

Standard Audit Attestation for

D-Trust GmbH

Reference: AA2024112901-Standard

Essen, 2024-12-12

To whom it may concern,

This is to confirm that “TÜV NORD CERT GmbH” has audited the CAs of “D-Trust GmbH” without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “**AA2024112901-Standard**” covers multiple Root-CAs and consists of 26 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,

Dr. Silke Keller
Reviewer

Matthias Wiedenhorst
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.

Headquarters
TÜV NORD CERT GmbH

Am TÜV 1
45307 Essen, Germany

Tel.: 0201 825-0
Fax: 0201 825-2517
info.tncert@tuev-nord.de
tuev-nord-cert.en

Director
Dipl.-Ing. Wolfgang Wielpütz
Dipl.-Oec. Sandra Gerhartz

Registration Office
Amtsgericht Essen
HRB 9976
VAT ID No.: DE 811389923
Tax No.: 111/5706/2193

Deutsche Bank AG, Essen
BIC (SWIFT-Code): DEUTDE33
IBAN-Code: DE26 3607 0050 0607 8950 00

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-12007-01-12¹ 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, 1 Auditor, 1 Trainee Auditor
- 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):

D-Trust GmbH, Kommandantenstraße 15, 10969 Berlin, Germany,
registered under "HRB 74346" at AG Charlottenburg, Berlin, Germany

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:

2023-10-08 to 2024-10-07

Point in time date:

none, as audit was a period of time audit

Audit dates:

2024-09-23 to 2024-09-24 (on-site)
2024-09-30 to 2024-10-02 (on-site)
2024-10-07 to 2024-10-11 (on-site)

Audit location:

10969 Berlin

Root 1: D-TRUST BR Root CA 1 2020

Standards considered

European Standards:

- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:

- 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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST BR Root CA 1 2020	E59AAA816009C22BFF5B25BAD37DF306F049797C1F81D85AB089E657BD8F0044	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP

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=DE, O=D-Trust GmbH, CN=D-TRUST BR CA 1-20-1 2020	199AB2AAAFF40401E0A3B7B87EE9964659EFA94A1FECBE918AE136E4B4E0A8	ETSI EN 319 411-1 V1.3.1, OVCP (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-TRUST BR CA 1-20-2 2020	B268D16934AB5BA232F179CD9F5C7FC07EA8583A56A9A7C1D6CB58FE0823BF5A	ETSI EN 319 411-1 V1.3.1, DVCP (Only with regard to key protection requirements, not yet activated for issuing)

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

Root 2: D-TRUST BR Root CA 2 2023

Standards considered

European Standards:

- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:

- 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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST BR Root CA 2 2023	0552E6F83FDF65E8FA9670E666DF28A4E21340B510CBE52566F97C4FB94B2BD1	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP

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=DE, O=D-Trust GmbH, CN=D-TRUST BR CA 2-23-1 2023	D904A27FD2D271DCFE40A1F471033CE48A4B5E1484753DA66F7166D6EBDC06E6	ETSI EN 319 411-1 V1.3.1, OVCP (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-TRUST BR CA 2-23-2 2023	6685871384605253C264F8D380A8D1DD50A6CA192788FF2D560CAFE541F807B8	ETSI EN 319 411-1 V1.3.1, DVCP (Only with regard to key protection requirements, not yet activated for issuing)

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

Root 3: D-TRUST EV Root CA 1 2020

Standards considered

European Standards:

- 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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST EV Root CA 1 2020	08170D1AA36453901A2F959245E347DB0C8D37ABAABC56B81AA100DC958970DB	ETSI EN 319 411-1 V1.3.1, EVCP

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=DE, O=D-Trust GmbH, CN=D-TRUST EV CA 1-20-1 2020	41C897473B0369FA74B1F4F9D7F89129485C1A305C0719A867DC8714E0870200	ETSI EN 319 411-1 V1.3.1, EVCP (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: D-TRUST EV Root CA 2 2023

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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST EV Root CA 2 2023	8E8221B2E7D4007836A1672F0DCC299C33BC07D316F132FA1A206D587150F1CE	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP

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=DE, O=D-Trust GmbH, CN=D-TRUST EV CA 2-23-1 2023	378CF8738654C8A8544812B1FF2632348225553DA80225692D0491C4A1EEAFB9	ETSI EN 319 411-1 V1.3.1, EVCP (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-TRUST EV CA 2-23-2 2023, 2.5.4.97=VATDE-202620438	5FF9F5A1C0ED7401E1C529F6D50C4ABB00B17B593358BD2D61DC0DD887DDD92F	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP (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

Root 5: D-TRUST Root CA 3 2013

Standards considered

European Standards:

- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)
- ETSI TS 119 411-6 V1.1.1 (2023-08)

CA Browser Forum Requirements:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.8
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.4
- 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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST Cloud PKI, Version 4.1 as of 2024-11-01, valid from 2024-11-08, D-Trust GmbH
- Certification Practice Statement of the E.ON SE PKI, Version 3.0 as of 2024-11-01, valid from 2024-11-08, D-Trust GmbH

