Mozilla - CA Program

Case Information

Case Number	00000073	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	D-TRUST	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include D-TRUST Root CA 3 2013 root cert	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1166723

General information about CA's associated organization

CA Email Alias 1	rootstores@bdr.de		
CA Email Alias 2			
Company Website	https://www.bundesdruckerei.de/de/167-d-trust-ssl-zertifikate	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Germany, Europe, Global	**Verified?**	Verified
Primary Market / Customer Base	D-TRUST GmbH is a subsidiary of Bundesdruckerei GmbH and is fully owned by the German State.	**Verified?**	Verified
Impact to Mozilla Users	In Europe we want to promote the use of signed and encrypted email. D-Trust is offering different types of certificates for this use case: Personal, Team and Device IDs.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	- Publicly Available CP and CPS: Yes - CA Hierarchy: Yes - Audit Criteria: Yes - Document Handling of IDNs in CP/CPS: Not applicable. - Revocation of Compromised Certificates: Yes	**Verified?**	Verified

- Verifying Domain Name Ownership: Not applicable
- Verifying Email Address Control: Yes
- Verifying Identity of Code Signing Certificate Subscriber: Not applicable
- DNS names go in SAN: Not applicable
- Domain owned by a Natural Person: Not applicable
- OCSP: Yes
- Network Security Controls: Yes, Audited by TUVIT

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	- Long-lived DV certificates: Not applicable - Wildcard DV SSL certificates: Not applicable - Email Address Prefixes for DV Certs: Not applicable - Delegation of Domain / Email validation to third parties: Yes, D-Trust has Trusted Service Providers, but they provide public-facing policy documentation and are audited by TUVIT. - Issuing end entity certificates directly from roots: No - Allowing external entities to operate subordinate CAs: No - Distributing generated private keys in PKCS#12 files: No, only in special cases for smart devices unable to support smartcards its distributed using a strong password on separate secure channel. - Certificates referencing hostnames or private IP addresses: Not applicable - Issuing SSL Certificates for Internal Domains: Not applicable - OCSP Responses signed by a certificate under a different root: No - SHA-1 Certificates: No - Generic names for CAs: No - Lack of Communication With End Users: No, see CPS - Backdating the notBefore date: No	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	D-TRUST Root CA 3 2013	**Root Case No**	R00000100
Request Status	Ready for Public Discussion	**Case Number**	00000073

Additional Root Case Information

Subject	Include D-TRUST Root CA 3 2013 Root Cert

Technical Information about Root Certificate

O From Issuer Field	D-Trust GmbH	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	D-Trust operates subordinate CAs for Trusted Service Providers (TSPs), who do the identity and email address	**Verified?**	Verified

	verification and issue the end entity certificates directly. The TSPs provide public-facing policy documentation, and are audited by TUVIT.		
Root Certificate Download URL	http://www.d-trust.net/cgi-bin /D-TRUST_Root_CA_3_2013.crt	**Verified?**	Verified
Valid From	2013 Sep 20	**Verified?**	Verified
Valid To	2028 Sep 20	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	Example Cert: https://bugzilla.mozilla.org /attachment.cgi?id=8730195	**Verified?**	Verified
CRL URL(s)	http://pki.intranet.eon.com /crls/EON_Group_CA_2_2013.crl http://crl.d-trust.net /crl/eon_group_ca_2_2013.crl CPS and CSM CPS section 2.3: Certificate revocation lists are published immediately following revocations. Even if no certificates were revoked, the TSP ensures that a new certificate revocation list is created at least every 24 hours.	**Verified?**	Verified
OCSP URL(s)	http://eon-ca-2-2013-xxi.ocsp.d-trust.net CPS and CSM CPS section 4.10: The status query service is available via the OCSP protocol. The availability of the service is indicated as a URL in the certificates.	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	Not requesting Websites trust bit.	**Verified?**	Not Applicable
CA/Browser Forum Lint Test		**Verified?**	Not Applicable
Test Website Lint Test		**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable

