Valencia, July 17th, 2019

Independent Assurance Report

To the management of Govern d'Andorra:

Scope

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at Andorra la Vella, PRINCIPAT D'ANDORRA, Govern d'Andorra disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, the provision of services in accordance with its Certification Practice Statement, and the effectiveness of 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 CA systems integrity throughout the period April 14th, 2018 to April 13th, 2019 for its CAs as enumerated in Appendix 1.

Govern d'Andorra does not escrow its CA keys. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

Govern d'Andorra management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1.

Our independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

Auren applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on Govern d'Andorra disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities

v2.1, 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:

(1) obtaining an understanding of Govern d'Andorra'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;
(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Govern d'Andorra 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.

Inherent limitations

Because of the nature and inherent limitations of controls, Govern d'Andorra 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:

- the CA did not disclose its business, key lifecycle management, certificate lifecycle management, and CA environment control practices throughout the whole applicable period.
- The CA's Certificate Policies and Certification Practice Statement(s) have not been reviewed and updated on a regular basis and, as a result, the CA has not maintained enough effective controls to provide reasonable

assurance that the CA services are provided in accordance with its Certificate Policies and Certification Practice Statement(s).

This caused WebTrust Criterion 1.1 which reads:

The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certification Practice Statement.

and WebTrust Criterion 2.1 which reads:

The CA maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.

to not be met.

During our procedures, we noted that

- The CA did not maintain enough effective controls to provide reasonable assurance that all the relevant subscriber information is properly authenticated in all cases (for the registration activities performed by Govern d'Andorra).

This caused WebTrust Criterion 6.1 which reads:

The CA maintains controls to provide reasonable assurance that:

For authenticated certificates

- *subscribers are accurately identified in accordance with the CA's disclosed business practices;*
- *subscribers' domain names and IP addresses are accurately validated in accordance with the CA's disclosed business practices; and*
- *subscribers' certificate requests are accurate, authorised and complete.*

For domain validated certificates

- *Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and*
- *Subscriber's certificate requests are accurate and complete.*

to not be met.

During our procedures, we noted that

- Several deficiencies were identified such as out of date operating systems, inappropriate access to computers and systems.

This caused WebTrust Criterion 3.6 which reads:

The CA maintains controls to provide reasonable assurance that CA system access is limited to authorised individuals. Such controls provide reasonable assurance that:

- *hypervisor, operating system, database, and network device access is limited to authorized individuals with predetermined task privileges;*
- *access to network segments housing CA systems is limited to authorised individuals, applications and services; and*
- *CA application use is limited to authorised individuals.*

to not be met.

During our procedures, we noted

- a lack of controls to ensure the continuity of the CA operations.

This caused WebTrust Criterion 3.8 which reads:

The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster or other type of business interruption. Such controls include, at a minimum:

- *the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system;*
- *the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;*
- *creating backups of systems, data, and configuration information at regular intervals in accordance with the CA's disclosed business practices, and storage of these backups at an alternate location; and*
- *the availability of an alternate site, equipment and connectivity to enable recovery.*

The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.

to not be met.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified section above, throughout the period April 14th, 2018 to April 13th, 2019, Govern d'Andorra has, in all material respects:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in:
  - DECLARACIÓ DE PRÀCTIQUES DE CERTIFICACIÓ AC CAMERFIRMA S.A. Com Prestador de Serveis de Certificació Digital del GOVERN D'ANDORRA – Version 1.0

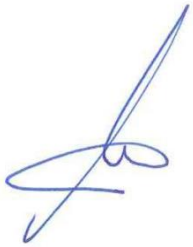
- maintained effective controls to provide reasonable assurance that:
  - Govern d'Andorra provides its services in accordance with Certification Practice Statement(s)

- 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 Govern d'Andorra)

- 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 the WebTrust Principles and Criteria for Certification Authorities v2.1.

This report does not include any representation as to the quality of Govern d'Andorra's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.1, nor the suitability of any of Govern d'Andorra's services for any customer's intended purpose.



F. Mondragon, Auditor

auren

Valencia, SPAIN

July 17th, 2019

APPENDIX 1 List of CAs in Scope

Root CAs
1. Global Chambersign Root – 2008
OV SSL Issuing CAs
N/A
EV SSL Issuing Cas
N/A
Other CAs
2. Entitat de Certificació de l'Administració Pública Andorrana

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=Global Chambersign Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	C9CDD3E9D57D23CE	rsaEncryption	4096 bit	sha1WithRSAEncryption	Aug 1 12:31:40 2008 GMT	Jul 31 12:31:40 2038 GMT	B9:09:CA:9C:1E:DB:D3:6C:3A:6B:AE:ED:54:F1:5B:93:06:35:2E:5E	136335439334A7698016A0D324DE72284E079D7B5220BB8FBD747816EEBEBACA
2	2	CN=Entitat de Certificació de l'Administració Pública Andorrana, L=Andorra la Vella, serialNumber=D-059888-N, O=M.I. Govern d'Andorra, C=AD	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	BBBBEEEE341353B9	rsaEncryption	4096 bit	sha1WithRSAEncryption	Jul 18 07:39:14 2013 GMT	Jul 13 07:39:14 2033 GMT	A6:B0:51:FD:9B:A0:46:48:2D:45:74:14:95:F7:D6:E2:9B:EF:F9:1E	62FDD1DD4DBD26940066AA030FCDA451B2BC2143FECE65A8AA03FC0BD311F0FD
2	2	CN=Entitat de Certificació de l'Administració Pública Andorrana, L=Andorra la Vella, serialNumber=D-059888-N, O=M.I. Govern d'Andorra, C=AD	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	BBBBEEEE165A6516	rsaEncryption	4096 bit	sha256WithRSAEncryption	Jul 19 10:43:31 2013 GMT	Jul 14 10:43:31 2033 GMT	A6:B0:51:FD:9B:A0:46:48:2D:45:74:14:95:F7:D6:E2:9B:EF:F9:1E	FBF1844EB206D27EB526F1C2B910FE045D8D6FC1F4D14CBC93135CF0704DA537