

- Obtaining and adequate understanding of the keys and Extended Validation certificates life cycle management business, information and business privacy controls and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party, over the continuity of key and certificate life cycle management operations, and finally, over the development, maintenance and guarantee of the integrity of the systems;
- Selective tests on transactions carried out in accordance with the disclosed EV certificate and key life cycle management business and information privacy 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.

Auditor's Opinion

In our opinion, for the period between the 21st of December 2014 to the 20th of December of 2015, Consorti AOC's Management Assertions regarding its Certification Authority Practices, are properly formulated in all material matters, in accordance with the AICPA/CPA Canada WebTrust Program for Certification Authorities – Extended Validation criteria with the following relevant exceptions:

- Specific errors in Certificate Content and Extensions such as incorrect encoding of `subject:jurisdictionOfIncorporationCountryName`, `subject:localityName`, `subject:organizationName` and `subject:organizationalUnitName` 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 inherent limitations control systems themselves, 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 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.

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

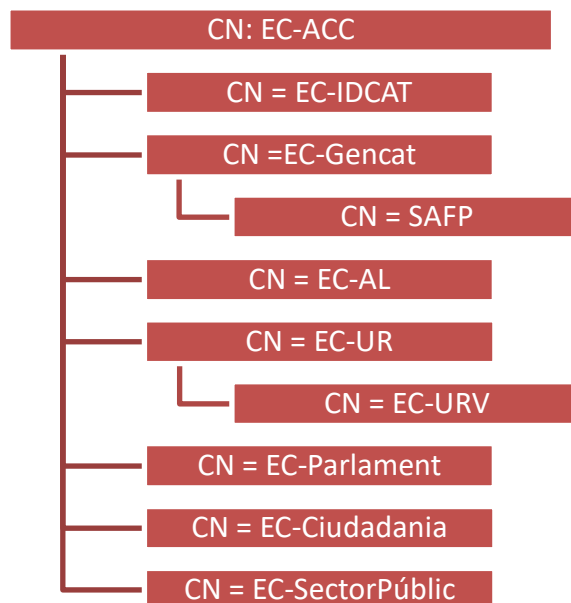


F. Mondragon, Auditor

auren

Appendix 1 Hierarchy

Consorti AOC hierarchy



Attestation of the Directors on its business practices and controls on SSL Extended Validation Certificates

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 SM/TM for Certification Authorities WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5

