Audit Attestation for

Firmaprofesional S.A.

Reference: 2302_FPR_FR

"Madrid, 2023-06-01"

To whom it may concern,

This is to confirm that DEKRA Testing and Certification S.A.U has audited the CAs of the Firmaprofesional, S.A. without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "2302_FPR_FR" covers multiple Root-CAs and consists of 10 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

DEKRA Testing and Certification S.A.U
C/ Severo Ochoa 2 y 6. Parque tecnológico de Andalucía
29590, Málaga. España
E-Mail: jose.rico@dekra.com
Phone: +34 95 261 91 00

With best regards,

JOSE EMILIO RICO
Director of eIDAS Certification Body

This attestation is based on the template version 3.0 as of 2023-02-20, that was approved for use by ACAB-c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• DEKRA Testing and Certification S.A.U, C/ Severo Ochoa 2 y 6. Parque tecnológico de Andalucía, 29590 Malaga, Spain, registered under “Registro Mercantil de Madrid, folio 92, inscripción 1ª.” • Accredited by ENAC under registration 134/C-PR337 for the certification of trust services according to “UNE-EN ISO/IEC 17065:2012” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”. Attestation of accreditation link: https://www.enac.es/documents/7020/9a29e298-3657-408e-b140-a8e70bf9dc09 • Insurance Carrier (BRG section 8.2):Allianz • Third-party affiliate audit firms involved in the audit:None.
Identification and qualification of the audit team
• Number of team members: 1 Lead auditor, 1 auditor and 1 technical expert. • Academic qualifications of team members: Lead auditor and auditor have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: • All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the

basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: None. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. • Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management
• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	Firmaprofesional S.A., Paseo Bonanova 47, 08017 Barcelona, Spain, registered under “Registro Mercantil de Barcelona, el 9 de noviembre de 2001, tomo 33996, folio 143, hoja B240292, inscripción primera.”.

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2022-03-28 to 2023-03-27
Audit dates:	2023-03-29 to 2023-05-29
Audit location:	CA - Av. de la Torre Blanca, 57. Edificio ESADECREAPOLIS. Barcelona 08173 Spain. CA- Edif. Caoba C/ Valportillo Primera, 22-24, 1ª. Madrid 28108 Spain. CPD - Calle José Agustín Goytisolo, 10-12. Barcelona 08908 Spain. CPD - PTV: Carrer dels Artesans, 7. Barcelona 08290 Spain.

Root 1: Autoridad de Certificacion Firmaprofesional CIF A62634068

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.4.1 (2021-11) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: ☒ EV SSL Certificate Guidelines, version 1.8.0 ☒ Baseline Requirements, version 2.0.0 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403-1 V2.3.1 (2020-06) ☒ ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

1. (CPS) Declaración de Prácticas de Certificación (CPS) de Firmaprofesional, S.A., version 230413 as of 2023-04-13
2. (CP) Política de Certificación. Certificados de firma electrónica, version 220510 as of 2022-05-10
3. (CP) Política de Certificación. Certificados de Sello Electrónico, version 230216 as of 2023-02-16
4. (CP) Política de Certificación. Certificados de Autenticación de sitios Web, version 220615 as of 2022-06-15
5. (CP) Política de Certificación. Certificados de Servicio Seguro, version 220615 as of 2022-06-15
6. (CP) Política de Servicio Cualificado. AUTORIDAD DE SELLADO CUALIFICADO DE TIEMPO DE FIRMAPROFESIONAL (TSA), version 220513 as of 2022-05-13

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.10 Collection of evidence

The audit team did not find any measure that could guarantee the integrity of the records generated by the systems in qualified time stamp service. [REQ-7.10-02]

Findings with regard to ETSI EN 319 411-1:

6.6.1 Certificate profile

Even though both, the certificates and the profiles, comply with ETSI standards. some documentary inconsistencies were found [GEN-6.6.1-02]

Findings with regard to ETSI EN 319 411-2:

None.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1832338, Firmaprofesional: 2023 - Ensure Timestamp service Logs Integrity: https://bugzilla.mozilla.org/show_bug.cgi?id=1832338
- Bug 1832342, Firmaprofesional: 2023 - documentary inconsistency: https://bugzilla.mozilla.org/show_bug.cgi?id=1832342
- Bug 1771722, Firmaprofesional: 2022 - Title field: https://bugzilla.mozilla.org/show_bug.cgi?id=1771722
- Bug 1771727 , Firmaprofesional: 2022 - Define Device Obsolescence Process: https://bugzilla.mozilla.org/show_bug.cgi?id=1771727
- Bug 1771724, Firmaprofesional: 2022 - CPS without correct explanation about difference between OCSP and CRL: https://bugzilla.mozilla.org/show_bug.cgi?id=1771724
- Bug 1769240, Firmaprofesional: 2022 - SSL certificates issued with wrong Organization ID number: https://bugzilla.mozilla.org/show_bug.cgi?id=1769240
- Bug 1771715, Firmaprofesional: 2022 - StateorProvince field: https://bugzilla.mozilla.org/show_bug.cgi?id=1771715

