Audit Attestation for

Multicert - Serviços de Certificação Electrónica, S.A.

Reference: DTQ.2017.001/16

Porto - Portugal, 2021-07-17

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.2017.001/16 and consists of 13 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: 2021.07.20 09:33:35 +0100

CARTÃO DE CIDADÃO

Paulo Borges
Lead Auditor

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: 26-07-2021 17:00:21

globaltrustedsign.com

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 • PECB Senior ISO 22301 Lead Auditor • PECB Senior Cybersecurity Manager • PECB ISO 20000 Lead Auditor • PECB Management Systems Auditor • PKI Auditor since 2006, with more than 40 international audits • eIDAS Auditor since 2016, with more than 20 international audits • Uptime Institute Datacenter ATS and AOS Expert Additional competences of team members: • 36 years of international ICT and Information Security consultancy, training, and audits • PECB trainer for ISO 27001, ISO 22301, ISO 20000, Cybersecurity and SCADA • APCER ISO 27001 certification auditor since 2012 • 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) • Portuguese 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 incl. 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

Audit Period covered for all policies:	2020-04-07 to 2021-04-06
Audit dates:	2021-04-12 to 2021-04-21 (full audit period, on remote) 2021-04-14 and 2021-04-15 (on site)
Audit Location:	Registration Authorities – PORTO and LISBON (on site and remote) CA and personalization services – PORTO and LISBON (on site) Dissemination Services – PORTO and LISBON (remote) Revocation Services – PORTO (remote)

Identification of the audited Root-CA:	Name of the root, e.g. common Name	
MULTICERT Root Certification Authority 01	Distinguished Name	CN = MULTICERT Root Certification Authority 01 O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
	SHA-256 fingerprint	604D32D036895AED3BFEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4
	Certificate Serial number	544DA5BC4035565A
	Applied policy	Multicert Certification Practices Statement (v10.0) Multicert Certificate Policy (v6.0)

The audit was performed as full period of time audit at the TSP's location in Lisbon and Porto, Portugal.

It took place from 2021-04-12 to 2021-04-21 and covered the period from 2020-04-07 to 2021-04-06.

The audit was performed according to the European Standards:

"ETSI EN 319 411-1, V1.2.2 (2018-04)"; "ETSI EN 319 411-2, V2.1.1 (2016-02)", and "ETSI EN 319 401, V2.2.1 (2018-04)"

as well as CA Browser Forum Requirements:

"EV SSL Certificate Guidelines, version 1.7.5" and "Baseline Requirements, version 1.7.4"

considering the requirements of the:

"ETSI EN 319 403-1 V2.3.1 (2020-06)" and "ETSI TS 119 403-2 V1.2.4 (2020-11)" for the Trust Service Provider Conformity Assessment.

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

1. Multicert Certification Practices Statement, version 10.0, as of 2020-12-17
2. Multicert Certificate Policy (v6.0), version 6.0, as of 2020-12-17

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

Findings about ETSI EN 319 401:

5. – Risk Assessment

Requirement REQ-5-04

The existence of risk treatment measures with outdated dates was evidenced, without proper justification, without identification of a new implementation date, nor identification of the possible impacts of non-compliance with the execution dates.

6.1 – Trust Service Practice Statement

Requirements REQ-6.1-03, 04 and 08

The use of digital document files in a shared folder provided by a local servers on an External Registration Authority is not defined by the MULTICERT_PR.CQ_13990 procedure, and the respective access and securitization rules are not formally defined.

This change was introduced in an uncontrolled manner in relation to the practices identified in the current procedure.

7.6 – Physical and environmental security

Requirements REQ.7-01; REQ.8-01, 02, 03, 05 and 08

The use of a communications equipment (4G router) at HAS (High Security Area) level 3 was detected to support the execution of the installation of new servers.

It was evidenced that this implementation was carried out without the respective risk analysis, adequate security controls for the described objective, nor obtained the respective authorization for the use of wireless communications.

In addition, the audited risk analysis does not identify any risk situation regarding the use of level 3 for this type of staging, nor for the support of 4G wireless communications.

Findings about ETSI EN 319 411-1:

None.

Findings about ETSI EN 319 411-2:

None.

