Audit Attestation for

Multicert - Serviços de Certificação Electrónica, S.A.

Reference: DTQ.2017.001/19

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 DTQ.2017.001/19 and consists of 10 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,

Assinado por: **Paulo Jorge Martins Borges**
Num. de Identificação: 05934012
Data: 2023.06.28 10:54:39 +0100

CHAVE MÓVEL

Assinado com Assinatura Digital Qualificada por:
JOSÉ FRANCISCO PIRES GROSSO CARDOSO LEITÃO
CEO
APCER - ASSOCIAÇÃO PORTUGUESA DE CERTIFICAÇÃO
Com procuração com delegação de competências.
Data: 28-06-2023 12:38:55

globaltrustedsign.com

_____

Paulo Borges
Lead Auditor

_____

José Leitão
APCER CEO

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.

	• 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, 2023-04-23, 2023-05-06 (Presential) 2023-04-04, 2023-04-06, 2023-04-10, 2023-05-02, 2023-05-03 (Remote)
Audit Location:	PORTO LISBON

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 319 412-1, v1.4.4 (2021-05) ETSI EN 319 412-2, v2.2.1 (2020-07) ETSI EN 319 412-3, v1.2.1 (2020-07) ETSI EN 319 412-4, v1.2.1 (2021-11) ETSI EN 319 412-5, v2.3.1 (2020-04) ETSI TS 119 412-1, v1.4.1 (2020-07) ETSI TS 119 495, v1.6.1 (2022-011) ETSI EN 319 421, V1.1.1 (2016-03) ETSI EN 319 422, v1.1.1 (2016-03) CA Browser Forum Requirements: EV SSL Certificate Guidelines, version 1.8.0 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)

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
3. [CPS] Declaração de Práticas de Validação Cronológica, version 5.0, as of 2022-03-31

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:

Evidence was recorded regarding the issue of qualified electronic signature certificates with a 5-year validity period, which is longer than the one defined by Multicert's documentation in force.

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.

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 319 401 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 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-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 Trust Services Certification Authority 005	Qualified Electronic Signatures	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)	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection)

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
MULTICERT Trust Services Certification Authority 002	Qualified Electronic Signatures	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)	not defined
MULTICERT Certification Authority 002	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+) ETSI EN 319 411-2 v2.4.1 (QCP-n, QCP-n-qscd)	not defined
MULTICERT Trust Services Certification Authority 005	Qualified Electronic Seals	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-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)
MULTICERT Trust Services Certification Authority 002	Qualified Electronic Seals	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 v2.3.1 (QCP-l, QCP-l-qscd)	not defined

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
MULTICERT Timestamping Certification Authority 005	Qualified Time Stamps	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)
MULTICERT Trust Services Certification Authority 001	Qualified Time Stamps	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
MULTICERT QWAC Certification Authority 005	Qualified Website Authentication	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 (LCP, OVCP, NCP, EVCP) ETSI EN 319 411-2 v2.4.1 (QEVCP-w)	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
MULTICERT SSL Certification Authority 001 Note: Signed by MULTICERT Root Certification Authority 01	Qualified Website Authentication	CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A., C=PT	FF453A5413EA558FE7062AB6FE831073E7F30FE6BA75B82EAD5209DB0775CAD0	ETSI EN 319 411-1 v1.3.1 (LCP, OVCP, NCP, EVCP) ETSI EN 319 411-2 v2.4.1 (QEVCP-w)	not defined

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
MULTICERT SSL Certification Authority 001 Note: Signed by Global Chambersign Root – 2008	Qualified Website Authentication	CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A., C=PT	06A57D1CD5879FBA2135610DD8D725CC268D2A6DE8A463D424C4B9DA89848696	ETSI EN 319 411-1 v1.3.1 (LCP, OVCP, NCP, EVCP) ETSI EN 319 411-2 v2.4.1 (QEVCP-w)	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

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.