The remediation measures taken by Firmaprofesional as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C = ES, CN = Autoridad de Certificacion Firmaprofesional CIF A62634068	04048028BF1F2864D48F9AD4D83294366A828856553F3B14303F90147F5D40EF	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, OVCP
CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	57DE0583EFD2B26E0361DA99DA9DF4648DEF7EE8441C3B728AFA9BCDE0F9B26A	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, OVCP

Table 1: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
C = ES, O = Firmaprofesional S.A., OU = Certificados Cualificados, serialNumber = A62634068, CN = AC Firmaprofesional - CUALIFICADOS	4CCF17C0C8C1C10D5876EC5E3280FE8D134DF36AEDD8444289B990BC3741E74F	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd	not defined
CN=AC Firmaprofesional - CUALIFICADOS, serialNumber=A62634068, OU=Certificados Cualificados, O=Firmaprofesional S.A., C=ES	2B75CC4F36759CFC4C6637B1E0E54359457DB57E74DE4D2DC5D02CDDFF2960CF	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd	not defined

CN= AC Firmaprofesional - Secure Web 2021 OU= Security Services OI= VATES-A62634068 O= Firmaprofesional S.A. C= ES	59228535D114E8D29F9B92D422518BC63DDCB57097428D8CC98777D907C6EEFE	ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, OVCP	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)
CN=AC Firmaprofesional - Secure Web 2022, OU=Security Services, 2.5.4.97=VATES-A62634068, O=Firmaprofesional S.A., C=ES	C068D776784255772BBC6AE9F70A536A410AD688A50DDEAFBF66BCC5254796F6	ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, OVCP	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)
CN=AC Firmaprofesional - Timestamp2021, OU=Security Services,2.5.4.97=VATES-A62634068,O=Firmaprofesional S.A.,C=ES	75B14D4D63806F30F538060F2EB65C1365BFC0CD7F3ECDC6C0070218B6E46759	ETSI EN 319 411-2 V2.4.1, QCP-l	1.3.6.1.5.5.7.3.8 (id-kp - timeStamping)
C = ES, O = SIGNE S.A., organizationIdentifier = VATES-A11029279, OU = Autoridad de Certificacion, CN = SIGNE Autoridad de Certificacion - 2020	B8DF384F1FCD6ECB3F4D7DD6380E54D354C61256560A599D80453247D93AF5EA	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection)
C = ES, emailAddress = ca1@firmaprofesional.com, L = C/ Muntaner 244 Barcelona, OU = Consulte http://www.firmaprofesional.com, OU = Jerarquia de Certificacion Firmaprofesional, O = Firmaprofesional S.A. NIF A-62634068, CN = AC Firmaprofesional - CA1	ECC4F857AF93F7C7EF742CA9C35454F424BC4B9EE3B0DE638570F581D601DDC6	ETSI EN 319 411-2 V2.4.1, QCP-l	not defined

Table 2: Sub-CA’s issued by the Root-CA or its Sub-CA’s in scope of the audit

Root 2: FIRMAPROFESIONAL CA ROOT-A WEB

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.4.1 (2021-11) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: ☒ EV SSL Certificate Guidelines, version 1.8.0 ☒ Baseline Requirements, version 2.0.0 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403-1 V2.3.1 (2020-06) ☒ ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

7. (CPS) Declaración de Prácticas de Certificación (CPS) de Firmaprofesional, S.A., version 230413 as of 2023-04-13
8. (CP) Política de Certificación. Certificados de Autenticación de sitios Web, version 220615 as of 2022-06-15
9. (CP) Política de Certificación. Certificados de Servicio Seguro, version 220615 as of 2022-06-15

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
None

Findings with regard to ETSI EN 319 411-1:
6.6.1 Certificate profile

Even though both, the certificates and the profiles, comply with ETSI standards. some documentary inconsistencies were found [GEN-6.6.1-02]

Findings with regard to ETSI EN 319 411-2:
None.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1785215, Firmaprofesional: Add "FIRMAPROFESIONAL CA ROOT-A WEB" Root Certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1785215
- Bug 1832342, Firmaprofesional: 2023 - documentary inconsistency: https://bugzilla.mozilla.org/show_bug.cgi?id=1832342

The remediation measures taken by Firmaprofesional as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN=FIRMAPROFESIONAL CA ROOT-A WEB, 2.5.4.97=VATES-A62634068,O=Firmaprofesional SA, C=ES	BEF256DAF26E9C69BDEC1602359798F3CAF71821A03E018257C53C65617F3D4A	ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, OVCP

Table 3: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
CN=FIRMAPROFESIONAL ICA A01 QWAC 2022, 2.5.4.97=VATES-A62634068, O=Firmaprofesional SA, C=ES	CC1B9F9E4370FB68141D28A115EAA863F8EADB7A04E2BD23B3C62F9D9F17C263	ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, OVCP	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)
CN=FIRMAPROFESIONAL ICA A02 NO QWAC 2022,2.5.4.97=VATES-A62634068,O=Firmaprofesional SA,C=ES	22FD54F933B17F458942C345E3AE625E405CE40B191B316B887CA3D02CCAC3B1	ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, OVCP	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)

Table 4: Sub-CA’s issued by the Root-CA or its Sub-CA’s in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2023-06-01	Initial attestation

End of the audit attestation letter.