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 sign-me advanced

fulfils all requirements defined in the standard (EN)

ETSI EN 319 411-1 V1.1.1 (2016-02), policy LCP.

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.

ETSI EN 319 411-1 2019 TÜViT® Trusted Site

Certificate ID: 67119.19

Certificate valid until 2021-01-28

Essen, 2019-01-28

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

DAkkS Deutsche Akkreditierungsstelle D-ZE-12022-01-01

Certification System

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 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67119, D-TRUST sign-me advanced", Version 2.1 as of 2019-01-25, TÜV Informationstechnik GmbH

Evaluation Requirements

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

- ETSI EN 319 411-1 V1.1.1 (2016-02): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements", Version 1.1.1, 2016-02, European Telecommunications Standards Institute

The applicable ETSI Certificate Policy is:

- LCP: Lightweight Certificate Policy

Evaluation Target

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

D-TRUST sign-me advanced:

Issuer of CA certificate (Root CA or intermediate CA): CN = D-TRUST Root CA 3 2013 Certificate Serial Number: 0f dd ac	
Name of CA (as in certificate)	**serial number of certificate**
CN = D-TRUST Application Certificates CA 3-2 2016	0f e4 8c

together with the following documents of the operator:

- "Certificate Policy of the D-TRUST GmbH", version 3.5 as of 2018-07-05, D-TRUST GmbH
- "Certification Practice Statement of the D-TRUST Cloud PKI", version 2.3 as of 2018-07-05, D-TRUST GmbH
- "Subscriber Agreement (sign-me)", Version 1.0, D-TRUST GmbH
- "Allgemeine Geschäftsbedingungen der Bundesdruckerei GmbH für Vertrauensdienste und weitere Zertifizierungs-dienste der D-TRUST", October 2018, Bundesdruckerei GmbH

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**

Scope of the Amendment

This amendment as of 2020-01-28 supplements the certificate with certificate ID: 67119.19 as of 2019-01-28 because of the conducted surveillance audit.

Certification System

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 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report – Surveillance Audit – ETSI EN 319 411-1, TUVIT-CA67119A1, D-TRUST sign-me advanced", Version 2.0 as of 2020-01-28, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1 V1.2.2:

- 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:

- LCP: Lightweight Certificate Policy

Evaluation Target

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

D-TRUST sign-me advanced:

Issuer of CA certificate (Root CA or intermediate CA): CN = D-TRUST Root CA 3 2013 Certificate Serial Number: 0FDDAC	
Name of CA (as in certificate)	**serial number of certificate**
CN = D-TRUST Application Certificates CA 3-2 2016	0FE48C

together with the documentation of the operator:

- ”Certificate Policy of the D-TRUST GmbH”, version 3.10 as of 2019-10-23, valid from 2019-11-12, D-TRUST GmbH
- “Certification Practice Statement of the D-TRUST Root PKI”, version 2.8 as of 2019-10-09, valid from 2019-11-12, D-TRUST GmbH
- “Certification Practice Statement of the D-TRUST Cloud PKI”, version 2.6 as of 2019-10-09, valid from 2019-11-12, D-TRUST GmbH
- “Subscriber Agreement (sign-me)”, version 1.1, D-TRUST GmbH
- “Allgemeine Geschäftsbedingungen der D-TRUST GmbH”, September 2019, D-TRUST GmbH

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