## Audit Attestation for

## Multicert - Serviços de Certificação Electrónica, S.A.

## Reference: DTNQ.2019.001/06

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 DTNQ.2019.001/06 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,

Assinado por : **PAULO JORGE MARTINS BORGES**
Num. de Identificação: 05934012
Data: 2021.07.20 09:24:12 +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

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

| | |
|---|---|
| Identification of the conformity assessment body (CAB): | APCER - Associação Portuguesa de Certificação<br>O 'Porto Bessa Leite Complex \| Rua António Bessa Leite, 1430 - 1º Esq., 4150-074 Porto<br>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)<br>Insurance Carrier:<br>Hiscox, S.A.<br>Insurance policy number: 2018868 |
| Identification and qualification of the audit team: | Number of audit team members: 1<br>Audit members identification: Paulo Jorge Martins Borges<br>Academic qualifications of team members:<br>• Degree in Electrotechnical Engineering<br>• PECB Senior ISO 27001 Lead Auditor<br>• PECB Senior ISO 22301 Lead Auditor<br>• PECB Senior Cybersecurity Manager<br>• PECB ISO 20000 Lead Auditor<br>• PECB Management Systems Auditor<br>• PKI Auditor since 2006, with more than 40 international audits<br>• eIDAS Auditor since 2016, with more than 20 international audits<br>• Uptime Institute Datacenter ATS and AOS Expert<br>Additional competences of team members:<br>• 36 years of international ICT and Information Security consultancy, training, and audits<br>• PECB trainer for ISO 27001, ISO 22301, ISO 20000, Cybersecurity and SCADA<br>• APCER ISO 27001 certification auditor since 2012<br>• APCER eIDAS certification auditor since 2016<br>• PECB ISO 27001, ISO 22301 and ISO 20000 auditor since 2018<br>• ISO 31000 and ISO 27005 Risk Management Expert<br>• National Security Auditor accredited by GNS (Portuguese eIDAS Supervisor Body)<br>• Portuguese navy officer responsible for fleet communications encryption<br>• 12 years as IBM Mainframes systems engineer<br>• Extensive knowledge of ETSI standards<br>• English and French reading and writing rate A<br>• Types of professional experience and practical audit experience:<br>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.<br>• Auditors code of conduct incl. independence statement:<br>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<br>• 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.<br>Lagoas Park - Edifício 3, Piso 3<br>2740-266 Porto Salvo – Oeiras<br>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)<br>2021-04-14 and 2021-04-15 (on site) |
| Audit Location: | Registration Authorities – PORTO and LISBON (on site and remote)<br>CA and personalization services – PORTO and LISBON (on site)<br>Dissemination Services – PORTO and LISBON (remote)<br>Revocation Services – PORTO (remote) |

# Audit Attestation Multicert DTNQ.2019.001/06

| 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<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT |
| | SHA-256 fingerprint | 604D32D036895AED3BFEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4 |
| | Certificate Serial number | 544DA5BC4035565A |
| | Applied policy | Multicert Certification Practices Statement (v10.0)<br>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)” and “ETSI EN 319 401, V2.2.1 (2018-04)”

as well as CA Browser Forum Requirements:

“Baseline Requirements, version 1.7.4”

and 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 "back office" tool was used by the External Registration Authority was replaced in December 2020.

This change was executed in an uncontrolled manner in relation to the functional and safety practices identified in the current Multicert 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.

This Audit Attestation also covers the following incidents as documented under for non-qualified digital services:

- Bug 1680083, Camerfirma: certificate with an incorrect OrganizationName

  https://bugzilla.mozilla.org/show_bug.cgi?id=1680083

- Bug 1637093, Multicert: AIA CA Issuer field pointing to PEM encoded cert

  https://bugzilla.mozilla.org/show_bug.cgi?id=1637093

The remediation measures taken by MULTICERT as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

The long-term effectiveness of the measures will be rechecked at the next regular audit.