No non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST Root CA 3 2013	A1A86D04121EB87F027C66F53303C28E5739F943FC84B38AD6AF009035DD9457	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 9: Root-CA 5 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=DE, O=D-Trust GmbH, CN=D-TRUST Application Certificates CA 3-1 2013	CB0F7B7670EA2B818ABE80587902434B30EF7A8C0273B84884243F89593EA630	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=D-Trust GmbH, CN=D-TRUST Application Certificates CA 3-1 2013	9441FD6CD383418465ED911E102A40D2AE82F7443940AAA1C7B49918FFE6028E	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=D-Trust GmbH, CN=D-TRUST Application Certificates CA 3-1 2013	3F25BD4C92D59A994931ABA53D81507C9EE6B90640BE275C4FF431D1DAB72396	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=D-Trust GmbH, CN=D-TRUST Application Certificates CA 3-2 2016, 2.5.4.97=NTRDE-HRB74346	7890EED59E95743C62826398129BC2F54AD414794AAC075BA67177332802B029	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (CA is not used for certificate issuance anymore)

C=DE, O=D-Trust GmbH, CN=E.ON Group CA 2 2013	43247EF5A09A0867BA4A7E1716463577AAD6EFA057BFF763B43FD2A979608FE2	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=E.ON SE, OU=CA, CN=E.ON CA 2 2013 XXI	8B1698B51BF6EF2C31C553E6FF7A7734901806BCC87704182D2293183348B334	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=E.ON SE, OU=CA, CN=E.ON CA 2 2013 XXI	43B3986A9908B9B0D76C78AA877DDC1B8C8E6AC2F441B9767E68DF5ECF096438	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=E.ON SE, OU=CA, CN=E.ON CA 2 2013 XXI	41D1CF86CDE9DB5EDDC90A9DE0A4F6014E997DDA271D5B3766E1E3214DCCD9C7	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=E.ON SE, OU=CA, CN=E.ON CA 2 2013 XXII	B2B7C755C80FBE20E2134A620157A53B5B0724B6947B4EED1CA9DF7951FC5D44	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (CA is not used for certificate issuance anymore)
C=DE, O=E.ON SE, OU=CA, CN=E.ON CA 2 2013 XXIII	99CADFF0B43B45405D471AB7F04817B04925D603007A57CA1BABA48BC8721BF6	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=E.ON SE, OU=CA, CN=E.ON CA 2 2013 XXIII	6F4EDF5918B4C2A7B3121333F757FFCB0C83EF8C821A10EF47228EFCEDE168D9	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=E.ON SE, OU=CA, CN=E.ON CA 2 2013 XXIII	0AB43E7D481D24B216412DEE945D40D73FA2596404172A8C3039BF5E97FD1EF8	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=D-Trust GmbH, OU=CA, CN=Partner CA 2 2013 XXIV	A099851198F66AA47D11D1FF42A6876E7F328C22184BC0B66559AF5A51459511	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (CA is not used for certificate issuance anymore)

Table 10: Sub-CA's issued by the Root-CA 5 or its Sub-CA's in scope of the audit

Root 6: D-TRUST Root Class 3 CA 2 2009

Standards considered

European Standards:

- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)
- ETSI TS 119 411-6 V1.1.1 (2023-08)

CA Browser Forum Requirements:

- 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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

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

- Bug 1861069, D-Trust: Issuance of 15 DV certificates containing 'serialNumber' field within subject
https://bugzilla.mozilla.org/show_bug.cgi?id=1861069
- Bug 1862082, D-Trust: Delay beyond 5 days in revoking misissued certificate
https://bugzilla.mozilla.org/show_bug.cgi?id=1862082
- Bug 1879529, D-Trust: "unknown" OCSP response for issued certificates
https://bugzilla.mozilla.org/show_bug.cgi?id=1879529
- Bug 1884714, D-Trust: LDAP-URL in Subscriber Certificate Authority Information Access field
https://bugzilla.mozilla.org/show_bug.cgi?id=1884714
- Bug 1913310, D-Trust: CRL-Entries without required CRL Reason Code
https://bugzilla.mozilla.org/show_bug.cgi?id=1913310

The remediation measures taken by D-Trust GmbH as described on Bugzilla (see links above) have been checked by the auditors and properly addressed the incidents.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA 2 2009	49E7A442ACF0EA6287050054B52564B650E4F49E42E348D6AA38E039E957B1C1	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 11: Root-CA 6 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=DE, O=D-Trust GmbH, CN=D-TRUST SSL CA 2 2020	972A181B60294EBA07333B9C1982440D43395ABA91D450EC0EFB485AED49D5A7	ETSI EN 319 411-1 V1.3.1, DVCP
C=DE, O=D-Trust GmbH, CN=D-TRUST SSL Class 3 CA 1 2009	6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 12: Sub-CA's issued by the Root-CA 6 or its Sub-CA's in scope of the audit

Root 7: D-TRUST Root Class 3 CA 2 EV 2009

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)
- ETSI TS 119 411-6 V1.1.1 (2023-08)

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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

