



Audit Attestation for D-Trust GmbH

Reference: AA2019120303

Essen, 2019-12-03

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number "**AA2019120303**" and consist 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

TÜV Informationstechnik GmbH – Member of TÜV NORD GROUP

Langemarckstrasse 20
45141 Essen, Germany
Phone: +49 201 8999-9
Fax: +49 201 8999-888
info@tuvit.de
www.tuvit.de

Court of jurisdiction:
Essen HRB 11687
VAT ID.: DE 176132277
Tax No.: 111/57062251

Commerzbank AG
SWIFT/BIC Code: DRES DEFF 360
IBAN: DE47 3608 0080 0525 4851 00

Management Board
Dirk Kretzschmar

| | | |
|---|---|--|
| 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 EV 2009 | |
| | Distinguished Name | CN = D-TRUST Root Class 3 CA 2 EV 2009, O = D-Trust GmbH, C = DE |
| | SHA-256 fingerprint | EEC5496B988CE98625B934092EEC2908BED0B0F316C2D4730C84EAF1F3D34881 |
| | Certificate Serial number | 0983F4 |
| | Applied policy | EVCP of ETSI EN 319 411-1 QCP-w of ETSI EN 319 411-2 |

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 2019-10-07 until 2019-10-10 and 2019-10-21 until 2019-10-24 and covered the period from 2018-10-08 until 2019-10-07. The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.2.2 (2018-04)", "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 "EV SSL Certificate Guidelines, version 1.7.0" and "Baseline Requirements, version 1.6.6" 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 3.10 as of 2019-10-23
2. Certification Practice Statement of the D-TRUST Root PKI, Version 2.8 as of 2019-10-09
3. Certification Practice Statement of the D-TRUST CSM PKI, Version 2.8 as of 2019-10-09

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CA's that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits.

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

Findings with regard to ETSI EN 319 401:

None.

Findings with regard to ETSI EN 319 411-1:

6.3.9 Certificate Revocation and suspension

Implementation of revocation of misissued certificates within the maximum timelines as specified within the Baseline Requirements shall be improved. [ETSI EN 319 411-1, REV-6.3.9-01]

Findings with regard to ETSI EN 319 411-2:

6.3.10 Certificate Status Service

Documentation and implementation of the CRL profile shall be improved. [ETSI EN 319 411-2, CSS-6.3.10-05]

No major non-conformities have been identified. For all minor 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 1509512, D-TRUST: syntax error in one tls certificate:
https://bugzilla.mozilla.org/show_bug.cgi?id=1509512
- Bug 1390990, D-TRUST: Non-BR-Compliant Certificate Issuance:
https://bugzilla.mozilla.org/show_bug.cgi?id=1390990
- Bug 1567588, D-TRUST: incorrectly formatted businessCategory entry:
https://bugzilla.mozilla.org/show_bug.cgi?id=1567588
- Bug 1580525, D-TRUST: Delayed revocation of EV certificates:
https://bugzilla.mozilla.org/show_bug.cgi?id=580525

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

| Identification of the Sub-CA | Distinguished Name | SHA-256 fingerprint | Certificate Serial number OID | Applied policy | Service | EKU | Validity |
|----------------------------------|--|--|-------------------------------|----------------------------|------------------------|-------------|-----------------------------|
| D-TRUST CA 2-2 EV 2016 | 2.5.4.97 = NTRDE-HRB74346, CN = D-TRUST CA 2-2 EV 2016, O = D-Trust GmbH, C = DE | 2316D05A2E2D347FA141135B98ED09F56E81F1CF5679793D3B39DD6D8E461A48 | 0FE48E | QCP-w of ETSI EN 319 411-2 | website authentication | not defined | 2016-11-16 until 2029-11-05 |
| D-TRUST SSL Class 3 CA 1 EV 2009 | CN = D-TRUST SSL Class 3 CA 1 EV 2009, O = D-Trust GmbH, C = DE | B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5E635BA5B4 | 099064 | EVCP of ETSI EN 319 411-1 | website authentication | not defined | 2009-11-12 until 2029-11-05 |

Table 1: Sub-CA's issued by the Root-CA

Modifications record

| Version | Issuing Date | Changes |
|----------------|---------------------|---------------------|
| Version 1.0 | 2019-12-03 | Initial attestation |

End of the audit attestation letter.