Audit Attestation for

Multicert - Serviços de Certificação Electrónica, S.A.

Reference: PSC-2024-0001_01

Madrid,2024-06-26

To whom it may concern,

This is to confirm that AENOR CONFÍA, S.A. has audited the CAs of the MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A., without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "PSC-2024-0001_01" a single Root-CA and consists of 9 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

AENOR CONFÍA, S.A.
Génova, 6. 28004 Madrid. España
E-Mail: info@aenor.com
Phone: 91 432 60 00

With best regards,

Rafael GARCÍA MEIRO
CEO
2024-06-26

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:	• AENOR CONFÍA, S.A. Génova, 6. 28004 Madrid. España. www.aenor.com • Accredited by ENAC under registration 01/C-PR329 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) respectively. Attestation of accreditation link: https://www.enac.es/documents/7020/5ae31445-73fa-4e16-acc4-78e079375c4f • Insurance Carrier (BRG section 8.2): MAPFRE • Third-party affiliate audit firms involved in the audit: none
Identification and qualification of the audit team:	• Number of team members: 1 Lead auditor • 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):	MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A. Estrada Casal do Canas, Lote 3 Edf. SIBS Alf II 2720-092 Amadora PORTUGAL

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:	2023-04-01 to 2024-03-31
Audit dates:	2024-04-17 2024-04-18 2024-04-19 2024-04-22 2024-04-23 2024-04-26
Audit location:	PORTO – PORTUGAL LISBON – PORTUGAL

Root 1: MULTICERT ROOT CERTIFICATION AUTHORITY 01

Standards considered:	European Standards: • ETSI EN 319 401 v2.3.1 (2021-05) • ETSI EN 319 411-1 v1.3.1 (2021-05) • ETSI EN 319 411-2 v2.4.1 (2021-11) • ETSI EN 319 421, V1.1.1 (2016-03) • ETSI TS 119 495 V.1.6.1 (2022-11) 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 full annual audit was based on the following policy and practice statement documents of the CA / TSP:

1. Multicert Certification Practices Statement, version 16.0, as of 2023-09-08
2. Multicert Certificate Policy, version 10.0, as of 2023-07-01
3. [CPS] Declaração de Práticas de Validação Cronológica, version 6.0, as of 2023-07-01

No major non-conformities have been identified during the audit.

In the following areas, one minor non-conformity has been identified throughout the audit:

Finding regarding:

1. ETSI EN 319 401 - REQ-6.1-03A
2. ETSI EN 319 411-1 GEN-6.5.1-12

The use of a task list on a repository page by Multicert's internal registration authority was presented as a procedure, which, however, does not constitute a formal or approved PKI document.
This task list cannot replace the formal procedure approved by the PKI Management Group.

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

During the audit period Multicert didn’t report any incident on Bugzilla.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID

CN=MULTICERT Root Certification Authority 01,
O=MULTICERT - Serviços de Certificação Electrónica S.A.,
C=PT
	604D32D036895AED3BFEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4	ETSI EN 319 401 v2.3.1
		ETSI EN 319 411-1 v1.3.1, LCP, NCP, NCP+, OVCP, EVCP
		ETSI EN 411-2 v2.4.1, QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QEVCP-w
		ETSI TS 119 495, QCP-w-psd2
		ETSI 319 421 v1.1.1

Table 1: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CAs, 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=MULTICERT Trust Services Certification Authority 005,
OU=Certification Authority,
O=MULTICERT - Serviços de Certificação Electrónica S.A.,
C=PT
	48A153E21E1B8C64DCBDCBA034DAB2EF8527A779A1BA2AA238ACC48A2C6FCACF	ETSI EN 319 411-1 v1.3.1 (LCP, NCP, NCP+)
		ETSI EN 319 411-2 v2.4.1 (QCP-n, QCP-n-qscd, QCP-l, 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)

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU

CN=MULTICERT Trust Services Certification Authority 002,
OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,
C=PT
	82CFDAE3A70B6E375A96ED3CFC912E81A020104A8BA886272B5963ADECA24411	ETSI EN 319 411-1 v1.3.1 (LCP, NCP, NCP+)
		ETSI EN 319 411-2 v2.4.1 (QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd)
			not defined

CN=MULTICERT Certification Authority 002,
OU=Accredited Certification Authority,
O=MULTICERT - Serviços de Certificação Electrónica S.A.,
C=PT
	914A87BDB2B35F73AEF7C213309A230921CD182C5668A6B5C4BE9BFF6A1C03B3	ETSI EN 319 411-1 v1.3.1 (LCP, NCP, NCP+)
		ETSI EN 319 411-2 v2.4.1 (QCP-n, QCP-n-qscd)
			not defined

CN=MULTICERT Timestamping Certification Authority 005,
OU=Certification Authority,
O=MULTICERT - Serviços de Certificação Electrónica S.A.,
C=PT
	E8627AC236183A420E1513839ACEEEF833D27A45512717A9BAFDE8506BB5C1CF	ETSI EN 319 411-1 v1.3.1
		ETSI EN 319 411-2 v2.4.1
		ETSI EN 319 421 v1.1.1
			1.3.6.1.5.5.7.3.8 (id-kp-timeStamping)

CN=MULTICERT Trust Services Certification Authority 001,
OU=MULTICERT Trust Services Provider,
O=MULTICERT - Serviços de Certificação Electrónica S.A.,
C=PT
	3F9B68C7508391B5885855DCE6E15EC7D7C8A03558471056EE286F70E7D5B132	ETSI EN 319 411-1 v1.3.1
		ETSI EN 319 411-2 v2.4.1
		ETSI EN 319 421 v1.1.1
			not defined

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU

CN = MULTICERT ADVANCED CERTIFICATION AUTHORITY 001
OU = CERTIFICATION AUTHORITY
O = MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
C = PT
	EF72A054691F855D52A31988439B75BDE49F03899ADF0EBC142CB96E3483D6F7	ETSI EN 319 411-1 v1.3.1 (LCP, NCP, NCP+)	not defined

CN = MULTICERT ADVANCED CERTIFICATION AUTHORITY 005
OU = CERTIFICATION AUTHORITY
O = MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
C = PT
	24EDD4E503A8D3FDB5FFB4AF66C887359901CBE687A5A0760D10A08EED99A7C3	ETSI EN 319 411-1 v1.3.1 (LCP, NCP, NCP+)	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
			1.3.6.1.5.5.7.3.4 (id-kp-emailProtection)

CN=MULTICERT QWAC Certification Authority 005,
OU=Certification Authority,
O=MULTICERT - Serviços de Certificação Electrónica S.A.,
C=PT
	35A1FAA8C81125666D26F0A6E864DDEAA70431CC1570DC883CF147CD196E4AB6	ETSI EN 319 411-1 v1.3.1 (OVCP, EVCP)
		ETSI EN 319 411-2 v2.4.1 (QEVCP-w)
		ETSI TS 119 495 (QCP-w-psd2)
			1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)
			1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)

Table 2: 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	2024-06-26	Initial Attestation

End of the audit attestation letter.