Valencia, March 13, 2020

Independent Assurance Report

To the management of Govern d'Andorra:

Scope

We have been engaged, in a reasonable assurance engagement, to report on Govern d'Andorra management's assertion that for its Certification Authority (CA) operations at Andorra la Vella, PRINCIPAT D'ANDORRA, throughout the period October 17, 2019 to January 16, 2020 for its CAs as enumerated in in Appendix 1, Govern d'Andorra has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Declaració de pràctiques de certificació PKI - Administració pública andorrana (2020)

- maintained effective controls to provide reasonable assurance that:
  - Govern d'Andorra provides its services in accordance with its 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; and
  - 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 v2.2.

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 v2.2.

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 v2.2, 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´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 sufficient personnel controls were not implemented. Specifically:

- A new employee was assigned a Trusted Role without meeting the requirements set forth in the DPC.

This caused WebTrust Criterion 3.3 which reads:

The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.

to not be met.

During our procedures, we noted that sufficient validation controls were not implemented. Specifically:

- 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 sufficient certificate issuing controls were not implemented. Specifically

- Some certificates were issued with errors regarding the X.509 standard.
- Certificates were issued with errors regarding the profiles defined by the CA.

This caused WebTrust Criterion 6.4 which reads:

The CA maintains controls to provide reasonable assurance that certificates are generated and issued in accordance with the CA's disclosed business practices.

to not be met.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified section above, throughout the period October 17, 2019 to January 16, 2020, Govern d'Andorra 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 v2.2.

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 v2.2, nor the suitability of any of Govern d'Andorra's services for any customer's intended purpose.

F. Mondragon, Auditor

auren

Valencia, SPAIN

March 13, 2020

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-19

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-19, 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	60AE862C57A0454C5E5D62	rsaEncryption	4096 bit	sha256WithRSAEncryption	Oct 17 14:44:16 2019 GMT	May 30 14:44:16 2038 GMT	C0:C1:74:4D:C6:C5:C1:07:7B:03:14:58:5D:58:40:C9:78:33:B8:6A	AD54D8979AA136E9F568E01234ACCA68C81A6F00F9629A7192753F76752BCA69

GOVERN D'ANDORRA MANAGEMENT'S ASSERTION

March 13, 2020

Govern d'Andorra Certification Authority operates the Certification Authority (CA) services known as "Entitat de Certificació de l'Administració Pública Andorrana-19", and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Subscriber key generation and management

The management of "Govern d'Andorra" is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls and certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Govern d'Andorra's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Govern d'Andorra management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Govern d'Andorra management's opinion, in providing its Certification Authority (CA) services at Andorra la Vella, PRINCIPAT D'ANDORRA, throughout the period October 17, 2019 to January 17, 2020, Govern d'Andorra has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Declaració de pràctiques de certificació PKI - Administració pública andorrana (2020)

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

- 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 authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

Jordi Gallardo Fernàndez
Ministre de Presidència, Economia i Empresa
Govern d'Andorra