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.

General Information	Data
CA Name	D-TRUST GmbH
Website URL (English version)	https://www.d-trust.net/internet/content/e_index.html
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Government
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	D-TRUST GmbH is a wholly owned subsidiary of Bundesdruckerei (100% Governmental), 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.

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

Info Needed	Data	Status / Notes
Certificate Name	D-TRUST Root Class 3 CA 2007	COMPLETE
Cert summary / comments	This root will eventually have three internally-operated subordinate CAs. It currently has one subordinate CA called D-TRUST Service Class 3 CA 1 2008 which issues website certificates. The other two subordinate CAs that will be created will be for email and code signing.	COMPLETE
The root CA certificate URL Download into FireFox and verify	https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2007.crt	COMPLETE
SHA-1 fingerprint.	FD:1E:D1:E2:02:1B:0B:9F:73:E8: EB:75:CE:23:43:6B:BC:C7:46:EB	COMPLETE
Valid from	05/16/2007	COMPLETE
Valid to	05/16/2022	COMPLETE
Cert Version	3	COMPLETE

Modulus length	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	http://www.d-trust.net/crl/d-trust_service_class_3_ca_1_2008.crl CPS section 2.3: CRLs are published periodically and until the issuing CA-certificate expires. A new CRL is issued instantly with each new revocation of a certificate under the CA-tree. Even if no revocation has occurred in the meantime, the CSP publishes a new CRL every day.	Is this CRL PEM encoded instead of DER encoded? When I try this url in Firefox I get the error ffffe009 According to http://www.mozilla.org/projects/security/pki/nss/ref/ssl/sslerr.html if my calculation is correct, this error corresponds to error code -8183 which would be "Security library: improperly formatted DER-encoded message." The RFC says the CRL must be DER encoded, meaning binary, not PEM. This is an issue.
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	http://users.ocsp.d-trust.net for SSL Certificates: http://ssl.ocsp.d-trust.net 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.	I have imported the root and set my OCSP service URL, yet I get an error trying to connect to https://ssl.d-trust.net in Firefox: Secure Connection Failed An error occurred during a connection to ssl.d-trust.net. Invalid OCSP signing certificate in OCSP response. (Error code: sec_error_ocsp_invalid_signing_cert) Does the OCSP signer chain up to this root?
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate	Hierarchy diagram is in section 1.1.3 of the CPS. This root will have 3 internally-operated sub-CAs: - D-TRUST Service Class 3 CA 1 2008 - Issuing CA for email (not yet created)	COMPLETE

CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	- Issuing CA for code signing (not yet created) All of these will be operated by the CA organization and under the same audited CPS.	
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	No subordinated CAs will be operated by third parties for this root.	COMPLETE
List any other root CAs that have issued cross-signing certificates for this root CA	None. Plan to create a link certificate for EV – certificates from EV – Root to D-TRUST Service CA 2007 as recommended by the CA/Browserforum	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites only Not email or code: The sub-CAs for email and code signing have not yet been created. There is no mention of code signing in the CPS.	COMPLETE
If SSL certificates are issued	OV	COMPLETE

within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber in addition to verifying the domain name. (This is commonly referred to as an OV certificate.) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)	Which Attributes are checked is stated in CPS Section 3.2.2; how they are checked is described in CPS Section 4.2.1 Identity Validation for Class 3 SSL: Paragraphs Register/non-Register and Domain CPS 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. CPS Section 3.2.2 Authentication of Organizations Organizations that are named in certificates or in whose name certificates are issued must authenticate themselves comprehensibly. The different validation procedures, which are described in chapter 4.2.1, are variably applied towards the DN-components as listed in chapter 3.1.4 – and possibly towards DN-components not explicitly listed in chapter 3.1.4 –, depending on the certificate’s class category. CPS Section 4.2.1 **Pers-Ident** An individual must personally identify himself to an RA, an official partner or an external provider that fulfills the requirements of the [CP] with his official ID (ID-card, passport or documents with equal standing) and be authenticated in turn. A valid ID-card or passport is deemed an acceptable identification document for individuals from the European Union or from states belonging to the Schengen-Agreement. Other documents with comparable status may be submitted instead. No copies of the identification documents are made or stored at the RA or CSP. **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** An organization's domain and possibly further attributes such as e-mail addresses are verified by a domain-enquiry in the official registers. Class 3-2: 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.	
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	Not EV From D-TRUST: "The D-TRUST Root Class 3 2007 is a None EV Class3 Root"	COMPLETE
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email	https://ssl.d-trust.net	COMPLETE

example.		
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	D-TRUST-Root PKI Certification Practice Statement in English https://bugzilla.mozilla.org/attachment.cgi?id=361775 CPS in German: http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CPS.pdf CP in German: http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CP.pdf	COMPLETE
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.)	Auditor: TÜV Informationstechnik GmbH (TÜViT) Auditor website: http://www.tuvit.de/english/Home.asp Audit Type: ETSI 102042 Audit Certificate: http://www.tuvit.de/certuvit/pdf/6704UE.pdf	COMPLETE 2008-06-18

Review CPS sections dealing with subscriber verification (COMPLETE)
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
    - 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. Class 3-2: 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.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - **Not enabling the email trust bit**
    - CPS Section 4.2.1: The CSP sends an e-mail to the e-mail address that needs verification. The receipt must be acknowledged (exchange of secrets). The findings are documented.
    - It's not clear what "without verification (application affirmation)" means in CPS section 3.2.2 in the table entry for Class 3 E-Mail-Address.
- Verify identity info in code signing certs is that of subscriber
    - **Not enabling the code signing trust bit.**

        - Code signing certificates will only be available for organisations. CPS Section 4.2.1 Register/Non-Register
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - The SSL certs are OV.
    - CPS section 6.3.2: The maximum validity period for class 3 certs is 5 years.
- Wildcard DV SSL certificates
    - The SSL certs are OV.
    - CPS Section 3.1.4: Special case: One or multiple domain names may be included in the CN. Wildcards are not permitted for EV-certificates.
- Delegation of Domain / Email validation to third parties
    - OK
- Issuing end entity certificates directly from roots
    - No
- Allowing external entities to operate unconstrained subordinate CAs
    - No subordinated CAs will be operated by third parties for this root.
- Distributing generated private keys in PKCS#12 files
    - Not applicable to the SSL certs
- Certificates referencing hostnames or private IP addresses
    - From D-TRUST: "We are issuing Intranet and SubjectAltNames certs containing either surely or potentially just host names. We are currently adopting our subscriber agreement making sure that in this case these types of certs are for internal use only / non-public applications."
- OCSP Responses signed by a certificate under a different root
    - OCSP responder cert chains up to this root.
- CRL with critical CIDP Extension
    - No

Verify Audits (COMPLETE)
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - On TUVIT website

- For EV CA’s, verify current WebTrust EV Audit done.
    - N/A
- Review Audit to flag any issues noted in the report
    - No issues noted