Key Generation Ceremony Report for

D- Trust GmbH

Reference: AA2023062801

Essen, 2024-08-02

To whom it may concern,

This is to confirm that “TÜV Informationstechnik GmbH” has audited a key generation ceremony of “D-Trust GmbH. The ceremony was followed in its entirety, completed successfully and without non-conformities in accordance with the applicable requirements.

This Key Generation Ceremony Report is registered under the unique identifier number “**AA2023062801**”, it covers multiple Root-CAs and consists of 9 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Am TÜV 1
45307 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Matthias Wiedenhorst
Reviewer

Monika Radziewicz-Lepczyńska
Lead Auditor

This attestation is based on the template version 3.0 as of 2023-02-20, that was approved for use by ACAB-c

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• TÜV Informationstechnik GmbH[1], Am TÜV 1, 45307 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany • Accredited by DAkkS under registration D-ZE-12022-01-01[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)”. • Insurance Carrier (BRG section 8.2): HDI Global SE • Third-party affiliate audit firms involved in the audit: None
Identification and qualification of the audit team
• Number of team members: 1 Lead Auditor • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: • All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and

[1] In the following termed shortly „TÜViT“
[2] https://www.dakks.de/en/accredited-body.html?id=D-ZE-12022-01-01

f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: None • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB • Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management
• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 Reviewer • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	D-Trust GmbH, Kommandantenstraße 15, 10969 Berlin, Germany, registered under "HRB 74346" at AG Charlottenburg, Berlin, Germany

Type of audit:	Point in time audit of key and certificate generation ceremony
Point in time date:	2023-05-09
Audit location:	10969 Berlin, Germany

A key generation script has been prepared in accordance with the normative requirements and with the rules stated in the policy and practice statement documents of the certification service provider. During generation of the keys and certificates, this script has been followed.

In particular:

- The key generation ceremony was performed by 3 individuals of the CA Owner acting in Trusted Roles
- The key generation ceremony was observed by 1 individual of the Conformity Assessment Body with independence from the CA Owner
- Principles of multiparty control and split knowledge were observed.
- The CA key pairs were generated in a physically secured environment as described in the CA’s CP & CPS.

- The CA key pairs were generated within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA’s CP & CPS.
- CA key pair generation activities were logged.
- Effective controls were maintained to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in its CP & CPS and the Key Generation Script.

The key generation ceremony has been witnessed in person.

No non-conformities have been identified during the audit.

Root 1: D-Trust BR Root CA 2 2023

Standards considered:	European Standards: ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.4.1 (2021-11) CA Browser Forum Requirements: ☒ Baseline Requirements, version 1.8.6 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ ETSI TS 119 403-2 V1.2.4 (2020-11)

The key ceremony audit was based on the following policy and practice statement documents of the CA / TSP:

1. Certificate Policy of D-TRUST GmbH, Version 5.0 as of 2023-06-26, D-Trust GmbH
2. D-TRUST Trust Service Practice Statement (TSPS), version 1.7 as of 2023-06-26
3. Certification Practice Statement of the D-TRUST CSM PKI, Version 3.9 as of 2023-06-26, D-Trust GmbH

This report covers the generation of the key pairs and certificates of the Root-CA and Sub-CAs referenced in the following tables.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST BR Root CA 2 2023	0552E6F83FDF65E8FA9670E666DF28A4E21340B510CBE52566F97C4FB94B2BD1	ETSI EN 319 411-1 V1.3.1, DVCP ETSI EN 319 411-1 V1.3.1, OVCP
	SHA-256 fingerprint of Subject Public Key Info	
	AC76F63A46E761B5ACC3259705C920CB7F0563D248D8D180F934AF68099A15F9	

Table 1: Root-CA generated during the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been generated in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	
C=DE, O=D-Trust GmbH, CN=D-TRUST BR CA 2-23-1 2023	D904A27FD2D271DCFE40A1F471033CE48A4B5E1484753DA66F7166D6EBDC06E6	ETSI EN 319 411-1 V1.3.1, OVCP
	A8217381D62CCB6FD688318979B4886E0273A92C59F1B00F12450A9FE6E01A67	
C=DE, O=D-Trust GmbH, CN=D-TRUST BR CA 2-23-2 2023	6685871384605253C264F8D380A8D1DD50A6CA192788FF2D560CAFE541F807B8	ETSI EN 319 411-1 V1.3.1, DVCP
	A861B28CD1D8FE2C4C91B96D940FA660BB615CC8F77B29AF7DA451FFAA483AD4	

Table 2: Sub-CA’s issued by the Root-CA or its Sub-CA’s during the audit

Root 2: D-Trust EV Root CA 2 2023

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.3.1 (2021-05) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.4.1 (2021-11) CA Browser Forum Requirements: ☒ EV SSL Certificate Guidelines, version 1.8.0 ☒ Baseline Requirements, version 1.8.6 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ ETSI TS 119 403-2 V1.2.4 (2020-11)

The key ceremony audit was based on the following policy and practice statement documents of the CA / TSP:

1. Certificate Policy of D-TRUST GmbH, Version 5.0 as of 2023-06-26, D-Trust GmbH
2. D-TRUST Trust Service Practice Statement (TSPS), version 1.7 as of 2023-06-26
3. Certification Practice Statement of the D-TRUST CSM PKI, Version 3.9 as of 2023-06-26, D-Trust GmbH

This report covers the generation of the key pairs and certificates of the Root-CA and Sub-CAs referenced in the following tables.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
C=DE, O=D-Trust GmbH, CN=D-TRUST EV Root CA 2 2023	8E8221B2E7D4007836A1672F0DCC299C33BC07D316F132FA1A206D587150F1CE	ETSI EN 319 411-1 V1.3.1, EVCP ETSI EN 319 411-2 V2.4.1, QEVCP-w
	SHA-256 fingerprint of Subject Public Key Info	
	E753CDD9F13413C7CA9CDA82962F8C0CE5ED13D1657312954AF5267EB2CB7C79	

Table 3: Root-CA generated during the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been generated in this audit.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	
C=DE, O=D-Trust GmbH, CN=D-TRUST EV CA 2-23-1 2023	378CF8738654C8A8544812B1FF2632348225553DA80225692D0491C4A1EEAFB9	ETSI EN 319 411-1 V1.3.1, EVCP
	F087D882024730E1C5CE772F59F778C903A5BFB7E5AFA699360ED6FFB4921B97	
C=DE, O=D-Trust GmbH, CN=D-TRUST EV CA 2-23-2 2023, 2.5.4.97=VATDE-202620438	5FF9F5A1C0ED7401E1C529F6D50C4ABB00B17B593358BD2D61DC0DD887DDD92F	ETSI EN 319 411-2 V2.4.1, QEVCP-w
	0B1CA088E3EFC7F340F599E1071B52334EDE26C0CF079AEF22EC13AEEB52A8B1	

Table 4: Sub-CA’s issued by the Root-CA or its Sub-CA’s during the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2023-06-28	Initial attestation
Version 2	2024-08-02	Attestation updated to the latest ACAB’c template version including more detailed information

End of the audit attestation letter.