Audit Attestation for

Multicert - Serviços de Certificação Electrónica, S.A.

Reference: DTNQ.2019.001/08

Porto - Portugal, 2023-06-28

To whom it may concern,

This is to confirm that APCER - Associação Portuguesa de Certificação 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 reference DTNQ.2019.001/08 and consists of 9 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

APCER - Associação Portuguesa de Certificação

O 'Porto Bessa Leite Complex | Rua António Bessa Leite, 1430 - 1º Esq., 4150-074 Porto
E-Mail: info@apcer.pt
Phone: +351 229 993 600
www.apcergroup.com

With best regards,

_____
Paulo Borges
Lead Auditor

_____
José Leitão
APCER CEO

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

I1133/01   **WWW.APCERGROUP.COM | Phone number: 229 993 600**   1 | 9

Identification of the conformity assessment body (CAB):	APCER - Associação Portuguesa de Certificação O 'Porto Bessa Leite Complex | Rua António Bessa Leite, 1430 - 1º Esq., 4150-074 Porto Accredited by IPAC under registration C0009 for the certification of trust services according to ETSI EN 319 403-1 V2.3.1 (2020-06), ETSI TS 119 403-2 v1.2.4 (2020-11), ETSI TS 119 403-3 v1.1.1 (2019-03) respectively. (http://www.ipac.pt/pesquisa/ficha_ocp.asp?id=C0009) Insurance Carrier: Hiscox, S.A. Insurance policy number: 2018868
Identification and qualification of the audit team:	Number of audit team members: 1 Audit members identification: Paulo Jorge Martins Borges Academic qualifications of team members: - Degree in Electrotechnical Engineering - PECB Senior ISO 27001 Lead Auditor and Lead Implementer - PECB Senior ISO 22301 Lead Auditor - PECB Senior ISO 27032 Cybersecurity Manager - PECB ISO 20000 Lead Auditor - PECB Management Systems Auditor - PECB Accredited Trainer on ISO 27001, 20000, 22301, 27032 and SCADA Security - PKI Auditor since 2006, with 68 international audits - eIDAS Auditor since 2016, with 42 international audits - Uptime Institute Datacenter ATS expert, ATP, AOS Expert and AOP, ASA - SWIFT Accredited Auditor Additional competences of team members: 36 years of international ICT and Information Security consultancy, training, and audits - APCER ISO 27001 certification auditor since 2012 - BUREAU VERITAS ISO 27001 certification auditor since 2023 - APCER eIDAS certification auditor since 2016 - PECB ISO 27001, ISO 22301 and ISO 20000 auditor since 2018 - ISO 31000 and ISO 27005 Risk Management Expert - National Security Auditor accredited by GNS (Portuguese eIDAS Supervisor Body) - Former Navy Officer responsible for fleet communications encryption 12 years as IBM Mainframes systems engineer - Extensive knowledge of ETSI standards - English and French reading and writing rate A Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence based on 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 attestation is based on the template version 3.0 as of 2023-02-20, that was approved for use by ACAB-c.

I1133/01　　　　　**WWW.APCERGROUP.COM** \| **Phone number: 229 993 600**　　　　　2 \| 9

	• Auditors code of conduct including independence statement: Code of Conduct as of Annex A, ETSI EN 319 403-1
Identification and qualification of the reviewer performing audit quality management:	• Number of Reviewers 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 trust service provider (TSP):	Multicert - Serviços de Certificação Electrónica, S.A. Lagoas Park - Edifício 3, Piso 3 2740-266 Porto Salvo – Oeiras Portugal

Type of audit:	Period of time, full audit.
Audit Period covered for all policies:	2022-04-07 to 2023-03-31
Audit dates:	2023-04-03, 2023-04-05, 2023-04-12, 2023-05-06 (Presential) 2023-04-04, 2023-04-06, 2023-04-10 (Remote)
Audit Location:	PORTO LISBON

