

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin, Germany

to confirm that its trust service

D-TRUST OVCP CAs

fulfils all requirements defined in the standard (EN)

ETSI EN 319 411-1 V1.2.2 (2018-04),
policy OVCP.

The appendix to the certificate is part of the certificate and
consists of 3 pages.

The certificate is valid only in conjunction with the evaluation
report.



Certificate ID: 67136.21

© TÜVIT - TÜV NORD GROUP - www.tuvit.de

Certificate validity:
2021-01-18 – 2023-01-28

Essen, 2021-01-18

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH

TÜV NORD GROUP

Langemarckstr. 20

45141 Essen, Germany

www.tuvit.de



Certificate

Certification Scheme

The certification body of TÜV Informationstechnik GmbH is accredited by “DAkKS Deutsche Akkreditierungsstelle GmbH” according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- “Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH”, version 2.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation Report

- „Audit Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67136, D-TRUST OVCP CAs“, version 2.1 as of 2021-01-11, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1

- ETSI EN 319 411-1 V1.2.2 (2018-04): „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“, Version 1.2.2, 2018-04, European Telecommunications Standards Institute

The applicable ETSI Certificate Policy is:

- OVCP: Organizational Validation Certificate Policy

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

D-TRUST OVCP CAs:

| Issuer of CA certificate (Root CA or Intermediate CA): | |
|---|--|
| CN = D-TRUST Root Class 3 CA 2 2009 | |
| Certificate Serial Number: 0983F3 | |
| Name of CA (as in certificate) | serial number of certificate |
| CN = D-TRUST SSL Class 3 CA 1 2009 | 099063 |
| CN = VR IDENT SSL CA 2020 | 60343953CF3A8 CA42BB44A442 92CBAF4 |

together with the documentation of the operator:

- Certificate Policy (CP) of D-TRUST GmbH, version 4.0 as of 2020-11-10, valid from 2020-11-12, D-TRUST
- D-TRUST Trust Service Practice Statement (TSPS), version 1.0 as of 2020-11-10, valid from 2020-11-12, D-TRUST
- Certification Practice Statement of the D-TRUST Root PKI, version 3.0 as of 2020-11-10, valid from 2020-11-12, D-TRUST
- Certification Practice Statement of the D-TRUST CSM PKI, version 3.0 as of 2020-11-10, valid from 2020-11-12, D-TRUST
- Allgemeine Geschäftsbedingungen der D-TRUST GmbH, version as of September 2019, D-TRUST

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.

- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

- 1 Publication and repository responsibilities**
- 2 Identification and authentication**
- 3 Certificate Life-Cycle operational requirements**
- 4 Facility, management, and operational controls**
- 5 Technical security controls**
- 6 Certificate, CRL, and OCSP profiles**
- 7 Compliance audit and other assessment**
- 8 Other business and legal matters**
- 9 Other provisions**