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

- Bug 1891225, D-Trust: Issuance of 15 certificates with incorrect subject attribute order
https://bugzilla.mozilla.org/show_bug.cgi?id=1891225
- Bug 1893610, D-Trust: Notice to affected Subscriber and person filing CPR not sent within 24 hours
https://bugzilla.mozilla.org/show_bug.cgi?id=1893610
- Bug 1896190, D-Trust: Issuance of an EV certificate containing a mixup of the Subject's postalCode and localityName
https://bugzilla.mozilla.org/show_bug.cgi?id=1896190
- Bug 1884714, D-Trust: LDAP-URL in Subscriber Certificate Authority Information Access field
https://bugzilla.mozilla.org/show_bug.cgi?id=1884714
- Bug 1913310, D-Trust: CRL-Entries without required CRL Reason Code

https://bugzilla.mozilla.org/show_bug.cgi?id=1913310

The remediation measures taken by D-Trust GmbH as described on Bugzilla (see links above) have been checked by the auditors and properly addressed the incidents.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA 2 EV 2009	EEC5496B988CE98625B934092EEC2908BED0B0F316C2D4730C84EAF1F3D34881	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 13: Root-CA 7 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=DE, O=D-Trust GmbH, CN=D-TRUST CA 2-2 EV 2016, 2.5.4.97=NTRDE-HRB74346	2316D05A2E2D347FA141135B98ED09F56E81F1CF5679793D3B39DD6D8E461A48	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C=DE, O=D-Trust GmbH, CN=D-TRUST SSL Class 3 CA 1 EV 2009	B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5E635BA5B4	ETSI EN 319 411-1 V1.3.1, EVCP ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 14: Sub-CA's issued by the Root-CA 7 or its Sub-CA's in scope of the audit

Root 8: D-Trust SBR Root CA 1 2022

Standards considered

European Standards:

- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)
- ETSI TS 119 411-6 V1.1.1 (2023-08)

CA Browser Forum Requirements:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.4
- 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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-Trust SBR Root CA 1 2022	D92C171F5CF890BA428019292927FE22F3207FD2B54449CB6F675AF4922146E2	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 15: Root-CA 8 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=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 1-22-1 2022, 2.5.4.97=VATDE-202620438	31FFA8D3F2439C62F2363FE56F4E245382A6D69D8A828B3539FA3875F8C5235B	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 1-22-2 2022, 2.5.4.97=VATDE-202620438	200E2C50111A71B07555E921D3BFB7EBDE47F7E41873E06753474362BC017BA2	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 1-22-3 2023, 2.5.4.97=VATDE-202620438	D087C970CED1BBCE2E9A73AA7A601CC6A8C877BF1FF3B6089AEDEAE585F2FABA	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)

C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 1-22-4 2024, 2.5.4.97=VATDE-202620438	DD69E93713BAE0F4B529A485BAE1FD25B61DDF6DBC25CDE25D0F365CD14CE4DE	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 1-22-5 2024, 2.5.4.97=VATDE-202620438	087C5E12093A48D3064C3352CF7B1017C57492E1BE02A3B032AC42ED079F9845	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)

Table 16: Sub-CA's issued by the Root-CA 8 or its Sub-CA's in scope of the audit

Root 9: D-Trust SBR Root CA 2 2022

Standards considered

European Standards:

- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)
- ETSI TS 119 411-6 V1.1.1 (2023-08)

CA Browser Forum Requirements:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.4
- 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:

- Certificate Policy (CP) of D-Trust GmbH, version 5.4 as of 2024-07-26, valid from 2024-07-26, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 2.2 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.4 as of 2024-10-11, valid from 2024-10-15, D-Trust GmbH

No non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=DE, O=D-Trust GmbH, CN=D-Trust SBR Root CA 2 2022	DBA84DD7EF622D485463A90137EA4D574DF8550928F6AFA03B4D8B1141E636CC	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 17: Root-CA 9 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=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 2-22-1 2022, 2.5.4.97=VATDE-202620438	CED8E0893E52A1C96AE65D9955A908C45003D7CEADE56B3E4717FD8F00EE0743	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 2-22-2 2022, 2.5.4.97=VATDE-202620438	6E87C6E63C8BEE394908B97D1079F8FF88C3930E0EBEC5708C159E2B83247FF0	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 2-22-3 2023, 2.5.4.97=VATDE-202620438	ED65312EB2E5F93293CCF370803CD3A66D1670C8D3A4825F5EA428F03F8ACCCC	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)

C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 2-22-4 2024, 2.5.4.97=VATDE-202620438	5A128127FFEF4C2F7443F6695B5C96B572DCD8092131449F1497728F2EE4C59B	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)
C=DE, O=D-Trust GmbH, CN=D-Trust SBR CA 2-22-5 2024, 2.5.4.97=VATDE-202620438	1B410BA647ADD270CEBF6F6C6CC4BD69533E868D710325383965EC32C5EF8938	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) (Only with regard to key protection requirements, not yet activated for issuing)

Table 18: Sub-CA's issued by the Root-CA 9 or its Sub-CA's in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2024-11-29	Initial attestation
Version 1.1	2024-12-12	ETSI TS 119 411-6 was missing and has been added

End of the audit attestation letter.