TLS EV Audit Attestation for

Sectigo (Europe) S.L.

Reference: AA2025011701-TLS-EV

Essen, 2025-01-30

To whom it may concern,

This is to confirm that “TÜV NORD CERT GmbH” has audited the CAs of “Sectigo (Europe) S.L.” without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “**AA2025011701-TLS-EV**”, covers multiple Root-CAs and consists of 12 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV NORD CERT GmbH
Business Entity IT
Am TÜV 1
45307 Essen, Germany
E-Mail: info.tncert@tuev-nord.de

With best regards,

Matthias Wiedenhorst	Dr. Silke Keller
Reviewer	Lead Auditor

This attestation is based on the template version 3.3 as of 2024-10-08, that was approved for use by ACAB-c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- TÜV NORD CERT GmbH, Am TÜV 1, 45307 Essen, Germany, registered under HRB 9976, Amtsgericht Essen, Germany
- Accredited by DAkkS under registration D-ZE-12007-01-12[1] for the certification of trust services according to “DIN EN ISO/IEC 17065:2013” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”.
- Insurance Carrier (BRG section 8.2):
  Allianz Global Corporate & Specialty SE
- Third-party affiliate audit firms involved in the audit:
  None.

Identification and qualification of the audit team

- Number of team members: 1 Lead Auditor, 2 Trainee Auditors
- 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.
- Additional competences of team members:
  All team members have knowledge of
  1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days;
  2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;
  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
  4) the Conformity Assessment Body's processes.
  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.
- 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:
  a) knowledge of the CA/TSP standards and other relevant publicly available specifications;
  b) understanding functioning of trust services and information security including network security issues;
  c) understanding of risk assessment and risk management from the business perspective;
  d) technical knowledge of the activity to be audited;
  e) general knowledge of regulatory requirements relevant to TSPs; and

[1] https://www.dakks.de/en/accredited-body.html?id=D-ZE-12007-01-12

f) knowledge of security policies and controls.

- 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.
- Additional qualification and experience Lead Auditor:
  On top of what is required for team members (see above), the Lead Auditor
  a) has acted as auditor in at least three complete TSP audits;
  b) has adequate knowledge and attributes to manage the audit process; and
  c) has the competence to communicate effectively, both orally and in writing.
- Special Credentials, Designations, or Certifications:
  All members are qualified and registered assessors within the accredited CAB.
- 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.

Identification and qualification of the reviewer performing audit quality management

- Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 Reviewer
- 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 CA / Trust Service Provider (TSP):

Sectigo (Europe) S.L., Rambla Catalunya, 86, 3 1, 08008, Barcelona, Spain, registered under "NIF B01683580" at Registro Mercantil de Barcelona, Spain

Type of audit:

☐ Point in time audit
☐ Period of time, after x month of CA operation
☒ Period of time, full audit

Audit period covered for all policies:

2023-11-12 to 2024-10-20

Point in time date:

none, as audit was a period of time audit

Audit dates:

2024-10-21 to 2024-10-24 (on-site)

Audit location:

BD7 1HR, Bradford, United Kingdom
M22 5QZ Wythenshawe, Manchester, United Kingdom
The redundant data center in the US has not been covered in person but is in scope of the Webtrust audits that Sectigo maintains as well.

Root 1: USERTrust RSA Certification Authority

Standards considered

European Standards:
- ETSI EN 319 411-2 V2.4.1 (2021-11)
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.8
- Network and Certificate System Security Requirements, version 2.0

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

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

- Sectigo eIDAS Certificate Policy, version 1.0.9 as of 2023-11-22
- Sectigo eIDAS Certification Practice Statement, Version 1.1.1 as of 2024-11-04

No non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as described in the following.
- Bug 1915883, Sectigo: Missing data in cabfOrganizationIdentifier: https://bugzilla.mozilla.org/show_bug.cgi?id=1915883
- Bug 1902748, Sectigo: QWAC certificates issued with incorrect subject:organizationIdentifier attribute value: https://bugzilla.mozilla.org/show_bug.cgi?id=1902748
- Bug 1897538, Sectigo: Incorrectly included registrationStateOrProvince in PSD-based cabfOrganizationIdentifier extension: https://bugzilla.mozilla.org/show_bug.cgi?id=1897538
- Bug 1869056, Sectigo: Inadequate vulnerability scanning and patching: https://bugzilla.mozilla.org/show_bug.cgi?id=1869056

