Valencia, December 20th, 2018

Independent Report on Agreed-upon criteria

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

We have performed the procedures on the following pages, which were agreed to by the management of Consorci AOC, with respect to examining the conformance of selected criteria for its Certification Authority (CA) operations at Barcelona, SPAIN for its CAs as enumerated in Appendix 1 as of December 20th, 2018 [12/20/2018].

This engagement was conducted 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. The sufficiency of these procedures is solely the responsibility of Consorci AOC. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

We were not engaged to and did not conduct an audit, the objective of which would be the expression of an opinion on the sufficiency of these procedures. Accordingly, we do not express such an opinion. The scope of these procedures was limited to Certification Authorities mentioned above during the fieldwork period of December 19th, 2018 through December 20th, 2018. we did not extend our procedures normally associated with a full-scope WebTrust report. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of the management of Consorci AOC and Browsers and is not intended to be and should not be used by anyone other than these specified parties.

Jose Miguel Cardona
auren
PLAZA AYUNTAMIENTO, 26 - 2ª
46002 VALENCIA

Independent Report on Agreed-upon criteria

Agreed-Upon Criteria	Procedures Performed	Procedure Notes	Procedure Results
The OCSP services of EC-ACC and EC-SectorPublic do not respond with a "good" status for Certificates that have not been issued.	Reviewed the OCSP Service for the Issuing certificates mentioned.	We tested the OCSP service for the issuing certificates mentioned for a sample of non-issued random serial numbers and verified both services respond "unknown"	No exceptions noted.

Agreed-Upon Criteria	Procedures Performed	Procedure Notes	Procedure Results
The Repository of EC-ACC and EC-SectorPublic do not include entries that indicate that a Certificate is suspended	Reviewed the CRL issued by EC-ACC and EC-SectorPublic	We analyzed the CRL issued by EC-SectorPublic on December 19th, 2018 with CRL Number 261d and noted there are 19 entries revoked with status "certificateHold". We verify that all these certificates contain one of the following Policy OIDs: • 1.3.6.1.4.1.15096.1.3.2.7.1.1: Recognized signature certificate for high-level public employee (T-CAT signatura) • 1.3.6.1.4.1.15096.1.3.2.7.1.2: Authentication certificate for high-level public employee (T-CAT authenticació) • 1.3.6.1.4.1.15096.1.3.2.7.3.1 Recognized authentication and signature certificate for mid-level public employees (T-CATP) • 1.3.6.1.4.1.15096.1.3.1.81.2.4: Personal Identity and Recognized Signature Certificate (CPISR-1) • 1.3.6.1.4.1.15096.1.3.1.82.3.4: Personal Identity and Recognized Signature Certificate with optional job title (CPISR-2 C) We analyzed the CRL issued by EC-ACC on November 16th, 2018 with CRL number 17 and verify there are no entries revoked with status "certificateHold"	Exception noted.

Agreed-Upon Criteria	Procedures Performed	Procedure Notes	Procedure Results
Consorci AOC performs a Vulnerability Scan on private IP addresses identified at least every three months and performs a Penetration Test on Consorci AOC's Certificate Systems on at least an annual basis	Reviewed vulnerability procedures. Reviewed vulnerability and pentest last reports.	The last vulnerability assessment for the private IP addresses identified was performed on October 16th, 2018 with no critical or high issues identified. According to the vulnerability assessment procedure the tests are conducted on a monthly basis. The penetration test for the CA Infrastructure was conducted on June 2018, and the penetration test for the CAOC infrastructure on November 2018.	No exceptions noted.
Formal procedures exist to update Linux systems of the CA equipment.	Reviewed the updates procedures for the CA equipment.	We could evidence a formal procedure to update Linux systems of the CA equipment.	No exceptions noted.

Apendix 1 List of CAs in Scope

Root CAs
1. EC-ACC
OV SSL Issuing CAs
3. EC-SectorPublic
EV SSL Issuing CAs
3. EC-SectorPublic
Private Trust Issuing CAs
None
Non-EV Code Signing Issuing CAs
None
EV Code Signing Issuing CAs
None
Secure Email (S/MIME) CAs
2. EC-Ciutadania 3. EC-SectorPublic
Document Signing CAs
None
Adobe CAs
None
Timestamp CAs
None
Other CAs
None

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	serialNumber	Key Algorithm	Key Size	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
1	1	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	-11D4C2142BDE21EB579D53FB0C223BFF	rsaEncryption	2048 bit	sha1WithRSAEncryption	Jan 7 23:00:00 2003 GMT	Jan 7 22:59:59 2031 GMT	A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D	88497F01602F3154246AE28C4D5AEF10F1D87EBB76626F4AE0B7F95BA7968799
1	2	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	524B25BD12ED8CFE4F8D37BBC29BA87F	rsaEncryption	2048 bit	sha256WithRSAEncryption	Apr 17 09:28:27 2012 GMT	Jan 7 22:59:59 2031 GMT	A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D	A5898E5BFB84295C043EC4034288AFB37E0D5A3866F17CB657B97F72DCB53BEC
2	1	CN=EC-Ciutadania, OU=Serveis Públics de Certificació, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	73EEAE15E3DFADA8541A95ECF258624F	rsaEncryption	2048 bit	sha256WithRSAEncryption	Sep 18 08:21:00 2014 GMT	Sep 18 08:21:00 2030 GMT	0B:68:59:3E:87:C8:A3:15:1A:E0:40:82:22:5F:9F:1D:B2:C5:37:15	0FD99AAE1FFCD5D9F0AD76EDDDCBEF6B884CC85C16BFCFA4B5246155D6597ED6
3	1	CN=EC-SectorPublic, OU=Serveis Públics de Certificació, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	71B065397C8E07D2541A967F75593792	rsaEncryption	2048 bit	sha256WithRSAEncryption	Sep 18 08:23:27 2014 GMT	Sep 18 08:23:27 2030 GMT	47:3C:DE:14:77:BB:6A:4F:47:91:A9:02:FF:D4:06:E1:73:DC:E2:D9	356A5F4D994E9EFA7CAEFC491768911D65EC25977465B610E2F29AA4472631C3