

Report of Independent Accountants

Addressed to:

Agencia Notarial de Certificación (ANCERT) Management

We have examined the accompanying assertion made by the management of **ANCERT** that provides its Certification Authority (CA) services at **Plaza Xavier Cugat 2, Ed. A. Sant Cugat del Vallès (08174), Barcelona, Spain** for the Root CA's and Subordinate CA's referenced in *Appendix A* during the period from **20 May 2022** through **19 May 2023**. **ANCERT** has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - <https://www.ancert.com/en>
 - <https://www.ancert.com/cps>
- maintained effective controls to provide reasonable assurance that:
 - **ANCERT-CA's** Certification Practice Statements are consistent with its Certificate Policies
 - **ANCERT-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 ANCERT-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 [Webtrust Services Principles and Criteria for Certification Authorities 2.2.2](#)

ANCERT'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.

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

ANCERT does not escrow its CA keys 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 American Institute of Certified Public Accountants. 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 **ANCERT**'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 **ANCERT** 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 **ANCERT**'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, **ANCERT** 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



Ernst & Young 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, **ANCERT'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 **ANCERT'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 **ANCERT's** CA services beyond those covered by the *Webtrust Services Principles and Criteria for Certification Authorities Version 2.2.2* criteria, or the suitability of any of **ANCERT's** services for any customer's intended purpose.

Ernst & Young LLP
30/06/2023

A handwritten signature in black ink, appearing to be 'Xavier Ferré', is written over a horizontal line.

Xavier Ferré - Partner

Accountants' report - Webtrust CA



Ernst & Young 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	SHA1 Fingerprint	SHA256 Fingerprint
AC Raíz Certificados Notariales V2 (ANCERTNOT_V2)	f6123aab7b58c18d436f7681d2f2b8d3ef17ea0b	09bd56052a1316f4684f740ea97d1c48	6F62DEB86C85585AE42E478DB4D76DB367585AE6	4BE8B5A1C76C6AEAD0611918FCCF9DBD398B67FB12294758BDF994D0F9682F60
AC Raíz Certificados CGN V2 (ANCERTCGN_V2)	056ee1a19aee07afcef5b4d3653d0450e2d09b44	0f388c70fea6955de95d9c87af790499	7EB1A0429BE5F428AC2B93971D7C8448A536070C	F4336BC2AC75950BECCF1C1F2F9DA6DDAFD1F41161CA71F59C76889BD474033
AC Subordinada Certificados Notariales Personales (ANCERTCP_V2)	5feedd2903014369c81e3d5b817ea5f3a176acf8	3e147be275f3b37294b5a0db64a5f5e0	C879D93F811B029A73B327A388681F99E37B86D0	C4472508C3BC689FC59E8BF77A6DDED FBB29A43316BD0946D544E54DFC001535
AC Subordinada Certificados Notariales Corporativos (ANCERTCNC_V2)	08a12c683580a4ff9cab116c0b33992d7119aa30	3c73f76ae7e08ca131e99f7b9daf0c6a	F3423F407FFEA3D6FFC95DDECE87A1B98F6F591D	0CA8B7A01506CAF AA1879E7491C662F8264EB3A2F1F0E0657DA3D6A912FF1487
AC Subordinada Certificados Notariales de Sistemas (ANCERTCS_V2)	db35b9311ffdf77cc3170dc9cbc8550bea157c0a	286a46411afded8385e0c27c05455ecb	4BFD05453746C78AB1A304E5E64A0C367F969FF8	186B5083F6CBE72E94172B57424B0DB7F0F58B2BAE8D7A9C946A4BBB5B4FD7F0
AC Subordinada FERN (ANCERTFERN_V2)	5f9340b5380824cef0bf234eb92f951368ae84fb	2b0a88107bb8e7d5cdf78ac2acee5e50	390FDE941FAACE9E0A823C88B7E3A392FA26A5BD	A885EC8218B1C96730B0264ECFBBDEE06C97B701FAF80DCB26920F5E727AD73
AC Subordinada Certificados para empleados (ANCERTCE_V2)	749a498dda48c68028d3489bce5772912aeb0393	03f0de1d15130a38d56efeba5820c613	EA9DB7B28563879D7CB490CFB80DF88C7C9329B2	E718F67C8B1F8E1FC0176A361C98E6299FD3F439CFA46EDDB46A57B4AC08B443

Webtrust CA Management assertion

Management's Assertion Regarding the Effectiveness of Its Controls over their Certification Authority Operations during the period from 20 May 2022 through 19 May 2023 based on [Webtrust Services Principles and Criteria for Certification Authorities 2.2.2.](#)

13/07/2023

We, as management of **ANCERT**, are responsible for operating a Certification Authority (CA) at **Plaza Xavier Cugat 2, Ed. A. Sant Cugat del Vallès (08174), Barcelona, Spain** for the Root CA's and Subordinate CA's listed in **Appendix A**.

