



**Audit Attestation for**

**EADTrust - EuropeanAgency of DigitalTrust S.L.**

**Reference: 2022/7411**

Thiene, 2022-05-27

To whom it may concern,

This is to confirm that “CSQA Certificazioni Srl” has audited the CAs of the **EADTrust - EuropeanAgency of DigitalTrust S.L.** without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number 2022/7411 and consists of 10 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

**CSQA Certificazioni Srl**  
Via S. Gaetano, 74  
36016 Thiene (VI), Italy  
Email: [csqa@csqa.it](mailto:csqa@csqa.it)  
Phone: +39 0445 313011

With best regards,

The Chief Executive Officer

**Subject:** Audit Attestation

<p>Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:</p>	<ul style="list-style-type: none"> <li>• <b>CSQA Certificazioni Srl</b>, Via S. Gaetano, 74, 36016 Thiene (VI) registered under VAT 02603680246</li> <li>• Accredited by the Italian National Accreditation Body (Accredia – <a href="http://www.accredia.it">www.accredia.it</a>) under registration <a href="#">014B</a> for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403 V2.2.2 (2015-08)” and/or “ETSI EN 319 403-1 V2.3.1 (2020-06)” respectively.</li> <li>• Insurance Carrier (BRG section 8.2): Zurich</li> <li>• Third-party affiliate audit firms involved in the audit: none.</li> </ul>
<p>Identification and qualification of the audit team:</p>	<ul style="list-style-type: none"> <li>• Number of team members: 4</li> <li>• Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security.</li> <li>• Additional competences of team members: All team members have knowledge of             <ol style="list-style-type: none"> <li>1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days;</li> <li>2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;</li> <li>3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and</li> <li>4) the Conformity Assessment Body's processes.</li> </ol> <p>Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic.</p> </li> <li>• Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in:             <ol style="list-style-type: none"> <li>a) knowledge of the CA/TSP standards and other relevant publicly available specifications;</li> <li>b) understanding functioning of trust services and information security including network security issues;</li> <li>c) understanding of risk assessment and risk management from the business perspective;</li> <li>d) technical knowledge of the activity to be audited;</li> </ol> </li> </ul>

	<p>e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls.</p> <ul style="list-style-type: none"> <li>• Types of professional experience and practical audit experience: 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. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.</li> <li>• Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor <ul style="list-style-type: none"> <li>a) has acted as auditor in at least three complete TSP audits;</li> <li>b) has adequate knowledge and attributes to manage the audit process; and</li> <li>c) has the competence to communicate effectively, both orally and in writing.</li> </ul> </li> <li>• Special skills or qualifications employed throughout audit: <ul style="list-style-type: none"> <li>○ ISMS Auditor (ISO/IEC 27001)</li> </ul> </li> <li>• Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB.</li> <li>• Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.</li> </ul>
<p>Identification and qualification of the reviewer performing audit quality management:</p>	<ul style="list-style-type: none"> <li>• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1</li> <li>• 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.</li> </ul>
<p>Identification of the CA / Trust Service Provider (TSP):</p>	<p><b>EADTrust - EuropeanAgency of DigitalTrust S.L.,</b> C/ Méntrida, 6 - 28043 - Madrid Registered under nº B-85626240</p>

Type of audit:	<input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input checked="" type="checkbox"/> Period of time, full audit
Audit period covered for all policies:	2021-05-13 to 2022-05-11
Point in time date:	none, as audit was pot audit
Audit dates:	2022-05-03 to 2022-05-11 (remote)
Audit location:	Data center and PKI locations: Calle Alba, 15 - 28043 – MADRID Registration authority locations, CA operations: Calle Méntrida, 6 - 28043 MADRID

Standards considered:	<p>European Standards:</p> <input checked="" type="checkbox"/> ETSI EN 319 411-2, V2.4.1 (2021-11) <input checked="" type="checkbox"/> ETSI EN 319 411-1, V1.3.1 (2021-05) <input checked="" type="checkbox"/> ETSI EN 319 401, V2.3.1 (2021-05)  <p>CA Browser Forum Requirements:</p> <input checked="" type="checkbox"/> EV SSL Certificate Guidelines, version 1.7.9 <input checked="" type="checkbox"/> Baseline Requirements, version 1.8.4  <p>For the Trust Service Provider Conformity Assessment:</p> <input checked="" type="checkbox"/> ETSI EN 319 403 V2.3.1 (2020-06) <input checked="" type="checkbox"/> ETSI TS 119 403-2 V1.2.4 (2020-11)
-----------------------	---

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

1. OPR-PG-V5.0- Declaración\_Prácticas\_Certificación\_DPC\_EADTrust
2. Publicly-Trusted-Certificates-EADTrust-CPS-English-CABForum-ETSI (V2.0)
3. Issuance of Natural Person Certificates (April 2020) (ES)
4. Issuance of Legal Entity Certificates (October 2020) (ES)
5. Issuance of PSD2 Certificates (April 2020) (ES)
6. Issuance of Web Certificates (October 2020) (ES)
7. Timestamp Service Policy (May 2021) (ES)

