

# Certificate

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 qualified signature card

fulfils all relevant requirements defined in regulation

## Reg. (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic signatures.

The appendix to the certificate is part of the certificate with the ID 97194.22 and consists of 3 pages.

Essen, 2023-11-16

Dr. Christoph Sutter, Head of Certification Body



Certificate validity:  
2022-11-16 – 2024-11-16



## 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 and according to eIDAS. The certification body performs its certification on the basis of the following accredited certification scheme:

- “Certification Scheme eIDAS (accredited scope) of the certification body of TÜV Informationstechnik GmbH”, version 2.1 as of 2023-01-30, TÜV Informationstechnik GmbH

## Conformity Assessment Report

- German document: “Konformitätsbewertungsbericht TUVIT.97194.TSP.11.2022, D-Trust qualified signature card” as of 2023-11-16, TÜV Informationstechnik GmbH

## Conformity Assessment Requirements

The conformity assessment requirements are defined in eIDAS:

- Regulation (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

for the following trust service:

- creation of qualified certificates for electronic signatures

## Conformity Assessment Target

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

### D-Trust qualified signature card

**Issuer of CA certificate (Root CA or Intermediate CA): CN = D-TRUST Root CA 2 2017**  
**Certificate Serial Number: OFE49E**

<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = D-TRUST CA 2-1 2020	4CB2C9F3EB858EAE128397AFA4D0E3DA

**Issuer of CA certificate (Root CA or Intermediate CA): CN = D-TRUST Root CA 2 2021  
Certificate Serial Number: 51E9D64957BCF2AFD6BC4C6073B253D0**

<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = D-TRUST CA 2-21-1 2021	6FDD578C17F258A72D262A50043176CA

**Issuer of CA certificate (Root CA or Intermediate CA): CN = D-TRUST Root CA 3 2016  
Certificate Serial Number: 0FE475**

<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = D-TRUST CA 3-1 2016	0FE476

**Issuer of CA certificate (Root CA or Intermediate CA): CN = D-TRUST Root CA 3 2021  
Certificate Serial Number: 6BC22A5479D8EA68A9C5A27A909BA938**

<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = D-TRUST CA 3-21-1 2021	69F4C9580F580F631488B9632371E72E
CN = D-TRUST CA 3-21-3 2022	410B4A72BA98334996BDE68C98959F1B

together with the documentation of the operator:

- Certification Policy (CP) of D-Trust GmbH, version 5.1 as of 2023-09-26, valid from 2023-09-28, D-Trust GmbH
- D-TRUST Trust Service Practice Statement, version 1.8 as of 2023-09-26, valid from 2023-09-28, D-Trust GmbH
- Certification Practice Statement of the D-TRUST Root PKI, version 3.10 as of 2023-05-25, valid from 2023-05-31, D-Trust GmbH
- PKI Disclosure Statement, version 2.1 as of 2022-11-18, valid from 2022-11-22, D-Trust GmbH
- GENERAL TERMS AND CONDITIONS OF BUSINESS OF D-TRUST GMBH, as of September 2019, D-Trust GmbH

## Conformity Assessment Result

- The target of conformity assessment fulfills all applicable conformity assessment requirements.
- The certification requirements defined in the certification scheme are fulfilled.

## Summary of the Conformity Assessment Requirements

The eIDAS contains the following general requirements for the trust service:

- 1 Data processing and protection**  
Requirements from eIDAS, Article 5

**2 Liability and burden of proof**

Requirements from eIDAS, Article 13 para. 2, 3

**3 Accessibility for persons with disabilities**

Requirements from eIDAS, Article 15

**4 Security requirements applicable to trust service providers**

Requirements from eIDAS, Article 19, para. 1, 2

**5 Supervision of qualified trust service providers**

Requirements from eIDAS, Article 20 para. 1

**6 Requirements for qualified trust service providers**

Requirements from eIDAS, Article 24, Para. 1 d), a), b), para. 2 a), b), c), d), e), f), g), h), i), j), k), para. 3, para. 4

**7 Requirements for creation of qualified certificates for electronic signatures**

Requirements from eIDAS, Article 28, para. 1, 2, 3, 4, Article 29, para. 1, 2