Audit Attestation for

D-Trust GmbH

Reference: AA2021121004

Essen, 2021-12-10

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 “**AA2021121004**” and consists of 7 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	Matthias Wiedenhorst
Reviewer	Leadauditor

Identification of the conformity assessment body (CAB):	• TÜV Informationstechnik GmbH[1], Am TÜV 1, 45307 Essen, Germany, registered under HRB 11687, Amtsgericht Essen, Germany • Accredited by DAkkS under registration D-ZE-12022-01[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, 2 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;

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

	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 • 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 o has acted as auditor in at least three complete TSP audits; o has adequate knowledge and attributes to manage the audit process; and o has the competence to communicate effectively, both orally and in writing. • 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 trust service provider (TSP):	D-Trust GmbH, Kommandantenstraße 15, 10969 Berlin, Germany, registered under HRB 74346 B, Amtsgericht Charlottenburg (Berlin), Germany

Audit Period covered for all policies:	2020-10-08 to 2021-10-07
Audit dates:	2021-09-27 to 2021-09-30 (on site) 2021-10-04 to 2021-10-07 (on site) 2021-10-11 to 2021-10-14 (on site)
Audit Location:	D-Trust GmbH, Kommandantenstraße 15, 10969 Berlin, Germany

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

Standards considered	European Standards: ☐ ETSI EN 319 411-2, V2.2.2 (2018-04) ☒ ETSI EN 319 411-1, V1.2.2 (2018-04) ☒ ETSI EN 319 401, V2.2.1 (2018-04) CA Browser Forum Requirements: ☐ EV SSL Certificate Guidelines, version 1.7.7 ☒ Baseline Requirements, version 1.7.9 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ ETSI TS 119 403-2 V1.2.4 (2020-11)

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

1. Certificate Policy (CP) of D-Trust GmbH, Version 4.2 as of 2021-06-18, valid from 2021-07-09, D-Trust GmbH
2. D-TRUST Trust Service Practice Statement (TSPS), Version 1.3 as of 2021-10-14, valid from 2021-10-15, D-Trust GmbH
3. Certification Practice Statement of the D-TRUST Root PKI, Version 3.5 as of 2021-10-14, valid from 2021-10-15, D-Trust GmbH
4. Certification Practice Statement of the D-TRUST CSM PKI, Version 3.4 as of 2021-10-14, valid from 2021-10-15, D-Trust GmbH

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

This Audit Attestation also covers the following incidents as documented under

- Bug 1682270, D-TRUST: Private Key Disclosed by Customer as Part of CSR https://bugzilla.mozilla.org/show_bug.cgi?id=1682270
- Bug 1691117, D-TRUST: Certificate with RSA key where modulus is not divisible by 8 https://bugzilla.mozilla.org/show_bug.cgi?id=1691117
- Bug 1647468, D-TRUST: D-TRUST: Wrong key usage (Key Encipherment) https://bugzilla.mozilla.org/show_bug.cgi?id=1647468

The remediation measures taken by D-Trust GmbH as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Identification of the audited Root-CA:			
Distinguished Name	C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA 2 2009	Applied policy	ETSI EN 319 411-1 V1.2.2, OVCP ETSI EN 319 411-1 V1.2.2, DVCP
SHA-256 fingerprint	49E7A442ACF0EA6287050054B52564B650E4F49E42E348D6AA38E039E957B1C1		

Table 1: Root-CA in scope of this attestation

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.

Identification of the audited Sub-CAs					
Distinguished Name	C=DE, O=D-Trust GmbH, CN=D-TRUST SSL CA 2 2020	Applied policy	ETSI EN 319 411-1 V1.2.2, DVCP	EKU	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)
SHA-256 fingerprint	972A181B60294EBA07333B9C1982440D43395ABA91D450EC0EFB485AED49D5A7				
Distinguished Name	C=DE, O=D-Trust GmbH, CN=D-TRUST SSL Class 3 CA 1 2009	Applied policy	ETSI EN 319 411-1 V1.2.2, OVCP	EKU	not defined
SHA-256 fingerprint	6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025				
Distinguished Name	C=DE, O=D-Trust GmbH, CN=VR IDENT SSL CA 2020[3]	Applied policy	ETSI EN 319 411-1 V1.2.2, OVCP	EKU	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)

[3] This CA has been revoked under the attendance of the auditor on 2021-10-14

SHA-256 fingerprint	007108194115F3C899F54EE67CB4DA87275EDC1D6798DA787E0758CFA6AE96B1

Table 2: Sub-CA's issued by the Root-CA or its Sub-CA's

Modifications record

Version	Issuing Date	Changes
Version 1.0	2021-12-10	Initial attestation

End of the audit attestation letter.