



Audit Attestation for

D-TRUST GmbH

Reference: AA2018120701

Essen, 2018-12-07

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 "**AA2018120701**" 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

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	ee c5 49 6b 98 8c e9 86 25 b9 34 09 2e ec 29 08 be d0 b0 f3 16 c2 d4 73 0c 84 ea f1 f3 d3 48 81
	Certificate Serial number	09 83 f4
	Applied policy	NCP and 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 October 8th 2018 until October 24th 2018 as well as on November 19th, 2018 and covered the period from October 8th 2017 until October 7th 2018. The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.1.1 (2016-02)", "ETSI EN 319 411-1, V1.1.1 (2016-02)" and "ETSI EN 319 401, V2.1.1 (2016-02)" as well as CA Browser Forum Requirements "EV SSL Certificate Guidelines, version 1.6.8" and "Baseline Requirements, version 1.6.0" 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 3.5 as of 2018-07-05
2. Certification Practice Statement of the D-TRUST Root PKI, Version 2.3 as of 2018-07-05
3. Certification Practice Statement of the D-TRUST CSM PKI, Version 2.3 as of 2018-07-05

The following non-critical finding was identified:

- The TSP shall improve the process and its documentation of a regular, at least yearly CP/CPS review. [ETSI EN 319 401, 6.1 f)]]
- On 2018-06-02, one certificate had been issued with syntax error. Details are documented in https://bugzilla.mozilla.org/show_bug.cgi?id=1509512.

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.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validy
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	23 16 d0 5a 2e 2d 34 7f a1 41 13 5b 98 ed 09 f5 6e 81 f1 cf 56 79 79 3d 3b 39 dd 6d 8e 46 1a 48	0f e4 8e	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	b0 93 5d c0 4b 4e 60 c0 c4 2d ef 7e c5 7a 1b 1d 8f 95 8d 17 98 8e 71 cc 80 a8 cf 5e 63 5b a5 b4	09 90 64	NCP and 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	2018-12-07	Initial attestation

End of the audit attestation letter.