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

I1133/01   WWW.APCERGROUP.COM | Phone number: 229 993 600   3 | 9

Standards considered:	European Standards:
	ETSI EN 319 401, V2.3.1 (2021-05)
	ETSI EN 319 411-1, V1.3.1 (2021-05)
	ETSI TS 119 412-1, v1.4.1 (2020-07)
	CA Browser Forum Requirements:
	Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, version 1.8.6
	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)

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

The full annual audit was based on the following policy and practice statement documents of the TSP:

1. Multicert Certification Practices Statement, version 14.0, as of 2023-01-14

2. Multicert Certificate Policy, version 9.0, as of 2023-01-14

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

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

Findings regarding ETSI EN 319 401:

REQ-7.6-02 and REQ-7.6-05
a) The definition of the rules for physical security, in relation to the new PKI Datacenter, , does not include, at level 3, the space where the dedicated Multicert communications rack is installed on the communications room. The doors of this rack were found to be without proper access control to its interior.
b) The door of the Subject SSCD provisioning compartment does not automatically retract.

REQ-7.6-03
There was evidence of lack of labelling of communications and energy cables, some of them placed after the physical security audit of the new PKI Datacenter, carried out in May 2022.
It should also be noted that Wi-Fi antennas were found on routers installed in the communications rack on level 3, which is installed in the communications room.

REQ-7.6-04
Evidence was recorded of the existence of a visit to the secondary Datacenter, during an ISO 27001 internal audit, which is not in the logbook used as a register for all visits to this compartment.

Findings regarding ETSI EN 319 411-1:

None.

Findings regarding ETSI EN 319 411-2:

None.

The non-conformity has been scheduled to be addressed by the corrective action plan of the Trust Service Provider, previously approved by the Lead Auditor.

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

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

I1133/01   **WWW.APCERGROUP.COM** | **Phone number: 229 993 600**   5 | 9

Distinguished Name	SHA-256 fingerprint	Applied policy OID
CN=MULTICERT Root Certification Authority 01, O=MULTICERT - Serviços de Certificação Electrónica S.A., C=PT	604D32D036895AED3BFEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4	ETSI EN 319 411-1 v1.3.1, LCP, NCP, NCP+, OVCP

Table 1: Root-CA in scope of the audit

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

I1133/01   **WWW.APCERGROUP.COM** | **Phone number: 229 993 600**   6 | 9

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:

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
MULTICERT Certification Authority 002	Non-Qualified Electronic Signatures	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+)	not defined
MULTICERT Advanced Certification Authority 001	Non-Qualified Electronic Signatures	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
MULTICERT Advanced Certification Authority 005	Non-Qualified Electronic Signatures	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)
MULTICERT SSL Certification Authority 005 **Note:** Signed by MULTICERT Root Certification Authority 01	Non-Qualified Website Authentication	CN=MULTICERT SSL Certification Authority 005, OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A., C=PT	41E1F1B8DBDD05D8AD04F2CA8A7342F461D99D79E7B466D49284B1909C28E2D8	ETSI EN 319 411-1 v1.3.1 (LCP, OVCP)	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)

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

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
MULTICERT SSL Certification Authority 001 **Note:** Signed by MULTICERT Root Certification Authority 01	Non-Qualified Website Authentication	CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A., C=PT	FF453A5413EA558FE7062AB6FE8310 73E7F30FE6BA75B82EAD5209DB0775 CAD0	ETSI EN 319 411-1 v1.3.1 (LCP, OVCP)	not defined
MULTICERT SSL Certification Authority 001 **Note:** Signed by Global Chambersign Root – 2008	Non-Qualified Website Authentication	CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A., C=PT	06A57D1CD5879FBA2135610DD8D72 5CC268D2A6DE8A463D424C4B9DA89 848696	ETSI EN 319 411-1 v1.3.1 (LCP, OVCP)	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

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

I1133/01   **WWW.APCERGROUP.COM** | **Phone number: 229 993 600**   8 | 9

Modification record

Version	Issuing Date	Changes
Version 1	2023-06-22	Initial Attestation
Version 1.1	2023-06-28	Final Version after revisions

End of the audit attestation letter.

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

I1133/01   **WWW.APCERGROUP.COM** | **Phone number: 229 993 600**   9 | 9