Bugzilla ID: 467891
Bugzilla Summary: Add Root CA "D-TRUST Root Class 3 CA 2007" to trusted list

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Info	
CA Name	D-TRUST GmbH
Website URL	https://www.d-trust.net/internet/content/e_index.html / ssl.d-trust.net
Organizational type	Commercial and sovereign tasks
Primary market / customer base	D-TRUST GmbH is a wholly owned subsidiary of Bundesdruckerei and is the only German trust center authorised to perform sovereign tasks. The primary market is the German speaking area (Austria, Germany, Switzerland) and B2B focused.
Impact to Mozilla Users	Please describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc. Note the Mozilla CA certificate policy: • Section 1: We will determine which CA certificates are included in software products distributed through mozilla.org, based on the benefits and risks of such inclusion to typical users of those products. • Section 6: We require that all CAs whose certificates are distributed with our software product ... provide some service relevant to typical users of our software products
CA Contact Information	CA Email Alias: info@d-trust.net An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: +49 (0)30 259391 0 Title / Department: D-Trust PKI Certification Practices

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**	**Data**
Certificate Name	D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 EV 2009
Cert summary / comments		
Root Cert URL	https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt	https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_EV_2009.crt

SHA-1 fingerprint	58:E8:AB:B0:36:15:33:FB:80:F7:9B:1B:6D:29:D3:FF:8D:5F:00:F0	96:C9:1B:0B:95:B4:10:98:42:FA:D0:D8:22:79:FE:60:FA:B9:16:83
Valid from	2009-11-05	2009-11-05
Valid to	2029-11-05	2029-11-05
Cert Version	3	3
Modulus length	2048	2048
Test Website	https://extranet.d-trust.net	https://ssl-test-ev.d-trust.net
CRL URL	CRL in end-entity cert is ldap. CRL URI in root and subCA: http://www.d-trust.net/crl/d-trust_root_class_3_ca_2_2009.crl When I try to import this crl into my Firefox browser I get the error: Error Importing CRL to local Database. Error Code:ffffe009	CRL in end-entity cert is ldap. CRL URI in root and subCA: http://www.d-trust.net/crl/d-trust_root_class_3_ca_2_ev_2009.crl When I try to import this crl into my Firefox browser I get the error: Error Importing CRL to local Database. Error Code:ffffe009
Update Frequency	Daily and immediately on an revocation event, OCSP: Currently there is no expiration time; the responder is updated together with the CRL on certificate activations and revocations. It is planned to establish a cache with expiration time up to 7 days.	
OCSP Responder URL	For test website, AIA in subCA: http://root-c3-ca2-2009.ocsp.d-trust.net AIA in end-entity cert: http://ssl-c3-ca1-2009.ocsp.d-trust.net	For test website, AIA in subCA: http://root-c3-ca2-ev-2009.ocsp.d-trust.net AIA in end-entity cert: http://ssl-c3-ca1-ev-2009.ocsp.d-trust.net Max time until OCSP responders updated to reflect end-entity revocation http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."
CA Hierarchy	This "D-TRUST Root Class 3 CA 2 2009" root currently has one internally-operated subordinate CA, "D-TRUST SSL Class 3 CA 1 2009", which signs end-entity certificates.	This "D-TRUST Root Class 3 CA 2 EV 2009" root currently has one internally-operated subordinate CA, "D-TRUST SSL Class 3 CA 1 EV 2009", which signs end-entity certificates.
SubCAs operated by 3rd parties	No subordinate CAs will be operated by third parties for this root.	No subordinate CAs will be operated by third parties for this root.

