

Audit attestation letter

To whom it may concern,

APCER – Associação Portuguesa de Certificação, located in O’Porto Bessa Leite Complex, Rua António Bessa Leite 1430 1º Esq, 4150-074 Porto, Portugal, is an accredited by IPAC with the certificate code C0009 for the certification of trust services according to NP EN ISO/IEC 17065:2014, Regulation (EU) No 910/2014 and ETSI EN 319 403, v2.2.2.

APCER therefore states that the TSP - Trust Services Provider **Multicert - Serviços de Certificação Electrónica, S.A.** was audited by the eIDAS qualified auditor **Paulo Jorge Martins Borges** for the following trust service: **“Non-Qualified certificates for website authentication”**.

Audit period:

The period of time audit was carried out remotely at TSP sites (Porto and Lisbon, both in Portugal) due to COVID-19 pandemic restrictions.

- Start/end date period covered by the audit: 2019-12-06 / 2020-04-06
- Audit Plan tasks start/end period: 2020-04-15 / 2020-04-28
- On-site audit tasks:
 - 2020-04-18: Multicert CA and RA audit
 - 2020-04-15: CEGER (external registration authority)

A local, in person, physical security controls audit was carried out on 2020-07-07.

Audit methodology:

APCER states that during the period of time above identified the following audit tasks were executed:

- Stage 1 – TSP and PKI documentation and practices
- Stage 2 – Physical security, technical infrastructure, incident and business continuity management
- Stage 3 – Issued specimen certificates for compliance analysis

During the stage 3 evidences were collected and duly analysed in order to ensure the compliance of the issued certificates.

Associated services:

Root CA	<u>MULTICERT Root Certification Authority 01</u>
Distinguished Name:	CN = MULTICERT Root Certification Authority 01 O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
Certificate serial number:	544DA5BC4035565A
SHA-256 fingerprint:	604D32D036895AED3BFEEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4
Applied Policy:	Multicert Certification Practices Statement (v7.0) Multicert Certificate Policy (v5.0)
Validity:	Not Before: Fri Apr 04 2014 09:59:47 GMT+0100 (WEST) Not after: Mon Apr 04 2039 09:59:47 GMT+0100 (WEST)

Intermediate CA's	MULTICERT SSL Certification Authority 005 Signed by MULTICERT Root Certification Authority 01
Distinguished Name:	CN = MULTICERT SSL Certification Authority 005 OU=Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
Certificate serial number:	3079BC698D7C1CC8518CF32D301C4025
SHA-256 fingerprint:	41E1F1B8DBDD05D8AD04F2CA8A7342F461D99D79E7B466D49284B1909C28E2D8
Applied Policy:	Multicert Certification Practices Statement (v7.0) Multicert Certificate Policy (v5.0)
Validity:	Not Before: Mon Dec 09 2019 19:35:00 GMT+0100 (WEST) Not after: Tue Jun 08 2032 19:35:00 GMT+0100 (WEST)

Intermediate CA's	MULTICERT SSL Certification Authority 001 Signed by MULTICERT Root Certification Authority 01
Distinguished Name:	CN = MULTICERT SSL Certification Authority 001 OU=Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
Certificate serial number:	28A0F9A278A99BEA
SHA-256 fingerprint:	FF453A5413EA558FE7062AB6FE831073E7F30FE6BA75B82EAD5209DB0775CAD0
Applied Policy:	Multicert Certification Practices Statement (v7.0) Multicert Certificate Policy (v5.0)
Validity:	Not Before: Tue Dec 12 2017 17:00:08 GMT+0100 (WEST) Not after: Wed Jun 12 2030 17:00:08 GMT+0100 (WEST)

Intermediate CA's	MULTICERT SSL Certification Authority 001 Signed by Global Chambersign Root – 2008
Distinguished Name:	CN = MULTICERT SSL Certification Authority 001 OU=Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
Certificate serial number:	01A4B767C5A58D8E
SHA-256 fingerprint:	06A57D1CD5879FBA2135610DD8D725CC268D2A6DE8A463D424C4B9DA89848696
Applied Policy:	Multicert Certification Practices Statement (v7.0) Multicert Certificate Policy (v5.0)
Validity:	Not Before: Tue Jul 03 2018 13:01:18 GMT+0100 (WEST) Not after: Tue May 20 2025 13:01:18 GMT+0100 (WEST)

Audit Criteria:

The TSP was audited according to the following audit criteria, considering the requirements of the ETSI EN 319 403, V2.2.2 for the Trust Service Provider Conformity Assessment.

Standard	Description
EN 319 401 v2.2.1	General Policy Requirements for Trust Service Providers
EN 319 411-1 v1.2.2	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements Full audit: General requirements, LCP, OVCP
CA/Browser Forum	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.6.9

CA applied Policies:

The TSP **Multicert - Serviços de Certificação Eletrónica, S.A.** has disclosed and maintained effective controls over its key and certificate life cycle management business and CA environmental control practices within the following Certification Practices Statement (CPS) and Certificate Policy (CP) documents:

- Multicert Certification Practices Statement (v7.0)
- Multicert Certificate Policy (v5.0)

Final Remarks:

The above audit shall be considered as a full audit for certification, in order to allow the TSP trust services publication on the TSL - Trust Services List.

The audit was completed successfully without critical findings.

The next audit shall be successfully finalized up to **2021-04-30**, in order to maintain the certificate validity as stated in the corresponding certificate issued by APCER for this TSP.

Audit letter issuance signature:

This audit letter was issued at **2020-08-19**.

This document is electronically signed by:

Lead Auditor

Paulo Borges

APCER CEO

José Leitão