TLS BR Audit Attestation for

Firmaprofesional S.A.

Reference: 2403_FPR_FR

"Madrid, 2024-06-03"

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.

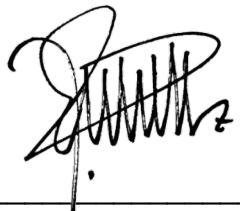
This present Audit Attestation Letter is registered under the unique identifier number 2403_FPR_FR covers multiple Root-CAs and consists of 10 pages.

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 Malaga, Spain
E-Mail: jose.rico@dekra.com
Phone: +34 95 261 91 00

With best regards,



JOSE EMILIO RICO
Director of eIDAS Certification Body

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 “EN ISO/IEC 17065:2012” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”. 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 and 2 technical experts. • Academic qualifications of team members: All team members 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., Passeig de Gràcia 50-Planta 1, 08007 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:	2023-03-28 to 2024-03-27
Audit dates:	2024-03-11 to 2024-05-29
Audit location:	CA - Passeig de Gracia 50, 2-1. Barcelona 08007 Spain CA - C/ de Cantabria 5 (Ed. Amura). Madrid 28108 Spain DC - Carrer Pablo Iglesias, 56. Barcelona 08908 Spain DC - 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 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.2 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 240520 as of 2024-05-24
2. (CP) Política de Certificación. Certificados de Autenticación de sitios Web, version 240520 as of 2024-05-24

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

Findings with regard to ETSI EN 319 401:
6.2 Terms and Conditions
Contact Information in Certificate practice statement shall be updated. [REQ-6.2-02]

Findings with regard to ETSI EN 319 411-1:
6.6.1 Certificate profile
Some inconsistencies were found in certificates and profiles [GEN-6.6.1-02]

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

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

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

- Bug 1889420, Firmaprofesional: Policy Qualifiers other than id-qt-cps present for certificate:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1889420
- Bug 1891251, Firmaprofesional: Delayed leaf revocation:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1891251

The remediation measures taken by Firmaprofesional S.A. 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
C = ES, CN = Autoridad de Certificacion Firmaprofesional CIF A62634068	04048028BF1F2864D48F9AD4D83294366A828856553F3B14303F90147F5D40EF	ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, OVCP
CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	57DE0583EFD2B26E0361DA99DA9DF4648DEF7EE8441C3B728AFA9BCDE0F9B26A	ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, OVCP

Table 1: Root-CA 1 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
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 V2.5.1, QNCP-W ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, OVCP
C = ES, O = Firmaprofesional S.A., organizationIdentifier = VATES-A62634068, OU = Security Services, CN = AC Firmaprofesional - Secure Web 2024	C3F5326537DB6477C4D7BF830FF5B401A7ADB29707702ADD98E62461F9EE67C7	ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, OVCP

Table 2: Sub-CA’s issued by the Root-CA 1 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 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.2 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 240520 as of 2024-05-24
2. (CP) Política de Certificación. Certificados de Autenticación de sitios Web, version 240520 as of 2024-05-24

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

Findings with regard to ETSI EN 319 401:

6.2 Terms and Conditions

Contact Information in Certificate practice statement shall be updated. [REQ-6.2-02]

Findings with regard to ETSI EN 319 411-1:

6.6.1 Certificate profile

Some inconsistencies were found in certificates and profiles [GEN-6.6.1-02]

Findings with regard to ETSI EN 319 411-2:

None.

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

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

- Bug 1889675, Firmaprofesional: Enable EV Treatment for Firmaprofesional CA Root-A Web: https://bugzilla.mozilla.org/show_bug.cgi?id=1889675
- Bug 1785215, Firmaprofesional: Add "FIRMAPROFESIONAL CA ROOT-A WEB" Root Certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1785215

The remediation measures taken by Firmaprofesional S.A. 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
CN=FIRMAPROFESIONAL CA ROOT-A WEB, 2.5.4.97=VATES-A62634068,O=Firmaprofesional SA, C=ES	BEF256DAF26E9C69BDEC1602359798F3CAF71821A03E018257C53C65617F3D4A	ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, OVCP

Table 3: Root-CA 2 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
CN=FIRMAPROFESIONAL ICA A01 QWAC 2022, 2.5.4.97=VATES-A62634068, O=Firmaprofesional SA, C=ES	CC1B9F9E4370FB68141D28A115EAA863F8EADB7A04E2BD23B3C62F9D9F17C263	ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, OVCP
CN=FIRMAPROFESIONAL ICA A02 NO QWAC 2022,2.5.4.97=VATES-A62634068,O=Firmaprofesional SA,C=ES	22FD54F933B17F458942C345E3AE625E405CE40B191B316B887CA3D02CCAC3B1	ETSI EN 319 411-1 V1.4.1, OVCP

Table 4: Sub-CA’s issued by the Root-CA 2 or its Sub-CA’s in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2024-06-03	Initial attestation

End of the audit attestation letter.