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

Findings with regard to ETSI EN 319 401:

There is no evidence about the remediation plan adopted by EAD in order to mitigate the vulnerabilities identified during the VA/PT (ref. PT 6/2021 and. SIS-DG-V.6.1-Mapa\_Red\_2022). [REQ-7.9-11]

In the PT report (ref. PT report 6/2021 and PT Report 4/2022) there are no evidence about: skills of the people that performed the test and tool used. [REQ-7.8-15]

During the inspection of the data center, has not been possible to verify that communication between distinct trustworthy systems was established through trusted channels that are isolated using physical separation from other communication channels (there were no usage of proper labelling and identification of the cables and connections). [REQ-7.8-11A]

Findings with regard to ETSI EN 319 411-1:

EADTrust doesn't foresee any recovery measure for CRL. In case of failure of the primary and unique source, they can't offer certificate status check service.[ OVR 6.4.8]

Findings with regard to ETSI EN 319 411-2:

None.

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as documented under:

No incident detected during the period.



Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN=EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019, C=ES O=European Agency of Digital Trust, S.L.	63EE5D2DE73AA95B4D5D0FE0C61A1759537DA69218B941A81D073F42D1337BE4	ETSI EN 319 411-2 V2.4.1 QNCP-w
CN=EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	7962291FEDA249C5F3FF1B6A5A33AB4DDC2FC40B10A08AB1E9479F61D618FD99	ETSI EN 319 411-2 V2.4.1 QEVCP-w
CN=EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	F244A8DB7267CF865CE99A14DC7169395D8B7B989935F9663322DF5EF6679B84	ETSI EN 319 411-2 V2.4.1 QNCP-w
CN=EADTrust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	67475A6A92A843EE017CFCE0ACF44645EC86420389727FB56B1A849EF22DFB01	ETSI EN 319 411-2 V2.4.1 QEVCP-w
CN=EADTrust RSA 4096 Root CA For Qualified Web DV/OV Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	47B3A2D7BD0802788621F37E6B1926EB79C13757628AE9ACEA2034200D3562EC	ETSI EN 319 411-2 V2.4.1; QNCP-w



Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN=EADTrust RSA 4096 Root CA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	BFC95F0875E85C50DE9F73DEDAF65756E706CB2D3293CF72167998978AA90FC8	ETSI EN 319 411-2 V2.4.1 QEVCP-w
CN=EADTrust RSA 8192 Root CA For Qualified Web DV/OV Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	AA290263088C8B92FCD0D361A5F3F2DA8190DB8A78D2753A072122EE9615C940	ETSI EN 319 411-2 V2.4.1 QNCP-w
CN=EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	31C7A29E8DC74BCCC2FE0D965A17E039C3EC5538FF54A8D019FB5DA6C854B748	ETSI EN 319 411-2 V2.4.1 QEVCP-w

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.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
CN=EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	0E1F3A20040ED5B272DCC939E7B8D5B0F4BED764C95CE16CB0A47CA4560A3695	ETSI EN 319 411-2 V2.4.1 QNCP-w	id_kp_serverAuth id-kp-clientAuth
CN=EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	B76911A3352D1A27B3C355F049CF6FBFC5E3E4975BFDBDBC1FA041327FC76D7C	ETSI EN 319 411-2 V2.4.1 QEVCP-w	id_kp_serverAuth id-kp-clientAuth
CN=EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	80AB1BAAC5CAA236E8801792FFC88DDCCE45A930FA30E578DB944D51282E1570	ETSI EN 319 411-2 V2.4.1 QNCP-w	id_kp_serverAuth id-kp-clientAuth
CN=EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	C8792B47355FA3D152AA5E86F37C27650BE1E05137BD36E8778ACF270BB18B54	ETSI EN 319 411-2 V2.4.1 QEVCP-w	id_kp_serverAuth id-kp-clientAuth
CN=EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	072C239E48EE4117F279351A1F39E2B2C85A34DA655243EFF18D99BCB10F914	ETSI EN 319 411-2 V2.4.1; QNCP-w	id_kp_serverAuth id-kp-clientAuth



Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
CN=EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	009DBAD686CECD81D13ACAC4F673DCBA5EEB789E63173CDE136CB2880C1DCE79	ETSI EN 319 411-2 V2.4.1 QEVCP-w	id_kp_serverAuth id-kp-clientAuth
CN=EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	A14616D1E8C0B49E0E21CAE2B542A8351A26747D3A18A45999C38BA1D078B6CB	ETSI EN 319 411-2 V2.4.1 QNCP-w	id_kp_serverAuth id-kp-clientAuth
CN=EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019, C=ES, O=European Agency of Digital Trust, S.L.	514A806A46D7B79725B92CEA06855415D924E76DC5D51E4ED5CA3955CB6EC85D	ETSI EN 319 411-2 V2.4.1 QEVCP-w	id_kp_serverAuth id-kp-clientAuth

**Table 2: Sub-CA’s issued by the Root-CA or its Sub-CA’s in scope of the audit**



**Modifications record**

Version	Issuing Date	Changes
Version 1	2022-05-27	Initial attestation

**End of the audit attestation letter.**