ANCERT's CA services provide the following certification authority services:

- **Subscriber registration**
- **Certificates issuance**
- **Certificates renewal**
- **Certificates distribution**
- **Certificate revocation**
- **Certificate validation**
- **Subscriber key generation and management**
- **Certificate status information processing**
- **Managing lifecycle of integrated circuit cards**

ANCERT does not escrow its CA keys and does not provide certificate suspension services.

Management of **ANCERT** is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website (<https://www.ancert.com>), CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to **ANCERT's** CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of **ANCERT** has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in **ANCERT** Management's opinion, in providing its CA services for the Root CA's and Subordinate CA's listed in **Appendix A** at **Plaza Xavier Cugat 2, Ed. A. Sant Cugat del Vallès (08174), Barcelona, Spain** during the period from **20 May 2022** through **19 May 2023**, **ANCERT** has:

- ▶ disclosed its Business, Key Life Cycle Management, and Certificate Life Cycle Management, and CA Environmental Control practices as below:
 - **Root and subordinate CA certificates:**
<http://www.ancert.com/liferay/web/ancert/descarga-de-certificados-raiz>

Webtrust CA Management assertion

- **CPS-EN:**
<https://www.ancert.com/en>
- **CPS-ES:**
<https://www.ancert.com/cps>

- ▶ maintained effective controls to provide reasonable assurance that:
 - **ANCERT-CA's** Certification Practice Statements are consistent with its Certificate Policies
 - **ANCERT-CA** 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 was established and protected throughout their life cycles;
 - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
 - the Subscriber information was properly authenticated (for the registration activities performed by **ANCERT**); and
 - subordinate CA certificate requests were accurate, authenticated and approved

- ▶ Maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data was restricted to authorized individuals;
 - the continuity of key and certificate management operations was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the Root Keys listed in Appendix A, based on the *Webtrust Services Principles and Criteria for Certification Authorities Version 2.2.2*, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

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

- 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 Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Very truly yours,

Agencia Notarial de Certificación (ANCERT)

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA1 Fingerprint	SHA256 Fingerprint
AC Raíz Certificados Notariales V2 (ANCERTNOT_V2)	f6123aab7b58c18d436f7681d2f2b8d3ef17ea0b	09bd56052a1316f4684f740ea97d1c48	6F62DEB86C85585AE42E478DB4D76DB367585AE6	4BE8B5A1C76C6AEAD0611918FCC9DBD398B67FB12294758BDF994D0F9682F60
AC Raíz Certificados CGN V2 (ANCERTCGN_V2)	056ee1a19aee07afcefb5d43653d0450e2d09b44	0f388c70fea6955de95d9c87af790499	7EB1A0429BE5F428AC2B93971D7C8448A536070C	F4336BC2AC75950BECCF1C1F2F9DA6DDDAFD1F41161CA71F59C76889BD474033
AC Subordinada Certificados Notariales Personales (ANCERTCP_V2)	5feedd2903014369c81e3d5b817ea5f3a176acf8	3e147be275f3b37294b5a0db64a5f5e0	C879D93F811B029A73B327A388681F99E37B86D0	C4472508C3BC689FC59E8BF77A6DDED FBB29A43316BD0946D544E54DFC001535
AC Subordinada Certificados Notariales Corporativos (ANCERTCNC_V2)	08a12c683580a4ff9cab116c0b33992d7119aa30	3c73f76ae7e08ca131e99f7b9daf0c6a	F3423F407FFE3D6FFC95DDECE87A1B98F6F591D	0CA8B7A01506CAF AA1879E7491C662F8264EB3A2F1F0E0657DA3D6A912FF1487
AC Subordinada Certificados Notariales de Sistemas (ANCERTCS_V2)	db35b9311ffdf77cc3170dc9cbc8550bea157c0a	286a46411afdcd8385e0c27c05455ecb	4BFD05453746C78AB1A304E5E64A0C367F969FF8	186B5083F6CBE72E94172B57424B0DB7F0F58B2BAE8D7A9C946A4BBB5B4FD7F0
AC Subordinada FERN (ANCERTFERN_V2)	5f9340b5380824cef0bf234eb92f951368ae84fb	2b0a88107bb8e7d5cdf78ac2acee5e50	390FDE941FAACE9E0A823C88B7E3A392FA26A5BD	A885EC8218B1C96730B0264ECFBBDEE06C97B701FAF80DCB26920F5E727AD73
AC Subordinada Certificados para empleados (ANCERTCE_V2)	749a498dda48c68028d3489bce5772912aeb0393	03f0de1d15130a38d56efeba5820c613	EA9DB7B28563879D7CB490CFB80DF88C7C9329B2	E718F67C8B1F8E1FC0176A361C98E6299FD3F439CFA46EDDB46A57B4AC08B443