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-](http://www.bundesdruckerei.de/de/167-) | **Verified?** | Verified |
|  | d-trust-ssl-zertifikate |  |  |
| **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 ofBundesdruckerei GmbH and is fully owned | **Verified?** | Verified |
|  | by the German State. |  |  |
| **Impact to Mozilla Users** | In Europe we want to promote the use of | **Verified?** | Verified |
|  | signed and encrypted email. D-Trust is |  |  |
|  | offering different types of certificates for |  |  |
|  | this use case: Personal, Team and Device |  |  |
|  | IDs. |  |  |

**Response to Mozilla's list of Recommended Practices**

**Recommended**

https://wiki.mozilla.org

**Recommended**

I have reviewed Mozilla's list of

**Practices**

/CA:Recommended\_Practices#CA\_Recommended\_Practices **Practices Statement**

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, please see attachment and**

http://www.eon.com/content/dam/eon-com/Info-Service/EON\_SE\_CP.pdf

https://www.uniper.energy/static/download/files/UNIPER\_CP.pdf

- 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: Yes, Online, please see cert sample

- Network Security Controls: Audited by TÜVIT please see audit reports

**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: 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,please see certs

- SHA-1 Certificates: No

- Generic names for CAs: No

- Lack of Communication With End Users: No, see CPS
 and attachment for “subscriber agreements”

- Backdating the notBefore date: No

**Verified?**

**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 | **Verified?** | Not applicable, only usage is eMail and client Auth, please attached files |
|  | up to this root. Note that this can be a |  |  |
|  | test site. - If requesting Email trust bit: |  |  |
|  | attach an example cert to the bug |  |  |
| **CRL URL(s)** | NEED CRL URLs and CRL issuing | **Verified?** | http://www.eon.com/content/dam/eon-com/Info-Service/EON\_SE\_CP\_EN.pdf |
|  | frequency for subscriber certs, with |  | See CP Chapter 2.3 crl are issued every 24h |
|  | reference to where this is documented in |  | Minimum |
|  | the CP/CPS |  |  |
| **OCSP URL(s)** | NEED OCSP URL and maximum OCSP | **Verified?** | See chapter 4.10.2 OCSP is updated 24/7 immediately (latest1 hour) after status change Example cert: |
|  | expiration time, with reference to where |  | URL=http://eon-ca-2-2013-xxi.ocsp.d-trust.net |
|  | this is documented in the CP/CPS |  |  |
| **Revocation Tested** | NEED: If requesting Websites trust bit, | **Verified?** | Not applicable  |
|  | need to test the Test Website with |  |  |
|  | https://certificate.revocationcheck.com/ |  |  |
| **Trust Bits** | Email; Websites | **Verified?** | eMail Trust Bit requested  |
| **SSL Validation Type** | DV; OV; EV | **Verified?** | Not applicable |
| **EV Policy OID(s)** | NEED: Are you requesting EV treatment | **Verified?** | No. |
|  | for this root? |  |  |
| **EV Tested** | NEED: If EV treatment is being | **Verified?** | Not applicable |
|  | requested, then provide successful |  |  |
|  | output from EV Testing as described here |  |  |
|  | https://wiki.mozilla.org |  |  |
|  | /PSM:EV\_Testing\_Easy\_Version |  |  |
| **Root Stores Included****In** |  | **Verified?** | Already included in Microsoft Rootstore since 2014 |
| **Mozilla Applied****Constraints** | NEED: Mozilla has the ability to name constrain root certs; e.g. to \*.gov or \*.mil. | **Verified?** | Not applicable |
|  | CAs should consider if such constraints |  |  |
|  | may be applied to their root certs. |  |  |

|  |  |
| --- | --- |
| **Digital Fingerprint Information** | ed |
|  | **SHA-1** 6C:7C:CC:E7:D4:AE:51:5F:99:08:CD:3F:F6:E8:C3:78:DF:6F:EF:97 **Verified?** Verifi**Fingerprint** |
| **SHA-256** 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?** Verifie**Fingerprint** | d |