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

During the audit period Multicert didn't report any incident on Bugzilla related to digital qualified services.

The Sub-CA that has been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below.

The TSP assured that all non-revoked Sub-CA that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits.

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	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, NCP, NCP+) EN 319 411-2 v2.2.2 (QCP-n, QCP-n-qscd) EN 319 412-1 v1.1.1 EN 319 412-2 v2.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1	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 Signatures	CN = MULTICERT Trust Services Certification Authority 002 OU = Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT	82CFDAE3A70B6E375A96ED3CFC912E81A020104A8BA886272B5963ADECA24411	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, NCP, NCP+) EN 319 411-2 v2.2.2 (QCP-n, QCP-n-qscd) EN 319 412-1 v1.1.1 EN 319 412-2 v2.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1	not defined

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
MULTICERT Certification Authority 002	Qualified Electronic Signatures	CN = MULTICERT Certification Authority 002 OU = Accredited Certification AuthorityO = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT	914A87BDB2B35F73AEF7C213309A230921CD182C5668A6B5C4BE9BFF6A1C03B3	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, NCP, NCP+) EN 319 411-2 v2.2.2 (QCP-n, QCP-n-qscd) EN 319 412-1 v1.1.1 EN 319 412-2 v2.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1	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	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, NCP, NCP+) EN 319 411-2 v2.2.2 (QCP-l, QCP-l-qscd) EN 319 412-1 v1.1.1 EN 319 412-3 v1.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1	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	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, NCP, NCP+) EN 319 411-2 v2.2.2 (QCP-l, QCP-l-qscd) EN 319 412-1 v1.1.1 EN 319 412-3 v1.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1	not defined

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
MULTICERT Certification Authority 002	Qualified Electronic Seals	CN = MULTICERT Certification Authority 002OU = Accredited Certification AuthorityO = MULTICERT - Serviços de Certificação Electrónica S.A.C = PT	914A87BDB2B35F73AEF7C213309A230921CD182C5668A6B5C4BE9BFF6A1C03B3	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, NCP, NCP+) EN 319 411-2 v2.2.2 (QCP-l, QCP-l-qscd) EN 319 412-1 v1.1.1 EN 319 412-3 v1.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1	not defined
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	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 EN 319 411-2 v2.2.2 EN 319 412-1 v1.1.1 EN 319 421 v1.1.1 EN 319 422 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	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 EN 319 411-2 v2.2.2 EN 319 412-1 v1.1.1 EN 319 421 v1.1.1 EN 319 422 v1.1.1	not defined

Intermediate CA	Trust Service	Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
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	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, OVCP, NCP, EVCP) EN 319 411-2 v2.2.2 (QCP-w) EN 319 412-1 v1.1.1 EN 319 412-4 v1.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1 ETSI TS 119 495 v1.4.1 CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.7.4 CA/Browser Forum Guidelines for The Issuance And Management Of Extended Validation Certificates v1.7.5	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)

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	Qualified Website Authentication	CN = MULTICERT SSL Certification Authority 001, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT	FF453A5413EA558FE7062AB6FE831073E7F30FE6BA75B82EAD5209DB0775CAD0	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, OVCP, NCP, EVCP) EN 319 411-2 v2.2.2 (QCP-w) EN 319 412-1 v1.1.1 EN 319 412-4 v1.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1 ETSI TS 119 495 v1.4.1 CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.7.4 CA/Browser Forum Guidelines for The Issuance And Management Of Extended Validation Certificates v1.7.5	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	EN 319 401 v2.2.1 EN 319 411-1 v1.2.2 (LCP, OVCP, NCP, EVCP) EN 319 411-2 v2.2.2 (QCP-w) EN 319 412-1 v1.1.1 EN 319 412-4 v1.1.1 EN 319 412-5 v2.2.1 ETSI TS 119 412-1 v1.3.1 ETSI TS 119 495 v1.4.1 CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.7.4 CA/Browser Forum Guidelines for The Issuance And Management Of Extended Validation Certificates v1.7.5	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 1: Sub-CA's issued by the Root-CA or its Sub-CA's

Modification record

Version	Issuing Date	Changes
Version 1	2021-07-17	Initial Attestation

End of the audit attestation letter.