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 Advanced CA's

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 4 pages.

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

ETSI EN 319 411-1 2018 TÜViT® Trusted Site

Certificate ID: 67118.18

Certificate valid until 2020-11-30

Essen, 2018-11-30

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-CA67118, D-TRUST Advanced CA's", Version 2.0 as of 2018-11-30, 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 Advanced CA's:

D-TRUST CA's

Issuer of CA certificate (Root CA or intermediate CA): CN = D-TRUST Root CA 2 2013 Certificate Serial Number: 0f cf 5b	
Name of CA (as in certificate)	**serial number of certificate**
CN = D-TRUST CA 2-1 2015	0f e4 41

Issuer of CA certificate (Root CA or intermediate CA): CN = COMODO RSA Certification Authority Certificate Serial Number: 4c aa f9 ca db 63 6f e0 1f f7 4e d8 5b 03 86 9d	
Name of CA (as in certificate)	**serial number of certificate**
CN = D-TRUST CA 2-1 2015	2c c6 7b 92 69 e8 7f 77 0d 71 c0 e4 9f f2 2e 3e

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 3-1 2013	0f e0 f6

E.ON CA's

Issuer of CA certificate (Root CA or intermediate CA): CN = E.ON Group CA 2 2013 Certificate Serial Number: 0f e4 3b	
Name of CA (as in certificate)	**serial number of certificate**
CN = E.ON CA 2 2013 XXI	10 1c a6
CN = E.ON CA 2 2013 XXII	10 1c aa
CN = E.ON CA 2 2013 XXIII	10 1c ab
CN = Partner CA 2 2013 XXIV	10 1c ac

Uniper CA's

Issuer of CA certificate (Root CA or intermediate CA): CN = Uniper Group CA 2 2015 Certificate Serial Number: 0f e4 4c	
Name of CA (as in certificate)	**serial number of certificate**
CN = Uniper CA 2 2015 XXXI	16 9a 5b
CN = Uniper CA 2 2015 XXXII	16 9a 5f
CN = Uniper CA 2 2015 XXXIII	16 9a 60

together with the documents of the operator:

- "Certificate Policy of D-TRUST GmbH", version 3.5 as of 2018-07-05, D-TRUST GmbH
- "Certification Practice Statement of the D-TRUST-Root PKI", version 2.3 as of 2018-07-05, D-TRUST GmbH
- "Certification Practice Statement of the D-TRUST CSM PKI", version 2.3 as of 2018-07-05, D-TRUST GmbH
- "Certification Practice Statement of the E.ON SE PKI", version 2.1 as of 2018-07-05, D-TRUST GmbH

- "Certification Practice Statement of the Uniper PKI", version 2.1 as of 2018-07-05, D-TRUST GmbH
- "Subscriber Agreement (not for SSL certificates)", version 1.1, 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

Scope of the Amendment

This amendment as of 2019-12-03 supplements the certificate with certificate ID: 67118.18 as of 2018-11-30 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 – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67118, D-TRUST Advanced CA's", Version 2.0 as of 2019-12-03, 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 Advanced CA's:

D-TRUST CA's

Issuer of CA certificate (Root CA or intermediate CA): CN = D-TRUST Root CA 2 2013 Certificate Serial Number: 0F CF 5B	
Name of CA (as in certificate)	**serial number of certificate**
CN = D-TRUST CA 2-1 2015	0F E4 41

Issuer of CA certificate (Root CA or intermediate CA): CN = COMODO RSA Certification Authority Certificate Serial Number: 4C AA F9 CA DB 63 6F E0 1F F7 4E D8 5B 03 86 9D	
Name of CA (as in certificate)	**serial number of certificate**
CN = D-TRUST CA 2-1 2015	2C C6 7B 92 69 E8 7F 77 0D 71 C0 E4 9F F2 2E 3E

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 3-1 2013	0F E0 F6

E.ON CA's

Issuer of CA certificate (Root CA or intermediate CA): CN = E.ON Group CA 2 2013 Certificate Serial Number: 0F E4 3B	
Name of CA (as in certificate)	**serial number of certificate**
CN = E.ON CA 2 2013 XXI	10 1C A6
CN = E.ON CA 2 2013 XXII	10 1C AA
CN = E.ON CA 2 2013 XXIII	10 1C AB
CN = Partner CA 2 2013 XXIV	10 1C AC

Uniper CA's

Issuer of CA certificate (Root CA or intermediate CA): CN = Uniper Group CA 2 2015 Certificate Serial Number: 0F E4 4C	
Name of CA (as in certificate)	**serial number of certificate**
CN = Uniper CA 2 2015 XXXI	16 9A 5B
CN = Uniper CA 2 2015 XXXII	16 9A 5F
CN = Uniper CA 2 2015 XXXIII	16 9A 60

together with the documentation of the operator:

- "Certificate Policy of D-TRUST GmbH", Version 3.10 as of 2019-10-23
- "Certification Practice Statement of the D-TRUST Root PKI", Version 2.8 as of 2019-10-09
- "Certification Practice Statement of the D-TRUST CSM PKI", Version 2.8 as of 2019-10-09
- "Certification Practice Statement of the E.ON SE PKI", Version 2.2 as of 2018-11-30

- "Certification Practice Statement of the UNIPER PKI", Version 2.2 as of 2018-11-30
- "Subscriber Agreement", version 1.5 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