**CA Hierarchy Information**

**CA Hierarchy**

The root “D-TRUST Root CA 3 2013” has three
D-TRUST internally-operated subCAs:

- D-TRUST Application Certificates CA 3-1 2013

- E.ON Group CA 2 2013

- UNIPER Group CA 2 2015

**Verified?**

“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

**Externally**

|  |  |  |  |
| --- | --- | --- | --- |
| **Operated SubCAs** | NEED:- If this root has any subordinate CA certificates that are | **Verified?** |  |
|  | operated by external third parties, then provide the |  | All SUB-CAs of this Root are D-TRUST internally operated subCAs: and under |
|  | information listed in the Subordinate CA Checklist, |  |  full control and audit |
|  | 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 |  | Not applicable, no Super CA |
|  | CAs, then those CAs must apply for inclusion |  |  |
|  | themselves as separate trust anchors. |  |  |
| **Cross Signing** | NEED: | **Verified?** |  |
|  | - List all other root certificates for which this root |  |  |
|  | certificate has issued cross-signing certificates. |  | Not applicable, no cross-certs existing, no |
|  | - List all other root certificates that have issued cross- |  |  |
|  | signing certificates for this root certificate. |  | cross-certs are prohibited by Policy |
|  | - If any such cross-signing relationships exist, it is |  | Only direct trust structures iusedimplemented |
|  | important to note whether the cross-signing CAs' |  |  |
|  | certificates are already included in the Mozilla root store |  |  |
|  | or not. |  |  |
| **Technical** | NEED: CP/CPS documentation describing the technical | **Verified?** |  |
| **Constraint on 3rd****party Issuer** | and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external |  | All SUB-CAs are D-TRUST are Internally operated and under full control and audit  |
|  | RAs as well as External subCAs. |  |  |
|  | References: |  | CPS of the D-TRUST CSM PKI Version 1.2 Chapter 1.3.2 |
|  | - section 7.1.5 of version 1.3 of the CA/Browser |  |  |
|  | Foruom's Baseline Requirements |  |  |
|  | - https:/[/www.mozilla.org/en-US/about/governance](http://www.mozilla.org/en-US/about/governance) |  |  |
|  | /policies/security-group/certs/policy/inclusion/ |  |  |
|  | - https://wiki.mozilla.org |  |  |
|  | /CA:CertificatePolicyV2.1#Frequently\_Asked\_Questions |  |  |