Cross-Signing	None	None
Trust Bits One or more of: • Websites • Email • Code Signing	Websites	Websites
SSL Validation Type DV, OV, and/or EV	OV CP section 1.1.3: Class-3-certificates are especially high-grade advanced certificates, that comply with most of the requirements for qualified certificates adhering to the stipulations of the German Signature Law [SigG] and fulfill all the requirements of [ETSI-F] „NCP“ and „NCP+“. SSL-certificates are only issued to legal entities. Class 3 EV-certificates do not comprise a separate class. Any explanations aimed at the compartment “Class 3” therefore also pertains to Class 3 EV-certificates. Differences are explicitly mentioned.	EV CP section 1.1.3: A special case of class-3 category certificates is represented by the class 3 SSL-EVcertificates, which follow the Guidelines for Extended Validation Certificates, CA/Browser Forum, version 1.1 April 2008 [GL-BRO] and [ETSI-F] “EVCP”.
EV policy OID(s)	Not applicable	1.3.6.1.4.1.4788.2.202.1
CP/CPS	D-Trust Document Repository: https://www.d-trust.net/repository German CPS: http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CPS.pdf German CP: http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CP.pdf English CPS: http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CPS-EN.pdf English CP: http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CP-EN.pdf	
AUDIT	Audit Type: WebTrust CA Auditor: Claus Harms Wirtschaftsprufer / Steuerberater Auditor Website: http://www.wirtschaftspruefer-harms.de Audit Report and Management’s Assertions: https://cert.webtrust.org/ViewSeal?id=1018 (2009.11.27) Audit Type: WebTrust EV Readiness Auditor: Claus Harms Wirtschaftsprufer / Steuerberater Auditor Website: http://www.wirtschaftspruefer-harms.de Audit Report and Management’s Assertions: https://cert.webtrust.org/ViewSeal?id=1025 (2009.11.27)	
Organization Identity Verification	CP section 3.2.2, Class 3: High-level identification and assessment. Personal participant identification as well as a thourough assessment of the applicant-data are conducted along the procedures defined for the creation of qualified certificates. Legal entities are verified in adherence with the [ETSI-F]- guidelines. The verification encompasses all of the DN-components. Class 3 EV-certificates: Identification and authentication as well as data verification follow the standards stated in [GL-BRO] and section H 30 [GL-BRO].	

	CPS Section 4.2.1 Organization Validation: Paragraph "Register / non-Register" Register: A manual or automatic comparison is made between the application data and excerpts of the commercial register. Admissible are state registers (such as registration courts, public revenue offices, professional statutory corporations or comparable) or private registers DUNS, comparable financial databases and others). A registry excerpt can only be accepted as valid, if it does not have an attribute such as “invalid” or “inactive” attached to it. Copies of the documents are kept either as hard-copies or in digital form. Non-Register: Government institutions/public corporations affirm certificate related information with an official seal and a signature. Copies of the documents are kept either as hard-copies or in digital form.
Domain Name Ownership / Control	I did not find sufficient information about the process used to confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. We require that this information be in a public-facing and audited document such as the CP or CPS. It is not sufficient to reference another document such as the Guidelines for Extended Validatoin Certificates, CA/Browser Forum [GL-BRO]. The information needs to be in the CA’s CP or CPS. Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership CPS Section 4.2.1 Domain: An organization’s domain and possibly further attributes such as e-mail addresses are verified by a domain-enquiry in the official registers. … The findings are documented. Domains that are not subject to registration (non Top-Level Domains) are not validated. The subscriber may only use such domains internally. This will most likely be a sticking point during the public discussion phase. Please see https://wiki.mozilla.org/CA:Problematic_Practices#Certificates_referencing_hostnames_or_private_IP_addresses and https://wiki.mozilla.org/CA:Problematic_Practices#Issuing_SSL_Certificates_for_Internal_Domains
Email Address Ownership / Control	Not requesting email trust bit.
Identity of Code Signing Subscriber	Not requesting code signing trust bit.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates ○ SSL certs are OV. • Wildcard DV SSL certificates ○ SSL certs are OV. • Email Address Prefixes for DV SSL Certs ○ SSL certs are OV.

	• Delegation of Domain / Email validation to third parties ○ **RA's are used.** CPS section 1.3.2: An RA identifies and authenticates applicants and processes. It also verifies the applications for different Certification Services. The CSP provides the RA with suitable hard- and software as well as work-flow processes that must be incorporated by the RA. The work-flow processes include detailed requirements for a step-by-step fulfillment of the RAs objectives as well as contingency procedures in case of errors (erroneous data, invalid documents etc.). • Issuing end entity certificates directly from roots ○ Not applicable. • Allowing external entities to operate unconstrained subordinate CAs ○ No sub-CAs operated by external entitites. • Distributing generated private keys in PKCS#12 files ○ Not applicable for Class 3 SSL certs. • Certificates referencing hostnames or private IP addresses ○ ? • Issuing SSL Certificates for Internal Domains ○ Internal domain names are allowed. Need more info. • OCSP Responses signed by a certificate under a different root ○ Test websites loaded into Firefox browser with OCSP enforced. • CRL with critical CIDP Extension ○ Unable to import the CRLs • Generic names for CAs ○ CA names have D-Trust in them.