Audit Attestation for

D-Trust GmbH

Reference: AA2020120302

Essen, 2020-12-03

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 “**AA2020120302**” and consists of 6 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Langemarckstr. 20
45141 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller
Reviewer

Matthias Wiedenhorst
Leadauditor

Identification of the conformity assessment body (CAB):	TÜV Informationstechnik GmbH[1], Langemarckstraße 20, 45141 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)".

Identification of the trust service provider (TSP):	D-Trust GmbH, Kommandantenstraße 15, 10969 Berlin, Germany, registered under HRB 74346 B, Amtsgericht Charlottenburg (Berlin), Germany

Identification of the audited Root-CA:	D-TRUST Root Class 3 CA 2 2009	
	Distinguished Name	C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA 2 2009
	SHA-256 fingerprint	49E7A442ACF0EA6287050054B52564B650E4 F49E42E348D6AA38E039E957B1C1
	Applied policy	ETSI EN 319 411-1 V1.2.2, DVCP policy ETSI EN 319 411-1 V1.2.2, OVCP policy

[1] In the following termed shortly „TÜViT"
[2] http://www.dakks.de/en/content/accredited-bodies-dakks?Regnr=D-ZE-12022-01-01

The audit was performed as full period of time audit at the TSP's location in Berlin, Germany. It took place from 2020-09-28 until 2020-10-15 and covered the period from 2019-10-08 until 2020-10-07. The audit was performed according to the European Standards "ETSI EN 319 411-1, V1.2.2 (2018-04)" and "ETSI EN 319 401, V2.2.1 (2018-04)" as well as CA Browser Forum Requirements "Baseline Requirements, version 1.7.2" considering the requirements of the "ETSI EN 319 403, V2.2.2 (2015-08)" for the Trust Service Provider Conformity Assessment.

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

1. Certificate Policy of D-TRUST GmbH, version 4.0 as of 2020-11-10, valid from 2020-11-12
2. TSPS – Trust Service Practice Statement D-TRUST, version 1.0 as of 2020-11-10, valid from 2020-11-12
3. Certification Practice Statement of the D-TRUST Root PKI, version 3.0 as of 2020-11-10, valid from 2020-11-12,
4. Certification Practice Statement of the D-TRUST CSM PKI, Version 3.0 as of 2020-11-10, valid from 2020-11-12

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in table 1 and that been covered in this audit.

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

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Documentation and implementation of product configuration processes shall be improved. [REQ-7.7-03)].

7.10 Collection of evidence
Documentation and implementation of archiving processes shall be improved. [REQ-7.10-01)]

Findings with regard to ETSI EN 319 411-1:
None.

For all 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

- Bug 1647468, D-TRUST : wrong key usage: https://bugzilla.mozilla.org/show_bug.cgi?id=1647468
- Bug 1610303, D-TRUST: issuance of non-conformant SSL certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1610303

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.

Distinguished Name	SHA-256 fingerprint	Applied policy	EKU
C=DE, O=D-Trust GmbH, CN=D-TRUST SSL CA 2 2020	972A181B60294EBA07333B9C1982440D43395ABA91D450EC0EFB485AED49D5A7	ETSI EN 319 411-1 V1.2.2, DVCP	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)
C=DE, O=D-Trust GmbH, CN=D-TRUST SSL Class 3 CA 1 2009	6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025	ETSI EN 319 411-1 V1.2.2, OVCP	not defined
C=DE, O=D-Trust GmbH, CN=VR IDENT SSL CA 2020	007108194115F3C899F54EE67CB4DA87275EDC1D6798DA787E0758CFA6AE96B1	ETSI EN 319 411-1 V1.2.2, OVCP	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)

Table 1: Sub-CA’s issued by the Root-CA or its Sub-CA’s

Modifications record

Version	Issuing Date	Changes
Version 1.0	2020-12-03	Initial attestation

End of the audit attestation letter.