Audit Attestation for

D-Trust GmbH

Reference: AA2019120302

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 “AA2019120302” and consist of 5 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 GmbH¹, Langemarckstraße 20, 45141 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany Accredited by DAkkS under registration D-ZE-12022-01² 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:

<table>
<thead>
<tr>
<th>D-TRUST Root Class 3 CA 2 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinguished Name</td>
</tr>
<tr>
<td>SHA-256 fingerprint</td>
</tr>
<tr>
<td>Certificate Serial number</td>
</tr>
<tr>
<td>Applied policy</td>
</tr>
</tbody>
</table>

¹ In the following termed shortly „TÜViT“


This template (version 2.2 as of 2019-05-28) was approved for use by ACAB-c.
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 319 411-1, 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:

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]

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 1563772, D-TRUST: Precertificate OU > 64 Characters: https://bugzilla.mozilla.org/show_bug.cgi?id=1563772

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.

This template (version 2.2 as of 2019-05-28) was approved for use by ACAB-c.
<table>
<thead>
<tr>
<th>Identification of the Sub-CA</th>
<th>Distinguished Name</th>
<th>SHA-256 fingerprint</th>
<th>Certificate Serial number OID</th>
<th>Applied policy</th>
<th>Service</th>
<th>EKU</th>
<th>Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-TRUST SSL Class 3 CA 1 2009</td>
<td>CN = D-TRUST SSL Class 3 CA 1 2009, O = D-Trust GmbH, C = DE</td>
<td>6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025</td>
<td>099063</td>
<td>OVCP of ETSI EN 319 411-1</td>
<td>Server authentication</td>
<td>Not defined.</td>
<td>2009-11-12 until 2029-11-05</td>
</tr>
</tbody>
</table>

Table 1: Sub-CA's issued by the Root-CA
End of the audit attestation letter.