Mozilla - CA Program

Case Information

Case Number	00000073	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	D-TRUST	**Request Status**	Need Information from CA

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	**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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices - Publicly Available CP and CPS: Yes - CA Hierarchy: Yes	**Verified?**	Need Response From CA

- Audit Criteria: Yes
- Document Handling of IDNs in CP/CPS: Not applicable.
- Revocation of Compromised Certificates:
- 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: ?
- Network Security Controls: ?

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	NEED CA's response to each of the items listed in https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices - Long-lived DV certificates: Not applicable - Wildcard DV SSL certificates: Not applicable - Email Address Prefixes for DV Certs: Not applicable - Delegation of Domain validation to third parties: Not applicable - Issuing end entity certificates directly from roots: No - Allowing external entities to operate subordinate CAs: ? - Distributing generated private keys in PKCS#12 files: ? - 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: ? - SHA-1 Certificates: ? - Generic names for CAs: No - Lack of Communication With End Users: - Backdating the notBefore date:	Verified?	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	D-TRUST Root CA 3 2013	Root Case No	R00000100
Request Status	Need Information from CA	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		Verified?	

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	NEED: - If requesting Websites trust bit: URL to a website whose SSL cert chains up to this root. Note that this can be a test site. - If requesting Email trust bit: attach an example cert to the bug	**Verified?**	Need Response From CA	
CRL URL(s)	NEED CRL URLs and CRL issuing frequency for subscriber certs, with reference to where this is documented in the CP/CPS	**Verified?**	Need Response From CA	
OCSP URL(s)	NEED OCSP URL and maximum OCSP expiration time, with reference to where this is documented in the CP/CPS	**Verified?**	Need Response From CA	
Revocation Tested	NEED: If requesting Websites trust bit, need to test the Test Website with https://certificate.revocationcheck.com/	**Verified?**	Need Response From CA	
Trust Bits	Email; Websites	**Verified?**	Need Response From CA	
SSL Validation Type	DV; OV; EV	**Verified?**	Need Response From CA	
EV Policy OID(s)	NEED: Are you requesting EV treatment for this root?	**Verified?**	Need Response From CA	
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org /PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA	
Root Stores Included In		**Verified?**	Need Response From CA	
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.	**Verified?**	Need Response From CA	

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	This root currently has two internally-operated subCAs: - D-TRUST Application Certificates CA 3-1 2013 - E.ON Group CA 2 2013	**Verified?**	Verified

			Verified?	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.		**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.		**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Foruom's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions		**Verified?**	Need Response From CA

Verification Policies and Practices

			Verified?	
Policy Documentation	Documents are provided in German and English.		**Verified?**	Verified
CA Document Repository	https://www.bundesdruckerei.de/de/2833-repository		**Verified?**	Verified
CP Doc Language	English			
CP	NEED: Which CP applies to this root?		**Verified?**	Need Response From CA
CP Doc Language	English			
CPS	NEED: Which CPS applies to this root?		**Verified?**	Need Response From CA
Other Relevant Documents			**Verified?**	Need Response From CA
Auditor Name	TUVIT		**Verified?**	Verified
Auditor Website	https://www.tuvit.de/		**Verified?**	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx		**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8608108 NEED: Audit statement for 2015.		**Verified?**	Need Response From CA
Standard Audit Type	ETSI TS 102 042		**Verified?**	Verified
Standard Audit Statement Date	11/28/2014		**Verified?**	Verified
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements		**Verified?**	Need Response From CA

BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	NEED only if requesting EV treatment	**Verified?**	Need Response From CA
EV Audit Type		**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org /CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference section 11 of the CA/Browser Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org /CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.	**Verified?**	Need Response From CA
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org /CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
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	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org	**Verified?**	Need Response From CA

	/CA:Information_checklist#Verification_Policies_and_Practices		
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA