

Accountants' report - Webtrust CA



EY Transforma Servicios de
Consultoría, S.L.
Edificio Sarrià Forum
Avda. Sarrià, 102 – 106
08017 Barcelona – España
Tel: +34 933 663 700

Report of Independent Accountants

Addressed to:

Govern d'Andorra

We have examined the accompanying assertion made by the management of **Govern d'Andorra** that provides its Certification Authority (CA) services at **Andorra** for the Root CA's and Subordinate CA's referenced in *Appendix A* during the period from **January 17th 2023** through **January 16th 2024**. **Govern d'Andorra** has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - <https://www.signaturaelectronica.ad/>
- maintained effective controls to provide reasonable assurance that:
 - **Govern d'Andorra**-CA's Certification Practice Statements are consistent with its Certificate Policies
 - **Govern d'Andorra**-CA's provides its services in accordance with its Certificate Policies and 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**-CA); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

based on the American Institute of Certified Public Accountants (AICPA)'s [Trust Services Principles and Criteria for Certification Authorities 2.2.2](#)

Govern d'Andorra's management is responsible for its assertion and for specifying the aforementioned Criteria. Our responsibility is to express an opinion on management's assertion based on our examination.

Accountants' report - Webtrust CA



EY Transforma Servicios de
Consultoría, S.L.
Edificio Sarrià Forum
Avda. Sarrià, 102 – 106
08017 Barcelona – España
Tel: +34 933 663 700

Govern d'Andorra makes use of external registration authorities for specific subscriber registration activities as disclosed in **Govern d'Andorra's** business practice disclosures. Our examination did not extend to the controls of external registration authorities.

Govern d'Andorra does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of **Govern d'Andorra's** key and certificate life cycle management business practices, policies, processes and controls, and its suitability of the design and implementation of the controls intended to achieve the Criteria and examining evidence supporting management's assertion and performing such other procedures over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance and operation of systems integrity as we considered necessary in the circumstances; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle 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. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

Our examination was not conducted for the purpose of evaluating **Govern d'Andorra's** cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, **Govern d'Andorra** may achieve reasonable, but not absolute assurance that all security events are prevented and, for those controls may provide reasonable, but not absolute assurance that its commitments and system requirements are achieved. 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.

Accountants' report - Webtrust CA



EY Transforma Servicios de
Consultoría, S.L.
Edificio Sarrià Forum
Avda. Sarrià, 102 – 106
08017 Barcelona – España
Tel: +34 933 663 700

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer;

(b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

In our opinion, **Govern d'Andorra's** management's assertion referred to above, is fairly stated, in all material respects, based on the aforementioned criteria.

The WebTrust seal of assurance for Certification Authority on **Govern d'Andorra's** website constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of **Govern d'Andorra's** CA services beyond those covered by the *Trust Services Principles and Criteria for Certification Authorities Version 2.2.2* criteria, or the suitability of any of **Govern d'Andorra's** services for any customer's intended purpose.

EY Transforma Servicios de Consultoría, S.L.

18/10/2024

Jose Luis Rojo - Partner

Accountants' report - Webtrust CA



EY Transforma Servicios de
Consultoría, S.L.
Edificio Sarrià Forum
Avda. Sarrià, 102 – 106
08017 Barcelona – España
Tel: +34 933 663 700

Appendix A

| Root/Subordinate Name | Subject Key Identifier | Certificate Serial Number | SHA256 Fingerprint |
|---|--|---------------------------|--|
| CA ACA ROOT (ca_gda) | abfc650bde03bbc2811829e 074d3c84db673e3f1 | 2d035bb6b18b1af0 | be789f1f031ed86a3a74c90 70cc06f972210dca5 |
| ACA ROOT / CA Subordinada ACA CA1 (subca_gda) | 2daf745435308c41f6bcdb1 da87f5a8aaaa11316 | 7c0a0d8873f83b87 | a54b856b91f8e9cfc06d553 4fb19d00b0e64f123 |
| Entitat de Certificació de l'Administració Pública Andorrana-19 | c0c1744dc6c5c1077b03145 85d5840c97833b86a | 60ae862c57a0454c5e5d62 | 12e26b9912e2e99469e7b7 93a6a108d05ea42f6a |