SMIME-BR Audit Attestation for

D-Trust GmbH

Reference: AA2023121501-SMIME-BR

Essen, 2023-12-15

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number “**AA2023121501-SMIME-BR**” covers multiple Root-CAs and consists of 11 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Am TÜV 1
45307 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller
Reviewer

Matthias Wiedenhorst
Lead Auditor

This attestation is based on the template version 3.2 as of 2023-08-24, 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 Informationstechnik GmbH[1], TÜV NORD GROUP, Am TÜV 1, 45307 Essen, Germany, registered under HRB 11687, Amtsgericht Essen, Germany
- Accredited by DAkkS under registration D-ZE-12022-01-01[2] for the certification of trust services according to "DIN EN ISO/IEC 17065:2013" and "ETSI EN 319 403 V2.2.2 (2015-08)".
- Insurance Carrier (BRG section 8.2):
  HDI Global 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
- 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;

[1] In the following termed shortly „TÜVIT"
[2] https://www.dakks.de/en/accredited-body.html?id=D-ZE-12022-01-01

e) general knowledge of regulatory requirements relevant to TSPs; and
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:

2022-10-08 to 2023-10-07

Point in time date:

none, as audit was a period of time audit

Audit dates:

2023-09-19 to 2023-09-21 (on-site)
2023-09-25 to 2023-09-26 (on-site)
2023-09-27 to 2023-09-28 (remote)
2023-10-04 to 2023-10-05 (remote)
2023-10-09 to 2023-10-11 (on-site)

Audit location:

10969 Berlin

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)

CA Browser Forum Requirements:
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.1
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.1

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 5.2 as of 2023-11-07, valid from 2023-11-22, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 1.9 as of 2023-11-21, valid from 2023-11-22, D-Trust GmbH
- Certification Practice Statement of the D-TRUST Root PKI, version 4.0 as of 2023-10-20, valid from 2023-11-03, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.1 as of 2023-11-21, valid from 2023-11-22, D-Trust GmbH
- Certification Practice Statement of the D-TRUST Cloud PKI, Version 3.8 as of 2023-11-23, valid from 2023-11-24, D-Trust GmbH
- Certification Practice Statement of the E.ON SE PKI, Version 2.8 as of 2023-08-28, valid from 2023-08-29, D-Trust GmbH
- Certification Practice Statement of the Uniper PKI, Version 2.7 as of 2023-08-28, valid from 2023-08-30, 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, LCP

Table 1: 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, LCP
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
C=DE, O=D-Trust GmbH, CN=E.ON Group CA 2 2013	43247EF5A09A0867BA4A7E1716463577AAD6EFA057BFF763B43FD2A979608FE2	ETSI EN 319 411-1 V1.3.1, LCP
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
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
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
C=DE, O=D-Trust GmbH, OU=CA, CN=Partner CA 2 2013 XXIV	A099851198F66AA47D11D1FF42A6876E7F328C22184BC0B66559AF5A51459511	ETSI EN 319 411-1 V1.3.1, LCP
C=DE, O=D-Trust GmbH, CN=Uniper Group CA 2 2015	B4B2810E787B8E6DBB8B0EA9242D8E195AD5BF4201FD98A09AEDAC8B5F23FAFE	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)
C=DE, O=Uniper Holding GmbH, OU=CA, CN=Uniper CA 2 2015 XXXI	F471920D5679EE48219F51CBF44F0F22A7305332B869025E26050C5BED762F72	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)
C=DE, O=Uniper Holding GmbH, OU=CA, CN=Uniper CA 2 2015 XXXII	EFA0A2F29EABB43EAD97AD067297656088679C0B2E297C2D898C4F12C9759805	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)
C=DE, O=Uniper Holding GmbH, OU=CA, CN=Uniper CA 2 2015 XXXIII	79B9D31504B604293570ECCDC8A92553F937FD823380E560793987037C8B181D	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)

C=DE, O=D-Trust GmbH, CN=Uniper Group CA 3 2020	A502172DEAF811DD7FA9BC3329AEA72589F2FAEC9401CB7348819C75F2E705B9	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)
C=DE, O=Uniper Holding GmbH, OU=CA, CN=Uniper CA 3 2020 XXXI	19D99B7FDD7EC707AC3023D72F50D4AB5199AF1FDD3013A96815CBC99B63BFD6	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)
C=DE, O=Uniper Holding GmbH, OU=CA, CN=Uniper CA 3 2020 XXXII	B576C4A703CB973079F8374EF359E4FD8788584B4E9FB4BC90A7E9F8C3838791	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)
C=DE, O=Uniper Holding GmbH, OU=CA, CN=Uniper CA 3 2020 XXXIII	364ED83755EA3EA8533856EFF72DE38271B54FF44905785EBF735BFFC29B6636	ETSI EN 319 411-1 V1.3.1, LCP (CA has been deactivated for certificate issuance on 2023-08-31)

Table 2: Sub-CA’s issued by the Root-CA 5 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)

CA Browser Forum Requirements:
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.1

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 5.2 as of 2023-11-07, valid from 2023-11-22, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 1.9 as of 2023-11-21, valid from 2023-11-22, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.1 as of 2023-11-21, valid from 2023-11-22, 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 ETSI EN 319 411-1 V1.3.1, LCP

Table 3: 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 (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 (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 (Only with regard to key protection requirements, not yet activated for issuing)

Table 4: 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)

CA Browser Forum Requirements:
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.1

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 5.2 as of 2023-11-07, valid from 2023-11-22, D-Trust GmbH
- D-TRUST Trust Service Practice Statement (TSPS), version 1.9 as of 2023-11-21, valid from 2023-11-22, D-Trust GmbH
- Certification Practice Statement of the D-TRUST CSM PKI, version 4.1 as of 2023-11-21, valid from 2023-11-22, 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 ETSI EN 319 411-1 V1.3.1, LCP

Table 5: 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 (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 (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 (Only with regard to key protection requirements, not yet activated for issuing)

Table 6: 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	2023-12-15	Initial attestation

End of the audit attestation letter.