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

Distinguished Name	SHA-256 fingerprint	Applied policy
C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	E793C9B02FD8AA13E21C31228ACCB08119643B749C898964B1746D46C3D4CBD2	ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 1: Root-CA 1 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
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication CA Natural R35	339E6B92BE5459F26A8DC3C5F3720933C838E236601B050048C047A123E6F8E7	ETSI EN 319 411-2 V2.4.1, QEVCP-w
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication CA R35	002393FA0A6825F77EF686E208620B97177791F02F07DB2518480FBE37CE7BD8	ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 2: Sub-CA's issued by the Root-CA 1 or its Sub-CA's in scope of the audit

Root 2: USERTrust ECC Certification Authority

Standards considered

European Standards:
- ETSI EN 319 411-2 V2.4.1 (2021-11)
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.8
- Network and Certificate System Security Requirements, version 2.0

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

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

- Sectigo eIDAS Certificate Policy, version 1.0.9 as of 2023-11-22
- Sectigo eIDAS Certification Practice Statement, Version 1.1.1 as of 2024-11-04

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1869056, Sectigo: Inadequate vulnerability scanning and patching: https://bugzilla.mozilla.org/show_bug.cgi?id=1869056

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

Distinguished Name	SHA-256 fingerprint	Applied policy
C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority	4FF460D54B9C86DABFBCFC5712E0400D2BED3FBC4D4FBDAA86E06ADCD2A9AD7A	ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 3: Root-CA 2 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
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication CA E35	562D6A5B4B067465FFD0FBFC9BB05755CDACF55B5EE5C6F910B8B53DB128F57A	ETSI EN 319 411-2 V2.4.1, QEVCP-w
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication Natural E35	A9841D2E47CBE6D71D8FAFDF38387F93F43D76D792504EFB17A21020C58C0B89	ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 4: Sub-CA's issued by the Root-CA 2 or its Sub-CA's in scope of the audit

Root 3: Sectigo Public Server Authentication Root E46

Standards considered

European Standards:
- ETSI EN 319 411-2 V2.4.1 (2021-11)
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.8
- Network and Certificate System Security Requirements, version 2.0

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

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

- Sectigo eIDAS Certificate Policy, version 1.0.9 as of 2023-11-22
- Sectigo eIDAS Certification Practice Statement, Version 1.1.1 as of 2024-11-04

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1869056, Sectigo: Inadequate vulnerability scanning and patching: https://bugzilla.mozilla.org/show_bug.cgi?id=1869056

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

Distinguished Name	SHA-256 fingerprint	Applied policy
C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root E46	C90F26F0FB1B4018B22227519B5CA2B53E2CA5B3BE5CF18EFE1BEF47380C5383	ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 5: Root-CA 3 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
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication CA E39	05461634195849A1BCCC99264912054FDEB987A52E661312AE9CCA3E3ED8D318	ETSI EN 319 411-2 V2.4.1, QEVCP-w (Only with regard to key protection requirements, not yet activated for issuing)
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication CA Natural E39	00C367A774B7CE9A0F791342383F865F2AF6CD37674B85167E6F239E313D60BB	ETSI EN 319 411-2 V2.4.1, QEVCP-w (Only with regard to key protection requirements, not yet activated for issuing)

Table 6: Sub-CA's issued by the Root-CA 3 or its Sub-CA's in scope of the audit

Root 4: Sectigo Public Server Authentication Root R46

Standards considered

European Standards:
- ETSI EN 319 411-2 V2.4.1 (2021-11)
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.8
- Network and Certificate System Security Requirements, version 2.0

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

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

- Sectigo eIDAS Certificate Policy, version 1.0.9 as of 2023-11-22
- Sectigo eIDAS Certification Practice Statement, Version 1.1.1 as of 2024-11-04

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1869056, Sectigo: Inadequate vulnerability scanning and patching: https://bugzilla.mozilla.org/show_bug.cgi?id=1869056

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

Distinguished Name	SHA-256 fingerprint	Applied policy
C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root R46	7BB647A62AEEAC88BF257AA522D01FFEA395E0AB45C73F93F65654EC38F25A06	ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 7: Root-CA 4 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
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication CA Natural R39	3CCF0306BED8C910B327A15F2159FDD1E414474F77696C3D98781B1160277BCA	ETSI EN 319 411-2 V2.4.1, QEVCP-w (Only with regard to key protection requirements, not yet activated for issuing)
C=ES, O=Sectigo (Europe) SL, CN=Sectigo Qualified Website Authentication CA R39	AC8C7EF96EB4B535FBFB4E7521F130536198A60DFF716312B22D4ACC4AFE9A7D	ETSI EN 319 411-2 V2.4.1, QEVCP-w (Only with regard to key protection requirements, not yet activated for issuing)

Table 8: Sub-CA's issued by the Root-CA 4 or its Sub-CA's in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2025-01-17	Initial attestation
Version 1.1	2025-01-30	Additional Root- and Sub-CAs added

End of the audit attestation letter.