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 Certification Authority 002 | Non-Qualified Electronic Signatures | CN = MULTICERT Certification Authority 002<br>OU = Accredited Certification Authority<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT | 914A87BDB2B35F73AEF7C213309A230921CD182C5668A6B5C4BE9BFF6A1C03B3 | EN 319 401 v2.2.1<br>EN 319 411-1 v1.2.2 (LCP, NCP, NCP+)<br>ETSI TS 119 412-1 v1.3.1 | not defined |
| MULTICERT Advanced Certification Authority 001 | Non-Qualified Electronic Signatures | CN = MULTICERT Advanced Certification Authority 001<br>OU = Certification Authority<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT | EF72A054691F855D52A31988439B75BDE49F03899ADF0EBC142CB96E3483D6F7 | EN 319 401 v2.2.1<br>EN 319 411-1 v1.2.2 (LCP, NCP, NCP+)<br>ETSI TS 119 412-1 v1.3.1 | not defined |
| MULTICERT Advanced Certification Authority 005 | Non-Qualified Electronic Signatures | CN = MULTICERT Advanced Certification Authority 005<br>OU = Certification Authority<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT | 24EDD4E503A8D3FDB5FFB4AF66C887359901CBE687A5A0760D10A08EED99A7C3 | EN 319 401 v2.2.1<br>EN 319 411-1 v1.2.2 (LCP, NCP, NCP+)<br>ETSI TS 119 412-1 v1.3.1 | 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)<br>1.3.6.1.5.5.7.3.4 (id-kp-emailProtection) |
| MULTICERT SSL Certification Authority 005<br>**<u>Note:</u>**<br>Signed by<br>MULTICERT Root Certification Authority 01 | Non-Qualified<br>Website Authentication | CN = MULTICERT SSL Certification Authority 005<br>OU = Certification Authority<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT | 41E1F1B8DBDD05D8AD04F2CA8A7342F461D99D79E7B466D49284B1909C28E2D8 | EN 319 401 v2.2.1<br>EN 319 411-1 v1.2.2 (LCP, OVCP)<br>Cab/Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates v1.7.4 | 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)<br>1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) |

This attestation is based on the template version 2.8 as of 2021-04-21, 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 005<br>**Note:**<br>Signed by<br>Global Chambersign Root – 2008 | Non-Qualified<br>Website Authentication | CN = MULTICERT SSL Certification Authority 005<br>OU = Certification Authority<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT | 0F17E376FE94E582D6EE649CDC516FF977E765C561AE087F31A3F5E8E66CCECD | EN 319 401 v2.2.1<br>EN 319 411-1 v1.2.2 (LCP, OVCP)<br>Cab/Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates v1.7.4 | 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)<br>1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) |
| MULTICERT SSL Certification Authority 001<br>**Note:**<br>Signed by<br>MULTICERT Root Certification Authority 01 | Non-Qualified<br>Website Authentication | CN = MULTICERT SSL Certification Authority 001<br>OU = Certification Authority<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT | FF453A5413EA558FE7062AB6FE831073E7F30FE6BA75B82EAD5209DB0775CAD0 | EN 319 401 v2.2.1<br>EN 319 411-1 v1.2.2 (LCP, OVCP)<br>Cab/Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates v1.7.4 | not defined |
| MULTICERT SSL Certification Authority 001<br>**Note:**<br>Signed by<br>Global Chambersign Root – 2008 | Non-Qualified<br>Website Authentication | CN = MULTICERT SSL Certification Authority 001<br>OU = Certification Authority<br>O = MULTICERT - Serviços de Certificação Electrónica S.A.<br>C = PT | 06A57D1CD5879FBA2135610DD8D725CC268D2A6DE8A463D424C4B9DA89848696 | EN 319 401 v2.2.1<br>EN 319 411-1 v1.2.2 (LCP, OVCP)<br>Cab/Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates v1.7.4 | 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)<br>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.**

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.