Bugzilla ID: 467891
Bugzilla Summary: Add "D-TRUST Root Class 3 CA 2 2009" and "D-TRUST Root Class 3 CA 2 EV 2009"

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	http://ssl.d-trust.net
Organizational type	Commercial and sovereign tasks
Primary market / customer base	D-TRUST GmbH, founded in Berlin in 1998, is a wholly owned subsidiary of Bundesdruckerei and is the only German trust center authorised to perform sovereign tasks. The development and marketing of high-security products for the electronic signature are carried out in Bundesdruckerei's high-security value printing building. The primary market is the German speaking area (Austria, Germany, Switzerland) and B2B focused.
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	This root currently has one internally-operated subordinate CA.	This root currently has one internally-operated subordinate CA.
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
Type of signing key	Sha256 RSA	Sha256 RSA
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 (NextUpdate 7 days)	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 (NextUpdate 7 days)
Update Frequency	CPS section 2.3: Even if no revocation has occurred in the meantime, the CSP publishes a new CRL every day.	

OCSP	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	subCA: http://root-c3-ca2-ev-2009.ocsp.d-trust.net end-entity: http://ssl-c3-ca1-ev-2009.ocsp.d-trust.net Comment #24: Our responder just gives real time certificate status answers, we do not practice OCSP stapeling or similar - so, expiration time is immediately after response.
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	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: http://ssl.d-trust.net/support/repository.php 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: ETSI TS 102 042 V2.1.2 (2010-04), policy NCP Auditor: TUVIT Auditor Website: http://www.tuvit.de/Zertifizierung.asp ETSI Certificate: http://www.tuvit.de/certuvit/pdf/6709UD_s.pdf (2011.03.18) Audit Type: ETSI TS 102 042 V2.1.2 (2010-04), policy EVCP Auditor: TUVIT Auditor Website: http://www.tuvit.de/Zertifizierung.asp ETSI Certificate: http://www.tuvit.de/certuvit/pdf/6710UD_s.pdf (2011.03.18)	
Organization Identity Verification	Only Class 3 certs are issued within the hierarchy of these roots. CP section 1.5.3: Class 3 SSL-EV-certificates as well as their Sub- and Root-CAs adhere to the specifications of the CA/Browser Forum Guidelines for Extended Validation Certificates [GL-BRO]. In the case of inconsistencies between this document and above mentioned guidelines, the [GL-BRO] takes precedence for Class 3 SSL EV CAs as well as their Sub- and Root-CAs.	

	CP section 1.6.3: [GL-BRO] = Guidelines for Extended Validation Certificates, CA/Browser Forum, Version 1.2 October 2009 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 12.2 [GL-BRO]. CPS section 4.2.1 defines the methods that may be used for identification and authentication.
Domain Name Ownership / Control	CPS Section 4.2.1: An organization's domain and possibly further attributes such as e-mail addresses are verified by a domain-enquiry in the official registers (WHOIS). Class 3-2: It is questioned whether the subscriber has the exclusive control of the domain. The findings are documented. With EV certificates in addition a review of the domain name for known phishing domains of blacklists is carried out. Domains that are not subject to registration (non Top-Level Domains) are not allowed. Check on the status of this before starting discussion. Comment #27: Would it be sufficient to integrate an standard block on our production system for all SSL requests, that includes a further task/step on our electronic checklist? The validation officer needs to check than the domain name included in the CN against this list. If the name is not on this list, than he/she needs to set the checkbox for this task on "checked". If this checkbox stays "unchecked" the request would stay pending and cannot be processed. If there is a positive finding on the list, the request will be forwarded as a potential security event to a separate production role "quality management" and potentially "security officer". Would that be ok? Comment #29: Yes, I believe so. Other CAs also responded to action #4 by saying that they have no automated cert issuance -- all their SSL cert approval and issuance is manual. I believe that the concern that #4 was meant to address can be met with the combination of multi-factor auth (action #3) and having no automated cert issuance.
Email Address Ownership	Not requesting email trust bit.
Identity of Code Signing Subscriber	Not requesting code signing trust bit.
Multi-factor Authentication	CP section 6.2.2: The HSM containing the CA-keys is situated in the high-security tract of the TrustCenter. To activate a private key, two authorized employees are necessary. The HSM can sign any desired amount of certificates after the private key is activated.
Network Security	See CPS section 6, Technical Security Provision. Comment #28: Besides the tests that the auditors are doing on a yearly basis, we do have of course a Intrusion Detection / Prevention & Firewall system in place. Furthermore we have a software that is also continously monitoring the integrity of our files & data bases.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates ○ SSL certs are OV or EV. ○ Comment #24: I have canceled the 5-year-option as a product for all of our SSL certs under the respective roots. The changes are already reflected on the enrollment page.

- Maximum validity period for EV certs is 27 months.
- Wildcard DV SSL certificates
  - SSL certs are OV or EV.
  - Wildcards are not permitted for EV certs.
- Email Address Prefixes for DV SSL Certs
  - SSL certs are OV.
- Delegation of Domain / Email validation to third parties
  - Comment #24: No external RA can perform validation / verification procedures under these roots.
- 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
  - Comment #24: We are not offering SSL certs for IP addresses or internal domain names.
- Issuing SSL Certificates for Internal Domains
  - Comment #24: We are not offering SSL certs for IP addresses or internal domain names.
- OCSP Responses signed by a certificate under a different root
  - Test websites loaded into Firefox browser with OCSP enforced.
- CRL with critical CIDP Extension
  - CRLs imported into my Firefox browser without error.
- Generic names for CAs
  - CA names have D-Trust in them.