Digital Fingerprint Information

SHA-1 Fingerprint	6C:7C:CC:E7:D4:AE:51:5F:99:08:CD:3F:F6:E8:C3:78:DF:6F:EF:97	**Verified?**	Verified
SHA-256 Fingerprint	A1:A8:6D:04:12:1E:B8:7F:02:7C:66:F5:33:03:C2:8E:57:39:F9:43:FC:84:B3:8A:D6:AF:00:90:35:DD:94:57	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The root “D-TRUST Root CA 3 2013” currently has four internally-operated subCAs: 1) D-TRUST Application Certificates CA 3-1 2013 -- Audit: https://www.tuvit.de/data/content_data/tuevit_en/6768UE_s.pdf 2) E.ON Group CA 2 2013 -- www.eon.com/pki -- CP (English): https://bugzilla.mozilla.org/attachment.cgi?id=8728132 -- Audit: https://www.tuvit.de/data/content_data/tuevit_en/6764UE_s.pdf 3) UNIPER Group CA 2 2015 -- www.uniper.energy/pki -- CP (English): https://www.uniper.energy/static/download/files/UNIPER_CP.pdf -- Audit: https://www.tuvit.de/data/content_data/tuevit_en/6769UE_s.pdf “UNIPER” is a new subsidiary and brand of “E.ON”, so it was decided to have two identical CA-Infrastructures with identical CP/CPS Procedures in parallel. 4) D-TRUST Application Certificates CA 3-2 2016 There was a full Audit by TÜVIT in December 2016, we expect the Audit Report and the CP latest Mid of January 2017. This will not be used for issuing EE-Certs before Audit and CP are published.	**Verified?**	Verified
Externally Operated SubCAs	All SUB-CAs of this Root are D-TRUST internally operated subCAs: and under full control and audit.	**Verified?**	Verified
Cross Signing	No cross-certs existing. Cross-certs are prohibited by Policy. Only direct trust structures.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	D-Trust operates subordinate CAs for Trusted Service Providers (TSPs), who do the identity and email address verification and issue the end entity certificates directly. The TSPs provide public-facing policy documentation, and are audited by TUVIT.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in German and English. To support a better audit practise D-TRUST has decided to develop one CPS for the "standard" issuing process managed within the CSM-System, please see https://www.bundesdruckerei.de/en/812-certificate-service-manager	**Verified?**	Verified

	all other issuing processes are covered by the generic CPS. Please see d-trust_root_pki_cps_v1.14_en.pdf		
CA Document Repository	https://www.bundesdruckerei.de/de/2833-repository	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.bundesdruckerei.de/sites/default/files/documents/2016/01/d-trust_cp_v2.1_en.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.bundesdruckerei.de/sites/default/files/documents/2016/01/d-trust_root_pki_cps_v1.14_en.pdf	**Verified?**	Verified
Other Relevant Documents	CSM CPS (English): https://www.bundesdruckerei.de/sites/default/files/documents/2016/01/d-trust_csm_pki_cps_v1.2_en.pdf E.ON CP (English): http://www.eon.com/content/dam/eon-com/Info-Service/EON_SE_CP_EN.pdf UNIPER CP (English): https://www.uniper.energy/static/download/files/UNIPER_CP.pdf	**Verified?**	Verified
Auditor Name	TUVIT	**Verified?**	Verified
Auditor Website	https://www.tuvit.de/	**Verified?**	Verified
Auditor Qualifications	http://www.dakks.de/en/content/accredited-bodies-dakks	**Verified?**	Verified
Standard Audit	https://www.tuvit.de/data/content_data/tuevit_en/6768UE_s.pdf https://bug1166723.bmoattachments.org/attachment.cgi?id=8813743	**Verified?**	Verified
Standard Audit Type	ETSI EN 319 411	**Verified?**	Verified
Standard Audit Statement Date	11/21/2016	**Verified?**	Verified
BR Audit	Not requesting Websites trust bit	**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	Not requesting Websites trust bit	**Verified?**	Not Applicable
SSL Verification Procedures		**Verified?**	Not Applicable
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	CPS and CSM CPS sections 3.2.2 and 3.2.3. CPS and CSM CPS section 4.2.1:	**Verified?**	Verified

	Individuals or organisations can be authenticated and further certificate-relevant data verified before or after submission of the application, but must be completed before certificates and key material, if any, and PINs are handed over. Individuals must be unambiguously identified; in addition to the full name, further attributes (such as place and date of birth or other applicable individual parameters) must be used to prevent individuals from being mistaken. If legal entities are named in the certificate or if legal entities are subscribers, the complete name and legal status as well as relevant register information must be verified. Identification is carried out according to section 3.2.3. The TSP defines the following verification methods: ...		
Email Address Verification Procedures	CSM CPS section 4.2.1: E-mail It must be possible to unambiguously assign the domain used in a registered e-mail address to the registered organisation. If this is not the case, the TSP sends an e-mail to the e-mail address to be confirmed, and receipt of this e-mail must be confirmed (exchange of secrets). The results of the inquiry are filed. CPS section 4.2.1: E-mail The TSP sends an e-mail to the e-mail address to be confirmed, and receipt of this e-mail must be confirmed (exchange of secrets). The results of the enquiry are filed.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS and CSM CPS section 5. E.ON CP Section 4.1: Authentication is HW and Password based, certificates for eMail are issued one-by-one,	**Verified?**	Verified
Network Security	CPS and CSM CPS section 6.7. The Network Security Requirements are included in TS 102 042 and are fully audited by TÜVIT.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.bundesdruckerei.de/en/3614-d-trust-roots	**Verified?**	Verified