**Verification Policies and Practices**

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy****Documentation** | Documents are provided in German and English. | **Verified?** | Verified |
| **CA Document****Repository** | https:/[/www.bundesdruckerei.de/de/2833-repository](http://www.bundesdruckerei.de/de/2833-repository) | **Verified?** | Verified |
| **CP Doc Language** | English |  |  |
| **CP** | NEED: Which CP applies to this root? | **Verified?** | Certificate policy of D-TRUST GmbH Version 2.1 |
|  |  |  | https://www.bundesdruckerei.de/sites/default/files/documents/2016/01/d-trust\_cp\_v2.1\_en.pdf |
| **CP Doc Language** | English |  |  |
| **CPS** | NEED: Which CPS applies to this root? | **Verified?** | Certification Practice Statement of the D-TRUST Root PKI Version 1.14 |
|  |  |  | https://www.bundesdruckerei.de/sites/default/files/documents/2016/01/d-trust\_root\_pki\_cps\_v1.14\_en.pdf |
| **Other Relevant****Documents** |  | **Verified?** | See attachment for “subscriber agreements” |
| **Auditor Name** | TUVIT | **Verified?** |  |
| **Auditor Website** | https:/[/www.tuvit.de/](http://www.tuvit.de/) | **Verified?** | Verified |
| **Auditor****Qualifications** | https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx | **Verified?** | Verified |
| **Standard Audit** | <https://www.tuvit.de/data/content_data/tuevit_de/6768UD_s.pdf> | **Verified?** | Please see attachment and |
|  | <https://www.tuvit.de/data/content_data/tuevit_de/6769UD_s.pdf>https://www.tuvit.de/data/content\_data/tuevit\_de/6764UD\_s.pdf |  | https://www.tuvit.de/de/zertifizierungssuchergebnisseite-1852.htm?group=&type=&search-term=ETSI |
| **Standard Audit****Type** | ETSI TS 102 042 | **Verified?** | Verified |
| **Standard Audit****Statement Date** | 20/01/2016 | **Verified?** | Verified |
| **BR Audit** | NEED: If requesting Websites trust bit, then also need a BR audit as | **Verified?** | Only eMail trust bit requested |
|  | described here: |  |  |
|  | https://wiki.mozilla.org/CA:BaselineRequirements |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BR Audit Type** |  |  | **Verified?** | Only eMail trust bit requested |
| **BR Audit** |  | **Verified?** | Only eMail trust bit requested |
| **Statement Date** |  |  |  |
| **EV Audit** | NEED only if requesting EV treatment | **Verified?** | Only eMail trust bit requested |
|  |  |  |  |
| **EV Audit Type** |  | **Verified?** | Only eMail trust bit requested |
|  |  |  |  |
| **EV Audit** |  | **Verified?** | Only eMail trust bit requested |
| **Statement Date** |  |  |  |
| **BR Commitment** | NEED section in the CP/CPS that has the commitment to comply | **Verified?** | Please see Chapter 8 of the Only eMail trust bit requested |
| **to Comply** | with the BRs as described in section 2.2 of version 1.3 of the |  | CPS D-TRUST CSM PKI Version 1.2 |
|  | CA/Browser Forum's Baseline Requirements. |  |  E.ON CPS and Audit report |
| **SSL Verification** | NEED if Websites trust bit requested... | **Verified?** | Only eMail trust bit requested |
| **Procedures** | 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 |  |  |
| **EV SSL** | NEED: If EV verification is performed, then provide URLs and | **Verified?** | Only eMail trust bit requested |
| **Verification****Procedures** | 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. |  |  |
| **Organization** | NEED: CP/CPS sections that describe identity and organization | **Verified?** | Only eMail trust bit requested |
| **Verification****Procedures** | verification procedures for cert issuance. |  | No orgs identified |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Email Address** | NEED if Email trust bit requested... | **Verified?** | Please see: |
| **Verification****Procedures** | 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. |  | CPS: D-TRUST CSM PKI |
|  | As per section 4 of https://wiki.mozilla.org |  | Version 1.2 Chapter 4.2.1 Identification and authentication procedure |
|  | /CA:Information\_checklist#Verification\_Policies\_and\_Practices |  | AND:Certificate Policy of the E.ON SE PKI V 1.4 Chapter 4.1http://www.eon.com/content/dam/eon-com/Info-Service/EON\_SE\_CP\_EN.pdf |
|  | https://wiki.mozilla.org |  |  |
|  | /CA:Recommended\_Practices#Verifying\_Email\_Address\_Control |  |  |
| **Code Signing** | Mozilla is no longer accepting requests to enable the Code Signing | **Verified?** | Not Applicable |
| **Subscriber****Verification Pro** | trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy. |  |  |
| **Multi-Factor** | NEED CA response (and corresponding CP/CPS sections/text) to | **Verified?** | Certificate Policy of the E.ON SE PKI V 1.4 Chapter 4.1:Authentication is HW and Password based, certificates for eMail are issued one-by-one, |
|  | **Authentication** | section 6 of https://wiki.mozilla.org |  |  |

/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?**

The Network Security Requirements are included in TS 102 042 and are fully audited by TÜVIT and see

CPS D-TRUST CSM PKI Version 1.2 Chapter 6.7

**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?**

Please see:
https://www.bundesdruckerei.de/en/3614-d-trust-roots